Institut Municipal Barcelona Innovació i Tecnologia
Direcció de Serveis de Seguretat de la Informació

Plec de prescripcions tècniques que regeix l'Acord Marc per a la contractació de serveis del Centre de Riscos i Operacions de Ciberresiliència (CROC) i dels serveis d'Operació de Seguretat i Anàlisis de Protecció (OSAP) de l'Ajuntament de Barcelona, amb criteris de contractació pública sostenible

1. Introducció

L'Institut Municipal Barcelona Innovació i Tecnologia (en endavant, BIT) és l'organisme autònom de l'Ajuntament de Barcelona responsable de subministrar, governar i protegir tots els serveis de les tecnologies de la informació i comunicació (TIC) a l'Ajuntament de Barcelona i als organismes i les empreses públiques que en depenen.

Concretament, BIT participa en el disseny i execució de l'estratègia TIC de l'Ajuntament de Barcelona, ofereix assessorament i suport en tots aquells projectes o programes de l'Ajuntament que requereixen una estratègia de sistemes d'informació i telecomunicacions, i, impulsa i executa projectes tecnològics de diversa índole.

BIT té la missió d'impulsar i garantir la transformació digital de l'Ajuntament de Barcelona mitjançant l'adopció de tecnologies i plataformes digitals, assegurant que la innovació es desplegui amb criteris de seguretat, sostenibilitat i eficiència, i acompanyant tota l'organització per incorporar la innovació que aquestes tecnologies poden aportar als serveis i processos de gestió, tot garantint un funcionament eficient i eficaç de l'administració amb un model integral de ciberseguretat i resiliència operativa basat en la prevenció, la protecció, la detecció i la resposta als incidents.

En aquest context, BIT ha evolucionat el seu model operatiu de seguretat per donar lloc al **Centre de Riscos i Operacions de Ciberresiliència (CROC)**, com a espai de coordinació de totes les activitats de **governança, gestió de riscos, compliment normatiu i ciberresiliència operativa** de l'Ajuntament per a la prevenció, detecció i resposta davant incidents de seguretat.

El CROC actua de manera complementària i coordinada amb els serveis d'Operació de Seguretat i Anàlisi de Protecció (OSAP), responsables de les operacions de seguretat, el monitoratge, la resposta tècnica i la protecció avançada dels sistemes municipals.

Aquesta estructura integrada —CROC i OSAP— constitueix el **model municipal de ciberresiliència**, que garanteix tant la gestió estratègica del risc com la capacitat operativa de resposta davant amenaces que puguin afectar la disponibilitat, integritat o confidencialitat dels serveis públics digitals.

BIT té la visió d'aconseguir que **Barcelona sigui una ciutat referent en ciberresiliència i confiança digital**, assegurant que els seus serveis essencials operin sota criteris d'eficiència, sostenibilitat i seguretat, amb una gestió pública transparent, ètica i responsable.

Els valors fonamentals de BIT són el compromís de servei públic posant en primer pla l'interès general i el benestar dels ciutadans; la co-creació fomentant la col·laboració per aconseguir

serveis més adaptats i efectius, l'agilitat i eficiència per fer un ús òptim dels recursos, la innovació per millorar la qualitat dels serveis oferts, i l'ètica i la transparència.

Entre les funcions de BIT es troben la gestió de la seguretat de la informació i la gestió de les telecomunicacions que suporten els diferents serveis TIC, fent focus en la prevenció, protecció, detecció i resposta als incidents de seguretat així com en l'administració, operació i evolució de les plataformes, l'equipament i els elements de seguretat necessaris per oferir aquests serveis amb la màxima qualitat i alineats amb els marcs normatius vigents (ENS, ISO 27001 i NIS2).

Aquest model consolida el CROC i l'OSAP com a peces complementàries d'un centre de ciberresiliència integral, capaç de gestionar el risc i garantir la continuïtat dels serveis crítics municipals.

La seguretat, continuïtat i privadesa és un dels objectius estratègics de BIT. Això inclou la seguretat lògica, la seguretat física i la ciberseguretat, situant la protecció i la continuïtat dels sistemes d'informació i de les dades de l'Ajuntament com una prioritat, i posicionant BIT com a referent de confiança digital per a totes les entitats municipals.

La transició digital i la seguretat és un dels eixos estratègics de BIT per al període 2024-2030, que es concreta en els objectius següents:

1. Promoure l'adopció de solucions digitals al cloud (en un entorn multi-cloud), garantint l'escalabilitat i la flexibilitat dels sistemes d'informació de l'Ajuntament de Barcelona.
2. Assegurar la continuïtat dels serveis TIC potenciant l'ús de mesures de redundància i reducció de l'obsolescència.
3. Protegir els serveis TIC de l'Ajuntament de Barcelona (IT, OT i Seguretat Física), així com els de totes les entitats dependents o vinculades, mitjançant la implementació de mesures de ciberseguretat per salvaguardar la informació i garantir el tractament segur de les dades.

És en aquest context que el BIT, a l'empara del que preveu la Llei 9/2017, de 8 de novembre, de Contractes del Sector Públic, decideix impulsar un **Acord Marc que doni cobertura a la contractació de serveis del Centre de Riscos i Operacions de Ciberresiliència (CROC) i dels serveis d'Operació de Seguretat i Anàlisi de Protecció (OSAP)** de l'Ajuntament de Barcelona.

Aquest Acord Marc ha de permetre mantenir i evolucionar els sistemes ja desplegats, així com estendre els serveis a altres entitats municipals que voluntàriament s'hi adhereixin, garantint una gestió coordinada i coherent de la seguretat a nivell municipal.

Els acords marc són instruments que busquen simplificar el procediment de contractació pública i alhora reduir les despeses que aquests porten associades. De fet, la incorporació

d'aquestes figures respon a una tendència actual d'optimitzar els processos administratius, incrementar la transparència i garantir una gestió més eficient i sostenible mitjançant la digitalització.

En concret, la LCSP 9/2017 preveu, l'existència dels acords marc dins de l'àmbit de la racionalització tècnica de la contractació amb l'objectiu de simplificar i abaratir els costos del procés de licitació i adjudicació.

Així doncs, amb la implantació d'aquest l'Acord Marc, s'espera obtenir importants beneficis (tant per als operadors econòmics com per a l'Ajuntament) resultat de la **racionalització del procés de contractació i la reducció dels terminis** d**els processos de contractació** de projectes TIC, doncs permetrà:

- Reduir càrrega administrativa i costos de gestió, gràcies a la unificació en un sol procediment dels tràmits necessaris per a diversos contractes sota l'empara de l'Acord Marc.
- Disposar de forma immediata d'un únic proveïdor homologat, amb el qual s'han definit prèviament els aspectes determinants de les futures licitacions basades, fent que la contractació sigui més àgil, coherent i eficient.

Addicionalment, l'establiment del present Acord Marc en l'àmbit de projectes TIC té com objectiu:

- **L'estructuració i ordenació de la contractació dels serveis del CROC i dels serveis OSAP,** establint un marc comú per a la preparació i seguiment dels contractes derivats.
    - Homogeneïtzació dels criteris de valoració en tots els contractes basats de l'Acord Marc.
    - Estandardització de la definició dels serveis i activitats inclosos en l'abast dels contractes basats.
    - Establiment dels mecanismes de control en l'execució de contractes relacionats amb la qualitat del servei i els resultats obtinguts.
- **L'establiment d'un model de relació amb el proveïdor** basat en la transparència, la traçabilitat i la millora contínua en matèria de seguretat.

Paral·lelament, atès que l'objecte principal del present Acord Marc és la prestació de serveis, els mitjans tecnològics que donen cobertura als serveis objecte del contracte formen part dels elements necessaris per a la seva correcta execució. Amb caràcter general, les llicències de les tecnologies de prevenció i de les fonts d'informació corporatives seran posades a disposició per l'Ajuntament o per l'entitat contractant, llevat que en la descripció d'algun dels paquets de servei s'estableixi expressament un règim diferent. Igualment, les consoles d'aquestes fonts

i tecnologies seran de titularitat i disponibilitat de l'Ajuntament o de l'entitat contractant, que en facilitarà l'accés necessari a l'adjudicatari per a la seva operació en el marc del servei contractat.

En aquest context, l'Ajuntament o l'entitat contractant posarà a disposició de l'adjudicatari les fonts d'informació, els registres, els esdeveniments i els accessos necessaris als entorns i consoles corporatives requerits per a la monitorització, operació, administració o configuració dels serveis objecte de contractació. Correspondrà a l'adjudicatari prestar el servei sobre aquestes fonts, tecnologies i entorns, d'acord amb els requisits, procediments i condicions establerts en el present plec i en els contractes basats que se'n derivin.

Així mateix, si per a la correcta prestació del servei ofert l'adjudicatari considera necessari incorporar eines, plataformes o components tecnològics addicionals, ja sigui per a la monitorització, correlació, orquestració, automatització, supervisió, suport operatiu o optimització de la configuració dels elements de protecció, aquests aniran íntegrament al seu càrrec i s'entendran inclosos dins del servei ofert, sense que això comporti cap obligació addicional de provisió per part de l'Ajuntament o de l'entitat contractant.

Queda expressament exclosa de l'abast de l'Acord Marc la provisió d'infraestructures físiques o de telecomunicacions de l'entitat contractant, incloent-hi CPDs, servidors, tallafocs, llocs de treball i altra infraestructura física corporativa, sens perjudici de l'obligació de l'adjudicatari d'aportar, quan sigui necessari per a la correcta prestació del servei ofert, els mitjans addicionals que formin part de la seva pròpia solució de servei.

En el present document s'especifiquen **les condicions i requeriments generals associats al procés de selecció**, que seran d'aplicació als futurs contractes basats que se'n derivin.

D'acord amb allò que estableix l'article 99.3 de la Llei 9/2017, de 8 de novembre, de contractes del sector públic, per la qual es transposen a l'ordenament jurídic espanyol les Directives del Parlament Europeu i del Consell 2014/23/UE i 2014/24/UE, de 26 de febrer de 2014 (en endavant, LCSP), l'objecte d'aquest contracte admet la seva divisió en les agrupacions i lots indicats a l'apartat següent, atès que cadascun dels lots és susceptible d'utilització i aprofitament separat però la totalitat constitueix una unitat funcional.

2. Objecte de l'Acord Marc

2.1 Antecedents

L'Ajuntament de Barcelona compta amb més de 15.000 persones treballadores i 14.000 estacions de treball repartides en més de 600 centres al territori municipal, dos centres de processament de dades i vàries sales tècniques que allotgen més de 1.000 servidors que suporten més de 300 sistemes d'informació i 1.000 aplicacions, més de 6.000 persones treballadores externes, més de 4.000 terminals mòbils, més de 1.300 punts Wi-Fi corporatius i 700 punts Wi-Fi públics a la ciutat, etc. En aquest context, els serveis de ciberseguretat i operació d'eines de protecció són fonamentals per garantir l'operativa diària i l'eficiència dels serveis municipals.

Per al desenvolupament de serveis de manera més eficient i sostenible, l'Ajuntament de Barcelona compta amb una sèrie d'entitats dependents adscrites. Aquestes entitats són ens amb personalitat jurídica pròpia i patrimoni independent i neixen per al compliment de finalitats específiques, tenint en compte criteris de rendibilitat econòmica i de recuperació de la inversió.

La creació d'aquests ens permet gestionar de manera eficaç i especialitzada determinats serveis, aconseguir més flexibilitat i autonomia de gestió, i servir amb objectivitat els interessos generals i actuar d'acord amb els principis d'eficàcia, jerarquia, descentralització, desconcentració i coordinació, amb submissió plena a la Constitució, a la llei i al dret.

Addicionalment, l'Ajuntament, amb l'objectiu de fomentar els interessos generals de la ciutat i la millora de la qualitat de vida dels ciutadans i ciutadanes, participa en la presa de decisions en àmbits en què es pot veure afectat, i col·labora amb altres administracions i entitats privades en àrees d'interès mutu o de competències compartides. Alhora, té participació, directa i indirecta, i en proporcions diverses, en un seguit d'empreses, i està representat en diferents consorcis, fundacions i associacions.

L'elevat grau d'interconnexió i imbricació de les xarxes de telecomunicacions i dels sistemes d'informació de l'Ajuntament de Barcelona i de les entitats vinculades o dependents fa necessari disposar d'una visió integral i coordinada en matèria de seguretat i gestió del risc, atès que un incident menor en qualsevol d'aquests entorns pot derivar en una afectació significativa a escala corporativa si no es gestiona, comunica i conté adequadament.

La transformació digital i l'adopció de models de treball híbrid i teletreball han redefinit les necessitats tecnològiques de l'Ajuntament. Actualment, el lloc de treball no es limita a l'espai físic d'una oficina, sinó que s'ha convertit en un concepte flexible, amb treballadors que poden operar des de qualsevol ubicació, ja sigui des de casa, des de zones de treball compartides o

en mobilitat, amb dispositius de treball corporatius o personals, o bé de proveïdors externs. Aquesta nova realitat planteja reptes rellevants en matèria de seguretat, govern de la identitat digital, control d'accessos i experiència d'usuari, especialment quan els treballadors accedeixen a recursos corporatius ubicats dins i fora de la xarxa municipal.

L'any 2024 BIT va crear la Direcció de Serveis de Seguretat de la Informació i dins d'aquesta direcció va crear el Departament de Govern i Estratègia de Seguretat i el Departament de Seguretat Operativa. Aquesta Direcció té per objectiu coordinar i liderar la seguretat de la informació i la ciberresiliència de totes les entitats municipals, aplicant estratègies innovadores i una gestió integral de riscos per protegir els serveis crítics i garantir un entorn digital segur i resilient, inspirant confiança ciutadana i posicionant l'Ajuntament de Barcelona com a referent en protecció digital..

D'acord a les polítiques de seguretat aprovades per la Direcció i a la regulació aplicable (ENS, RGPD, NIS2, etc), i de forma coordinada amb el Departament de Govern i Estratègia de Seguretat, el Departament de Seguretat Operativa, es despleguen els serveis del Centre de Riscos i Operacions de Ciberresiliència (CROC), responsables de la governança, gestió de riscos, compliment normatiu i coordinació de la resposta davant incidents, i els serveis d'Operació de Seguretat i Anàlisi de Protecció (OSAP), orientats a les operacions de seguretat, el monitoratge continu, la detecció d'amenaces i la protecció avançada dels sistemes municipals.

L'objectiu conjunt és protegir els serveis TIC municipals en tots els àmbits —IT, OT i seguretat física—, mitjançant la implementació de mesures de ciberresiliència i de protecció de la informació que salvaguardin les dades i garanteixin la seva disponibilitat, integritat i confidencialitat.

Tal com detalla l'article 5 de l'Esquema Nacional de Seguretat (ENS), l'objectiu últim de la seguretat de la informació és garantir que una organització podrà complir els seus objectius, desenvolupar les seves funcions i exercir les seves competències fent servir sistemes d'informació, i per això formula els següents principis bàsics:

- Seguretat com a procés integral.
- Gestió de la seguretat basada en riscos.
- Prevenció, detecció, resposta i conservació.
- Existència de línies de defensa.
- Vigilància contínua.
- Reavaluació periòdica.
- Diferenciació de responsabilitats.

A més, l'article 8 detalla les accions relatives als aspectes de prevenció, detecció, resposta i conservació, per tal de minimitzar les vulnerabilitats dels sistemes d'informació i aconseguir

que les amenaces no es materialitzin, o bé en cas que ho facin no afectin greument la informació que gestionen o els serveis que presten, garantint la disponibilitat dels serveis durant tot el cicle vital de la informació digital.

Finalment, l'article 10 detalla que la vigilància contínua permetrà la detecció d'activitats o comportaments anòmals i l'oportuna resposta. D'altra banda, l'avaluació permanent de l'estat de seguretat dels actius permetrà mesurar la seva evolució, detectant vulnerabilitats i identificant deficiències de configuració.

Les mesures de seguretat s'han de reavaluar i actualitzar periòdicament, adequant la seva eficàcia a l'evolució dels riscos i els sistemes de protecció, podent arribar a un replantejament de la seguretat, si fos necessari.

2.2 Objecte

L'objecte de l'acord marc és l'homologació d'empreses per la realització dels serveis del Centre de Riscos i Operacions de Ciberresiliència (CROC) i dels serveis d'Operació de Serveis i eines Avançades de Protecció (OSAP) de l'Ajuntament de Barcelona, amb mesures de contractació pública sostenible.

Aquests serveis tenen per finalitat **garantir la gestió integral del risc, la ciberresiliència i la seguretat operativa municipal**, assegurant la **prevenció, detecció, resposta, recuperació i aprenentatge** davant incidents, així com la **governança, l'operació i l'evolució de les plataformes de protecció i de control de seguretat corporatives.**

Amb aquest model, l'Ajuntament de Barcelona reforça la seva capacitat per actuar de manera **proactiva, coordinada i eficient** davant les amenaces que afecten la continuïtat i la confiança dels serveis públics digitals.

L'Acord Marc estableix:

- **Un catàleg modular de paquets funcionals**, que permet a cada entitat adherida seleccionar, segons les seves necessitats i nivell de maduresa, els serveis adequats al seu context de risc, als seus actius i al seu pressupost.
- **Uns serveis generals obligatoris i comuns** a qualsevol paquet contractat, que garanteixen la coherència, la qualitat, la integració i la traçabilitat de totes les activitats.
- **Els mecanismes de governança, supervisió i control**, incloent els processos de seguiment, avaluació, rendició de comptes i millora contínua, amb indicadors que permetin mesurar l'eficàcia i la maduresa del servei.

- **L'alineament amb la normativa i els marcs de referència aplicables**, especialment l'**ENS**, el **RGPD**, la **Directiva NIS2**, el **Reglament de Ciberresiliència**, les **guies del CCN-STIC** i la **norma CCN-STIC 896 sobre Serveis de Seguretat Gestionats.**

En aquest marc, els serveis s'estructuren en **dues agrupacions principals** i complementàries:

- **Serveis CROC (Centre de Riscos i Operacions de Ciberresiliència):** inclouen les funcions de governança, compliment normatiu, anàlisi i gestió de riscos, planificació de la resiliència, coordinació de crisis, seguiment d'indicadors i suport estratègic a la direcció municipal.
- **Serveis OSAP (Operació de Seguretat i Anàlisi de Protecció):** inclouen l'operació, administració i evolució de les plataformes i eines de seguretat corporatives, així como la supervisió tècnica, la detecció i resposta davant incidents, i la seva integració amb els processos de gestió del risc i de ciberresiliència.

Amb aquest Acord Marc, l'Ajuntament de Barcelona vol **disposar d'un model integral, homogeni i sostenible de serveis gestionats de seguretat i resiliència**, que permeti:

- Reforçar la **ciberresiliència municipal** i la confiança digital.
- Optimitzar recursos i racionalitzar la contractació de serveis especialitzats.
- Garantir el **compliment normatiu** i la coherència amb els marcs reguladors europeus i estatals.
- Millorar la **coordinació, la capacitat de resposta i l'aprenentatge organitzatiu** davant les amenaces digitals presents i futures, promovent la millora contínua i la sostenibilitat en la prestació dels serveis..

2.3 Model funcional del CROC i de l'OSAP i alineament normatiu

Per garantir una operació de ciberresiliència integral i alineada amb els objectius estratègics de l'Ajuntament de Barcelona, es proposa un model funcional basat en la col·laboració entre el **Centre de Riscos i Operacions de Ciberresiliència (CROC)** i l'**Operació de Serveis i eines Avançades de Protecció (OSAP)**.

El CROC constitueix el centre neuràlgic de vigilància, detecció, contenció i resposta davant ciberincidents, mentre que l'OSAP és l'equip responsable de l'operació, administració i evolució de les eines de protecció corporatives que donen suport a aquesta activitat.

Aquesta estructura dual permet disposar d'un ecosistema de seguretat coordinat, modular i escalable, on cada servei aporta valor complementari i s'adapta a les necessitats de cada entitat municipal adherida.

Model funcional del CROC

El CROC s'organitza en quatre seccions funcionals (Prevenció, Detecció, Contenció i Resposta) i una funció de Governança transversal, que assegura coherència, control i millora contínua.

És per això que l'Ajuntament requereix serveis que garanteixin:

1. **Prevenció de ciberincidents:** mitjançant la identificació i el coneixement dels actius (dades, maquinari, programari, sistemes, dependències, serveis, persones, proveïdors, etc.) i dels riscos de ciberseguretat associats, permetent identificar la superfície d'exposició i prioritzar esforços de mitigació d'acord amb l'estratègia corporativa de gestió de riscos. Inclou auditories tècniques i proves d'intrusió per identificar vulnerabilitats i febleses de la infraestructura TIC, i avaluar l'eficàcia de les mesures de seguretat existents. També contempla la vigilància digital i la intel·ligència d'amenaces per detectar de forma proactiva amenaces i riscos abans que es materialitzin.
2. **Protecció davant ciberincidents:** un cop els riscos i vulnerabilitats són identificats, aquest servei ha de col·laborar amb l'**Operació de Serveis i eines Avançades de Protecció (OSAP)** per implementar i mantenir mesures preventives sobre les plataformes de seguretat corporatives (p. ex. tallafocs, antivirus, EDR, IDS/IPS, WAF, sistemes de filtratge o protecció de correu, etc.). L'objectiu és reduir la probabilitat i l'impacte dels ciberatacs, garantint el bastionat dels sistemes TIC, l'aplicació oportuna de pegats de seguretat i la millora contínua de la postura de seguretat.
3. **Detecció de ciberincidents:** en horari 24x7, per detectar i analitzar possibles ciberatacs i compromisos de seguretat, identificar anomalies, indicadors de compromís i altres esdeveniments potencialment maliciosos. El servei ha d'incloure la resposta automatitzada (contenció i mitigació) d'incidents simples i recurrents documentats en playbooks aprovats, la cerca proactiva d'amenaces (threat hunting), i el suport directe a les activitats de resposta i recuperació davant incidents greus.
4. **Resposta i recuperació de ciberincidents:** en horari 24x7, per contenir els efectes dels incidents greus, realitzar activitats d'anàlisi avançada, mitigació, erradicació i anàlisi forense, garantint la custòdia de proves digitals, l'elaboració d'informes i la coordinació amb l'equip de resposta municipal. Inclou també el suport en la gestió de cibercrisis i la validació de la recuperació segura dels sistemes afectats.
5. **Governança dels serveis d'operació de ciberseguretat:** per alinear-se amb els objectius corporatius, garantir el compliment normatiu, establir polítiques, rols, responsabilitats i mètriques per avaluar el rendiment del CROC, i promoure la millora contínua i la comunicació entre el CROC, la Direcció de Serveis de Seguretat de la Informació i les altres àrees municipals implicades.

Model funcional de l'OSAP

L'Operació de Serveis i eines Avançades de Protecció (OSAP) complementa funcionalment el CROC i centra la seva activitat en la gestió i operació de les eines de protecció corporatives.

Les seves funcions principals inclouen:

- Administrar i operar les plataformes de protecció (tallafocs, IPS/IDS, protecció de correu, WAF, EDR, XDR, microCLAUDIA, etc.) segons les directrius i polítiques definides per la Direcció de Serveis de Seguretat de la Informació.
- Aplicar configuracions, actualitzacions i pegats de seguretat de manera controlada, assegurant la traçabilitat i la reversibilitat dels canvis.
- Assegurar la integració d'aquestes plataformes amb el CROC per facilitar la detecció i la resposta coordinada.
- Realitzar tasques d'evolució tècnica i optimització de les eines de protecció, incorporant noves funcionalitats o millores de rendiment.
- Participar en les activitats de resposta a incidents sota la coordinació del CROC quan sigui necessari.
- Mantenir la documentació tècnica actualitzada i col·laborar en la transferència de coneixement.

Aquest model complementari entre el CROC i l'OSAP garanteix una defensa municipal integrada, basada en la col·laboració, la coherència tecnològica i la millora contínua, assegurant el compliment de les normatives i marcs de referència aplicables en matèria de ciberseguretat.

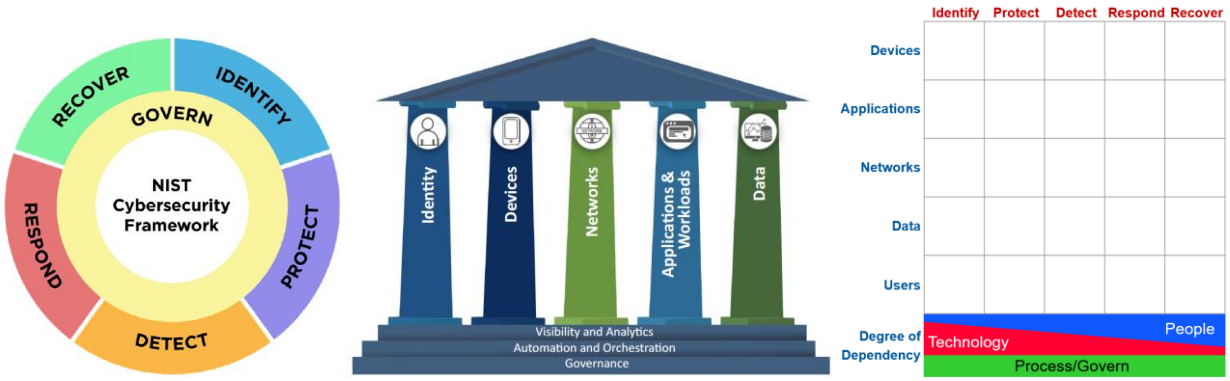
Alineament normatiu

El model funcional del CROC i de l'OSAP s'alinea amb els principals marcs normatius i directrius europees i estatals, entre les quals destaquen:

- El Reial Decret 311/2022, de 3 de maig, pel que es regula l'Esquema Nacional de Seguretat (ENS).
- El Reglament (UE) 2016/679, de 27 d'abril, de protecció de les persones físiques pel que fa al tractament de dades personals (RGPD).
- La Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDPGDD).
- La Llei Orgànica 7/2021, de 26 de maig, de protecció de dades personals tractades per a fins de prevenció, detecció, investigació i enjudiciament d'infraccions penals i d'execució de sancions penals.

- El Reglament (UE) 2019/881, de 15 d'abril de 2019 (ENISA i certificació de la ciberseguretat).
- La Directiva (UE) 2022/2555, de 14 de desembre de 2022 (NIS2).
- El Reglament (UE) 2024/1689, de 13 de juny de 2024 (Intel·ligència Artificial).
- El Reglament d'execució (UE) 2024/2690, de 17 d'octubre de 2024, pel que s'estableixen les disposicions d'aplicació de la Directiva NIS2.
- El Reglament (UE) 2024/2847, de 23 d'octubre de 2024 (de Ciberresiliència).
- El Reglament (UE) 2025/37, de 19 de desembre de 2024, pel que es modifica el Reglament (UE) 2019/881 en allò que es refereix als Serveis de Seguretat Gestionats.
- La guia CCN-STIC 896 (agost-2025) relativa al Perfil de Compliment Específic per a Serveis de Seguretat Gestionats (PCE-SSG).

A més, aquest model s'inspira en **marcs de referència internacionals** com el **NIST Cybersecurity Framework 2.0**, el **Zero Trust Maturity Model (ZTMM 2.0) de CISA** i la **Cyber Defense Matrix** de Sounil Yu, que aporten bones pràctiques per establir un model municipal de ciberresiliència modern, resilient i amb capacitat de millora contínua.



2.4 Situació de partida dels serveis de ciberseguretat i protecció avançada

El teletreball, juntament amb l'adopció de noves eines de treball col·laboratiu (per exemple, l'entorn M365), han fomentat l'accés a la informació i als serveis corporatius des de qualsevol dispositiu, ubicació i moment. Addicionalment, l'ús de solucions al núvol de tipus **SaaS, PaaS i IaaS** en entorns multi-cloud (Azure, AWS, GCP, IBM Cloud, etc.), el desplegament de plataformes d'orquestració de contenidors basades en Kubernetes (per exemple, Openshift Container Platform) i la progressiva adopció de tecnologies emergents com la **IA** o la **IoT**, representen reptes que impulsen i fan evolucionar la postura de ciberresiliència municipal.

La millora de la formació dels equips, l'adopció de bones pràctiques i l'establiment de sinèrgies entre diferents unitats han permès reforçar els processos de seguretat operativa i la coordinació entre els equips del CROC i de l'OSAP.

El desplegament de noves eines de seguretat (EDR, complementàries a les plataformes SIEM existents) ha millorat la detecció, anàlisi i contenció de comportaments maliciosos.

L'ús del **múltiple factor d'autenticació (MFA)** per protegir l'accés als serveis corporatius ha reduït de manera significativa l'impacte del phishing.

A més, la incorporació de plataformes especialitzades de gestió de l'exposició i de vulnerabilitats ha permès detectar i mitigar vulnerabilitats en serveis crítics, reduint la superfície d'exposició i millorant la maduresa de la postura de seguretat.

En aquest context, les capacitats d'ingesta i correlació de les plataformes SIEM on-premise han estat superades pel volum d'esdeveniments generats per les fonts tradicionals (tallafocs, proxies, etc.) i per la necessitat d'integrar noves fonts (on-premise i cloud). Per aquest motiu, es considera més adient evolucionar cap a una plataforma **SIEMaaS multi-tenant com a servei**, que garanteixi escalabilitat, flexibilitat, traçabilitat de costos i retenció adequada de logs segons requisits normatius i forenses.

Avui dia, les capacitats d'**orquestració i automatització de la resposta (SOAR)** són essencials per fer front a ciberatacs cada cop més sofisticats i automatitzats. Aquesta automatització, tanmateix, ha de seguir pautes prèviament acordades i amb supervisió humana quan sigui necessari. Per això, es considera indispensable que la plataforma SIEMaaS incorpori també capacitats SOAR, que permetin executar procediments de resposta a incidents (playbooks) aprovats, amb l'objectiu de contenir amenaces abans que tinguin impacte.

L'àmbit del CROC abasta la seguretat operativa de la infraestructura **IT, OT, IoT, Industrial IoT i la seguretat física** dels emplaçaments on es troben els dispositius més crítics. Aquest abast es complementa amb l'activitat de l'OSAP, responsable de l'operació i gestió de les eines de protecció que donen suport a les tasques de detecció i resposta del CROC. Aquest model reforça la decisió d'implantar una plataforma **SIEM/SOAR as a Service** que reculli la telemetria de tots aquests entorns i faciliti la detecció, gestió i mitigació d'incidents i vulnerabilitats de seguretat.

BIT té actualment l'encàrrec de proporcionar serveis de ciberresiliència i operació de seguretat a l'Ajuntament de Barcelona, així com als organismes autònoms locals i a les entitats públiques

empresarials vinculades o dependents. Addicionalment, ha d'acompanyar aquestes entitats per assegurar el compliment de les polítiques corporatives, col·laborar en la implantació de serveis comuns i en projectes a demanda, així com coordinar la resposta davant incidents greus.

L'objectiu d'aquest Acord Marc és oferir a totes les entitats vinculades o dependents de l'Ajuntament de Barcelona un **catàleg modular de serveis CROC i OSAP**, que complementi els serveis existents, fomenti l'aplicació de polítiques, protocols i metodologies comunes, i millori les capacitats d'operació, detecció i resposta de la ciberseguretat tant de manera individual com col·lectiva.

2.5 Estructura de lots i incompatibilitats

El present Acord Marc, promogut per l'Institut Municipal Barcelona Innovació i Tecnologia (BIT), té per objecte la selecció d'una única empresa prestatària de serveis per cadascun dels lots, amb la finalitat de fixar les condicions tècniques i funcionals a què s'hauran d'ajustar els contractes basats que es pretenguin adjudicar durant el període de vigència.

Els serveis objecte d'aquest Acord Marc inclouen **el Centre de Riscos i Operacions de Ciberresiliència (CROC)** i **l'Operació de Serveis i eines Avançades de Protecció (OSAP)**, considerant que el recurs a aquest instrument no s'efectua de forma abusiva ni de manera que la competència es vegi obstaculitzada, restringida o falsejada, tal com estableix l'article 219.1 de la LCSP.

Les contractacions basades en aquest Acord Marc podran ser impulsades:

- Per BIT, que inclourà la provisió de serveis a l'Ajuntament de Barcelona, els Organismes Autònoms Locals i les Entitats Públiques Empresarials.
- Per la resta d'entitats vinculades o dependents de l'Ajuntament de Barcelona (Societats Mercantils Municipals, Societats Mercantils amb participació minoritària, Consorcis, Fundacions i Associacions).

Cada entitat podrà contractar de manera independent un o diversos paquets funcionals, corresponents als lots definits, segons les seves necessitats específiques i el seu nivell de maduresa. Aquesta estructura modular permet escalar els serveis i adaptar-los a diferents contextos organitzatius, mantenint alhora la coherència tècnica i procedimental del conjunt del model municipal.

Així mateix, l'estructura de lots afavoreix **que cada organisme pugui governar els seus serveis de ciberresiliència i operació de protecció amb autonomia**, i al mateix temps garantir **una resposta coordinada i integrada a nivell municipal**, assegurant la coherència en la detecció, la resposta, protecció i governança de la seguretat de la informació davant ciberamenaces.

2.5.1 Divisió en lots

Per garantir una contractació eficient i adaptada a les diferents necessitats de les entitats municipals, el present Acord Marc s'estructura en **tres lots diferenciats, dos vinculats als serveis del Centre de Riscos i Operacions de Ciberresiliència (CROC) i un lot dedicat a l'Operació de Serveis i eines Avançades de Protecció (OSAP)**. Aquesta divisió permet assegurar una major especialització, transparència i traçabilitat en la prestació dels serveis, així com una millor coordinació entre la detecció, la resposta i l'operació de les plataformes de protecció.

Lot 1. Serveis del Centre de Riscos i Operacions de Ciberresiliència.

Aquest lot comprèn els serveis necessaris per garantir la **prevenció, detecció, contenció, resposta i recuperació d'incidents de seguretat**, d'acord amb el model funcional descrit al present plec. Inclou els serveis operatius essencials per:

- Monitorar i detectar ciberamenaces i incidents en modalitat 24x7.
- Prevenir incidents mitjançant auditories tècniques, gestió de vulnerabilitats i vigilància digital.
- Executar accions de contenció immediata per limitar l'impacte dels incidents.
- Donar resposta i recuperar serveis davant incidents greus de seguretat, incloent l'anàlisi forense i el suport en cibercrisis.
- Administrar i operar les plataformes que suportin els serveis de prevenció, detecció i resposta.

Lot 2. Serveis d'avaluació i validació del CROC

Aquest lot té per objectiu proporcionar una **visió independent i objectiva sobre l'estat de maduresa i eficàcia del CROC** i sobre l'evolució de les seves capacitats. La segregació d'aquest lot garanteix que l'avaluació sigui realitzada per un proveïdor independent del que presta els serveis operatius, assegurant imparcialitat i fomentant un cicle de millora contínua. Inclou:

- Avaluacions periòdiques de la maduresa i les capacitats del CROC, amb metodologies reconegudes.
- Serveis de validació de la seguretat mitjançant exercicis Red Team, Blue Team o Purple Team.
- Elaboració de fulls de ruta per a la millora contínua de les capacitats de prevenció, protecció, detecció, contenció, resposta i resiliència.

Lot 3. Operació de Serveis i eines Avançades de Protecció (OSAP)

Aquest lot dona cobertura a la **gestió i operació de les plataformes de protecció corporatives**, imprescindibles per a la defensa global dels serveis municipals i complementàries a les activitats del CROC. El lot comprèn:

- **L'administració i operació de les plataformes de protecció definides en el present plec tècnic** (p. ex. tallafocs, IDS/IPS, protecció de correu, accés remot segur, WAF, etc.).
- **La coordinació de les activitats de manteniment i suport tècnic d'aquestes eines**, assegurant-ne la disponibilitat, l'actualització i la configuració segura.
- **L'aplicació i evolució de les configuracions de seguretat** per adaptar-se a noves necessitats o amenaces.
- **La integració amb el CROC** per garantir una detecció i resposta coordinada.
- **Administrar i monitoritzar tota la plataforma tecnològica** així com la resolució de peticions, incidències i problemes per tal de proveir la màxima disponibilitat dels serveis.
- **La proposta de millores i optimitzacions** en les plataformes operades, d'acord amb l'estratègia de seguretat municipal i les directrius de la Direcció de Serveis de Seguretat de la Informació.

2.5.2 Incompatibilitats

Amb l'objectiu de garantir la **transparència, la competència efectiva i la independència en l'avaluació dels serveis**, en el Plec de Clàusules Administratives Particulars d'aquest Acord Marc s'estableixen restriccions en la participació a la licitació i en l'adjudicació entre els diferents lots, amb la finalitat d'evitar conflictes d'interès i assegurar la imparcialitat dels resultats.

2.5.3 Abast de les contractacions basades

Les contractacions que es derivin del present Acord Marc tindran per objecte cobrir les necessitats concretes de les entitats municipals adherides, dins d'un marc comú que garanteixi coherència i coordinació a nivell municipal. Aquestes contractacions podran contemplar, en primer lloc, el desplegament inicial dels serveis del Centre de Riscos i Operacions de Ciberresiliència (CROC) i de l'Operació de Serveis i eines Avançades de Protecció (OSAP), adaptant-los a les característiques i requeriments específics de cada entitat en funció de la seva maduresa, dels serveis crítics que calgui protegir i dels riscos associats. El desplegament inclourà la configuració, integració i validació dels serveis, eines i fluxos de treball necessaris per garantir la correcta operativa i la coordinació amb la Direcció de Serveis de Seguretat de la Informació.

A més, les contractacions basades podran contemplar l'ampliació modular i escalable dels serveis ja implantats, de manera que aquests es puguin estendre a nous entorns, col·lectius o unitats organitzatives, incorporant progressivament noves fonts de dades, sistemes, aplicacions i serveis dins del marc del CROC o de l'OSAP. Aquesta ampliació permetrà també afegir nous paquets funcionals en coherència amb l'estratègia municipal de seguretat de la informació i ciberresiliència digital.

Les entitats adherides podran disposar igualment de serveis de suport operatiu que reforcin les seves capacitats de prevenció, protecció, detecció i resposta. Aquests serveis inclouran, entre d'altres, la gestió de vulnerabilitats i exposició, el bastionat d'entorns TIC, l'operació diària de les eines de protecció, l'assistència tècnica especialitzada i el suport a la coordinació i resposta davant incidents de seguretat..

Finalment, l'abast de les contractacions inclou la necessitat d'assegurar que tots els serveis contractats es mantenen alineats amb les polítiques corporatives de la informació, privadesa i resiliència digital de l'Ajuntament, de manera que es garanteixi una resposta homogènia i coordinada a nivell municipal. D'aquesta manera, els serveis derivats de l'Acord Marc contribuiran no només a enfortir la seguretat i l'eficiència de cada entitat individual, sinó també a consolidar una defensa col·lectiva municipal davant les amenaces digitals que afecten la ciutat en el seu conjunt.

3. Abast

3.1 Descripció de l'abast

El present Acord Marc estableix l'abast dels **serveis del Centre de Riscos i Operacions de Ciberresiliència (CROC)** i de **l'Operació de Serveis i eines Avançades de Protecció (OSAP)**, amb l'objectiu de proporcionar a l'Ajuntament de Barcelona i a les entitats vinculades o dependents un marc estable, flexible i escalable per a la contractació de serveis de prevenció, detecció, contenció, resposta i recuperació davant de ciberamenaces, així com per a la gestió i operació de les eines de protecció corporatives i altres eines incloses al nus de telecomunicacions. L'abast es defineix d'acord amb tres eixos principals: les funcions del servei CROC i de l'OSAP, els tipus d'actius objecte de protecció i el nivell de maduresa de les capacitats del servei en cada entitat.

Pel que fa a les funcions, els serveis es classifiquen en **govern del CROC, prevenció, detecció, contenció, resposta, recuperació i millora contínua** (lot independent), així com en **operació de serveis i eines de protecció (OSAP)**. Cadascuna d'aquestes funcions es concreta en **paquets funcionals diferenciats**, que poden ser contractats de manera independent i que es troben graduats en subnivells de maduresa.

En relació amb els actius, l'abast cobreix la informació i les dades, els serveis i aplicacions corporatives, les identitats i credencials d'accés, els dispositius i equips tant d'entorns informàtics com industrials i de dispositius connectats, les xarxes i les infraestructures de comunicacions, les plataformes i serveis al núvol, els contenidors i els orquestradors, els sistemes de còpies de seguretat i de recuperació, les plataformes de seguretat i monitoratge, els hipervisors i entorns de virtualització, els sistemes basats en intel·ligència artificial, les claus criptogràfiques i els sistemes de gestió de claus, així com les instal·lacions físiques i els entorns híbrids.

Quant a la maduresa, cada paquet funcional s'ofereix en tres subnivells: **inicial, avançat i òptim**, per adaptar-se al nivell de maduresa i als recursos disponibles de cada entitat.

El catàleg de serveis inclòs en l'abast es compon de **paquets funcionals CROC i OSAP**. En l'àmbit de la **prevenció i detecció** s'inclouen la gestió de vulnerabilitats i de l'exposició, les auditories i proves de seguretat, els serveis de vigilància digital i d'intel·ligència d'amenaces, l'inventari i classificació d'actius, així com el monitoratge i detecció d'incidents per cadascun dels tipus d'actius.

En l'àmbit de la **protecció (OSAP)** es preveu l'operació i administració de les plataformes de seguretat que donen cobertura a la protecció de llocs de treball, dispositius mòbils i servidors,

identitats i accessos, informació i dades, serveis de correu i col·laboració, xarxes i entorns al núvol, aplicacions i contenidors, sistemes industrials i de IoT, entorns d'intel·ligència artificial, còpies de seguretat, hipervisors, plataformes de ciberseguretat i gestió criptogràfica.

En l'àmbit de la **resposta i recuperació**, s'inclouen els serveis de resposta a incidents, anàlisi forense i recuperació post-incident.

Finalment, en l'àmbit transversal s'incorporen la capacitació i conscienciació en seguretat, la governança i el compliment, i l'avaluació externa i millora contínua de les capacitats del CROC.

Els serveis definits han de permetre incorporar noves tecnologies de seguretat o funcionalitats durant la vigència de l'Acord, mantenint-se dins de la família funcional corresponent, i han de ser prestats en alineament amb la normativa vigent i aplicable, incloent la Directiva NIS2, l'Esquema Nacional de Seguretat i les guies del Centre Criptològic Nacional. Els serveis generals de suport operatiu, gestió del canvi, monitoratge i manteniment queden implícitament inclosos en l'execució de tots els paquets funcionals contractats. L'abast definit és aplicable a totes les entitats vinculades o dependents de l'Ajuntament de Barcelona, amb independència de la seva mida, els seus actius o el seu nivell de maduresa en matèria de seguretat.

El catàleg de serveis es troba estructurat en tres eixos per tal d'adequar l'oferta de serveis a les necessitats operatives de cada entitat, als actius objecte de protecció, al nivell de maduresa de les seves capacitats, a l'estratègia de seguretat de la informació i al seu pressupost disponible:

- Funcions del servei CROC i OSAP
    - Govern del CROC, Prevenció, Detecció, Contenció, Resposta i Recuperació.
    - Operació de Serveis i eines Avançades de Protecció (OSAP), que dona suport a les funcions anteriors mitjançant l'administració i gestió de les plataformes de protecció.
- Tipus d'actius de l'entitat
    - Dades, Serveis, Identitats, Dispositius (IT, OT i IoT), Xarxes, Aplicacions.
    - Instal·lacions, Serveis al Núvol, Contenidors i Orquestradors, sistemes de còpies de seguretat, Hipervisors i plataformes de virtualització, Sistemes d'Intel·ligència Artificial, Claus criptogràfiques i sistemes de gestió de claus.
- Nivell de maduresa de les capacitats del servei a l'entitat:
    - Inicial, Avançat, Òptim.

Aquest Acord Marc dona resposta a la necessitat de disposar de serveis de ciberresiliència i d'operació de protecció moderns i escalables, dissenyats per protegir els recursos digitals de

l'Ajuntament de Barcelona en un context on el treball híbrid, la mobilitat dels usuaris i l'adopció d'aplicacions SaaS han fet obsolet el model de seguretat tradicional basat en perímetres de xarxa i en solucions únicament on-premise. Aquests serveis de seguretat gestionats han de permetre oferir unes capacitats de prevenció, protecció, detecció, resposta i recuperació de ciberincidents coherents i coordinades a totes les entitats vinculades o dependents de l'Ajuntament de Barcelona, independentment de la ubicació dels usuaris, els dispositius, les aplicacions, la informació i els serveis.

D'acord a la Directiva (UE) 2022/255 del Parlament Europeu i del Consell, de 14 de desembre de 2022, relativa a les mesures destinades a garantir un elevat nivell comú de ciberseguretat en tota la Unió (NIS2), i d'acord a la guia CCN-SITC-896 de Perfil de Compliment Específic per a Serveis de Seguretat Gestionats, els proveïdors de serveis de seguretat gestionats (SSG) en àmbits com la resposta a incidents, les proves de penetració, les auditories tècniques i la consultoria exerceixen un paper especialment important prestant assistència a les entitats en els seus esforços de prevenció, detecció, resposta i recuperació en relació amb els incidents. Tanmateix, els propis proveïdors de serveis de seguretat gestionats també han estat víctimes de ciberatacs i plantegen un risc especial com a conseqüència de la seva estreta integració amb les activitats de les entitats. Per aquest motiu, d'una banda, les organitzacions prestadores de serveis de seguretat gestionats han d'evidenciar les seves capacitats operatives, així com les seves competències tècniques, garantint que els serveis prestats seran de qualitat; i d'altra banda, els mitjans emprats per prestar els serveis SSG hauran de complir els requisits necessaris de seguretat que garanteixin que són protegits i són confiables per realitzar la seva funció de forma segura per a la pròpia entitat i per aquelles que contractin els seus serveis.

3.2 Catàleg de serveis

Tal com s'ha indicat en l'apartat anterior, els serveis a contractar sota el present Acord Marc es concreten mitjançant la definició d'un **catàleg de paquets funcionals CROC i OSAP independents**, que constitueixen les **unitats mínimes de contractació**. Cada paquet dona resposta a una necessitat específica dins de l'arquitectura de seguretat operativa i pot ser contractat de forma autònoma en el marc d'un contracte basat.

El **catàleg de serveis** inclou un conjunt de **trenta un paquets funcionals**, cadascun estructurat en tres subnivells de maduresa, inicial, avançat i òptim, , excepte els paquets de protecció, que es defineixen com a serveis únics sense subdivisió. Aquesta estructura permet adaptar l'abast i la profunditat de les capacitats a les necessitats i als recursos de cada entitat. Aquest catàleg abasta tot el cicle de la ciberseguretat i s'articula en cinc grans blocs funcionals:

- **Prevenció**:
    - Gestió de vulnerabilitats i exposició. Inclòs en Lot 1.
    - Auditories i proves de seguretat. Inclòs en Lot 1.
    - Serveis d'intel·ligència d'amenaces. Inclòs en Lot 1.
    - Inventari i classificació d'actius. Inclòs en Lot 1.
- **Protecció**:
    - Protecció de llocs de treball i dispositius mòbils. Inclòs en Lot 3.
    - Protecció dels servidors. Inclòs en Lot 3.
    - Protecció de la identitat i els accessos. Inclòs en Lot 3.
    - Protecció de la informació. Inclòs en Lot 3.
    - Protecció del correu i dels entorns de col·laboració. Inclòs en Lot 3.
    - Protecció de xarxes i telecomunicacions. Inclòs en Lot 3.
    - Protecció d'aplicacions i APIs. Inclòs en Lot 3.
    - Protecció de serveis al núvol. Inclòs en Lot 3.
    - Protecció de tecnologies emergents i especialitzades (sistemes industrials, dispositius connectats, intel·ligència artificial i criptografia). Inclòs en Lot 3.
    - Protecció d'hipervisors i plataformes de virtualització. Inclòs en Lot 3.
    - Protecció de contenidors i orquestradors. Inclòs en Lot 3.
- **Detecció**:
    - Monitoratge i detecció d'incidents a llocs de treball i dispositius mòbils. Inclòs en Lot 1.
    - Monitoratge i detecció d'incidents a servidors. Inclòs en Lot 1.
    - Monitoratge i detecció d'incidents a identitats i accessos. Inclòs en Lot 1.
    - Monitoratge i detecció d'incidents a informació i dades. Inclòs en Lot 1.
    - Monitoratge i detecció d'incidents a correu i entorns de col·laboració. Inclòs en Lot 1.

  - Monitoratge i detecció d'incidents a xarxes i telecomunicacions. Inclòs en Lot 1.
  - Monitoratge i detecció d'incidents a aplicacions i APIs. Inclòs en Lot 1.
  - Monitoratge i detecció d'incidents a serveis al núvol. Inclòs en Lot 1.
  - Monitoratge i detecció d'incidents a tecnologies emergents i especialitzades (sistemes industrials, dispositius connectats, intel·ligència artificial i criptografia). Inclòs en Lot 1.
  - Monitoratge i detecció d'incidents a hipervisors i plataformes de virtualització. Inclòs en Lot 1.
  - Monitoratge i detecció d'incidents a contenidors i orquestradors. Inclòs en Lot 1.

- **Resposta i recuperació**:
  - Resposta a incidents. Inclòs en Lot 1.
  - Recuperació post-incident. Inclòs en Lot 1.
- **Funcions transversals**:
  - Capacitació i conscienciació. Inclòs en Lot 1.
  - Governança i compliment. Inclòs en Lot 1.
  - Avaluació externa i millora contínua del CROC. Inclòs en Lot 2.

Tots els paquets funcionals inclouen de manera obligatòria un conjunt de serveis generals, que l'adjudicatari haurà de prestar de forma transversal en qualsevol contracte basat. Aquests serveis generals comprenen:

- La direcció i el seguiment dels projectes.
- La documentació tècnica i funcional.
- La formació als equips municipals.
- La coordinació amb l'equip d'operacions de l'entitat municipal.
- El traspàs operatiu dels serveis desplegats.

Cada paquet funcional i els serveis associats hauran de respectar les **condicions generals establertes en aquest plec**, així com els **requisits tècnics i normatius aplicables**, amb l'objectiu de garantir la **qualitat, la seguretat, l'escalabilitat i la integració** dels serveis dins l'ecosistema digital municipal.

Queden expressament exclosos de l'abast d'aquest Acord Marc:

- El subministrament i la gestió d'infraestructures físiques com ara telecomunicacions, centres de processament de dades, servidors, llocs de treball o dispositius terminals, excepte aquells actius directament vinculats a la prestació del servei
- El suport a dispositius de la ciutadania, incloent telèfons, tauletes o equips particulars.
- El suport directe als dispositius d'usuari final del personal municipal, com ara microinformàtica o serveis de primer nivell, excepte quan hagin estat afectats per un incident de seguretat.
- Qualsevol altra activitat pròpia de les unitats de negoci o serveis funcionals que fan ús dels serveis de seguretat però que no estan relacionades amb el seu desplegament ni operació tècnica.

3.3 Paquets funcionals contractables

Els serveis objecte del present Acord Marc es concreten mitjançant **paquets funcionals independents**, cadascun dels quals constitueix una **unitat mínima de contractació**. Cada paquet correspon a una funcionalitat específica dins de l'arquitectura municipal de ciberresiliència i de seguretat operativa i pot ser contractat de manera autònoma en el marc d'un contracte basat, d'acord amb les necessitats de cada entitat municipal.
El **catàleg de paquets funcionals** s'articula al voltant de cinc grans àmbits del cicle de la ciberseguretat:

- **Prevenció**, que inclou la gestió de vulnerabilitats i exposició, les auditories i proves de seguretat, els serveis d'intel·ligència d'amenaces i l'inventari i classificació d'actius.
- **Protecció**, que incorpora la protecció de la seguretat dels llocs de treball i dispositius mòbils (incloent-hi ordinadors personals i entorns virtuals d'escriptori), la protecció de servidors, la protecció de la identitat i els accessos, la protecció de la informació i les dades, la protecció del correu i els entorns de col·laboració, la seguretat de xarxes i telecomunicacions, la protecció d'aplicacions i APIs (Interfase de Programació d'Aplicacions), la seguretat de serveis al núvol, la protecció de tecnologies emergents i especialitzades com ara sistemes industrials, dispositius connectats, intel·ligència artificial i criptografia, la protecció dels hipervisors i plataformes de virtualització, i la protecció de contenidors i orquestradors.
- **Detecció**, que es concreta en els serveis de monitoratge i detecció d'incidents de seguretat, a partir del monitoratge de la seguretat dels llocs de treball i dispositius mòbils (incloent-hi ordinadors personals i entorns virtuals d'escriptori), dels servidors,

de les identitats i els accessos, de la informació i les dades, del correu i els entorns de col·laboració, de les xarxes i telecomunicacions, de les aplicacions i APIs, dels serveis al núvol i de les tecnologies emergents i especialitzades com ara sistemes industrials, dispositius connectats, intel·ligència artificial i criptografia, dels sistemes de còpies de seguretat, de les plataformes de ciberseguretat, de la protecció dels hipervisors i plataformes de virtualització, i dels contenidors i orquestradors.

- **Resposta i recuperació**, que abasta els serveis de resposta a incidents i de recuperació post-incident.
- **Funcions transversals**, que inclouen la capacitació i conscienciació del personal municipal, la governança i el compliment normatiu, i l'avaluació externa i la millora contínua del CROC.

Alguns d'aquests paquets es troben disponibles en **tres subnivells de maduresa —inicial, avançat i òptim—**, la qual cosa permet adaptar l'abast i la profunditat dels serveis a les necessitats, recursos i grau de maduresa en matèria de seguretat de cada entitat. Aquesta gradació garanteix una evolució escalable i modular, des de serveis essencials fins a capacitats avançades i altament integrades.

Els paquets funcionals, per la seva naturalesa modular i complementària, **es poden combinar lliurement** en els contractes basats, i hauran de ser prestats de forma homogènia, garantint en tot moment la continuïtat operativa i l'alineament amb l'estratègia global de seguretat definida per l'Ajuntament de Barcelona.

A continuació es detalla la llista completa dels paquets funcionals amb els seus subpaquets (nivells de maduresa: Inicial, Avançat, Òptim). Això constitueix el catàleg complet i modular del CROC-OSAP:

3.3.1 Lot 1. Serveis del Centre de Riscos i Operacions de Ciberresiliència

PREVENCIÓ:

P1. Gestió de vulnerabilitats i exposició

P1-A. Inicial: Revisió periòdica de vulnerabilitats en equips i serveis bàsics.

P1-B. Avançat: Anàlisi de vulnerabilitats en entorns industrials, dispositius connectats i serveis al núvol.

P1-C. Òptim: Gestió contínua de l'exposició, simulació d'atacs i revisió en IA i sistemes de xifratge

P2. Auditories i proves de seguretat

P2-A. Inicial: Proves bàsiques d'intrusió i auditories tècniques d'equips.

P2-B. Avançat: Proves avançades en aplicacions, serveis al núvol i codi font.

P2-C. Òptim: Exercicis d'atac realista, auditories en IA i gestió de claus de seguretat.

P3. Serveis d'intel·ligència d'amenaces

P3-A. Inicial: Vigilància bàsica d'amenaces i riscos reputacionals.

P3-B. Avançat: Anàlisi de frau digital i riscos en canals mòbils, gestió de plataforma d'intel·ligència.

P3-C. Òptim: Intel·ligència especialitzada en entorns informàtics i industrials, riscos de la cadena de subministrament.

P4. Inventari i classificació d'actius

P4-A. Inicial: Registre manual d'actius i càrrega a la base de dades corporativa.

P4-B. Avançat Descobriment automàtic parcial i etiquetatge.

P4-C. Òptim Descobriment completament automatitzat i actualització en temps real.

DETECCIÓ (monitoratge ciberseguretat)

P16. Monitoratge i detecció d'incidents a llocs de treball i dispositius mòbils (PC, VDIs i mòbils)

P16-A. Inicial: Monitoratge antivirus i protecció bàsica.

P16-B. Avançat: Detecció i resposta avançada en llocs de treball i dispositius mòbils.

P16-C. Òptim: Gestió integrada amb resposta automatitzada, contenció immediata i caça d'amenaces sobre llocs de treball i dispositius mòbils.

P17. Monitoratge i detecció d'incidents a servidors

P17-A. Inicial: Monitoratge protecció bàsica de servidors físics i virtuals.

P17-B. Avançat: Detecció i resposta avançada en entorns crítics i servidors d'aplicacions.

P17-C. Òptim: Gestió integrada amb resposta automatitzada, contenció immediata i caça d'amenaces sobre servidors.

P18. Monitoratge i detecció d'incidents a identitats i accessos

P18-A. Inicial: Monitoratge bàsic de directoris i autenticació multifactor simple.

P18-B. Avançat: Detecció d'anomalies i integració amb sistemes de monitoratge central.

P18-C. Òptim: Gestió integrada i adaptativa de riscos amb resposta automatitzada, contenció immediata i caça d'amenaces sobre identitats.

P19. Monitoratge i detecció d'incidents a informació i dades

P19-A. Inicial: Monitoratge bàsic de pèrdua d'informació en correu i equips.

P19-B. Avançat: Detecció avançada en serveis al núvol i aplicacions.

P19-C. Òptim: Gestió integrada amb resposta automatitzada, contenció immediata i caça d'amenaces de fuites de dades.

P20. Monitoratge i detecció d'incidents a correu i col·laboració

P20-A. Inicial: Monitoratge bàsic de correu brossa i programari maliciós.

P20-B. Avançat: Detecció avançada contra suplantacions i adjunts maliciosos.

P20-C. Òptim: Gestió integrada amb resposta automatitzada, contenció immediata i caça d'amenaces al correu i entorns de col·laboració.

P21. Monitoratge i detecció d'incidents a xarxes i telecomunicacions

P21-A. Inicial: Monitoratge bàsic de tallafocs, proxys i serveis bàsics de seguretat de xarxa.

P21-B. Avançat: Monitoratge de passarel·les segures, protecció d'aplicacions web i accés remot segur.

P21-C. Òptim: Monitoratge de control d'accés sense perímetre, serveis al núvol, APIs i detecció d'amenaces en xarxa. Gestió integrada amb resposta automatitzada, contenció immediata i caça d'amenaces a xarxes i telecomunicacions.

P22. Monitoratge i detecció d'incidents a aplicacions

P22-A. Inicial: Monitoratge bàsic sistemes de publicació segura i revisió de configuracions bàsiques.

P22-B. Avançat: Monitoratge de proves de seguretat automatitzades i integració amb desenvolupament.

P22-C. Òptim: Monitoratge en temps real d'aplicacions i APIs, seguretat en microserveis, i caça d'amenaces a aplicacions.

P23. Monitoratge i detecció d'incidents a serveis al núvol

P23-A. Inicial: Monitoratge bàsic d'ús d'aplicacions al núvol.

P23-B. Avançat: Monitoratge protecció de càrregues de treball i de configuracions al núvol.

P23-C. Òptim: Monitoratge protecció integral d'aplicacions natives, governança de dades sensibles, gestió integrada amb resposta automatitzada, contenció immediata i caça d'amenaces a serveis al núvol.

P24. Monitoratge i detecció d'incidents a tecnologies emergents i especialitzades (OT, IoT, IA i criptografia)

P24-A. Inicial: Monitoratge bàsic de sistemes industrials i dispositius connectats.

P24-B. Avançat: Detecció d'amenaces en xarxes industrials i monitoratge sistemes de gestió centralitzada de claus.

P24-C. Òptim: Detecció avançada en entorns industrials, detecció incidents IA i preparació detecció incidents post-quàntica.

P25. Monitoratge i detecció d'incidents a hipervisors i plataformes de virtualització

P25-A. Inicial: Monitoratge bàsic d'hipervisors i plataformes de virtualització.

P25-B. Avançat: Detecció d'amenaces en hipervisors i plataformes de virtualització.

P25-C. Òptim: Detecció avançada d'amenaces en hipervisors i plataformes de virtualització

P26. Monitoratge i detecció d'incidents a contenidors i orquestradors

P26-A. Inicial: Monitoratge bàsic de contenidors i orquestradors.
P26-B. Avançat: Detecció d'amenaces en contenidors i orquestradors.
P26-C. Òptim: Detecció avançada d'amenaces en contenidors i orquestradors.

RESPOSTA I RECUPERACIÓ

P27. Resposta a incidents
Gestió de crisis i anàlisi tècnic forense.
Resposta integral a incidents amb anàlisi judicial i simulacres.

P28. Recuperació post-incident
P28-A. Inicial: Plans de recuperació bàsics.
P28-B. Avançat: Execució de mesures i proves parcials de continuïtat.
P28-C. Òptim: Simulacions completes i exercicis integrats.

TRANSVERSALS

P29. Capacitació i conscienciació
P29-A. Inicial: Campanyes bàsiques de sensibilització.
P29-B. Avançat: Simulacions de phishing i tallers especialitzats.
P29-C. Òptim: Programes continus i avaluacions regulars

P30. Governança i compliment
P30-A. Inicial: Quadres de comandament bàsics i informes.
P30-B. Avançat: Seguiment d'indicadors i plans de millora.
P30-C. Òptim: Fulls de ruta estratègics i auditories externes.

3.3.2 Lot 2. Serveis d'avaluació i validació del CROC

TRANSVERSALS

P31. Avaluació i millora contínua
P31-A. Diagnosi bàsica del nivell de seguretat.
P31-B. Avaluacions periòdiques i recomanacions.
P31-C. Exercicis de validació realista i plans de millora contínua.

3.3.3 Lot 3. Operació de Serveis i eines Avançades de Protecció (OSAP)

PROTECCIÓ (administració i operació de ciberseguretat)

P5. Protecció de llocs de treball i dispositius mòbils (PC, VDIs i mòbils).
Servei integral de govern i protecció dels dispositius finals: ordinadors d'escriptori, portàtils, estacions virtuals i dispositius mòbils.

P6. Protecció de servidors.
Servei integral de protecció dels servidors físics, màquines virtuals, contenidors i càrregues de treball desplegades en entorns híbrids.

P7. Protecció d'identitat i accessos.
Govern i protecció de les identitats digitals i dels mecanismes d'accés als sistemes municipals.

P8. Protecció d'informació i dades.
Govern i protecció de la informació municipal, tant en repòs com en trànsit i ús, assegurant que les dades sensibles estiguin correctament identificades, classificades i protegides.

P9. Protecció servei de correu i col·laboració.
Servei integral de protecció del correu electrònic i de les plataformes de col·laboració corporatives, incloent serveis de missatgeria, compartició de fitxers i entorns de treball col·lectius

P10. Protecció de xarxes i serveis de telecomunicacions.
Servei integral de protecció de la infraestructura de xarxa i de les telecomunicacions municipals, incloent els centres de dades, les oficines corporatives, els serveis exposats a internet i les connexions remotes.

P11. Protecció d'aplicacions i APIs.
Servei de protecció integral de les aplicacions municipals, incloent portals web, aplicacions mòbils, sistemes interns i interfícies de programació.

P12. Protecció de serveis al núvol.
Servei integral de protecció dels entorns municipals allotjats al núvol, incloent infraestructures, plataformes i aplicacions en escenaris públics, privats i híbrids.

P13. Protecció de tecnologies emergents i especialitzades (OT, IoT, IA i criptografia).
Servei de protecció avançada per a aquells àmbits tecnològics emergents i especialitzats que presenten riscos específics per a l'Ajuntament, incloent sistemes industrials, dispositius connectats, plataformes d'intel·ligència artificial i entorns criptogràfics.

P14. Protecció d'hipervisors i plataformes de virtualització.
Servei de protecció avançada per als entorns d'hipervisors i plataformes de virtualització que allotgen sistemes crítics de l'Ajuntament.

P15. Protecció de contenidors i orquestradors.
Servei de protecció avançada per als entorns de contenidors i sistemes d'orquestració (com Kubernetes, OpenShift o equivalents) utilitzats per a l'execució d'aplicacions i serveis municipals.

4. Descripció dels serveis a prestar per l'adjudicatari de Lot 1

A continuació es detallen els serveis que haurà de prestar l'adjudicatari en el marc dels contractes basats que se'n derivin del present Acord Marc per al desplegament, operació i evolució dels serveis del Centre de Riscos i Operacions de Ciberresiliència (CROC).

En primer lloc, es descriuen els **serveis generals obligatoris**, aplicables a qualsevol contracte basat derivat d'aquest acord, independentment del paquet funcional contractat. Aquests serveis constitueixen la base comuna que garanteix la coherència, la integració i la qualitat tècnica de totes les prestacions. L'adjudicatari haurà de proporcionar, com a mínim, la direcció i el seguiment dels projectes, la documentació tècnica i funcional, la formació necessària als equips municipals, la coordinació amb l'equip d'operacions de l'entitat municipal i el traspàs operatiu dels serveis desplegats. Igualment, haurà d'assegurar la correcta gestió del canvi, la supervisió continuada de les activitats i la traçabilitat de totes les actuacions realitzades.

Tot seguit, es descriuen els **paquets funcionals específics contractables de forma independent**, que constitueixen les unitats mínimes de prestació dels serveis. Cadascun d'ells cobreix funcionalitats concretes dins del cicle de la ciberseguretat, estructurades en els àmbits de prevenció, protecció, detecció, resposta i recuperació, així com en funcions transversals de governança i compliment, capacitació i conscienciació, i avaluació i millora contínua. En l'àmbit de la resposta, s'inclou de manera expressa l'execució de mesures de contenció inicial necessàries per limitar la propagació d'un incident, independentment de qui operi les plataformes tecnològiques del Lot 3 (OSAP), garantint així una actuació immediata i coordinada del CROC. Alguns d'aquests paquets es troben graduats en tres subnivells de maduresa —inicial, avançat i òptim— per tal d'adaptar la prestació a les necessitats i capacitats de cada entitat municipal.

Per la seva naturalesa modular i complementària, els diferents paquets es poden combinar lliurement en els contractes basats, i hauran de ser prestats de forma homogènia, garantint

així la continuïtat operativa i l'alineament amb l'estratègia global de seguretat definida per l'Ajuntament de Barcelona.

4.1 Serveis generals inclosos

De manera transversal a tots els contractes basats que es derivin del present Acord Marc, es defineix un conjunt de serveis generals que l'adjudicatari haurà de prestar obligatòriament com a part de l'execució de qualsevol paquet funcional relacionat amb els serveis del Centre de Riscos i Operacions de Ciberresiliència (CROC).

En aquest Lot 1 no s'inclouen serveis corresponents a l'Operació de Serveis i eines Avançades de Protecció (OSAP) ni serveis d'avaluació i millora contínua del CROC, els quals es regulen en els lots específics corresponents.

Aquests serveis generals constitueixen l'eix de suport operatiu, coordinació i control de qualitat dels projectes, i tenen com a objectiu garantir l'homogeneïtat, la traçabilitat i la integració de totes les actuacions que es desenvolupin en el marc d'aquest Acord Marc. Inclouen les activitats següents:

- **Direcció global del servei contractat**, amb la coordinació i el seguiment de totes les tasques previstes en cada contracte basat, assegurant la interlocució fluida amb la direcció de projecte de les entitats adherides i la coordinació entre tots els agents implicats, siguin tècnics, funcionals, operatius o proveïdors externs.

- **Planificació, supervisió i seguiment del projecte**, incloent l'elaboració i manteniment del pla de treball, amb cronograma, fites, dependències, identificació de riscos, mecanismes de control i informes de seguiment, garantint la comunicació regular amb els responsables municipals designats.

- **Gestió mitjançant eines corporatives**, amb l'ús obligatori de les eines de gestió de projectes determinades per les entitats adherides, mantenint tota la informació degudament registrada i actualitzada i assegurant la traçabilitat completa de les accions i decisions.

- **Presa i validació de requisits funcionals i tècnics**, amb la recollida, documentació i validació conjunta amb els responsables municipals, aportant estimacions d'esforç, impactes operatius i consideracions tècniques o econòmiques.

- **Generació i actualització de documentació tècnica**, que haurà d'incloure com a mínim:
    - Documentació funcional i tècnica de les solucions de seguretat desplegades.
    - Procediments d'operació i manuals d'usuari.
    - Documentació de canvis, incidències, configuracions aplicades i control de versions.
    - Registre formal de decisions, validacions i lliuraments.
- **Reporting i seguiment executiu**, amb l'emissió d'informes periòdics sobre l'estat del projecte, l'evolució de la implantació, l'estat de la plataforma, les mètriques de servei i d'ús, així com l'elaboració d'una memòria de tancament amb valoració i propostes de millora.
- **Gestió de la qualitat**, mitjançant el control de l'execució del servei per garantir el compliment dels requisits establerts, la realització de proves i revisions, l'execució d'auditories de qualitat, la proposta de millores i l'alineament amb les millors pràctiques del sector.
- **Gestió del tancament del projecte**, que haurà d'incloure el lliurament complet de la documentació, el traspàs formal del servei a l'equip d'operacions de l'entitat municipal, la valoració final del servei prestat i, si escau, l'aixecament de l'acta de conformitat.

Aquests serveis generals són de compliment obligatori i s'han d'incloure de manera inherent en l'execució de qualsevol paquet funcional contractat dins d'aquest Acord Marc, amb independència de la seva naturalesa, abast o finalitat.

Correlació i resposta multidomini

De manera transversal, l'adjudicatari haurà de garantir que els serveis del Centre de Riscos i Operacions de Ciberresiliència (CROC) disposin d'una capacitat nativa de correlació i resposta multidomini, entesa com la facultat d'analitzar, relacionar i actuar sobre esdeveniments i incidents que afectin simultàniament diversos tipus d'actius, plataformes i entorns tecnològics.

Aquesta capacitat és essencial per a la protecció de l'ecosistema municipal i s'ha d'aplicar de manera homogènia en tots els paquets funcionals contractables del Lot 1.

Concretament, l'adjudicatari haurà de garantir que:

1. **Cobertura d'àmbits múltiples:** El CROC haurà de poder integrar, analitzar i correlacionar esdeveniments provinents de múltiples àmbits tecnològics, entre els quals s'inclouen, de forma descriptiva però no limitativa:
    - gestió d'identitats i accessos,
    - llocs de treball i dispositius mòbils,
    - servidors i càrregues de treball,
    - xarxes corporatives i comunicacions,
    - aplicacions i serveis corporatius,
    - interfícies i integracions,
    - serveis i entorns al núvol,
    - informació i dades,
    - entorns especialitzats o tecnologies emergents,
    - infraestructures de virtualització i orquestració,
    - plataformes i serveis de seguretat,
    - sistemes de còpia, recuperació i continuïtat..
2. **Correlació avançada d'esdeveniments:** El CROC haurà de disposar de capacitats per correlacionar automàticament esdeveniments provinents de diversos dominis, evitant una anàlisi fragmentada i permetent:
    - identificar moviments laterals,
    - detectar seqüències d'atac avançades,
    - analitzar patrons de compromís,
    - reconèixer campanyes sostingudes,

- relacionar esdeveniments aparentment inconnexos.

Aquestes correlacions hauran de basar-se en mecanismes avançats d'enriquiment i contextualització..

3. **Resposta coordinada:** el CROC haurà de poder aplicar mesures de resposta de manera sincronitzada i coherent a través dels diferents dominis implicats en l'incident, com ara:
   - bloqueig o restricció d'identitats compromeses (identitat),
   - aïllament de dispositius o sistemes (endpoint o servidor),
   - contenció temporal del tràfic o serveis (comunicacions),
   - prevenció d'exfiltracions o moviments no autoritzats de dades,
   - aplicació coordinada de mesures de mitigació en diversos entorns.
4. **Visibilitat i traçabilitat completa:** cada incident multidomini ha de quedar registrat de forma integral, amb traçabilitat completa i accessible per als responsables municipals incloent com a mínim:
   - vector inicial,
   - evolució i propagació,
   - dominis afectats,
   - decisions operatives,
   - mesures de contenció i resposta,
   - restauració del servei i tancament.
5. **Automatització progressiva:** El servei haurà de garantir una evolució progressiva cap a un entorn més automatitzat, eficient i resilient, independentment del nivell de maduresa contractat per cada entitat. L'objectiu final és disposar d'un model operatiu capaç d'anticipar-se, contenir i remediar amenaces de manera cada vegada més àgil, coherent i eficient, amb el suport de tecnologies d'intel·ligència artificial que reforcin tant la ciberresiliència com la qualitat del servei. Això implica:
   - integrar l'IA per millorar la detecció, la correlació i la priorització d'amenaces,

- incorporar automatitzacions supervisades en els processos de detecció i resposta,
- reduir la dependència d'intervenció manual en accions repetitives o de primera línia i accelerar la resposta operativa,
- potenciar una resposta més ràpida i consistent davant incidents,
- assegurar que totes les automatitzacions i usos d'IA respectin les directrius municipals, la normativa vigent i la supervisió tècnica corresponent.

4.1.1 Requisits tècnics generals del servei

Els requisits tècnics generals definits a continuació són d'aplicació obligatòria a qualsevol paquet funcional contractat en el marc del present Acord Marc i constitueixen les condicions mínimes que ha de complir el servei proposat pel licitador.

Aquests requisits tenen com a objectiu assegurar la **coherència tècnica, l'escalabilitat, l'eficiència operativa, l'optimització contínua i el compliment normatiu** del servei dins de l'ecosistema digital municipal. Tots ells seran objecte de valoració i verificació tant en el procés de licitació com durant l'execució dels contractes basats.

Per cadascun dels requeriments, el licitador haurà d'indicar en una **matriu de conformitat** (veure Annex 2) el seu grau de compliment segons les opcions següents:

- "**Compleix**"
- "**No compleix**"
- "**No aplica**"

REQ-TCN-001. Servei industrialitzat: El servei haurà d'estar basat en un model industrialitzat, capaç d'incorporar de manera homogènia tots els casos d'ús definits a les diferents tecnologies presents a les entitats municipals. Així mateix, haurà de permetre la incorporació de nous casos d'ús identificats i desenvolupats en altres clients de l'adjudicatari, garantint que l'Ajuntament es beneficiï de la millora contínua i de l'efecte d'escala propi d'un servei compartit i madur.

REQ-TCN-002. Plataforma com a servei: El servei haurà de proporcionar, de manera gestionada i sota modalitat de servei, una plataforma de monitoratge, correlació i orquestració que inclogui capacitats de detecció, resposta automatitzada i repositori centralitzat de registres, amb escalabilitat horitzontal..

REQ-TCN-003. Incorporació progressiva d'intel·ligència artificial: El servei haurà d'integrar funcionalitats basades en intel·ligència artificial i aprenentatge automàtic per millorar la detecció, correlació i anàlisi d'incidents, i haurà d'incloure un pla d'evolució que permeti incrementar la maduresa d'aquestes capacitats durant la vigència del contracte.

REQ-TCN-004. Automatització de processos: El servei haurà d'incorporar automatismes per a la gestió de processos de seguretat, des de la resposta a incidents recurrents fins a l'execució de tasques de configuració o integració. Els fluxos d'automatització hauran d'estar documentats, ser revisables per les entitats contractants i poder evolucionar al llarg del contracte.

REQ-TCN-005. Optimització de recursos: El servei haurà de demostrar la capacitat de reduir de manera progressiva els recursos dedicats per mantenir un mateix perímetre de cobertura i uns mateixos nivells de seguretat, gràcies a la incorporació d'automatismes, processos d'IA i millores operatives.

REQ-TCN-006. Escalabilitat i modularitat: El servei haurà de ser escalable per cobrir increments en el nombre d'usuaris, dispositius i servidors, i modular per permetre afegir noves capacitats o integrar tecnologies emergents sense impactar l'operació existent.

REQ-TCN-007. Independència de la ubicació: La protecció i el monitoratge hauran de ser consistents tant per a usuaris i dispositius dins de la xarxa corporativa com per a aquells que treballin en mobilitat o des de fora de les dependències municipals.

REQ-TCN-008. Compliment normatiu: El servei haurà de garantir el compliment de la Directiva NIS2, l'Esquema Nacional de Seguretat i les guies tècniques del CCN, i assegurar que les dades i registres es mantinguin exclusivament en centres de dades ubicats dins la Unió Europea.

REQ-TCN-009. Disponibilitat i rendiment: El servei haurà de garantir una disponibilitat mínima del 99,9% sota acords de nivell de servei (SLA) i uns temps de resposta que preservin

l'experiència de l'usuari, establint límits màxims de latència en la inspecció del tràfic i en els processos de detecció i resposta d'acord als ANS definits al capítol 11.

REQ-TCN-010. Transparència i traçabilitat: El servei haurà de disposar d'una consola de gestió accessible per als responsables municipals, que permeti consultar en temps real l'estat del servei, els incidents registrats, les accions automatitzades executades i els resultats de les mesures d'optimització.

REQ-TCN-011. Evolució i millora contínua: El licitador haurà de presentar un pla d'evolució del servei, revisat anualment, que inclogui l'adopció de noves funcionalitats de detecció i resposta, l'optimització basada en IA i l'automatització de processos, garantint la millora contínua del servei durant tota la vigència del contracte.

REQ-TCN-012. Integració amb plataforma ITSM de l'entitat: El servei haurà d'integrar-se completament amb la plataforma ITSM (IT Service Management) de l'entitat contractant per tal de registrar, documentar i gestionar les alertes, els incidents de seguretat, les peticions de servei, les peticions de canvi, etc, sense que això suposi cap cost addicional per a l'entitat.

REQ-TCN-013. Documentació operativa: El servei haurà de documentar mitjançant protocols i procediments operatius de seguretat totes les activitats que es realitzin durant l'execució del contracte. Aquests protocols i procediments operatius de seguretat hauran de ser revisats periòdicament pel servei i aprovats per l'autoritat competent abans de la seva entrada en vigor. Tota la documentació operativa generada serà propietat de l'entitat contractant i un cop finalitzat el servei s'ha de garantir el lliurament de la documentació generada i validada, i la destrucció de la documentació en mans del proveïdor. El servei haurà de disposar de procediments d'actuació per a l'actualització de les eines, així com els processos de marxa enrere davant d'errors o incidències. El servei també haurà de disposar de procediments d'operació i escalat d'incidents a especialistes i fabricants. El servei haurà de mantenir actualitzada la documentació relativa a l'administració i operació de les diferents solucions objecte del servei.

REQ-TCN-014. Personal especialitzat: el servei haurà de disposar de personal especialitzat en cadascun dels diferents àmbits del servei, i el personal haurà de comptar amb certificacions reconegudes nacional o internacionalment que acreditin aquest coneixement especialitzat, per tal que l'organització prestadora de Serveis de Seguretat Gestionats (SSG) pugui evidenciar les seves capacitats operatives i la seva competència tècnica.

REQ-TCN-015. Procediment d'emergència: el servei haurà de disposar dels recursos necessaris i d'un procediment d'actuació en cas d'emergència en horari 24x7 que detalli els

mitjans de contacte (com a mínim de forma telefònica), les persones de contacte i el procediment d'actuació en cas que es detecti una vulnerabilitat crítica que requereixi atenció immediata.

REQ-TCN-016. Certificació de Conformitat amb l'ENS: tots els mitjans, sistemes i recursos empleats per l'organització prestadora de SSG per tal de prestar cadascun dels diferents àmbits del servei hauran de disposar de la Certificació de Conformitat amb l'Esquena Nacional de Seguretat (RD 311/2022, de 3 de maig) per a categoria MITJANA o superior, o bé evidenciar l'adient adopció d'un conjunt mínim de 36 mesures de seguretat (recollides a l'apartat 5.1 de la guia CCN-STIC-896) que resultin d'aplicació a cada cas concret i que inclouran el compromís formal d'obtenir la Conformitat amb l'ENS en un termini no superior a 12 mesos. En cas de disposar de serveis al núvol per prestar els SSG, el proveïdor de serveis al núvol on s'allotgi part de la infraestructura dels SSG de ciberseguretat haurà de disposar dels seus sistemes d'informació certificats en categoria ALTA de l'ENS.

REQ-TCN-017. Atracció, promoció i retenció del talent: el servei haurà de demostrar que implementa mesures per atraure, promocionar i retenir el talent, especialment el talent femení, fomentant la igualtat de gènere en el sector de la ciberseguretat.

REQ-TCN-018. Correlació multidomini d'esdeveniments de seguretat: el servei haurà de correlacionar esdeveniments de seguretat provinents de múltiples fonts (dispositius, identitats, trànsit de xarxa, etc) per detectar moviments sospitosos que no serien visibles en l'anàlisi d'un únic àmbit o domini. Els esdeveniments de seguretat s'hauran d'emmagatzemar i custodiar en format original tal com s'han rebut, i també en format analitzat ("parsejat"), amb una retenció en calent de com a mínim 6 mesos, una retenció en tebi de 6 mesos addicionals, i una retenció en fred de com a mínim 6 mesos addicionals. S'hauran de poder fer cerques avançades tant sobre els registres en format original, com en format "parsejat".

REQ-TCN-019. Retenció d'alertes i incidents de seguretat: les alertes i els incidents de seguretat detectats pel sistema de correlació d'esdeveniments de seguretat hauran d'emmagatzemar-se com a mínim en calent durant com a mínim 6 mesos, en tebi durant 6 mesos addicionals, i en fred durant com a mínim 6 mesos addicionals, juntament amb tots els esdeveniments de seguretat vinculats a la detecció, i totes les accions dutes a termes pel CROC en resposta a l'incident. En cas d'incidents de criticitat alta o superior l'entitat podrà sol·licitar estendre la retenció més enllà dels 18 mesos, sense cap cost addicional.

REQ-TCN-020. Integració indicadors de ciberintel·ligència amb el CROC municipal: el servei haurà de permetre que els indicadors obtinguts alimentin directament els mecanismes de detecció i resposta (SIEM, SOAR, EDR, XDR, etc.).

REQ-TCN-021. Elaboració propostes de comunicació tècnica a l'usuari relativa al servei: el servei haurà d'elaborar les propostes de comunicació tècnica a l'usuari final relativa al servei que hauran de ser validades amb, i gestionades a través de, l'entitat contractant abans de fer-se arribar a l'usuari.

REQ-TCN-022. Capacitat d'integració amb qualsevol dels productes i serveis del CPSTIC: el servei haurà de suportar la integració de qualsevol dels productes i serveis inclosos dins el Catàleg de Productes i Serveis STIC (CPSTIC) detallats a la guia CCN-STIC-105, i de qualsevol de les solucions de ciberseguretat que ofereix el CCN-CERT.

REQ-TCN-023. Monitorització general dels sistemes objecte del contracte: el servei haurà de monitorar la salut de tots els sistemes objecte del contracte sota la seva administració i operació.

REQ-TCN-024. Gestió de llicències, casos de suport i garanties esteses de fabricant dels sistemes objecte del contracte: el servei haurà de gestionar les llicències, casos de suport i les garanties esteses de fabricant de tots els sistemes objecte del contracte sota la seva administració i operació.

REQ-TCN-025. Servei d'implantació de paquet o subpaquet: el servei haurà d'oferir a l'entitat contractant la possibilitat d'implantar cadascun dels paquets de servei de forma individual, integrant les capacitats humanes, de processos i tecnològiques de l'entitat dins l'àmbit de servei del paquet en qüestió, en el termini màxim de 90 dies. En cas que durant el cicle de vida del servei l'entitat contractant substitueixi (p.e. canvi d'EDR) o incorpori una nova capacitat tecnològica (p.e. afegir SWG) dins l'àmbit de servei del mateix paquet o subpaquet, aquest canvi s'haurà de gestionar com una ampliació del paquet o subpaquet. El servei també haurà d'oferir a l'entitat contractant implantar subpaquets amb capacitats de servei addicionals.
Durant la fase d'implantació el servei haurà de migrar tots els logs de seguretat (recents i històrics) de les solucions SIEM i repositori de logs on-premise a la solució SIEMaaS al núvol. En cas que no es completi la migració de tots els logs dins la fase d'implantació, el servei serà responsable del llicenciament i dels serveis d'administració i operació de les plataformes SIEM i respositori de logs on-premise de l'entitat contractant mentre es completa la migració de tots els logs a la solució SIEMaaS.

Durant la fase d'implantació del servei dels paquets de detecció el servei ha de tenir la capacitat de correlacionar esdeveniments i alertes de seguretat detectades tant pel SIEMaaS al núvol com pel SIEM on-premise, en cas que l'entitat en disposi d'un.
El servei disposarà del termini màxim d'implantació del paquet o subpaquet per certificar-se en les capacitats tecnològiques objecte del servei, en cas que no en disposi de certificació vigent prèvia. En cas contrari, no podrà oferir els serveis mentre no disposi d'una certificació vigent amb personal propi o bé subcontractant un servei de suport especialitzat certificat.

REQ-TCN-026. Servei d'ampliació de paquet o subpaquet: el servei haurà d'oferir a l'entitat contractant la possibilitat d'ampliar les unitats incloses dins l'abast de cadascun dels paquets de servei de forma individual, integrant les capacitats humanes, de processos i tecnològiques de l'entitat dins l'àmbit de servei del paquet en qüestió prèviament implantat, en el termini màxim de 30 dies. En cas que durant el cicle de vida del servei l'entitat contractant substitueixi o incorpori una nova capacitat tecnològica dins l'àmbit de servei del mateix paquet, aquest canvi s'haurà de gestionar també com una ampliació del paquet.

REQ-TCN-027. Servei d'explotació de paquet o subpaquet: el servei haurà d'oferir a l'entitat contractant un servei recurrent mensual d'explotació de cadascun dels paquets de servei de forma individual, integrant les capacitats humanes, de processos i tecnològiques de l'entitat dins l'àmbit de servei del paquet en qüestió. En cas que durant el cicle de vida del servei l'entitat contractant substitueixi o incorpori una nova capacitat tecnològica dins l'àmbit de servei del mateix paquet que sigui inclosa dins la mateixa família de productes (p.e. EDR) del catàleg CPSTIC (guia CCN-STIC-105), el servei d'explotació haurà d'assumir sense cost addicional l'explotació d'aquesta nova capacitat tecnològica un cop ampliat el paquet. En cas que durant el cicle de vida del servei l'entitat contractant incorpori una nova capacitat tecnològica dins l'àmbit de servei del mateix paquet que no sigui inclosa dins la mateixa família de productes (p.e. SWG) del catàleg CPSTIC (guia CCN-STIC-105), el cost del servei recurrent mensual d'explotació serà incrementat en el número d'unitats contractades del mateix paquet o subpaquet.

REQ-TCN-028. Pertinença a organitzacions de resposta a incidents: L'empresa adjudicatària haurà d'acreditar que és membre actiu de FIRST (Forum of Incident Response and Security Teams), amb capacitat operativa demostrada en els seus grups de treball i canals de coordinació. Igualment, haurà d'acreditar que forma part de la Red Nacional de SOCs impulsada pel CCN-CERT amb categoria o nivell Oro, garantint així la coordinació operativa i l'accés a fluxos prioritaris de ciberintel·ligència, alertes tempranes i mesures de resposta en situacions d'emergència. La pertinença a aquestes organitzacions haurà de ser vigent durant tota l'execució del contracte i haurà de renovar-se o mantenir-se sense interrupcions.

4.1.2 Paquet P1-A – Gestió de vulnerabilitats i exposició (nivell inicial)

El paquet P1-A té per objectiu establir un servei bàsic i recurrent de **determinació i anàlisi de vulnerabilitats** en horari 8x5 sobre els actius informàtics de l'entitat municipal. Aquest nivell inicial ha de permetre identificar vulnerabilitats en equips, aplicacions i serveis exposats, valorar el seu risc i facilitar informació per a la seva mitigació. El servei ha de servir com a punt de partida per reduir la superfície d'exposició i establir un procés continu de millora de la seguretat.

El paràmetre quantificador d'aquest servei serà el número d'actius únics que hagin estat objecte d'una anàlisi de vulnerabilitats en els darrers 30 dies. Els actius podran ser dominis d'internet (FQDNs: Fully Qualified Domain Names) o adreces IP descobertes pel sistema de gestió de la superfície d'exposició, i també estacions de treball, servidors físics or virtuals, dispositius OT/IoT, càrregues de treball al núvol, nodes hipervisors o kubernetes, etc, d'acord al tipus d'actius inclosos en cadascun dels nivells d'aquest paquet de serveis. Un actiu (p.e. servidor) amb diferents interfícies o diferents adreces IP es considerarà un únic actiu.

El paquet P1 inclou els serveis d'administració i operació de la plataforma d'escaneig i gestió del risc de les vulnerabilitats i de l'exposició fent servir les capacitats tecnològiques de l'entitat contractant (a mode d'exemple: EDR, eina d'escaneig de vulnerabilitats, etc), així com de la resta de solucions necessàries per prestar el servei.

Funcionalitats que ha de suportar el servei

El servei de gestió de vulnerabilitats en el nivell inicial haurà de complir, com a mínim, les funcionalitats següents, que hauran de ser validades mitjançant la matriu de compliment especificada a l'Annex 2:

REQ-TCN-029. Escaneig periòdic: el servei haurà de realitzar escaneigs periòdics, com a mínim mensualment, de vulnerabilitats en llocs de treball, servidors bàsics, i aplicacions i serveis accessibles des d'internet.

REQ-TCN-030. Identificació de vulnerabilitats crítiques: el servei haurà de detectar i classificar les vulnerabilitats segons el seu nivell de risc, amb especial atenció a les crítiques i altes d'acord amb estàndards de referència.

REQ-TCN-031. Informes executius i tècnics: el servei haurà de generar, com a mínim mensualment, informes diferenciats per a responsables executius i equips tècnics, amb

inventari d'actius, vulnerabilitats trobades, nivell de risc i recomanacions de mitigació, i quadres de comandament amb la informació més rellevant del servei per afavorir la presa de decisions.

REQ-TCN-032. Classificació i priorització: les vulnerabilitats hauran de ser identificades (mitjançant CVE o EUVD), classificades i prioritzades d'acord amb la seva gravetat i impacte potencial en el servei, no només considerant el seu CVSS v3.1 o v4.0.

REQ-TCN-033. Integració amb la CMDB: els resultats dels escaneigs hauran de poder-se relacionar amb l'inventari d'actius de la CMDB corporativa. L'adjudicatària serà l'encarregada de fer la integració amb la CMDB de l'entitat contractant. En cas que l'entitat contractant no disposi de CMDB, el servei li podrà oferir una CMDB pròpia del servei que inclogui només els actius objecte del servei.

REQ-TCN-034. Integració amb la solució SIEMaaS i SOARaaS: el servei haurà d'integrar la solució d'escaneig i gestió del risc de les vulnerabilitats a les solucions SIEMaaS i SOARaaS incloses dins del servei per tal de poder correlacionar els esdeveniments de seguretat amb les vulnerabilitats presents a cadascun dels actius, i també poder invocar automàticament l'escaneig d'algun actiu puntualment, si escau.

REQ-TCN-035. Històric de resultats: la solució haurà de conservar un històric de resultats, com a mínim 13 mesos, que permeti analitzar l'evolució de l'exposició al llarg del temps.

REQ-TCN-036. Horari de servei: 8x5. Les persones que integrin el servei hauran de ser operatives de 9h a 17h de dilluns a divendres per tal d'atendre incidències, consultes, peticions de servei, etc. Els escaneigs periòdics de vulnerabilitats es podran planificar fora d'aquest horari, però el seu resultat serà analitzat i les vulnerabilitats detectades seran gestionades dins d'aquest horari.

REQ-TCN-037. Documentació operativa: el servei haurà de mantenir procedimentada l'operativa per a la identificació, anàlisi i report de vulnerabilitats, així com per realitzar el seguiment per validar la seva remediació. El servei també haurà de mantenir actualitzada la documentació relativa als processos d'operació i gestió de vulnerabilitats.

REQ-TCN-038. Suport i seguiment per validar la remediació: el servei haurà d'oferir suport a l'equip tècnic encarregat de l'administració del sistema afectat per la vulnerabilitat per resoldre els seus dubtes, i haurà de fer seguiment per validar la seva correcta remediació.

REQ-TCN-039. Registre de vulnerabilitats: el servei haurà de fer servir una eina específica (p.e. ANA del CCN-CERT), o bé qualsevol altra eina certificada continguda al catàleg CPSTIC

(guia CCN-STIC-105, que inclogui tant el registre i seguiment de les vulnerabilitats identificades, com el suport a la seva remediació.

REQ-TCN-040. Gestió de tiquets: el servei haurà de fer servir l'eina de gestió de tiquets (ITSM) de l'entitat per a la notificació, suport i seguiment de la remediació de les vulnerabilitats.

REQ-TCN-041. Procediment d'emergència: el servei haurà de disposar dels recursos necessaris i d'un procediment d'actuació en cas d'emergència en horari 24x7 que detalli els mitjans de contacte (com a mínim de forma telefònica), les persones de contacte i el procediment d'actuació en cas que es detecti una vulnerabilitat crítica que requereixi atenció immediata.

REQ-TCN-042. Personal especialitzat: el servei haurà de disposar de personal especialitzat en la gestió de vulnerabilitats que haurà de comptar amb experiència contrastada i amb certificacions reconegudes nacional o internacionalment.

REQ-TCN-043. No intrusivitat: les tècniques emprades hauran de minimitzar l'impacte sobre la disponibilitat i el rendiment dels sistemes analitzats, i s'executaran en la data i hora prèviament acordada i autoritzada per l'entitat.

REQ-TCN-044. Formació bàsica: l'adjudicatari haurà de proporcionar formació als equips municipals per a la correcta lectura i interpretació dels informes de vulnerabilitats.

Activitats a realitzar per part de l'adjudicatari

L'adjudicatari serà responsable, per a cada contracte basat que inclogui aquest paquet, de:

- Desplegar i configurar les eines necessàries per a l'escaneig de vulnerabilitats.
- Executar els escaneigs periòdics acordats amb l'entitat.
- Analitzar els resultats i validar les deteccions per reduir falsos positius.
- Elaborar i lliurar els informes executius i tècnics.
- Donar suport als equips municipals en la interpretació dels resultats i la priorització de les accions de mitigació.
- Documentar les activitats realitzades i mantenir l'històric de vulnerabilitats detectades.

Resultats esperats

- Servei operatiu de gestió de vulnerabilitats amb cobertura inicial sobre els actius prioritzats de l'entitat.
- Informes executius i tècnics amb classificació de riscos i recomanacions de mitigació.
- Integració bàsica de les dades amb la CMDB corporativa.
- Integració bàsica amb la solució SIEMaaS i SOARaaS corporativa.
- Històric inicial de vulnerabilitats establert com a línia de base.
- Equips municipals sensibilitzats i formats en la interpretació dels resultats.

4.1.3 Paquet P1-B – Gestió de vulnerabilitats i exposició (nivell avançat)

El paquet P1-B té per objectiu ampliar les capacitats establertes al nivell inicial (P1-A), incorporant noves funcionalitats que permetin gestionar de manera més completa i contextualitzada les vulnerabilitats dels actius municipals. Aquest nivell avançat amplia l'abast a entorns híbrids i complexos, reforça la visibilitat sobre l'exposició i millora la capacitat de priorització de les mesures de mitigació.

Aquest paquet **incorpora tots els requisits establerts en el P1-A** i els complementa amb els següents:

Funcionalitats que ha de suportar el servei

REQ-TCN-045. Cobertura d'entorns OT i IoT: el servei haurà d'incloure l'anàlisi de vulnerabilitats en sistemes de control industrial, sensors i dispositius connectats.

REQ-TCN-046. Anàlisi de serveis al núvol: el servei haurà de contemplar la detecció i gestió de vulnerabilitats en aplicacions i serveis allotjats a plataformes al núvol.

REQ-TCN-047. Gestió de la superfície d'atac externa: el servei haurà d'identificar i inventariar de manera contínua els actius exposats a internet i les vulnerabilitats associades.

REQ-TCN-048. Anàlisi de còpies de seguretat i hipervisors: el servei haurà de revisar la seguretat de sistemes de còpies de seguretat i plataformes de virtualització.

REQ-TCN-049. Vulnerabilitats en sistemes d'identitat i accessos: el servei haurà de detectar vulnerabilitats en directoris, plataformes d'autenticació i sistemes de gestió d'accés.

REQ-TCN-050. Anàlisi de contenidors i orquestradors: el servei haurà de detectar vulnerabilitats en entorns de contenidors i plataformes d'orquestració.

REQ-TCN-051. Priorització basada en riscos contextuals: el servei haurà de classificar i prioritzar les vulnerabilitats combinant criteris tècnics amb el context de l'actiu afectat (criticitat, impacte, explotabilitat).

REQ-TCN-052. Integració amb processos de gestió: els resultats hauran de poder alimentar de forma estructurada els processos de gestió de riscos i governança de seguretat de l'entitat.

REQ-TCN-053. Horari de servei: 12x5. Les persones que integren el servei han de ser operatives de 8h a 20h de dilluns a divendres per tal d'atendre incidències, consultes, peticions de servei, etc. Els escaneigs periòdics de vulnerabilitats es podran planificar fora d'aquest horari, però el seu resultat serà analitzat i les vulnerabilitats detectades seran gestionades dins d'aquest horari.

Activitats a realitzar per part de l'adjudicatari

- Ampliar l'abast dels escaneigs per incloure entorns OT, IoT i serveis al núvol.
- Executar revisions periòdiques de vulnerabilitats en còpies de seguretat, hipervisors i sistemes d'identitat.
- Incorporar processos d'anàlisi de contenidors i d'orquestradors.
- Elaborar informes avançats amb priorització contextualitzada i plans de mitigació.
- Integrar els resultats dins dels processos de gestió de riscos municipals.
- Donar suport als equips municipals en la definició i execució de plans de mitigació.

Resultats esperats

- **Cobertura ampliada** de vulnerabilitats en entorns híbrids (IT, OT, IoT i núvol).
- **Inventari validat** d'actius exposats a internet i estat de seguretat associat.

- **Informes executius i tècnics avançats**, amb priorització contextualitzada segons l'impacte i el risc.
- **Integració efectiva** dels resultats dins els processos de gestió de riscos i governança de seguretat de l'entitat.
- **Millora de la capacitat de resposta** i planificació de mesures correctives.

4.1.4 Paquet P1-C – Gestió de vulnerabilitats i exposició (nivell òptim)

El paquet P1-C té per objectiu assolir el màxim nivell de maduresa en la gestió de vulnerabilitats, establint un model de **gestió contínua de l'exposició a amenaces (CTEM)** que permeti identificar, validar i mitigar de manera iterativa i permanent les debilitats de l'entitat municipal. Aquest nivell òptim complementa i amplia les capacitats dels nivells anteriors, incorporant tecnologies avançades d'anàlisi, correlació i validació automatitzada dels controls de seguretat, així com la revisió de nous àmbits tecnològics de caràcter crític.

El subpaquet P1C inclou el llicenciament i els serveis d'administració i operació de les solucions BAS i CTEM, o equivalents.

Aquest paquet **incorpora tots els requisits establerts en els nivells P1-A i P1-B** i els amplia amb les funcionalitats següents:

REQ-TCN-054. Anàlisi d'instal·lacions físiques: revisió de vulnerabilitats en infraestructures físiques vinculades a la seguretat de la informació (sistemes de control d'accés, climatització, sensors IoT crítics).

REQ-TCN-055. Anàlisi de sistemes d'intel·ligència artificial: detecció de vulnerabilitats, riscos i biaixos en els sistemes d'IA utilitzats en processos municipals.

REQ-TCN-056. Revisió de claus i sistemes criptogràfics: validació de la seguretat en sistemes de gestió de claus, certificats digitals, signatura electrònica i mecanismes de xifratge.

REQ-TCN-057. Gestió contínua de l'exposició a amenaces (CTEM): el servei haurà d'implementar un cicle iteratiu de cinc fases —identificació, priorització, validació, mitigació i verificació— integrat amb la monitorització 24x7 del CROC i amb els processos de gestió de riscos corporatius.

REQ-TCN-058. Simulació d'infraccions i atacs (BAS): incorporació de tècniques de simulació d'atacs per validar l'eficàcia de les mesures de protecció i detecció implantades.

REQ-TCN-059. Models predictius: ús d'anàlisi avançada i dades d'intel·ligència global per anticipar vulnerabilitats emergents i tendències d'atac.

REQ-TCN-060. Integració total amb processos de gestió de riscos: alimentació automàtica dels resultats dins dels quadres de comandament i dels processos de governança corporatius.

REQ-TCN-061. Validació contínua de controls: el servei haurà de verificar de manera periòdica i automatitzada l'eficàcia dels controls de seguretat desplegats.

REQ-TCN-062. Horari de servei: 12x7. Les persones que integren el servei han de ser operatives de 8h a 20h de dilluns a diumenge per tal d'atendre incidències, consultes, peticions de servei, etc. Els escaneigs periòdics de vulnerabilitats es podran planificar fora d'aquest horari, però el seu resultat serà analitzat i les vulnerabilitats detectades seran gestionades dins d'aquest horari.

Activitats a realitzar per part de l'adjudicatari

- Implantar un programa complet de **CTEM**, amb cicles iteratius i calendaritzats per avaluar i mitigar l'exposició.
- **Validació contínua de controls de seguretat**, incorporant metodologies de Breach & Attack Simulation i d'avaluació iterativa.
- Correlacionar les dades de vulnerabilitats amb els incidents detectats pel CROC i les tendències d'amenaces globals.
- Revisar periòdicament la seguretat de **sistemes físics, d'IA i de criptografia**.
- Proporcionar informes **predictius, comparatius i de tendència** sobre l'evolució de l'exposició.
- Integrar els resultats dins dels **processos de gestió de riscos municipals** i quadres de comandament estratègics.
- Donar suport als responsables municipals en la definició de **fulls de ruta de millora contínua** basats en CTEM.

Resultats esperats

- **Cobertura integral i contínua** de vulnerabilitats en tots els àmbits (físic, digital, IA i criptogràfic).
- **CTEM implantat i operatiu**, amb cicles iteratius i informes de validació regulars.
- **Simulacions d'atac periòdiques**, que permetin comprovar de manera pràctica la robustesa de les defenses.
- **Capacitat predictiva** davant vulnerabilitats emergents i tendències d'atac.
- **Integració total** amb la governança de riscos de l'Ajuntament i els seus quadres de comandament.
- **Evolució proactiva i sostenible**, orientada a un model de seguretat resilient i adaptatiu.
- **Validació iterativa** i contínua dels controls de seguretat, assegurant la seva eficàcia davant noves tècniques d'atac.

4.1.5 Paquet P2-A – Auditories i proves de seguretat (nivell inicial)

El paquet P2-A té per objectiu establir les bases d'un programa d'**auditories tècniques i proves d'intrusió** orientat a identificar vulnerabilitats en els sistemes municipals i validar la robustesa mínima dels controls desplegats. Aquest nivell inicial es concep com una primera línia de diagnosi, centrada en **infraestructures IT bàsiques, serveis crítics exposats i entorns OT/IoT essencials**, amb l'objectiu de proporcionar a les entitats una visió realista del seu nivell de resistència davant ciberatacs.

Aquest paquet no només té valor com a exercici tècnic, sinó també com a eina de conscienciació i de priorització estratègica, ja que permet establir una línia de base de seguretat sobre la qual evolucionar cap als nivells avançats i òptims.

El paràmetre quantificador d'aquest servei seran paquets de 40h (5 jornades) d'auditories tècniques i proves d'intrusió realitzades en els darrers 30 dies. Es consideraran auditories tècniques i proves d'intrusió de nivell de complexitat BAIXA (40h), MITJANA (80h), o bé ALTA (160h).

El paquet P2 inclou els serveis d'administració i operació de la plataforma BAS (Breach and Attack Simulation), així com els serveis d'administració i operació i el llicenciament de la resta de solucions necessàries per prestar el servei.

Funcionalitats que ha de suportar el servei

REQ-TCN-063. Proves d'intrusió de caixa negra en entorns IT: el servei haurà de simular atacs externs sense coneixement previ dels sistemes, reproduint el punt de vista d'un atacant real.

REQ-TCN-064. Proves d'intrusió de caixa grisa en entorns IT: el servei haurà d'incloure proves amb coneixement parcial, com les que podria dur a terme un usuari amb privilegis limitats.

REQ-TCN-065. Proves d'intrusió bàsiques en entorns OT i IoT: les proves hauran de validar l'existència de vulnerabilitats en sistemes industrials i dispositius connectats, aplicant metodologies no intrusives que assegurin la continuïtat del servei.

REQ-TCN-066. Auditoria tècnica d'infraestructures bàsiques: revisió de configuracions de tallafocs, xarxes Wi-Fi, plataformes antivirus, serveis essencials i dispositius mòbils.

REQ-TCN-067. Informe tècnic i executiu: el servei haurà de generar, com a mínim mensualment, informes diferenciats per a perfils tècnics i de direcció, incloent vulnerabilitats trobades, riscos associats i recomanacions prioritzades, i quadres de comandament amb la informació més rellevant del servei per afavorir la presa de decisions.

REQ-TCN-068. Traçabilitat i referenciació: cada vulnerabilitat haurà d'estar vinculada a l'actiu corresponent i referenciada en catàlegs internacionals (CVE, CWE, OWASP Top 10 quan correspongui). Les vulnerabilitats hauran de ser identificades (mitjançant CVE o EUVD), classificades i prioritzades d'acord amb la seva gravetat i impacte potencial en el servei, no només considerant el seu CVSS v3.1 o v4.0.

REQ-TCN-069. Respecte a la continuïtat de servei: les proves hauran de ser planificades i executades de manera controlada, evitant la interrupció dels serveis municipals i s'executaran en la data i hora prèviament acordada i autoritzada per l'entitat.

REQ-TCN-070. Horari de servei: 8x5. Les persones que integrin el servei hauran de ser operatives de 9h a 17h de dilluns a divendres per tal d'atendre incidències, consultes, peticions de servei, etc. Les auditories tècniques es planificaran preferentment dins d'aquest horari. Excepcionalment es podran planificar fora d'aquest horari, però el seu resultat serà analitzat i les vulnerabilitats detectades seran gestionades dins d'aquest horari.

REQ-TCN-071. Documentació operativa: el servei haurà de mantenir procedimentada l'operativa per a l'execució de les autories tècniques, així com per realitzar el seguiment per validar la seva remediació.

REQ-TCN-072. Pla d'acció de mitigació de vulnerabilitats detectades: el servei haurà de facilitar un pla d'acció per mitigar les vulnerabilitats detectades, oferir suport a l'equip tècnic encarregat de l'administració del sistema afectat per la vulnerabilitat per resoldre els seus dubtes, i assegurar-se que siguin incloses al cicle continu de gestió de vulnerabilitats.

REQ-TCN-073. Registre de vulnerabilitats: el servei haurà de fer servir una eina específica (p.e. ANA del CCN-CERT), o bé qualsevol altra eina certificada continguda al catàleg CPSTIC (guia CCN-STIC-105, que inclogui tant el registre i seguiment de les vulnerabilitats identificades, com el suport a la seva remediació.

REQ-TCN-074. Gestió de tiquets: el servei haurà de fer servir l'eina de gestió de tiquets (ITSM) de l'entitat per a la notificació, suport i seguiment de la remediació de les vulnerabilitats.

REQ-TCN-075. Procediment d'emergència: el servei haurà de disposar dels recursos necessaris i d'un procediment d'actuació en cas d'emergència en horari 24x7 que detalli els mitjans de contacte, les persones de contacte i el procediment d'actuació en cas que es detecti una vulnerabilitat crítica que requereixi atenció immediata.

REQ-TCN-076. Personal especialitzat: el servei haurà de disposar de personal especialitzat en la gestió i execució d'autories tècniques i proves d'intrusió que haurà de comptar amb experiència contrastada i amb certificacions reconegudes nacional o internacionalment (p.e. CEH: Certified Ethical Hacker).

REQ-TCN-077. Tècniques i metodologies: el servei emprarà tècniques i metodologies avalades internacionalment com OSSTMM (Open Source Security Testing Methodology Manual), OWASP (Open Web Application Security Project), PTES (Penetration Testing Execution Standard), ISSAF (Information Systems Security Assessment Framework), OWISAM (Open Wireless Security Assessment Methodology), etc, en funció de l'abast o actius a tractar.

Activitats a realitzar per part de l'adjudicatari

- Definir conjuntament amb l'entitat municipal l'abast i l'estratègia de les proves, establint els sistemes prioritaris a avaluar.
- Executar proves d'intrusió bàsiques en entorns IT i OT/IoT, amb documentació clara de metodologies i resultats.

- Realitzar auditories de configuració en els principals dispositius de seguretat i serveis essencials.
- Analitzar i validar les vulnerabilitats detectades, diferenciant falsos positius de vulnerabilitats explotables.
- Generar informes executius i tècnics, adaptats als diferents nivells de responsabilitat dins de l'Ajuntament.
- Presentar els resultats als responsables municipals i facilitar sessions de conscienciació sobre els riscos identificats.

Resultats esperats

- **Identificació inicial de vulnerabilitats** en infraestructures IT, OT i IoT bàsiques.
- **Informes tècnics i executius diferenciats**, amb evidències documentades i recomanacions accionables.
- **Establiment d'una línia de base de seguretat** que permeti mesurar l'evolució en futurs exercicis.
- **Millora immediata de la consciència de risc**, tant per part dels equips tècnics com de la direcció.
- **Preparació per a la progressió** cap a auditories més avançades i simulacions de ciberatacs complexes (nivells P2-B i P2-C).

4.1.6 Paquet P2-B – Auditories i proves de seguretat (nivell avançat)

El paquet P2-B té per objectiu portar les capacitats bàsiques establertes al nivell inicial (P2-A) cap a un entorn més madur i profund, ampliant l'abast a **aplicacions, serveis al núvol, entorns OT/IoT i infraestructures virtualitzades**. Aquest nivell avançat proporciona una visió real i detallada del grau de resistència de les entitats municipals davant vectors d'atac sofisticats, i introdueix pràctiques alineades amb els estàndards més exigents de la indústria (CREST, OSSTMM, OWASP, NIST SP 800-115).

Aquest paquet **incorpora tots els requisits definits en el P2-A** i els amplia amb les funcionalitats següents:

Funcionalitats que ha de suportar el servei

REQ-TCN-078. Proves d'intrusió de caixa blanca en entorns IT: execució de proves exhaustives amb coneixement complet de l'entorn per identificar debilitats de disseny, configuració i arquitectura que no serien detectables en proves externes.

REQ-TCN-079. Proves avançades en entorns OT i IoT: execució de proves controlades, de caixa grisa o blanca, que permetin validar la seguretat de sistemes industrials i dispositius connectats, assegurant la no interrupció de processos crítics.

REQ-TCN-080. Auditoria de seguretat de codi: aplicació combinada d'anàlisi estàtic (SAST), dinàmic (DAST) i dels components de tercers presents (SCA), així com revisió manual per identificar vulnerabilitats lògiques i de seguretat en el codi d'aplicacions municipals, així com integració al canal CI/CD de DevSecOps.

REQ-TCN-081. Auditoria tècnica d'aplicacions i serveis: revisió integral d'aplicacions web, aplicacions mòbils i serveis d'ús intern o públic, amb especial atenció a la detecció de vulnerabilitats OWASP Top 10, controls d'accés insegurs i errors de configuració.

REQ-TCN-082. Auditoria de contenidors i orquestradors: anàlisi de seguretat en plataformes basades en contenidors i sistemes d'orquestració, incloent revisió de les imatges, permisos i seguretat dels desplegaments.

REQ-TCN-083. Auditoria de serveis al núvol: revisió de configuracions i controls de seguretat en entorns multicloud (públics, privats i híbrids), incloent gestió de permisos, seguretat d'APIs i protecció de dades sensibles.

REQ-TCN-084. Auditoria de xarxes de comunicacions: revisió exhaustiva dels segments de xarxa, configuracions de control d'accés, protocols insegurs i dispositius perimetrals, assegurant la resiliència de les comunicacions.

REQ-TCN-085. Informes executius i tècnics avançats: lliurament d'informes diferenciats, amb detall tècnic de cada vulnerabilitat i el seu vector d'explotació, així com una visió executiva orientada a la presa de decisions estratègiques i priorització de recursos.

REQ-TCN-086. Horari de servei: 12x5. Les persones que integrin el servei hauran de ser operatives de 8h a 20h de dilluns a divendres per tal d'atendre incidències, consultes, peticions de servei, etc. Les auditories tècniques es planificaran preferentment dins d'aquest horari.

Excepcionalment es podran planificar fora d'aquest horari, però el seu resultat serà analitzat i les vulnerabilitats detectades seran gestionades dins d'aquest horari.

Activitats a realitzar per part de l'adjudicatari

- **Planificació estratègica:** definir amb els responsables municipals l'abast de cada projecte, establint prioritats en funció del risc per a la continuïtat dels serveis públics i la protecció de la ciutadania.
- **Execució de proves especialitzades:** dur a terme proves d'intrusió avançades, incloent simulacions d'atacs interns i externs, amb metodologies reconegudes internacionalment i adaptades a entorns OT/IoT.
- **Revisió de codi i aplicacions:** analitzar aplicacions municipals i de tercers utilitzats, detectant vulnerabilitats en processos de desenvolupament i desplegament.
- **Auditoria d'infraestructura híbrida:** validar la seguretat en contenidors, serveis al núvol i xarxes de comunicació, integrant els resultats dins de la visió global de seguretat.
- **Elaboració d'informes diferenciats:** lliurar informes tècnics per a equips d'operació i informes executius per a responsables de decisió, amb recomanacions clares i prioritzades.
- **Acompanyament en la mitigació:** donar suport als equips municipals en la definició i aplicació de mesures correctives, així com en l'avaluació de la seva eficàcia.

Resultats esperats

- **Cobertura ampliada** de la seguretat a aplicacions, serveis al núvol, contenidors i entorns OT/IoT.
- **Identificació de vulnerabilitats complexes** no detectables en proves inicials.
- **Informes tècnics i executius avançats**, que permetin prendre decisions basades en risc i impacte.
- **Millora substancial de la postura de seguretat**, mitjançant la integració dels resultats amb processos de gestió de riscos i governança.

- **Preparació reforçada davant actors amenaçadors sofisticats**, anticipant-se a vectors d'atac emergents i tècniques utilitzades en la ciberdelinqüència i l'APT (Advanced Persistent Threats).

4.1.7 Paquet P2-C – Auditories i proves de seguretat (nivell òptim)

El paquet P2-C té per objectiu assolir el **màxim nivell de maduresa en auditories i proves de seguretat**, establint un model de validació contínua i realista de la postura de seguretat de l'Ajuntament i les seves entitats dependents. Aquest nivell incorpora auditories especialitzades en àmbits crítics com la intel·ligència artificial i la criptografia.

Aquest paquet **incorpora tots els requisits establerts en P2-A i P2-B** i els amplia amb les següents funcionalitats:

Funcionalitats que ha de suportar el servei

REQ-TCN-087. Auditoria de sistemes d'intel·ligència artificial: el servei haurà de validar la robustesa i seguretat dels sistemes d'IA utilitzats per l'Ajuntament, identificant riscos d'explotació, biaixos i vulnerabilitats associades a models d'aprenentatge automàtic.

REQ-TCN-088. Auditoria de sistemes criptogràfics i de gestió de claus: el servei haurà de revisar de manera exhaustiva els sistemes de xifratge, la gestió del cicle de vida de claus i certificats i la preparació per a l'era post-quàntica.

REQ-TCN-089. Informes estratègics i fulls de ruta: el servei haurà de proporcionar informes executius que no només recullin vulnerabilitats, sinó que defineixin un full de ruta estratègic de millora contínua, alineat amb les directives NIS2 i les guies del CCN.

REQ-TCN-090. Horari de servei: 12x7. Les persones que integrin el servei hauran de ser operatives de 8h a 20h de dilluns a diumenge per tal d'atendre incidències, consultes, peticions de servei, etc. Les auditories tècniques es planificaran preferentment dins d'aquest horari. Excepcionalment es podran planificar fora d'aquest horari, però el seu resultat serà analitzat i les vulnerabilitats detectades seran gestionades dins d'aquest horari.

Activitats a realitzar per part de l'adjudicatari

- **Execució d'auditories especialitzades en IA i criptografia**, garantint la cobertura dels nous àmbits tecnològics que impacten en la seguretat municipal.
- Executar **simulacions periòdiques d'atacs** (reals i controlats) per validar mesures de protecció i detecció.
- **Integració dels resultats** dins dels processos de gestió de riscos i governança, alimentant directament els quadres de comandament del CROC.
- **Elaboració d'informes tècnics i estratègics**, incloent recomanacions accionables i un full de ruta per a la millora contínua de la seguretat.

Resultats esperats

- **Capacitat validada de defensa realista** davant actors amenaçadors avançats, mitjançant exercicis de Red Team i Purple Team.
- **Cobertura integral** d'auditories en entorns innovadors i crítics (IA, criptografia, cadena de subministrament).
- **Integració total** dels resultats dins dels processos de governança i risc, amb traçabilitat completa.
- **Full de ruta estratègic** que permet orientar la millora contínua i garantir l'alineament amb la NIS2, l'ENS i les directrius del CCN.
- **Cultura organitzativa reforçada**, amb capacitat de resposta transversal i coordinada davant incidents de màxima gravetat.

4.1.8 Paquet P3-A – Serveis d'intel·ligència d'amenaces (nivell inicial)

El paquet P3-A té per objectiu establir una primera capa de **ciberintel·ligència operativa** que permeti a l'Ajuntament i a les entitats dependents disposar d'informació estructurada i accionable sobre les amenaces més rellevants. Aquest nivell inicial s'orienta a **vigilar, detectar i alertar** sobre indicadors d'activitat maliciosa i riscos emergents (Deep i Dark Web), amb un abast centrat en la protecció de la reputació institucional, els empleats i els serveis digitals més exposats.

Aquesta intel·ligència bàsica constitueix la base per evolucionar cap a un model més madur de detecció i anàlisi en temps real (nivell avançat i òptim).

El paràmetre quantificador d'aquest servei serà el número d'actius o paraules clau (en grups de 50 unitats) que hagin estat objecte dels serveis de ciberintel·ligència en els darrers 30 dies. Les paraules clau podran ser marques, dominis, identitats digitals de personal VIP i perfils institucionals monitorats, perfils monitorats a xarxes socials i altres espais digitals per a detectar suplantacions, CPEs (Common Platform Enumeration) de les tecnologies monitorades, aplicacions mòbils monitorades, i proveïdors inclosos dins l'anàlisi de riscos a la cadena de subministrament. Una part dels actius inclosos serà fixa durant la durada del contracte, mentre que una altra part podrà variar en funció de l'evolució tecnològica o dels canvis de l'entorn digital de l'entitat. El servei inclourà un número de remediacions anuals igual al 20% dels actius objecte dels serveis de ciberintel·ligència.

El paquet P3 inclou el llicenciament i els serveis d'administració i operació de la plataforma de serveis d'intel·ligència d'amenaces i de vigilància digital, així com de la resta de solucions necessàries per prestar el servei.

Funcionalitats que ha de suportar el servei

REQ-TCN-091. Vigilància d'amenaces genèriques: el servei haurà de recopilar informació sobre campanyes de malware, phishing i altres atacs de gran difusió que puguin afectar entitats públiques.

REQ-TCN-092. Alerta primerenca de riscos tecnològics: el servei haurà de proporcionar avisos anticipats sobre vulnerabilitats crítiques, incidents globals i noves tècniques d'explotació.

REQ-TCN-093. Vigilància de reputació, marca i logo: el servei haurà de monitorar dominis, perfils en xarxes socials i altres espais digitals per detectar suplantacions de la identitat corporativa o usos indeguts de la marca i del logo.

REQ-TCN-094. Monitoratge de compromís d'identitats: el servei haurà d'identificar si credencials o dades personals de treballadors municipals apareixen en filtracions públiques o espais de distribució il·lícita.

REQ-TCN-095. Prevenció de suplantació de VIPs i perfils institucionals: el servei haurà de detectar intents de suplantació d'alts càrrecs municipals i comptes institucionals oficials, tant a xarxes socials com a altres espais digitals. El servei proporcionarà un informe específic mensual.

REQ-TCN-096. Recuperació d'informació de fonts obertes (OSINT), xarxes socials (SOCMINT) i fonts humanes (HUMINT i vHUMINT): el servei haurà de recopilar i filtrar informació rellevant de fonts obertes (Internet, Deep Web i Dark Web), de xarxes socials (SOCMINT) i de fonts humanes (HUMINT i vHUMINT) per anticipar riscos emergents.

REQ-TCN-097. Informes periòdics d'intel·ligència: el servei haurà de generar informes regulars, com a mínim mensualment, i quadres de comandament amb la informació més rellevant del servei per afavorir la presa de decisions, que descriguin les principals amenaces detectades i les recomanacions bàsiques per mitigar-les.

REQ-TCN-098. Horari de servei: 8x5. Les persones que integrin el servei hauran de ser operatives de 9h a 17h de dilluns a divendres per tal d'atendre incidències, consultes, peticions de servei, etc.

REQ-TCN-099. Documentació operativa: el servei haurà de mantenir procedimentada l'operativa per a la notificació, escalat i seguiment d'amenaces i abusos identificats, així com els processos de vigilància digital.

REQ-TCN-100. Gestió de baixes de recursos fraudulents: el servei haurà de gestionar la baixa dels recursos fraudulents; documentar els procediments de comunicació amb tercers per a la retirada i/o la sol·licitud de baixa del contingut maliciós o suplantació d'identitat, de perfils a xarxes socials, d'adreces IP, de dominis o qualsevol altre tipus de contingut fraudulent identificat pel servei que afecti a l'entitat; confirmar i comunicar la baixa a l'entitat un cop completada; i finalment monitorar durant com a mínim un mes el recurs fraudulent per detectar si torna a activar-se.

REQ-TCN-101. Gestió de tiquets: el servei haurà de fer servir l'eina de gestió de tiquets (ITSM) de l'entitat per a la notificació, suport i seguiment de les alertes de seguretat identificades pel servei d'intel·ligència d'amenaces.

REQ-TCN-102. Procediment d'emergència: el servei haurà de disposar dels recursos necessaris i d'un procediment d'actuació en cas d'emergència en horari 24x7 que detalli els mitjans de contacte, les persones de contacte i el procediment d'actuació en cas que es detecti una amenaça crítica que requereixi atenció immediata.

REQ-TCN-103. Personal especialitzat: el servei haurà de disposar de personal especialitzat en la vigilància digital i en la intel·ligència d'amenaces que haurà de comptar amb experiència contrastada i amb certificacions reconegudes nacional o internacionalment.

Activitats a realitzar per part de l'adjudicatari

- Configurar i mantenir mecanismes de vigilància bàsica d'amenaces i riscos reputacionals.
- Analitzar les dades recollides i validar-ne la rellevància per a l'entorn municipal.
- Emetre avisos periòdics i alertes puntuals als responsables municipals quan es detectin riscos potencialment crítics.
- Elaborar informes executius i tècnics amb recomanacions d'acció.
- Donar suport als equips municipals en la interpretació de la informació i en la definició de mesures preventives.

Resultats esperats

- **Disponibilitat d'informació accionable** sobre les principals amenaces que poden afectar el consistori i les seves entitats.
- **Alertes primerenques** sobre vulnerabilitats i riscos tecnològics emergents.
- **Protecció de la reputació i identitat digital** de l'Ajuntament i dels seus representants.
- **Major consciència de risc** per part dels responsables municipals, facilitant la presa de decisions preventives.
- **Base sòlida** per evolucionar cap a serveis de ciberintel·ligència més avançats i predictius (P3-B i P3-C).

4.1.9 Paquet P3-B – Serveis d'intel·ligència d'amenaces (nivell avançat)

El paquet P3-B té per objectiu consolidar i ampliar les capacitats establertes en el nivell inicial (P3-A), proporcionant un **servei de ciberintel·ligència més estructurat i especialitzat**, capaç de gestionar fonts pròpies i externes, detectar fraus digitals i analitzar riscos específics associats a canals mòbils i serveis en línia. Aquest nivell avançat permet a l'Ajuntament disposar d'una visió més completa de l'ecosistema d'amenaces i anticipar-se a vectors d'atac amb un grau més gran de precisió.

Aquest paquet **incorpora tots els requisits establerts en el P3-A** i els amplia amb els següents:

Funcionalitats que ha de suportar el servei

REQ-TCN-104. Plataforma pròpia d'intel·ligència: el servei haurà d'alimentar la plataforma centralitzada de ciberintel·ligència (per exemple, basada en MISP o equivalent) de l'entitat contractant per integrar, correlacionar i gestionar els indicadors de compromís (IoC) i d'atac (IoA).

REQ-TCN-105. Vigilància de frau online: el servei haurà de detectar i notificar intents de frau en línia que utilitzin la marca de l'Ajuntament o els seus serveis com a vector d'engany.

REQ-TCN-106. Detecció de riscos en canals mòbils: el servei haurà d'identificar aplicacions falses, perfils fraudulents i amenaces que afectin dispositius mòbils utilitzats pels treballadors municipals o la ciutadania.

REQ-TCN-107. Anàlisi avançada de riscos reputacionals: el servei haurà de monitorar i avaluar, amb tècniques d'anàlisi avançada, campanyes de desinformació o dany reputacional a l'Ajuntament.

REQ-TCN-108. Automatització de correlació: la plataforma haurà de poder correlacionar dades de múltiples fonts (OSINT, SOCMINT, HUMINT, ciberintel·ligència comercial, indicadors propis del CROC) per generar alertes més precises i reduir falsos positius.

REQ-TCN-109. Informes d'intel·ligència avançats: a més dels informes bàsics del nivell inicial, el servei haurà de proporcionar dossiers més detallats sobre actors d'amenaça, tècniques utilitzades i tendències de cibercriminalitat rellevants per al sector públic.

Activitats a realitzar per part de l'adjudicatari

- Implantar i gestionar la plataforma d'intel·ligència centralitzada.
- Integrar fonts internes i externes d'informació, validant la qualitat i la rellevància de les dades.
- Detectar i notificar casos de frau online i riscos en canals mòbils.
- Emetre informes avançats sobre actors d'amenaça, incidents rellevants i recomanacions preventives.

- Coordinar-se amb el CROC municipal per garantir que la intel·ligència alimenti els processos de detecció i resposta.
- Proporcionar sessions de briefing periòdiques per actualitzar responsables municipals sobre les principals tendències detectades.

Resultats esperats

- **Consolidació d'una plataforma pròpia d'intel·ligència** que centralitzi i correlacioni informació rellevant.
- **Detecció activa de frau online** i riscos en canals mòbils vinculats a la marca de l'Ajuntament.
- **Integració de la intel·ligència amb el CROC**, convertint-la en acció operativa dins dels processos de detecció i resposta.
- **Informes avançats i dossiers estratègics**, orientats a la presa de decisions informades.
- **Capacitat d'anticipació reforçada**, que permeti reduir el temps entre la detecció d'una amenaça i l'adopció de mesures preventives.

4.1.10 Paquet P3-C – Serveis d'intel·ligència d'amenaces (nivell òptim)

El paquet P3-C té per objectiu assolir la màxima maduresa en **ciberintel·ligència estratègica i operativa**, situant l'Ajuntament en un model proactiu i predictiu. Aquest nivell no només ofereix informació per a la detecció i resposta, sinó que integra la intel·ligència dins de la **planificació estratègica de seguretat**, alineant-se amb les directives NIS2, les guies del CCN i les millors pràctiques de la comunitat internacional d'intel·ligència.

Aquest paquet **incorpora tots els requisits establerts en P3-A i P3-B** i els amplia amb les següents funcionalitats:

Funcionalitats que ha de suportar el servei

REQ-TCN-110. Intel·ligència multientorn (IT, OT i IoT): el servei haurà de proporcionar intel·ligència específica sobre amenaces que afectin tant sistemes informàtics tradicionals com entorns industrials i dispositius connectats.

REQ-TCN-111. Anàlisi de riscos a la cadena de subministrament: el servei haurà d'identificar i monitorar riscos derivats de proveïdors, terceres parts i col·laboradors externs, establint mecanismes d'alerta primerenca.

REQ-TCN-112. Integració de ciberintel·ligència estratègica: el servei haurà de proporcionar informació sobre tendències geopolítiques, campanyes d'actors estatals i riscos transnacionals que puguin impactar en els serveis municipals.

REQ-TCN-113. Correlació avançada amb intel·ligència global: el servei haurà d'integrar dades procedents de comunitats internacionals, CERTs, agències de seguretat i altres administracions públiques, garantint la seva aplicabilitat a l'entorn municipal.

REQ-TCN-114. Intel·ligència de frau financer i ciberdelinqüència organitzada: el servei haurà de detectar campanyes avançades de frau en línia, extorsió digital i activitats il·lícites relacionades amb actors de crim organitzat.

REQ-TCN-115. Integració amb models de predicció: el servei haurà de disposar de capacitats d'anàlisi avançada (IA/ML) que permetin predir l'aparició de noves amenaces o tendències d'explotació.

REQ-TCN-116. Informes estratègics per a la direcció municipal: els resultats hauran d'incloure dossiers estratègics que ajudin els òrgans de govern municipal a prendre decisions informades sobre inversions i prioritats de seguretat.

REQ-TCN-117. Exercicis d'intel·ligència col·laborativa: el servei haurà de participar en simulacions i exercicis conjuntament amb altres administracions i organismes, compartint informació i enriquint la capacitat de resposta.

Activitats a realitzar per part de l'adjudicatari

- Monitorar i analitzar fonts globals d'intel·ligència, adaptant-les al context municipal.
- Detectar riscos i vulnerabilitats en la cadena de subministrament digital i tecnològica.
- Generar informes estratègics i operatius sobre actors amenaçadors i tendències emergents.

- Correlacionar dades d'intel·ligència amb els incidents registrats al CROC municipal.
- Participar en comunitats d'intercanvi d'intel·ligència i en exercicis de ciberseguretat col·laboratius.
- Assessorar la direcció municipal en matèria de riscos i en la definició de polítiques de seguretat a llarg termini.

Resultats esperats

- **Visió integral** de les amenaces que impacten entorns IT, OT i IoT.
- **Capacitat predictiva** per anticipar riscos en la cadena de subministrament i campanyes d'atac globals.
- **Integració de la intel·ligència amb la governança estratègica**, alineant seguretat i presa de decisions de la direcció municipal.
- **Cooperació internacional i interadministrativa**, que reforça la posició de l'Ajuntament dins de l'ecosistema de ciberseguretat.
- **Maduresa màxima del CROC municipal**, amb capacitat d'adaptar-se a un panorama d'amenaces en constant evolució.

4.1.11 Paquet P4-A – Inventari i classificació d'actius (nivell inicial)

El paquet P4-A té per objectiu establir un servei bàsic d'**identificació i registre d'actius** que proporcioni a l'Ajuntament i a les entitats dependents una visibilitat mínima sobre els recursos que s'han de protegir. Aquest nivell inicial se centra en l'exploració manual i l'ús d'eines bàsiques per generar un **catàleg inicial d'actius**, incorporant-lo a la **CMDB corporativa** i establint la traçabilitat amb els serveis crítics que aquests actius suporten.

Aquest paquet constitueix la base per evolucionar cap a un inventari automatitzat i una classificació completa segons criticitat i sensibilitat de la informació (nivells avançat i òptim).

El paràmetre quantificador d'aquest servei serà el número d'usuaris interns de l'entitat contractant objecte del servei.

El paquet P4 inclou el llicenciament i els serveis d'administració i operació de la plataforma d'exploració, inventari i classificació d'actius, així com de la resta de solucions necessàries per prestar el servei.

Funcionalitats que ha de suportar el servei

REQ-TCN-118. Exploració manual d'actius: el servei haurà de dur a terme activitats manuals i semiautomàtiques per identificar sistemes, aplicacions i dispositius de l'entitat.

REQ-TCN-119. Etiquetatge i categorització inicial: cada actiu detectat haurà d'estar associat a metadades bàsiques (tipologia, ubicació, propietari funcional, estat).

REQ-TCN-120. Importació manual a la CMDB: el servei haurà de permetre registrar els actius identificats dins de la CMDB corporativa seguint els processos establerts.

REQ-TCN-121. Traçabilitat amb serveis crítics: els actius inventariats hauran d'estar vinculats als serveis que suporten, especialment aquells considerats crítics per a la continuïtat municipal.

REQ-TCN-122. Informe executiu i tècnic: el servei haurà de generar informes que mostrin l'inventari bàsic, les categories definides i els primers indicadors de cobertura.

REQ-TCN-123. Horari de servei: 8x5. Les persones que integrin el servei hauran de ser operatives de 9h a 17h de dilluns a divendres per tal d'atendre incidències, consultes, peticions de servei, etc.

Activitats a realitzar per part de l'adjudicatari

- Planificar conjuntament amb l'entitat municipal l'abast de l'exploració inicial d'actius.
- Realitzar l'exploració manual i semiautomàtica amb eines de suport bàsic.
- Etiquetar i categoritzar cada actiu segons criteris establerts per l'Ajuntament.
- Importar els resultats a la CMDB corporativa.
- Generar i presentar informes tècnics i executius amb l'estat de l'inventari inicial.

Resultats esperats

- **Inventari inicial d'actius** disponibles en l'entorn municipal.

- **CMDB corporativa enriquida** amb dades bàsiques d'actius identificats.
- **Traçabilitat establerta** entre actius i serveis crítics.
- **Consciència inicial** sobre l'abast i la diversitat dels recursos que cal protegir.

4.1.12 Paquet P4-B – Inventari i classificació d'actius (nivell avançat)

El paquet P4-B té per objectiu ampliar les capacitats establertes al nivell inicial (P4-A), incorporant processos **automatitzats de descoberta i etiquetatge d'actius**, així com una integració més eficient amb la CMDB corporativa. Aquest nivell avançat permet assolir una **major cobertura i precisió**, reduint la dependència de processos manuals i establint la base per a un inventari continu i dinàmic.

Aquest paquet **incorpora tots els requisits establerts en el P4-A** i els amplia amb les funcionalitats següents:

Funcionalitats que ha de suportar el servei

REQ-TCN-124. Descobriment automatitzat d'actius: el servei haurà de disposar d'eines capaces de detectar sistemes, aplicacions, dispositius de xarxa i entorns virtuals mitjançant exploracions programades.

REQ-TCN-125. Etiquetatge automàtic parcial: els actius descoberts hauran de ser etiquetats automàticament segons tipologia i característiques tècniques bàsiques.

REQ-TCN-126. Validació manual supervisada: els resultats del descobriment automatitzat hauran de ser revisats i validats per tècnics de l'adjudicatari abans de la seva incorporació definitiva a la CMDB.

REQ-TCN-127. Integració semiautomàtica amb la CMDB: el servei haurà de permetre exportar i importar dades de manera estandarditzada entre les eines de descoberta i la CMDB corporativa.

REQ-TCN-128. Detecció d'actius no autoritzats: el servei haurà d'identificar actius desconeguts o no inventariats prèviament i generar alertes específiques.

REQ-TCN-129. Informes avançats de cobertura: els informes hauran d'incloure mètriques sobre la cobertura del descobriment automatitzat i l'evolució de l'inventari respecte al nivell inicial.

Activitats a realitzar per part de l'adjudicatari

- Desplegar eines de descoberta automatitzada d'actius en l'entorn municipal.
- Configurar exploracions periòdiques i recollir resultats per a la seva validació.
- Etiquetar i categoritzar automàticament els actius detectats.
- Realitzar validació manual supervisada i integració a la CMDB corporativa.
- Identificar i notificar actius no autoritzats o desconeguts.
- Generar informes tècnics i executius amb l'estat de cobertura i l'evolució respecte a P4-A.

Resultats esperats

- **Inventari més complet i fiable** d'actius municipals, amb cobertura superior al nivell inicial.
- **CMDB corporativa enriquida** mitjançant integració semiautomàtica de dades.
- **Detecció proactiva d'actius no autoritzats**, millorant la postura de seguretat.
- **Reducció de l'esforç manual** i augment de l'eficiència en la gestió de l'inventari.
- **Traçabilitat millorada** entre actius, serveis i riscos.

4.1.13 Paquet P4-C – Inventari i classificació d'actius (nivell òptim)

El paquet P4-C té per objectiu assolir un model de **gestió d'actius dinàmic, integral i predictiu**, que permeti disposar d'un inventari sempre actualitzat i alineat amb els processos de governança de riscos municipals. Aquest nivell òptim elimina la dependència de processos manuals, incorpora mecanismes intel·ligents de classificació i garanteix la traçabilitat completa entre actius, serveis i riscos.

Aquest paquet **incorpora tots els requisits establerts en els nivells P4-A i P4-B** i els amplia amb les següents funcionalitats:

Funcionalitats que ha de suportar el servei

REQ-TCN-130. Descobriment continu i en temps real: el servei haurà de detectar i inventariar automàticament nous actius en el moment que s'incorporen a la xarxa o als serveis municipals.

REQ-TCN-131. Etiquetatge i classificació intel·ligent: els actius hauran de ser classificats de manera automàtica segons criteris de tipologia, criticitat, sensibilitat de la informació i dependència de serveis.

REQ-TCN-132. Integració nativa amb la CMDB: la informació d'actius haurà de ser actualitzada en temps real dins de la CMDB corporativa, sense necessitat de processos manuals ni semiautomàtics.

REQ-TCN-133. Correlació amb processos de governança de riscos: els actius inventariats hauran d'alimentar directament els processos de gestió de riscos i de compliment normatiu, permetent obtenir mètriques comparatives.

REQ-TCN-134. Detecció automàtica d'anomalies: el servei haurà de detectar patrons anòmals en la incorporació d'actius (p. ex. dispositius no autoritzats, canvis sobtats en configuracions) i generar alertes immediates.

REQ-TCN-135. Quadres de comandament estratègics: el servei haurà de proporcionar dashboards en temps real amb visibilitat sobre la totalitat dels actius, el seu estat de seguretat i la seva relació amb els serveis crítics.

REQ-TCN-136. Capacitats predictives: el servei haurà d'incloure mecanismes basats en IA capaços de predir canvis en l'inventari i anticipar riscos vinculats a l'evolució tecnològica o a la introducció de nous actius.

Activitats a realitzar per part de l'adjudicatari

- Implantar i operar mecanismes de descobriment i inventari d'actius en temps real.
- Configurar i mantenir processos d'etiquetatge i classificació intel·ligent segons la criticitat.
- Integrar la informació en la CMDB de manera nativa i sense intervenció manual.

- Correlacionar les dades d'actius amb els processos de governança i gestió de riscos.
- Generar alertes automàtiques davant anomalies i canvis inesperats en l'inventari.
- Oferir informes predictius i dashboards estratègics per a responsables municipals.

Resultats esperats

- **Inventari complet i dinàmic**, actualitzat en temps real i amb classificació intel·ligent.
- **Traçabilitat total** entre actius, serveis crítics i riscos associats.
- **Automatització plena** dels processos d'inventari, reduint al mínim l'esforç manual.
- **Visibilitat estratègica** per als responsables municipals mitjançant quadres de comandament.
- **Capacitat predictiva** per anticipar riscos associats a nous actius i tendències tecnològiques.
- **Maduresa màxima en la gestió d'actius**, amb integració directa en els processos de seguretat i governança.

4.1.14 Paquet P16-A – Monitoratge i detecció d'incidents a llocs de treball i dispositius mòbils (nivell inicial)

El paquet P16-A té per objectiu establir un servei bàsic de monitoratge d'alertes i detecció d'incidents en horari 24x7 sobre els ordinadors i dispositius mòbils corporatius (telèfons, PDAs, tauletes, etc), proporcionant a l'Ajuntament i a les entitats dependents una primera línia de visibilitat sobre l'estat de seguretat d'aquests equips. Aquest nivell inicial permet disposar d'informació centralitzada i recurrent sobre esdeveniments de seguretat i incidents elementals, establint la línia de base per evolucionar cap a nivells més avançats de resposta i investigació.

El paràmetre quantificador d'aquest servei serà el número d'usuaris interns de l'entitat contractant objecte del servei.

El paquet P16 inclou el llicenciament i els serveis d'administració i operació de les solucions SIEMaaS i SOARaaS integrant les solucions de gestió de dispositius i de protecció dels llocs de treball i dispositius mòbils (de forma descriptiva però no limitativa: SCCM, UEM, EPP, EDR, XDR,

MTD, protecció navegació, etc) de que disposi l'entitat contractant, així com la resta de solucions (Threat Hunting, BAS, Threat Intel, etc) necessàries per prestar el servei. Als efectes de valorar l'esforç requerit pel servei, s'ha d'estimar que tots els usuaris disposen d'estació de treball corporativa i que un terç disposen de terminal mòbil corporatiu.

Tanmateix, el paquet P16 no inclou el llicenciament de les solucions de protecció dels llocs de treball i dispositius mòbils.

Funcionalitats que ha de suportar el servei

REQ-TCN-137. Ingesta i normalització d'alertes: el servei haurà de recollir i normalitzar les alertes i registres generats pels sistemes de gestió i de protecció dels dispositius (p.e. EPP, EDR, MTD, etc) i per l'activitat pròpia dels equips (arrencada, aturada, canvis de configuració, instal·lació de programari).

REQ-TCN-138. Triatge inicial de primer i segon nivell (L1–L2): el servei haurà de revisar, filtrar i classificar les alertes segons la seva gravetat, eliminant falsos positius i escalant al procés de gestió d'incidents quan sigui necessari.

REQ-TCN-139. Casos d'ús deterministes: el servei haurà de suportar deteccions basades en indicadors coneguts (IOC, hash, procés, USB, connexions a dominis maliciosos) per a la identificació immediata de compromisos bàsics. Els casos d'ús hauran de ser documentats.

REQ-TCN-140. Seguretat a la navegació des de llocs de treball i dispositius mòbils: el servei haurà de monitorar i detectar incidents que puguin afectar els dispositius o les identitats dels usuaris quan naveguin per internet.

REQ-TCN-141. Accions remotes bàsiques: el servei haurà de poder sol·licitar o executar accions prèviament aprovades com l'aïllament d'un equip, l'eliminació d'un procés, la quarantena d'un fitxer o el bloqueig temporal d'un perifèric.

REQ-TCN-142. Notificació a l'usuari afectat: el servei haurà de preveure la comunicació a l'usuari final de les mesures aplicades en el seu dispositiu, d'acord amb els protocols establerts.

REQ-TCN-143. Informes periòdics: el servei haurà de generar informes tècnics i executius amb el resum de dispositius monitorats, incidents detectats, tendències i recomanacions bàsiques de millora.

REQ-TCN-144. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per integrar en el futur fonts de dades de noves tecnologies de protecció d'endpoints i mòbils (per exemple, solucions de gestió unificada de dispositius –UEM–, plataformes de seguretat en entorns virtualitzats o tecnologies emergents de detecció basada en IA).

Activitats a realitzar per part de l'adjudicatari

- Configurar i posar en marxa la recollida d'esdeveniments bàsics en ordinadors, portàtils i dispositius mòbils.
- Normalitzar i integrar aquesta informació dins de la plataforma central de monitoratge.
- Revisar i classificar les alertes, amb escalat al procés de gestió d'incidents quan correspongui.
- Executar o sol·licitar accions remotes bàsiques prèviament aprovades.
- Notificar als usuaris afectats quan s'apliquin mesures que impactin en el seu dispositiu.
- Elaborar informes periòdics diferenciats per a responsables tècnics i executius.
- Donar suport inicial als equips municipals en la interpretació de resultats i en la definició de mesures de millora.

Resultats esperats

- Disposar d'una visibilitat mínima sobre l'activitat i l'estat de seguretat dels dispositius corporatius.
- Capacitat de detectar i notificar amenaces conegudes i anomalies elementals.
- Possibilitat d'aplicar accions remotes bàsiques de contenció en els dispositius afectats.
- Informació periòdica, clara i accionable per a tècnics i directius.
- Capacitat d'adaptar-se a noves plataformes i solucions de seguretat d'endpoints en el futur.
- Establiment d'una línia de base sòlida per evolucionar cap al nivell avançat (P16-B).

4.1.15 Paquet P16-B – Monitoratge i detecció d'incidents a llocs de treball i dispositius mòbils (nivell avançat)

El paquet P16-B té per objectiu proporcionar un nivell avançat de monitoratge d'alertes, detecció d'incidents i resposta inicial en horari 24x7 sobre els ordinadors i dispositius mòbils corporatius, ampliant les capacitats establertes al nivell bàsic i incorporant mecanismes de detecció contextual i d'anàlisi més profunda. Aquest nivell permet identificar compromisos més sofisticats i actuar de forma remota per contenir els incidents abans que tinguin un impacte major.

Aquest paquet incorpora tots els requisits establerts en el P16-A i els amplia amb les següents funcionalitats:

REQ-TCN-145. Detecció de comportaments anòmals en dispositius: el servei haurà d'identificar anomalies complexes, com execució de processos no habituals, ús d'eines legítimes per a finalitats malicioses (LOLBins), intents de persistència o modificació de claus de sistema.

REQ-TCN-146. Triatge forense inicial: el servei haurà de poder recopilar remotament evidències tècniques bàsiques, com volcada de memòria, registres d'activitat i fitxers sospitosos, sempre que sigui possible, per donar suport a la investigació posterior.

REQ-TCN-147. Playbooks de contenció guiada: el servei haurà de disposar de procediments definits i acordats amb l'entitat contractant per aplicar accions de contenció inicial, com revertir canvis de configuració, bloquejar executables per editor o aplicar restriccions temporals d'ús.

REQ-TCN-148. Informes ampliats: el servei haurà de generar informes que incloguin una descripció dels incidents avançats detectats, les mesures de contenció aplicades, les causes probables i recomanacions específiques per evitar recurrències.

REQ-TCN-149. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per integrar, a mesura que apareguin, noves tecnologies de detecció avançada en dispositius i eines de resposta forense remota.

Activitats a realitzar per part de l'adjudicatari

- Correlacionar i analitzar esdeveniments de dispositius amb informació d'identitat i trànsit de xarxa.
- Configurar i mantenir regles avançades de detecció de comportaments anòmals.
- Executar accions de contenció remota inicial segons els playbooks establerts.
- Recollir i custodiar evidències bàsiques per a la investigació d'incidents.
- Elaborar informes detallats amb la descripció dels incidents i les recomanacions de millora.

Resultats esperats

- Capacitat de detectar compromisos més sofisticats en ordinadors i dispositius mòbils.
- Possibilitat de contenir remotament incidents en fases inicials amb protocols guiats.
- Disponibilitat d'evidències tècniques per donar suport a investigacions forenses.

- Informes ampliats que permetin prendre decisions de millora sobre la seguretat dels equips.
- Capacitat d'incorporar noves plataformes i tecnologies avançades a mesura que apareguin.
- Evolució natural cap al nivell òptim (P16-C), amb capacitats de hunting i validació contínua.

4.1.16 Paquet P16-C – Monitoratge i detecció d'incidents a llocs de treball i dispositius mòbils (nivell òptim)

El paquet P16-C té per objectiu assolir un nivell òptim de monitoratge d'alertes, detecció d'incidents i resposta en horari 24x7 sobre els ordinadors i dispositius mòbils corporatius, establint capacitats proactives d'investigació i validació contínua. Aquest nivell garanteix que l'Ajuntament pugui anticipar-se a compromisos complexos, validar constantment l'eficàcia de les deteccions i evolucionar cap a un servei madur i resilient davant tècniques d'atac en permanent evolució.

Aquest paquet incorpora tots els requisits establerts en el P16-B i els amplia amb les següents funcionalitats:

REQ-TCN-150. Caça d'amenaces (Threat hunting) continu: el servei haurà de dur a terme activitats de cerca activa i recurrent d'indicadors de compromís en els dispositius, basant-se en tècniques conegudes i noves hipòtesis de compromís encara no reflectides en alertes prèvies.

REQ-TCN-151. Detecció avançada amb models de comportament: el servei haurà d'identificar anomalies complexes a partir de models de comportament i risc contextual, incloent patrons d'ús inusuals, combinacions d'activitat sospitosa i desviacions respecte a la línia de base establerta.

REQ-TCN-152. Validació contínua de deteccions i playbooks (BAS): el servei haurà de validar periòdicament l'eficàcia dels mecanismes de detecció i de les respostes automatitzades mitjançant proves controlades que permetin detectar llacunes i ajustar configuracions.

REQ-TCN-153. Anàlisi de causa arrel automatitzada (RCA): el servei haurà d'oferir capacitat per reconstruir l'origen i l'impacte complet d'un incident en els dispositius, identificant vectors d'entrada, propagació i conseqüències, de manera semi o totalment automatitzada.

REQ-TCN-154. Millora contínua de casos d'ús: el servei haurà de revisar i optimitzar de manera recurrent els casos de detecció i resposta, amb mètriques clares de fiabilitat (per exemple, taxa de falsos positius i temps mitjà fins a la detecció efectiva).

REQ-TCN-155. Adaptabilitat a tecnologies futures: el servei haurà d'estar preparat per integrar, a mesura que es desenvolupin, plataformes emergents de detecció i resposta per a endpoints, així com tecnologies basades en intel·ligència artificial i machine learning.

Activitats a realitzar per part de l'adjudicatari

- Desenvolupar i executar activitats de hunting continu en els dispositius corporatius.
- Configurar i mantenir models de detecció basats en comportament i risc contextual.
- Realitzar validacions periòdiques de deteccions i playbooks mitjançant exercicis controlats.
- Dur a terme anàlisis de causa arrel per als incidents crítics i documentar-ne les lliçons apreses.
- Elaborar informes tècnics i executius amb resultats de maduresa, mètriques de detecció i propostes de millora.

Resultats esperats

- Capacitat d'anticipar-se a compromisos avançats mitjançant hunting continu.
- Detecció més robusta i adaptada a contextos reals d'ús.
- Validació constant de l'eficàcia de deteccions i playbooks.
- Major velocitat i qualitat en la identificació de causes i impactes dels incidents.
- Evolució contínua del servei mitjançant la revisió i millora de casos d'ús i mètriques fiables.
- Flexibilitat per incorporar noves tecnologies d'endpoint i de detecció basada en IA.

4.1.17 Paquet P17-A – Monitoratge i detecció d'incidents a servidors (nivell inicial)

El paquet P17-A té per objectiu establir un servei bàsic de monitoratge d'alertes i detecció d'incidents en horari 24x7 sobre els servidors corporatius, ja siguin físics, virtuals o allotjats en entorns híbrids. Aquest nivell inicial permet disposar d'una primera línia de visibilitat sobre

l'activitat dels servidors i identificar incidents elementals que puguin comprometre la disponibilitat, integritat o confidencialitat dels serveis municipals.

El paràmetre quantificador d'aquest servei serà el número de servidors i càrregues de treball de l'entitat contractat objecte del servei.

El paquet P17 inclou el llicenciament i els serveis d'administració i operació de les solucions SIEMaaS i SOARaaS integrant les solucions de gestió i de protecció dels servidors i càrregues de treball (de forma descriptiva però no limitativa: EPP, EDR, XDR, etc) de que disposi l'entitat contractant, així com la resta de solucions (Threat Hunting, BAS, Threat Intel, etc) necessàries per prestar el servei.

Tanmateix, el paquet P17 no inclou el llicenciament de les solucions de protecció dels servidors i càrregues de treball.

Funcionalitats que ha de suportar el servei

REQ-TCN-156. Ingesta d'alertes de sistemes i proteccions: el servei haurà d'incorporar les alertes i registres generats pels sistemes operatius, eines de detecció en servidors (EPP, EDR, XDR) i sistemes de detecció d'intrusions d'hoste (HIDS).

REQ-TCN-157. Casos d'ús deterministes en servidors: el servei haurà de detectar situacions elementals com l'ús indegut de comptes de servei, modificacions no autoritzades en fitxers o configuracions, i execució de binaris amb privilegis elevats.

REQ-TCN-158. Seguretat a la navegació des de servidors: el servei haurà de monitorar i detectar incidents que puguin afectar els servidors quan naveguin per internet.

REQ-TCN-159. Contenció remota pre-aprovada: el servei haurà de poder executar o sol·licitar accions bàsiques prèviament acordades, com aïllar temporalment un servidor de la xarxa, bloquejar l'execució d'un hash concret o aturar un servei sospitós.

REQ-TCN-160. Classificació i triatge inicial: el servei haurà de revisar i classificar les alertes rebudes, assignant-ne un nivell de gravetat i escalant-les al procés de gestió d'incidents quan correspongui.

REQ-TCN-161. Informes periòdics: el servei haurà de generar informes amb el resum de servidors monitorats, incidents detectats, tendències observades i recomanacions bàsiques de millora.

REQ-TCN-162. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per integrar alertes de noves tecnologies de protecció de servidors i serveis que puguin aparèixer en el futur (per exemple, seguretat en contenidors o mecanismes d'hardening automatitzat).

Activitats a realitzar per part de l'adjudicatari

- Configurar i posar en marxa la recollida d'alertes i registres dels sistemes operatius i eines de protecció de servidors.
- Definir i aplicar casos d'ús deterministes per a deteccions bàsiques.
- Executar o sol·licitar accions de contenció remota bàsiques prèviament aprovades.
- Revisar i classificar alertes segons la seva gravetat i escalar-les quan sigui necessari.
- Elaborar informes periòdics diferenciats per a responsables tècnics i executius.
- Donar suport inicial als equips municipals en la interpretació de resultats i definició de mesures de millora.

Resultats esperats

- Visibilitat mínima establerta sobre l'activitat i estat de seguretat dels servidors corporatius.
- Capacitat de detectar i notificar anomalies bàsiques relacionades amb comptes de servei, canvis no autoritzats i execució de binaris elevats.
- Possibilitat d'aplicar accions remotes bàsiques de contenció en els servidors afectats.
- Disponibilitat d'informes periòdics amb informació accionable per a tècnics i directius.
- Preparació per evolucionar cap al nivell avançat (P17-B), amb correlació i resposta més sofisticada.

4.1.18 Paquet P17-B – Monitoratge i detecció d'incidents a servidors (nivell avançat)

El paquet P17-B té per objectiu proporcionar un nivell avançat de monitoratge d'alertes, detecció d'incidents i resposta inicial en horari 24x7 sobre els servidors corporatius, ampliant les capacitats establertes al nivell bàsic. Aquest nivell permet detectar compromisos més sofisticats, correlacionar esdeveniments en funció de la seva criticitat i actuar de manera remota sobre servidors crítics de l'Ajuntament per contenir incidents abans que afectin serveis essencials.

Aquest paquet incorpora tots els requisits establerts en el P17-A i els amplia amb les següents funcionalitats:

REQ-TCN-163. Correlació amb CMDB i criticitat: el servei haurà d'integrar les alertes i esdeveniments dels servidors amb la informació de la base de dades de configuració (CMDB) i la classificació de criticitat, prioritzant la resposta en funció de l'impacte potencial sobre els serveis municipals.

REQ-TCN-164. Detecció d'escala de privilegis i moviment lateral: el servei haurà de disposar de mecanismes per detectar intents d'escalar privilegis i moviments laterals entre servidors, identificant patrons de compromís més enllà de l'equip inicialment afectat.

REQ-TCN-165. Triatge forense inicial en servidors crítics: el servei haurà de recopilar de manera remota i controlada evidències bàsiques (fitxers de registre, configuracions, captures de memòria) en servidors crítics, preservant la informació necessària per a una anàlisi posterior.

REQ-TCN-166. Coordinació de finestres de resposta amb operacions: el servei haurà d'establir procediments per coordinar amb els equips d'operacions municipals l'aplicació de mesures de resposta, assegurant la contenció dels incidents sense comprometre la continuïtat del servei.

REQ-TCN-167. Informes ampliats: el servei haurà de generar informes que descriguin incidents avançats, les accions de contenció aplicades, l'anàlisi preliminar de causes i recomanacions de millora específiques per als servidors.

REQ-TCN-168. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per integrar alertes i processos de resposta provinents de noves tecnologies de virtualització, contenidors o altres plataformes emergents d'infraestructura.

Activitats a realitzar per part de l'adjudicatari

- Correlacionar i prioritzar esdeveniments de seguretat de servidors segons la seva criticitat i dependència amb serveis municipals.
- Detectar intents d'escalar privilegis i moviments laterals entre servidors.
- Recollir evidències bàsiques de manera remota en servidors crítics afectats.
- Coordinar amb operacions les accions de contenció per minimitzar l'impacte sobre la continuïtat del servei.

- Elaborar informes detallats amb la descripció dels incidents i recomanacions de millora.

Resultats esperats

- Capacitat de prioritzar i gestionar incidents en funció de la criticitat dels servidors i serveis afectats.
- Detecció d'activitats avançades com escales de privilegis i moviments laterals.
- Disponibilitat d'evidències inicials per a la investigació forense de servidors crítics.
- Coordinació efectiva amb operacions per equilibrar contenció i continuïtat de servei.
- Informes ampliats que permetin millorar la seguretat i resiliència dels servidors.
- Preparació per evolucionar cap al nivell òptim (P6-C), amb hunting i validació contínua.

4.1.19 Paquet P17-C – Monitoratge i detecció d'incidents a servidors (nivell òptim)

El paquet P17-C té per objectiu assolir un nivell òptim de monitoratge d'alertes, detecció d'incidents i resposta en horari 24x7 sobre els servidors corporatius, establint capacitats proactives de caça d'amenaces (threat hunting), validació contínua i aprenentatge. Aquest nivell garanteix que l'Ajuntament pugui anticipar-se a compromisos complexos, centrar els esforços en els servidors més crítics ("crown jewels") i disposar d'una millora contínua en la protecció de serveis essencials.

Aquest paquet incorpora tots els requisits establerts en el P17-B i els amplia amb les següents funcionalitats:

REQ-TCN-169. Caça d'amenaces (Threat Hunting) orientada a servidors crítics ("crown jewels"): el servei haurà de dur a terme activitats recurrents de cerca proactiva d'indicadors de compromís en els servidors més sensibles, amb un enfocament específic en aquells que allotgin dades o serveis essencials.

REQ-TCN-170. Validació contínua de controls de seguretat: el servei haurà de verificar periòdicament l'eficàcia dels mecanismes de protecció aplicats als servidors, utilitzant tècniques de simulació controlada (BAS) i consultes d'integritat per comprovar que no hi hagi desviacions respecte a la configuració segura establerta.

REQ-TCN-171. Priorització basada en risc de servei: el servei haurà de valorar cada incident no només pel seu impacte tècnic, sinó també pel risc que representi sobre els serveis

municipals associats, assegurant que la resposta sigui proporcional a la importància del servei compromès.

REQ-TCN-172. Anàlisi de causa arrel automatitzada (RCA): el servei haurà de reconstruir de manera semi o totalment automatitzada la cadena d'esdeveniments d'un incident, identificant l'origen, la propagació i l'impacte final sobre els servidors i serveis afectats.

REQ-TCN-173. Lliçons apreses i recomanacions de hardening: el servei haurà de documentar per cada incident crític les lliçons apreses i proporcionar recomanacions concretes de reforç de la seguretat (hardening), que hauran d'incloure configuracions, controls preventius i bones pràctiques operatives.

REQ-TCN-174. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per integrar tecnologies emergents de seguretat per a entorns híbrids i multicloud, com controls específics per contenidors, microserveis o plataformes serverless.

Activitats a realitzar per part de l'adjudicatari

- Dur a terme hunting recurrent orientat als servidors crítics definits com a "crown jewels".
- Verificar periòdicament l'eficàcia dels controls aplicats als servidors mitjançant proves controlades.
- Prioritzar la gestió dels incidents segons el risc i l'impacte sobre els serveis municipals.
- Realitzar anàlisis de causa arrel automatitzades per als incidents de major rellevància.
- Documentar lliçons apreses i recomanacions de hardening per reforçar la seguretat dels servidors.
- Incorporar noves fonts i tecnologies de seguretat a mesura que s'adoptin nous models d'infraestructura.

Resultats esperats

- Capacitat d'anticipar-se a compromisos avançats en els servidors més crítics.
- Confirmació periòdica de l'eficàcia dels controls mitjançant validació contínua.
- Resposta orientada a la continuïtat dels serveis, amb priorització basada en el risc de negoci.
- Disponibilitat d'anàlisis de causa arrel automatitzades per accelerar la resolució d'incidents.
- Millora progressiva de la seguretat dels servidors gràcies a les lliçons apreses i recomanacions de hardening.
- Flexibilitat per evolucionar cap a nous entorns tecnològics i plataformes emergents.

4.1.20 Paquet P18-A – Monitoratge i detecció d'incidents a identitats i accessos (nivell inicial)

El paquet P18-A té per objectiu establir un servei bàsic de monitoratge d'alertes i detecció d'incidents en horari 24x7 sobre els sistemes d'identitat i accés municipals, incloent els serveis d'autenticació centralitzada i els mecanismes de multifactor. Aquest nivell inicial proporciona visibilitat sobre els intents d'accés i ús de credencials, permetent detectar anomalies elementals i aplicar respostes bàsiques davant incidents que puguin comprometre la seguretat dels comptes d'usuari.

El paràmetre quantificador d'aquest servei serà el número d'usuaris interns de l'entitat contractant objecte del servei.

El paquet P18 inclou el llicenciament i els serveis d'administració i operació de les solucions SIEMaaS i SOARaaS integrant les solucions de gestió i de protecció d'identitats i accessos (de forma descriptiva però no limitativa: sistemes de directori actiu, IAM, ITDR, PAM, SSO, MFA, UEBA, plataformes AAA, VPN, ZTNA, etc), així com la resta de solucions (Threat Hunting, BAS, Threat Intel, etc) necessàries per prestar el servei.

Tanmateix, el paquet P18 no inclou el llicenciament de les solucions de protecció d'identitats i accessos.

Funcionalitats que ha de suportar el servei

REQ-TCN-175. Monitoratge de sistemes d'identitat i accessos: el servei haurà d'incorporar i supervisar les alertes i esdeveniments generats pels següents sistemes (de forma descriptiva, però no limitativa): sistemes de directori actiu, sistemes de gestió d'identitat i accessos (IAM), de detecció i resposta d'amenaces a la identitat (ITDR), els sistemes de gestió de comptes privilegiats (PAM), d'autenticació única (SSO) i multifactor (MFA), de les plataformes AAA (Radius, Tacacs+), d'anàlisi de comportament d'usuaris i entitats (UEBA), i d'accés remot (VPN, ZTNA, etc).

REQ-TCN-176. Gestió d'incidents de VPN i ZTNA: el servei haurà de detectar i gestionar incidents relacionats amb l'ús de xarxes privades virtuals VPN i ZTNA (Zero Trust Network Access), incloent la reutilització de credencials o accessos sospitosos a hores no habituals.

REQ-TCN-177. Casos d'ús per anomalies d'accés: el servei haurà de detectar patrons bàsics com desplaçaments impossibles (*impossible travel*), intents de força bruta distribuïda (*password spraying*, *stuffing*) o atacs de fatiga de multifactor (MFA fatigue).

REQ-TCN-178. Resposta bàsica sobre comptes: el servei haurà de poder executar o sol·licitar accions prèviament aprovades com el restabliment de credencials, el bloqueig temporal de comptes sospitosos o la revocació de sessions actives.

REQ-TCN-179. Classificació i triatge inicial: el servei haurà de revisar i classificar les alertes rebudes segons la seva gravetat, establint criteris d'escalat al procés de gestió d'incidents quan sigui necessari.

REQ-TCN-180. Informes periòdics d'identitat: el servei haurà de generar informes tècnics i executius amb el resum d'incidents detectats, tendències d'autenticació i recomanacions bàsiques de millora.

REQ-TCN-181. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per integrar fonts d'alerta d'eines emergents de gestió d'identitat i d'autenticació avançada, incloent serveis d'identitat sobirana o federacions en entorns multicloud.

Activitats a realitzar per part de l'adjudicatari

- Configurar i posar en marxa la recollida d'esdeveniments dels sistemes d'identitat i accessos (IAM, SSO, MFA, etc).
- Detectar i gestionar incidents relacionats amb l'ús de VPN i credencials compromeses.
- Definir i mantenir casos d'ús bàsics per a la detecció d'anomalies d'accés.
- Executar o sol·licitar accions bàsiques de resposta en comptes compromesos.
- Revisar i classificar alertes segons la seva gravetat i escalar-les quan correspongui.
- Elaborar informes periòdics diferenciats per a responsables tècnics i executius.

Resultats esperats

- Visibilitat mínima sobre els intents d'accés i l'ús de credencials en sistemes corporatius.
- Capacitat de detectar i notificar incidents elementals d'identitat i autenticació.
- Detecció i gestió d'incidents bàsics vinculats a l'ús de VPN.
- Possibilitat d'aplicar mesures de resposta bàsiques per contenir accessos sospitosos.
- Informes periòdics que permetin prendre decisions de millora en la gestió d'identitat.
- Preparació per evolucionar cap al nivell avançat (P18-B), amb detecció d'anomalies contextuals i resposta remota més sofisticada.

4.1.21 Paquet P18-B – Monitoratge i detecció d'incidents a identitats i accessos (nivell avançat)

El paquet P18-B té per objectiu proporcionar un nivell avançat de monitoratge d'alertes, detecció d'incidents i resposta inicial en horari 24x7 sobre els sistemes d'identitat i accés municipals, ampliant les capacitats establertes al nivell bàsic. Aquest nivell introdueix l'anàlisi de comportament d'usuaris i privilegis, la detecció d'abusos en comptes privilegiats i la capacitat d'aplicar mesures de contenció guiades per reduir el risc d'un incident abans que tingui un impacte significatiu.

Aquest paquet incorpora tots els requisits establerts en el P18-A i els amplia amb les següents funcionalitats:

REQ-TCN-182. Anàlisi de comportament d'usuaris i privilegis (UEBA): el servei haurà d'integrar mecanismes per detectar anomalies en el comportament d'usuaris i comptes privilegiats, com patrons d'accés inusuals, ús fora d'horari o desviacions respecte a la línia de base establerta.

REQ-TCN-183. Detecció d'abús de comptes privilegiats (PAM): el servei haurà de ser capaç d'identificar intents d'abús de comptes amb privilegis elevats, com l'ús indegut d'eines d'administració, escalades no autoritzades o compartició il·lícita de credencials privilegiades.

REQ-TCN-184. Contenció remota guiada: el servei haurà de disposar de playbooks per aplicar mesures de contenció remota sobre comptes sospitosos, incloent la desactivació temporal, el pas a un grup de quarantena o la rotació forçada de secrets i claus.

REQ-TCN-185. Revisió de comptes d'alt risc: el servei haurà de realitzar revisions ràpides i sistemàtiques dels comptes considerats d'alt risc (per exposició, privilegis o activitat sospitosa), assegurant la seva monitorització prioritària.

REQ-TCN-186. Informes ampliats d'identitat: el servei haurà de generar informes que incloguin descripcions d'incidents avançats, accions de contenció aplicades, recomanacions de reforç de controls i evolució de l'activitat dels comptes privilegiats.

REQ-TCN-187. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per integrar fonts d'alerta d'eines emergents de gestió d'identitats i privilegis, com solucions d'accés just-in-time o gestió descentralitzada d'identitat.

Activitats a realitzar per part de l'adjudicatari

- Analitzar el comportament d'usuaris i privilegis per detectar anomalies.
- Identificar intents d'abús de comptes privilegiats.
- Executar mesures de contenció guiades per a comptes sospitosos.
- Revisar periòdicament els comptes d'alt risc per garantir-ne el seguiment.
- Elaborar informes ampliats amb la descripció d'incidents, accions aplicades i recomanacions de millora.

Resultats esperats

- Capacitat de detectar anomalies avançades en l'ús d'identitats i privilegis.
- Possibilitat de contenir incidents inicials mitjançant accions remotes guiades.
- Major control i supervisió dels comptes d'alt risc i privilegiats.
- Informes ampliats que permetin reforçar la governança i seguretat de la identitat.
- Preparació per evolucionar cap al nivell òptim (P18-C), amb resposta adaptativa i integració completa en entorns Zero Trust.

4.1.22 Paquet P18-C – Monitoratge i detecció d'incidents a identitats i accessos (nivell òptim)

El paquet P18-C té per objectiu assolir un nivell òptim de monitoratge d'alertes, detecció d'incidents i resposta en horari 24x7 sobre els sistemes d'identitat i accés municipals, establint capacitats proactives d'hunting, validació contínua i resposta adaptativa. Aquest nivell garanteix que l'Ajuntament pugui anticipar-se a compromisos avançats, comprendre el camí complet d'un abús de privilegis i evolucionar cap a un model de seguretat basat en principis de Zero Trust.

Aquest paquet incorpora tots els requisits establerts en el P18-B i els amplia amb les següents funcionalitats:

REQ-TCN-188. Caça d'amenaces (Threat Hunting) d'identitat: el servei haurà de dur a terme activitats recurrents de cerca proactiva de riscos en identitats i privilegis, incloent la detecció de camins de privilegi explotables, comptes orfes o privilegis acumulats indegudament.

REQ-TCN-189. Validació contínua de deteccions d'identitat: el servei haurà de posar a prova de manera periòdica les deteccions mitjançant simulacions d'atacs d'identitat, per comprovar l'eficàcia dels mecanismes de monitoratge i resposta.

REQ-TCN-190. Anàlisi de causa arrel automatitzada del camí de privilegis: el servei haurà de reconstruir de manera semi o totalment automatitzada la cadena d'esdeveniments d'un incident d'identitat, des de l'accés inicial fins a l'abús de privilegis, identificant els passos i usuaris implicats.

REQ-TCN-191. Recomanacions de política adaptativa: el servei haurà de generar propostes de polítiques d'accés adaptatives, com l'aplicació de mecanismes de verificació addicional (*step-up authentication*) només en escenaris de risc identificats.

REQ-TCN-192. Informes de maduresa i millora contínua: el servei haurà de generar informes que integrin resultats de hunting, validacions, RCA i recomanacions de política adaptativa, amb un full de ruta per a l'evolució cap a Zero Trust.

REQ-TCN-193. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per incorporar fonts i capacitats de seguretat en tecnologies emergents d'identitat, com identitats descentralitzades, identitat sobirana digital o entorns híbrids multicloud.

Activitats a realitzar per part de l'adjudicatari

- Dur a terme activitats de hunting per identificar camins de privilegi, comptes orfes i acumulació de permisos.
- Realitzar validacions periòdiques mitjançant simulacions d'atacs d'identitat.
- Reconstruir incidents complexos amb RCA automatitzada del camí de privilegis.
- Elaborar recomanacions de polítiques d'accés adaptatives per reduir riscos.
- Generar informes executius i tècnics amb resultats i propostes de millora contínua.

Resultats esperats

- Capacitat d'anticipar-se a compromisos avançats mitjançant hunting específic d'identitat.
- Confirmació recurrent de l'eficàcia de les deteccions a través de simulacions d'atac.
- Reconstrucció automatitzada del camí d'abús de privilegis en incidents d'identitat.
- Disponibilitat de polítiques adaptatives per reforçar el control d'accessos en funció del risc.
- Evolució constant cap a un model de seguretat Zero Trust en l'àmbit de la identitat i els accessos.

4.1.23 Paquet P19-A – Monitoratge i detecció d'incidents a informació i dades (nivell inicial)

El paquet P19-A té per objectiu establir un servei bàsic de monitoratge d'alertes i detecció d'incidents en horari 24x7 sobre la informació i les dades gestionades per l'Ajuntament i les entitats dependents. Aquest nivell inicial proporciona visibilitat sobre moviments elementals de dades, intents d'exfiltració bàsica i l'aplicació de controls de contenció senzills per reduir el risc de pèrdua d'informació.

El paràmetre quantificador d'aquest servei serà el número d'usuaris interns de l'entitat contractant objecte del servei.

El paquet P19 inclou el llicenciament i els serveis d'administració i operació de les solucions SIEMaaS i SOARaaS integrant les solucions de protecció de la informació i les dades (de forma descriptiva però no limitativa: DLP, DSPM, etc), així com la resta de solucions (Threat Hunting, BAS, Threat Intel, etc) necessàries per prestar el servei.

Tanmateix, el paquet P19 no inclou el llicenciament de les solucions de protecció de la informació i les dades.

Funcionalitats que ha de suportar el servei

REQ-TCN-194. Ingesta d'alertes de DLP: el servei haurà d'incorporar i normalitzar les alertes generades per sistemes de prevenció de pèrdua de dades (DLP) desplegats en endpoints, xarxa, correu electrònic i aplicacions SaaS.

REQ-TCN-195. Detecció d'exfiltració bàsica de dades: el servei haurà de detectar intents elementals d'exfiltració de dades, com enviaments no autoritzats per correu, càrrega de fitxers a serveis externs o còpies a dispositius extraïbles.

REQ-TCN-196. Monitoratge d'etiquetatge: el servei haurà de supervisar l'aplicació d'etiquetes de classificació de dades, detectant absències o incoherències bàsiques en l'ús dels esquemes establerts.

REQ-TCN-197. Contenció bàsica de moviments de dades: el servei haurà de poder aplicar o sol·licitar mesures de contenció prèviament aprovades, com bloquejar l'enviament d'un fitxer, forçar-ne l'encriptació o posar-lo en quarantena per revisió posterior.

REQ-TCN-198. Classificació i triatge inicial: el servei haurà de revisar i classificar les alertes segons la seva gravetat i escalar-les al procés de gestió d'incidents quan correspongui.

REQ-TCN-199. Informes periòdics de dades: el servei haurà de generar informes tècnics i executius amb el resum d'incidents detectats, dades afectades i recomanacions bàsiques de millora.

REQ-TCN-200. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per integrar alertes de noves solucions de protecció de dades que puguin sorgir en el futur, incloent serveis nadius de núvol, aplicacions SaaS avançades i tecnologies emergents de governança de dades.

Activitats a realitzar per part de l'adjudicatari

- Configurar i posar en marxa la ingesta d'alertes dels sistemes DLP existents en endpoints, xarxa, correu i SaaS.
- Definir i mantenir casos d'ús per detectar intents bàsics d'exfiltració i incoherències en l'etiquetatge.
- Executar o sol·licitar accions de contenció bàsiques sobre documents sospitosos.
- Revisar i classificar alertes segons la seva gravetat i escalar-les quan sigui necessari.
- Elaborar informes periòdics diferenciats per a responsables tècnics i executius.

Resultats esperats

- Visibilitat mínima sobre l'estat de la seguretat de les dades municipals.
- Capacitat de detectar i notificar intents elementals d'exfiltració de dades.
- Possibilitat d'aplicar mesures bàsiques de contenció per protegir informació sensible.
- Informes periòdics que permetin avaluar l'eficàcia del control de dades i establir millores.
- Preparació per evolucionar cap al nivell avançat (P19-B), amb deteccions contextuals i resposta més sofisticada.

4.1.24 Paquet P19-B – Monitoratge i detecció d'incidents a informació i dades (nivell avançat)

El paquet P19-B té per objectiu proporcionar un nivell avançat de monitoratge d'alertes, detecció d'incidents i resposta inicial en horari 24x7 sobre la informació i les dades corporatives, ampliant les capacitats establertes al nivell bàsic. Aquest nivell introdueix la

correlació d'origen i destí de les dades, la detecció d'exfiltracions encobertes i la capacitat de donar resposta inicial a incidents amb notificacions a les parts afectades.

Aquest paquet incorpora tots els requisits establerts en el P19-A i els amplia amb les següents funcionalitats:

REQ-TCN-201. Correlació origen-destí de dades: el servei haurà de correlacionar esdeveniments de moviment de dades tenint en compte l'origen (usuari, dispositiu, aplicació) i el destí (altres aplicacions, serveis de núvol, repositoris externs), per detectar patrons de risc.

REQ-TCN-202. Detecció d'exfiltració encoberta: el servei haurà d'identificar intents d'exfiltració avançada basats en tècniques com compressió de fitxers, fragmentació, xifratge no autoritzat o ofuscació de contingut.

REQ-TCN-203. Resposta inicial a incidents de dades: el servei haurà de poder aplicar mesures de resposta inicial prèviament aprovades, com bloqueig de l'exfiltració en curs, quarantena del document i notificació immediata a l'usuari afectat i al gestor de dades responsable.

REQ-TCN-204. Preservació d'evidències de dades: el servei haurà de recopilar i custodiar un paquet mínim d'evidències tècniques de dades compromeses (còpies de fitxers sospitosos, registres de transferència, captures de metadades) per facilitar la investigació forense posterior.

REQ-TCN-205. Informes ampliats de seguretat de dades: el servei haurà de generar informes que incloguin incidents d'exfiltració encoberta detectats, accions de resposta aplicades, evidències preservades i recomanacions de millora.

REQ-TCN-206. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per incorporar fonts i mecanismes de seguretat de dades emergents, com solucions natives de protecció en entorns SaaS avançats o eines d'observabilitat de dades en temps real.

Activitats a realitzar per part de l'adjudicatari

- Correlacionar els moviments de dades entre orígens i destins diversos (usuari, dispositiu, aplicació, núvol).
- Detectar intents d'exfiltració encoberta mitjançant compressió, fragmentació o ofuscació.

- Executar accions de resposta inicial i enviar notificacions als usuaris i gestors de dades afectats.
- Preservar i custodiar evidències mínimes de dades compromeses per investigació forense.
- Elaborar informes ampliats amb incidents, accions i recomanacions específiques.

Resultats esperats

- Capacitat de detectar intents avançats d'exfiltració encoberta de dades.
- Correlació contextual d'origen i destí que permeti entendre millor els incidents.
- Resposta inicial efectiva i notificació immediata a les parts afectades.
- Disponibilitat d'evidències mínimes per a investigacions forenses de dades.
- Informes ampliats que orientin la millora contínua de la protecció de la informació.
- Preparació per evolucionar cap al nivell òptim (P19-C), amb governança integrada i resposta automatitzada.

4.1.25 Paquet P19-C – Monitoratge i detecció d'incidents a informació i dades (nivell òptim)

El paquet P19-C té per objectiu assolir un nivell òptim de monitoratge d'alertes, detecció d'incidents i resposta en horari 24x7 sobre la informació i les dades corporatives, establint capacitats proactives de *hunting*, validació contínua i governança integrada. Aquest nivell garanteix que l'Ajuntament pugui anticipar-se a compromisos avançats, validar periòdicament l'eficàcia de les regles de protecció de dades i establir recomanacions de governança que reforcin la seguretat de la informació.

Aquest paquet incorpora tots els requisits establerts en el P19-B i els amplia amb les següents funcionalitats:

REQ-TCN-207. Caça d'amenaces (Threat Hunting) de dades: el servei haurà de dur a terme activitats recurrents de cerca proactiva de riscos en la informació, incloent la detecció de cadenes sensibles (números de targetes, identificadors personals, dades confidencials) i patrons d'ús inusuals de documents.

REQ-TCN-208. Validació contínua de regles DLP: el servei haurà de comprovar de manera periòdica l'eficàcia de les regles de prevenció de pèrdua de dades (DLP), mitjançant exercicis controlats que permetin identificar llacunes i ajustar configuracions.

REQ-TCN-209. Anàlisi de causa arrel automatitzada (RCA): el servei haurà de reconstruir de manera semi o totalment automatitzada la traçabilitat d'un incident de dades, des de la informació compromesa fins a l'actor implicat, identificant el vector i les conseqüències.

REQ-TCN-210. Recomanacions de governança de dades: el servei haurà de generar recomanacions específiques per reforçar la governança de la informació, incloent re-etiquetatge de documents, segregació de conjunts de dades i millora de les polítiques de classificació.

REQ-TCN-211. Informes de maduresa i millora contínua: el servei haurà de generar informes que integrin resultats de hunting, validacions de regles, RCA i recomanacions de governança, establint fulls de ruta per a l'evolució del control de dades.

REQ-TCN-212. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per incorporar fonts i mecanismes de seguretat de dades emergents, com eines d'observabilitat en temps real, tecnologies de *data lineage* o plataformes d'IA aplicada a la governança de dades.

Activitats a realitzar per part de l'adjudicatari

- Dur a terme hunting actiu per detectar dades sensibles i patrons d'ús inusuals.
- Realitzar validacions periòdiques de les regles DLP i ajustar-les segons els resultats.
- Reconstruir incidents de dades mitjançant RCA automatitzada.
- Proposar recomanacions de governança per millorar classificació, etiquetatge i segregació.
- Elaborar informes executius i tècnics amb resultats i fulls de ruta de millora contínua.

Resultats esperats

- Capacitat d'anticipar-se a compromisos avançats mitjançant *hunting* específic de dades.
- Confirmació recurrent de l'eficàcia de les regles de protecció i detecció de pèrdua de dades.
- Traçabilitat completa dels incidents des de la dada afectada fins a l'actor responsable.
- Reforç de la governança mitjançant recomanacions de re-etiquetatge i segregació.
- Evolució constant del model de protecció i governança de dades municipals.

4.1.26 Paquet P20-A – Monitoratge i detecció d'incidents a correu i col·laboració (nivell inicial)

El paquet P20-A té per objectiu establir un servei bàsic de monitoratge d'alertes i detecció d'incidents en horari 24x7 sobre els canals de correu electrònic i les plataformes de col·laboració corporativa, que són vectors habituals d'atac. Aquest nivell inicial permet identificar intents elementals de correu brossa i programari maliciós, i aplicar mesures bàsiques de contenció per reduir riscos de compromís.

El paràmetre quantificador d'aquest servei serà el número d'usuaris interns de l'entitat contractant objecte del servei.

El paquet P20 inclou el llicenciament i els serveis d'administració i operació de les solucions SIEMaaS i SOARaaS integrant les solucions de protecció del servei de correu i dels entorns de col·laboració (de forma descriptiva però no limitativa: Email and Collaboration Security Platforms, etc), així com de la resta de solucions (Threat Hunting, BAS, Threat Intel, etc) necessàries per prestar el servei.

Tanmateix, el paquet P20 no inclou el llicenciament de les solucions de protecció del servei de correu i dels entorns de col·laboració.

Funcionalitats que ha de suportar el servei

REQ-TCN-213. Ingesta d'alertes de correu i col·laboració: el servei haurà d'incorporar i normalitzar alertes de plataformes de correu electrònic i de col·laboració (servidors de correu, suites ofimàtiques en núvol, xats corporatius).

REQ-TCN-214. Detecció bàsica de correu maliciós: el servei haurà de detectar i reportar intents de *spam*, adjunts amb programari maliciós conegut i enllaços a llocs maliciosos simples.

REQ-TCN-215. Contenció inicial: el servei haurà de poder sol·licitar o executar accions predefinides com bloquejar l'entrega de correus sospitosos, posar-los en quarantena o eliminar fitxers adjunts maliciosos.

REQ-TCN-216. Supervisió de plataformes de col·laboració: el servei haurà de revisar activitats bàsiques en canals de col·laboració (pujada de fitxers, enllaços compartits) per identificar intents evidents de distribució de programari maliciós.

REQ-TCN-217. Informes periòdics: el servei haurà de generar informes tècnics i executius amb el resum de correus bloquejats, incidents detectats i recomanacions bàsiques.

REQ-TCN-218. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per integrar fonts d'alerta de noves eines de col·laboració i canals de comunicació emergents.

Activitats a realitzar per part de l'adjudicatari

- Configurar i posar en marxa la ingesta d'alertes de correu i col·laboració.
- Definir i mantenir casos d'ús bàsics contra *spam* i programari maliciós conegut.
- Executar o sol·licitar accions de contenció inicial prèviament aprovades.
- Revisar i classificar les alertes, escalant-les quan sigui necessari.
- Elaborar informes periòdics diferenciats per a responsables tècnics i executius.

Resultats esperats

- Visibilitat mínima sobre intents de correu brossa i fitxers maliciosos en canals de col·laboració.
- Capacitat de detectar i contenir amenaces bàsiques de correu electrònic i col·laboració.
- Informes periòdics amb informació accionable per als responsables municipals.
- Preparació per evolucionar cap al nivell avançat (P20-B), amb detecció de suplantacions i anàlisi més sofisticada d'adjunts.

4.1.27 Paquet P20-B – Monitoratge i detecció d'incidents a correu i col·laboració (nivell òptim)

El paquet P20-B té per objectiu proporcionar un nivell avançat de monitoratge d'alertes, detecció d'incidents i resposta inicial en horari 24x7 sobre les plataformes de correu electrònic i col·laboració, ampliant les capacitats bàsiques amb deteccions contextuals i mecanismes per identificar suplantacions, adjunts avançats i vectors d'atac complexos. Aquest nivell permet protegir l'Ajuntament davant campanyes de phishing dirigides (*spear phishing*), abús de canals legítims i atacs híbrids que combinen enginyeria social i tècniques avançades d'evasió.

Aquest paquet incorpora tots els requisits establerts en el P20-A i els amplia amb les següents funcionalitats:

REQ-TCN-219. Detecció avançada de suplantació (BEC/DMARC): el servei haurà d'identificar intents de *Business Email Compromise* (BEC), anomalies en els registres SPF/DKIM/DMARC i tècniques de *lookalike domains* orientades a enganyar els usuaris.

REQ-TCN-220. Anàlisi d'adjunts complexos: el servei haurà d'integrar mecanismes per a la detonació de fitxers en *sandboxes* avançades, inspecció de macros ofuscades i desxifrat de fitxers protegits per contrasenya quan hi hagi indicadors de risc.

REQ-TCN-221. Correlació amb identitat i comportament: el servei haurà de relacionar esdeveniments de correu i col·laboració amb el perfil d'usuari (horaris habituals, patrons d'accés, dispositius associats) per detectar anomalies com enviaments massius des de comptes compromesos.

REQ-TCN-222. Casos d'ús avançats en col·laboració: el servei haurà de detectar intents de distribució de programari maliciós en canals corporatius (Teams, SharePoint, OneDrive, etc.), incloent pujada de fitxers encriptats sospitosos, enllaços interns maliciosos o abús de connectors externs.

REQ-TCN-223. Resposta inicial sobre incidents de correu: el servei haurà de poder executar accions de contenció com bloqueig dinàmic de dominis i remitents, revocació d'enviaments interns, quarantena massiva de missatges i bloqueig d'adjunts en flux.

REQ-TCN-224. Preservació d'evidències: el servei haurà de recopilar automàticament *headers* complets, cadenes d'autenticació, còpies de missatges i *payloads* per suportar la investigació forense i la traçabilitat d'incidents.

REQ-TCN-225. Informes ampliats: el servei haurà de generar informes que incloguin deteccions de suplantació, adjunts analitzats, correlació amb comptes d'usuari i recomanacions de reforç de polítiques (p. ex., ajustos DMARC).

REQ-TCN-226. Adaptabilitat a noves amenaces: el servei haurà de ser capaç d'incorporar deteccions per tècniques emergents, com *consent phishing*, abús de tokens OAuth i *app integrations* malicioses en plataformes SaaS.

Activitats a realitzar per part de l'adjudicatari

- Integrar fonts de detecció avançades contra BEC i anomalies de domini.
- Analitzar adjunts sospitosos en *sandboxes* i entorns controlats.
- Correlacionar alertes de correu amb identitat i comportament d'usuaris.
- Detectar anomalies i vectors maliciosos en plataformes de col·laboració.
- Executar accions de contenció inicial ràpida (bloqueig/quarantena/rollback).
- Preservar evidències tècniques per a investigació i traçabilitat.

- Elaborar informes executius i tècnics amb resultats i recomanacions.

Resultats esperats

- Capacitat de detectar i contenir intents avançats de suplantació i *spear phishing*.
- Major precisió en la detecció gràcies a la correlació amb identitat i comportament.
- Contenció ràpida i coordinada de campanyes de correu maliciós.
- Evidències completes disponibles per a investigacions forenses i legals.
- Evolució natural cap al nivell òptim (P20-C), amb resposta automatitzada i protecció integral contra usurpació de dominis i perfils corporatius.

4.1.28 Paquet P20-C – Monitoratge i detecció d'incidents a correu i col·laboració (nivell òptim)

El paquet P20-C té per objectiu assolir un nivell òptim de monitoratge d'alertes, detecció d'incidents i resposta en horari 24x7 sobre les plataformes de correu electrònic i col·laboració, establint capacitats d'automatització completa, *hunting* avançat i protecció de la identitat digital corporativa. Aquest nivell permet anticipar-se a campanyes sofisticades de phishing, reduir dràsticament el temps de resposta i reforçar la confiança en els canals oficials de comunicació de l'Ajuntament.

Aquest paquet incorpora tots els requisits establerts en el P20-B i els amplia amb les següents funcionalitats:

REQ-TCN-227. Resposta automàtica end-to-end: el servei haurà d'automatitzar completament les accions de contenció i resposta davant incidents de correu i col·laboració, incloent quarantena massiva, revocació d'enviaments interns, eliminació d'adjunts en flux i bloqueig dinàmic de dominis o remitents.

REQ-TCN-228. Caça d'amenaces (Threat Hunting) en canals de correu i col·laboració: el servei haurà de dur a terme activitats recurrents de *hunting* per detectar dominis nous registrats per a suplantació, perfils corporatius falsos i intents de *account takeover* no detectats per alertes tradicionals.

REQ-TCN-229. Validació contínua de deteccions (BAS de phishing): el servei haurà de simular de manera periòdica campanyes de phishing i *consent phishing* controlades, per validar l'eficàcia dels mecanismes de detecció i resposta automàtica.

REQ-TCN-230. Protecció contra usurpació de dominis i marques: el servei haurà de monitorar dominis similars (*typosquatting*, *lookalike*), perfils fraudulents a xarxes socials i intents d'apropiació d'imatge corporativa, establint alertes i respostes coordinades.

REQ-TCN-231. RCA automatitzada en incidents de correu: el servei haurà de reconstruir de manera semi o totalment automatitzada la cadena de l'atac (des del correu inicial fins a la interacció de l'usuari) i generar informes amb les lliçons apreses.

REQ-TCN-232. Recomanacions de polítiques avançades: el servei haurà de proposar ajustos continus en polítiques de DMARC, SPF, DKIM, així com en configuracions de plataformes de col·laboració per reforçar la resiliència davant noves tècniques.

Activitats a realitzar per part de l'adjudicatari

- Configurar i mantenir playbooks d'automatització per a resposta completa end-to-end.
- Realitzar *hunting* actiu de dominis similars i perfils falsos a internet.
- Executar simulacions de phishing controlades com a part de la validació contínua.
- Monitorar i escalar incidents d'usurpació de dominis i perfils corporatius.
- Generar informes de RCA i recomanacions de millora contínua.

Resultats esperats

- Reducció significativa del temps de resposta gràcies a l'automatització completa.
- Capacitat d'identificar proactivament campanyes de phishing i intents d'usurpació abans que afectin els usuaris.
- Confirmació recurrent de l'eficàcia dels controls de seguretat mitjançant BAS de phishing.
- Protecció reforçada de la identitat digital de l'Ajuntament contra dominis fraudulents i perfils falsos.
- Evolució constant de les polítiques i configuracions de seguretat en correu i col·laboració.

4.1.29 Paquet P21-A – Monitoratge i detecció d'incidents a xarxes i serveis de telecomunicacions (nivell inicial)

El paquet P21-A té per objectiu establir un servei bàsic de monitoratge d'alertes i detecció d'incidents en horari 24x7 sobre les infraestructures de xarxa i comunicacions municipals, incloent els elements que donen suport a la connectivitat interna i externa. Aquest nivell inicial proporciona visibilitat sobre esdeveniments i anomalies bàsiques de la xarxa, assegurant que les alertes essencials siguin centralitzades i gestionades de manera adequada.

El paràmetre quantificador d'aquest servei serà el número d'usuaris interns de l'entitat contractant objecte del servei.

El paquet P21 inclou el llicenciament i els serveis d'administració i operació de les solucions SIEMaaS i SOARaaS integrant les solucions de protecció de les xarxes i dels serveis de telecomunicacions (de forma descriptiva però no limitativa: NGFW, IDS/IPS, DDI, NDR, NAC, etc) de que disposi l'entitat contractant, així com la resta de solucions (Threat Hunting, BAS, Threat Intel, etc) necessàries per prestar el servei.

Tanmateix, el paquet P21 no inclou el llicenciament de les solucions de protecció de les xarxes i dels serveis de telecomunicacions.

Funcionalitats que ha de suportar el servei

REQ-TCN-233. Monitoratge d'elements de xarxa: el servei haurà d'incorporar i supervisar les alertes i esdeveniments generats per tallafocs de nova generació (NGFW), sistemes de prevenció d'intrusions (IDP/IPS), detecció i prevenció d'amenaces avançades (Threat Prevention) i plataformes de detecció de trànsit de xarxa (NDR), plataformes DDI (DNS, DHCP, IPAM).

REQ-TCN-234. Casos d'ús deterministes de xarxa: el servei haurà de detectar activitats bàsiques com comunicacions amb servidors de comandament i control (C2), consultes DNS sospitoses, intents d'escaneig de xarxa i exfiltració elemental de dades.

REQ-TCN-235. Contenció remota pre-aprovada: el servei haurà de poder sol·licitar o executar accions de contenció prèviament acordades, com el bloqueig d'adreces IP, dominis, URL o ports concrets identificats com a maliciosos.

REQ-TCN-236. Classificació i triatge inicial: el servei haurà de revisar i classificar les alertes rebudes segons el seu nivell de gravetat, establint criteris d'escalat al procés de gestió d'incidents quan sigui necessari.

REQ-TCN-237. Informes periòdics de xarxa: el servei haurà de generar informes amb un resum d'incidents detectats, tendències observades i recomanacions bàsiques de millora en la configuració i ús de la xarxa.

REQ-TCN-238. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per integrar fonts d'alerta de tecnologies de xarxa emergents, com solucions de seguretat en entorns SD-WAN o serveis de connectivitat basats en núvol.

Activitats a realitzar per part de l'adjudicatari

- Configurar i posar en marxa la recollida d'alertes i esdeveniments dels dispositius de xarxa.
- Definir i mantenir casos d'ús deterministes per a detecció de C2, DNS sospitós, escaneig i exfiltració bàsica.
- Executar o sol·licitar accions de contenció remota bàsiques prèviament aprovades.
- Revisar i classificar alertes segons la seva gravetat, amb escalat quan correspongui.
- Elaborar informes periòdics diferenciats per a responsables tècnics i executius.

Resultats esperats

- Visibilitat mínima sobre l'activitat i l'estat de seguretat de les infraestructures de xarxa i comunicacions.
- Capacitat de detectar i notificar anomalies bàsiques de trànsit i intents d'accés maliciós.
- Possibilitat d'aplicar accions de contenció bàsiques com el bloqueig d'IP, dominis o ports.
- Informes periòdics que permetin prendre decisions de millora en la gestió i configuració de la xarxa.
- Establiment d'una línia de base sòlida per evolucionar cap al nivell avançat (P7-B).

4.1.30 Paquet P21-B – Monitoratge i detecció d'incidents a xarxes i comunicacions (nivell avançat)

El paquet P21-B té per objectiu proporcionar un nivell avançat de monitoratge d'alertes, detecció d'incidents i resposta inicial en horari 24x7 sobre les infraestructures de xarxa i

comunicacions municipals, ampliant les capacitats establertes al nivell bàsic. Aquest nivell introdueix la detecció d'anomalies complexes en el trànsit, la correlació amb altres dominis i la capacitat de contenció segmentada per reduir l'impacte d'un incident abans que afecti serveis crítics.

Aquest paquet incorpora tots els requisits establerts en el P21-A i els amplia amb les següents funcionalitats:

REQ-TCN-239. Detecció d'anomalies de flux i lateralitat: el servei haurà de ser capaç d'identificar patrons de trànsit inusuals, moviments laterals i comunicacions internes sospitoses que indiquin compromisos més sofisticats.

REQ-TCN-240. Correlació amb identitat i endpoints: el servei haurà de relacionar esdeveniments de xarxa amb informació d'identitat d'usuaris i activitat d'ordinadors/dispositius per detectar comportaments anòmals contextualitzats.

REQ-TCN-241. Contenció segmentada: el servei haurà de poder aplicar o sol·licitar accions de contenció més precises, com ara l'ús de llistes de control d'accés (ACLs) dinàmiques o regles temporals de bloqueig, amb l'objectiu de limitar l'impacte sense interrompre serveis essencials.

REQ-TCN-242. Coordinació en resposta a atacs DDoS: el servei haurà de coordinar amb els proveïdors i els equips d'operació municipals la resposta davant atacs de denegació de servei distribuïda (DDoS), assegurant l'activació de mecanismes de mitigació adequats.

REQ-TCN-243. Informes ampliats de xarxa: el servei haurà de generar informes que incloguin descripcions d'anomalies detectades, correlacions amb altres dominis, mesures de contenció aplicades i recomanacions específiques de millora.

REQ-TCN-244. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per integrar fonts d'alerta i mecanismes de resposta de noves tecnologies de xarxa avançada (per exemple, SDN, 5G privades o serveis de xarxa gestionada).

Activitats a realitzar per part de l'adjudicatari

- Analitzar el trànsit de xarxa per detectar anomalies de flux i moviments laterals.
- Correlacionar els esdeveniments de xarxa amb informació d'identitat i dispositius.

- Executar o sol·licitar mesures de contenció segmentada mitjançant ACLs o llistes de bloqueig dinàmiques.
- Coordinar amb proveïdors i operacions la resposta davant atacs DDoS.
- Elaborar informes detallats amb incidents detectats, accions aplicades i recomanacions de millora.

Resultats esperats

- Capacitat de detectar compromisos més sofisticats mitjançant anàlisi de flux i lateralitat.
- Major precisió en la detecció gràcies a la correlació amb identitat i dispositius.
- Possibilitat de contenir incidents limitant l'impacte sobre serveis essencials mitjançant contenció segmentada.
- Coordinació eficaç davant atacs DDoS amb els proveïdors i operacions municipals.
- Informes ampliats que permetin millorar contínuament la seguretat de la xarxa.
- Preparació per evolucionar cap al nivell òptim (P21-C), amb capacitats de hunting i validació contínua.

4.1.31 Paquet P21-C – Monitoratge i detecció d'incidents a xarxes i comunicacions (nivell òptim)

El paquet P21-C té per objectiu assolir un nivell òptim de monitoratge d'alertes, detecció d'incidents i resposta en horari 24x7 sobre les infraestructures de xarxa i comunicacions municipals, establint capacitats de hunting, validació contínua i millora permanent dels mecanismes de detecció i resposta. Aquest nivell permet anticipar-se a compromisos avançats, verificar l'eficàcia dels controls i adaptar-los contínuament a noves tècniques d'atac.

Aquest paquet incorpora tots els requisits establerts en el P21-B i els amplia amb les següents funcionalitats:

REQ-TCN-245. Caça d'amenaces (Threat Hunting) de xarxa: el servei haurà de dur a terme activitats proactives i recurrents de cerca d'indicadors de compromís en la xarxa, incloent la detecció de beacons, canals encoberts i tècniques basades en l'ús d'eines legítimes (living-off-the-land).

REQ-TCN-246. Validació contínua de deteccions de xarxa (BAS): el servei haurà de realitzar simulacions controlades d'atacs de comandament i control (C2) i exfiltració de dades per comprovar l'eficàcia dels mecanismes de detecció, anàlisi i contenció implementats.

REQ-TCN-247. Anàlisi de causa arrel (RCA) automatitzada: el servei haurà de reconstruir de manera semi o totalment automatitzada el camí d'atac en incidents de xarxa, identificant l'origen, la propagació i l'impacte sobre els serveis municipals afectats.

REQ-TCN-248. Millora contínua de casos d'ús: el servei haurà de revisar i optimitzar de manera periòdica els casos de detecció de xarxa, ajustant els llindars de sensibilitat i incorporant noves regles per reduir falsos positius i millorar la velocitat de detecció.

REQ-TCN-249. Informes de maduresa i millora contínua: el servei haurà de generar informes amb resultats de hunting, validació i RCA, així com recomanacions concretes per a l'evolució del servei de seguretat de xarxa.

REQ-TCN-250. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per incorporar deteccions i respostes en tecnologies de xarxa emergents com SDN, xarxes 5G privades o arquitectures basades en SASE.

Activitats a realitzar per part de l'adjudicatari

- Dur a terme hunting actiu en la xarxa amb cerca de beacons i canals encoberts.
- Executar proves periòdiques de detecció mitjançant simulacions de C2 i exfiltració.
- Reconstruir el camí d'atac mitjançant anàlisi de causa arrel automatitzada.
- Revisar i ajustar els casos d'ús i llindars de detecció de manera contínua.
- Elaborar informes executius i tècnics amb resultats de hunting, validació i recomanacions de millora.

Resultats esperats

- Capacitat d'anticipar-se a compromisos avançats mitjançant hunting de xarxa.
- Confirmació periòdica de l'eficàcia dels mecanismes de detecció, anàlisi i contenció.
- Major precisió en la detecció gràcies a l'anàlisi automatitzada del camí d'atac.
- Reducció de falsos positius i millora del temps de detecció gràcies a l'ajust continuat de llindars.
- Informes de maduresa que orientin l'evolució de la seguretat de xarxa.
- Flexibilitat per incorporar noves tecnologies i arquitectures de comunicació.

4.1.32 Paquet P22-A – Monitoratge i detecció d'incidents a aplicacions i APIs (nivell inicial)

El paquet P22-A té per objectiu establir un servei bàsic de monitoratge d'alertes i detecció d'incidents en horari 24x7 sobre les aplicacions corporatives municipals, especialment aquelles que donen suport a serveis digitals i portals ciutadans. Aquest nivell inicial proporciona visibilitat sobre vulnerabilitats i intents d'explotació comuns, així com capacitat de contenció bàsica davant incidents que puguin comprometre la disponibilitat o integritat de les aplicacions.

El paràmetre quantificador d'aquest servei serà el número d'aplicacions de l'entitat contractant objecte del servei.

El paquet P22 inclou el llicenciament i els serveis d'administració i operació de les solucions SIEMaaS i SOARaaS integrant les solucions de protecció de les aplicacions i APIs (solucions per publicar i equilibrar la càrrega d'aplicacions, AntiDDoS, WAF, WAAP, etc) de que disposi l'entitat contractant, així com la resta de solucions (Threat Hunting, BAS, Threat Intel, etc) necessàries per prestar el servei.

Tanmateix, el paquet P22 no inclou el llicenciament de les solucions de protecció les aplicacions i les APIs (interfícies de programació d'aplicacions).

Funcionalitats que ha de suportar el servei

REQ-TCN-251. Ingesta d'alertes d'aplicació: el servei haurà d'incorporar i normalitzar els esdeveniments i alertes generades per tallafocs d'aplicació web (WAF), solucions de protecció avançada d'aplicacions web i APIs (WAAP), controladors de distribució d'aplicacions (ADC) i plataformes d'integració o gestió centralitzada d'aplicacions (iCM).

REQ-TCN-252. Detecció d'explotacions comunes: el servei haurà de detectar intents d'explotació de vulnerabilitats habituals en aplicacions web, com injeccions de codi SQL (SQLi), scripts entre llocs (XSS), o bypass d'autenticació.

REQ-TCN-253. Canvis de configuració no autoritzats: el servei haurà de supervisar i identificar modificacions inesperades o no aprovades en la configuració de les aplicacions o dels components que les protegeixen.

REQ-TCN-254. Contenció bàsica d'incidents: el servei haurà de poder aplicar o sol·licitar accions remotes bàsiques prèviament aprovades, com el bloqueig d'una regla o signatura concreta, o la creació d'una regla temporal per interrompre un atac en curs.

REQ-TCN-255. Classificació i triatge inicial: el servei haurà de revisar i classificar les alertes rebudes, establint-ne la gravetat i escalant-les al procés de gestió d'incidents quan correspongui.

REQ-TCN-256. Informes periòdics: el servei haurà de generar informes tècnics i executius amb el resum d'aplicacions monitorades, incidents detectats i recomanacions bàsiques de millora.

REQ-TCN-257. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per integrar alertes i capacitats de seguretat d'aplicacions emergents, com serveis nadius de protecció en entorns de contenidors o plataformes de microserveis.

Activitats a realitzar per part de l'adjudicatari

- Configurar i posar en marxa la recollida d'esdeveniments de WAF, WAAP, ADC i altres plataformes d'aplicació.
- Definir i mantenir casos d'ús per a l'explotació de vulnerabilitats comunes.
- Supervisar i identificar canvis no autoritzats en configuracions d'aplicació.
- Executar o sol·licitar accions de contenció bàsica prèviament aprovades.
- Revisar i classificar les alertes generades, amb escalat al procés de gestió d'incidents quan sigui necessari.
- Elaborar informes periòdics diferenciats per a responsables tècnics i executius.

Resultats esperats

- Visibilitat mínima sobre els intents d'explotació i estat de seguretat de les aplicacions corporatives.
- Capacitat de detectar i contenir de manera bàsica atacs habituals com SQLi, XSS o bypass d'autenticació.
- Integració de les aplicacions dins del procés central de monitoratge i resposta.
- Informes periòdics amb informació accionable per a tècnics i directius.
- Preparació per evolucionar cap al nivell avançat (P8-B), amb correlació i deteccions contextuals.

4.1.33 Paquet P22-B – Monitoratge i detecció d'incidents a aplicacions i APIs (nivell avançat)

El paquet P22-B té per objectiu proporcionar un nivell avançat de monitoratge d'alertes, detecció d'incidents i resposta inicial en horari 24x7 sobre les aplicacions corporatives, ampliant les capacitats establertes al nivell bàsic. Aquest nivell permet detectar usos anòmals i compromisos més sofisticats, correlacionant esdeveniments amb vulnerabilitats conegudes i integrant-se amb els equips de desenvolupament per aplicar mesures de contenció o correcció ràpida.

Aquest paquet incorpora tots els requisits establerts en el P22-A i els amplia amb les següents funcionalitats:

REQ-TCN-258. Correlació amb vulnerabilitats conegudes: el servei haurà de relacionar les alertes i esdeveniments d'aplicació amb la informació disponible sobre vulnerabilitats documentades, establint prioritats en funció de la seva gravetat i exposició.

REQ-TCN-259. Correlació amb registres d'aplicació: el servei haurà d'integrar i analitzar els registres interns de les aplicacions (logs d'ús i errors) per detectar anomalies vinculades a patrons de compromís.

REQ-TCN-260. Detecció d'anomalies d'ús: el servei haurà d'identificar patrons d'ús anormals, com abusos lògics de funcionalitats, volums de peticions inusuals o accions repetitives que puguin indicar un atac.

REQ-TCN-261. Coordinació amb equips de desenvolupament: el servei haurà de disposar de mecanismes de coordinació amb els equips de desenvolupament per aplicar mesures de contenció, hotfix o rollback de canvis quan sigui necessari per resoldre incidents.

REQ-TCN-262. Preservació d'evidències: el servei haurà de recopilar i custodiar les evidències bàsiques generades en incidents d'aplicació (fitxers de registre, peticions sospitoses, captures de trànsit) per garantir la seva disponibilitat en futures investigacions.

REQ-TCN-263. Informes ampliats: el servei haurà de generar informes que descriguin anomalies d'ús detectades, correlacions amb vulnerabilitats, mesures de contenció adoptades i recomanacions de millora.

REQ-TCN-264. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per integrar fonts d'alerta i mecanismes de resposta d'entorns emergents com aplicacions en contenidors, microserveis o serveis natius de núvol.

Activitats a realitzar per part de l'adjudicatari

- Correlacionar esdeveniments d'aplicació amb vulnerabilitats conegudes i registres interns.
- Detectar anomalies d'ús vinculades a abusos lògics o volumetria sospitosa.
- Coordinar amb els equips de desenvolupament l'aplicació de mesures de contenció, hotfix o rollback.
- Preservar evidències tècniques per a la investigació d'incidents.
- Elaborar informes ampliats amb descripció d'incidents, accions aplicades i recomanacions específiques.

Resultats esperats

- Capacitat de detectar compromisos més sofisticats a les aplicacions municipals.
- Major precisió en la detecció gràcies a la correlació amb vulnerabilitats i registres interns.
- Coordinació eficient amb equips de desenvolupament per aplicar respostes ràpides i segures.
- Disponibilitat d'evidències per donar suport a investigacions i processos judicials si escau.
- Informes ampliats que facilitin la millora contínua de la seguretat de les aplicacions.
- Preparació per evolucionar cap al nivell òptim (P22-C), amb hunting i integració DevSecOps.

4.1.34 Paquet P22-C – Monitoratge i detecció d'incidents a aplicacions i APIs (nivell òptim)

El paquet P22-C té per objectiu assolir un nivell òptim de monitoratge d'alertes, detecció d'incidents i resposta en horari 24x7 sobre les aplicacions corporatives municipals, establint capacitats proactives de *threat hunting*, validació contínua i integració plena en els fluxos de desenvolupament segur (DevSecOps). Aquest nivell permet anticipar-se a compromisos avançats, assegurar la qualitat de les deteccions i integrar la gestió d'incidents dins el cicle de vida del programari.

Aquest paquet incorpora tots els requisits establerts en el P22-B i els amplia amb les següents funcionalitats:

REQ-TCN-265. Caça d'amenaces (Threat hunting) d'aplicació: el servei haurà de dur a terme activitats recurrents de cerca proactiva d'indicadors de compromís i patrons d'abús lògic en les aplicacions, fins i tot quan no hi hagi alertes prèvies.

REQ-TCN-266. Validació contínua de deteccions amb BAS a capa 7: el servei haurà de posar a prova de manera periòdica els mecanismes de detecció mitjançant simulacions controlades d'atacs en aplicacions web (injeccions, exfiltració, abús de funcionalitats), comprovant-ne l'eficàcia.

REQ-TCN-267. Anàlisi de causa arrel automatitzada "request-to-code": el servei haurà de poder reconstruir de manera semi o totalment automatitzada el recorregut complet d'un incident, des de la petició maliciosa fins a la línia de codi afectada, per agilitzar la resposta i la correcció.

REQ-TCN-268. Integració amb DevSecOps: el servei haurà d'establir criteris d'entrada i sortida d'incidents dins el flux de desenvolupament i operació, de manera que qualsevol vulnerabilitat o compromís detectat quedi gestionat i resolt com a part del cicle de vida del programari.

REQ-TCN-269. Informes de maduresa i millora contínua: el servei haurà de generar informes que recullin els resultats del hunting, validacions i RCA, així com recomanacions concretes per evolucionar la seguretat de les aplicacions.

REQ-TCN-270. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per integrar deteccions i respostes en arquitectures emergents d'aplicacions, com microserveis, *serverless* o entorns de baixa codi (*low-code/no-code*).

Activitats a realitzar per part de l'adjudicatari

- Dur a terme *hunting* actiu per identificar patrons d'abús lògic en aplicacions.
- Realitzar validacions periòdiques mitjançant simulacions de BAS a capa 7.
- Reconstruir incidents complexos mitjançant anàlisi de causa arrel "request-to-code".
- Integrar la gestió d'incidents dins els fluxos DevSecOps municipals.
- Elaborar informes executius i tècnics amb resultats i recomanacions de millora contínua.

Resultats esperats

- Capacitat d'anticipar-se a compromisos avançats en aplicacions municipals.
- Confirmació recurrent de l'eficàcia de les deteccions gràcies a exercicis BAS.
- Disponibilitat d'anàlisis de causa arrel que vinculin peticions malicioses amb codi font.
- Integració plena de la seguretat i la resposta d'incidents en els processos de desenvolupament i operació.
- Evolució constant de la seguretat d'aplicacions mitjançant lliçons apreses i noves capacitats tecnològiques.

4.1.35 Paquet P23-A – Monitoratge i detecció d'incidents a entorns al núvol (nivell inicial)

El paquet P23-A té per objectiu establir un servei bàsic de monitoratge d'alertes i detecció d'incidents en horari 24x7 sobre els serveis al núvol utilitzats per l'Ajuntament i les entitats dependents, tant en entorns públics com híbrids. Aquest nivell inicial proporciona visibilitat sobre configuracions de seguretat essencials i incidents elementals que poden comprometre la disponibilitat o confidencialitat de la informació allotjada en el núvol.

El paràmetre quantificador d'aquest servei serà el número de càrregues de treball al núvol de l'entitat contractant objecte del servei.

El paquet P23 inclou el llicenciament i els serveis d'administració i operació de les solucions SIEMaaS i SOARaaS integrant les solucions de protecció d'entorns i serveis al núvol (CNAPP, CSPM, CWPP, CIEM, IaS Scanning, etc) de que disposi l'entitat contractant, així com la resta de solucions (Threat Hunting, BAS, Threat Intel, etc) necessàries per prestar el servei.

Tanmateix, el paquet P23 no inclou el llicenciament de les solucions de protecció d'entorns i serveis al núvol.

Funcionalitats que ha de suportar el servei

REQ-TCN-271. Ingesta d'alertes de serveis al núvol: el servei haurà d'incorporar i normalitzar les alertes generades per plataformes de seguretat específiques per al núvol, incloent eines de broker de seguretat d'aplicacions al núvol (CASB), plataformes de gestió de configuracions de seguretat (CSPM) i serveis nadius dels proveïdors de núvol.

REQ-TCN-272. Casos d'ús bàsics en entorns de núvol: el servei haurà de detectar situacions elementals de risc, com l'exposició de claus o credencials, la presència de contenidors o buckets oberts, i sessions d'usuari amb activitat sospitosa.

REQ-TCN-273. Remediació remota pre-aprovada: el servei haurà de poder executar o sol·licitar accions prèviament acordades de contenció i remediació bàsica, com revocar un token d'autenticació, tancar una sessió sospitosa o rotar claus compromeses.

REQ-TCN-274. Classificació i triatge inicial: el servei haurà de revisar i classificar les alertes rebudes segons la seva gravetat, establint criteris d'escalat al procés de gestió d'incidents quan sigui necessari.

REQ-TCN-275. Informes periòdics de seguretat al núvol: el servei haurà de generar informes tècnics i executius amb el resum de serveis monitorats, incidents detectats i recomanacions bàsiques de millora.

REQ-TCN-276. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per integrar alertes de noves tecnologies de seguretat al núvol que puguin sorgir en el futur, com eines de monitoratge específiques per a microserveis o plataformes sense servidor (*serverless*).

Activitats a realitzar per part de l'adjudicatari

- Configurar i posar en marxa la ingesta d'alertes de CASB, CSPM i serveis nadius de proveïdors de núvol.
- Definir i mantenir casos d'ús bàsics per a la detecció de claus exposades, buckets oberts i sessions sospitoses.
- Executar o sol·licitar accions de remediació remota bàsiques prèviament aprovades.
- Revisar i classificar les alertes generades, amb escalat al procés de gestió d'incidents quan correspongui.
- Elaborar informes periòdics diferenciats per a responsables tècnics i executius.

Resultats esperats

- Visibilitat mínima sobre la seguretat dels serveis al núvol municipals.
- Capacitat de detectar i notificar incidents elementals com claus exposades, recursos oberts i sessions sospitoses.
- Possibilitat d'aplicar mesures de contenció i remediació bàsiques de forma remota.
- Informes periòdics que facilitin la millora contínua de la seguretat al núvol.
- Preparació per evolucionar cap al nivell avançat (P23-B), amb correlació i deteccions contextuals més sofisticades.

4.1.36 Paquet P23-B – Monitoratge i detecció d'incidents a serveis al núvol (nivell avançat)

El paquet P23-B té per objectiu proporcionar un nivell avançat de monitoratge d'alertes, detecció d'incidents i resposta inicial en horari 24x7 sobre els serveis al núvol, ampliant les capacitats establertes al nivell bàsic. Aquest nivell introdueix la correlació d'esdeveniments amb informació d'identitat i càrregues de treball, així com la capacitat de detectar abusos d'API i aplicar mesures de contenció directa sobre recursos compromesos.

Aquest paquet incorpora tots els requisits establerts en el P23-A i els amplia amb les següents funcionalitats:

REQ-TCN-277. Correlació amb identitat i càrregues de treball: el servei haurà de relacionar alertes i esdeveniments amb informació de gestió d'identitats al núvol (CIEM) i plataformes de protecció de càrregues de treball (CWPP), per millorar la detecció de compromisos contextuals.

REQ-TCN-278. Detecció d'abús d'API i deriva de configuració: el servei haurà de ser capaç d'identificar comportaments anòmals en l'ús d'API (accés massiu, crides no autoritzades) i desviacions respecte a configuracions segures establertes en els serveis al núvol.

REQ-TCN-279. Resposta inicial sobre recursos: el servei haurà de poder executar o sol·licitar accions de contenció remota inicial, com posar en quarantena una instància compromesa, aplicar regles de denegació en polítiques de seguretat o deshabilitar recursos en risc.

REQ-TCN-280. Preservació d'evidències forenses: el servei haurà de recopilar i custodiar evidències bàsiques en entorns de núvol, com ara instantànies (snapshots), captures de configuració i registres d'activitat, assegurant la seva integritat per a investigacions posteriors.

REQ-TCN-281. Informes ampliats de seguretat al núvol: el servei haurà de generar informes que descriguin anomalies detectades, mesures de contenció aplicades, evidències recollides i recomanacions específiques per a cada entorn.

REQ-TCN-282. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per integrar fonts d'alerta i mecanismes de resposta d'entorns multicloud i serveis emergents, com plataformes *serverless* o contenidors gestionats.

Activitats a realitzar per part de l'adjudicatari

- Correlacionar alertes de serveis al núvol amb informació d'identitat i càrregues de treball.
- Detectar abusos d'API i desviacions de configuració respecte a les pràctiques segures establertes.
- Executar o sol·licitar accions de contenció inicial com quarantena d'instàncies o aplicació de polítiques de denegació.
- Recollir i preservar evidències tècniques (snapshots, registres) per a investigacions forenses.
- Elaborar informes ampliats amb descripció dels incidents i recomanacions específiques de millora.

Resultats esperats

- Capacitat de detectar compromisos avançats en serveis al núvol relacionats amb identitat i càrregues de treball.
- Possibilitat de contenir incidents inicialment mitjançant quarantena o polítiques restrictives.
- Disponibilitat d'evidències bàsiques per a investigacions forenses en entorns de núvol.
- Informes ampliats que facilitin la millora contínua de la seguretat en entorns multicloud.
- Preparació per evolucionar cap al nivell òptim (P9-C), amb hunting i auto-remediació validada.

4.1.37 Paquet P23-C – Monitoratge i detecció d'incidents a serveis al núvol (nivell òptim)

El paquet P23-C té per objectiu assolir un nivell òptim de monitoratge d'alertes, detecció d'incidents i resposta en horari 24x7 sobre els serveis al núvol municipals, establint capacitats proactives d'hunting, validació contínua i auto-remediació guiada. Aquest nivell garanteix que l'Ajuntament pugui anticipar-se a compromisos complexos en entorns multicloud, validar l'eficàcia de les deteccions i aplicar respostes segures i consistents mitjançant baranes de seguretat (*guardrails*).

Aquest paquet incorpora tots els requisits establerts en el P23-B i els amplia amb les següents funcionalitats:

REQ-TCN-283. Caça d'amenaces (Threat Hunting) multicloud: el servei haurà de dur a terme activitats recurrents de hunting per identificar patrons avançats d'atac en entorns de múltiples proveïdors de núvol, com el salt entre comptes (*account hopping*) o la creació de perfils d'administrador ocults (*shadow admins*).

REQ-TCN-284. Validació contínua de deteccions (BAS cloud): el servei haurà de provocar de manera controlada alertes en entorns de núvol per validar l'eficàcia dels mecanismes de detecció i resposta, assegurant que funcionen davant tècniques d'atac emergents.

REQ-TCN-285. Anàlisi de causa arrel (RCA) automatitzada: el servei haurà de reconstruir de manera semi o totalment automatitzada la cadena d'esdeveniments d'un incident al núvol, representant-la en forma de gràfic de dependències entre recursos, identitats i serveis afectats.

REQ-TCN-286. Millora contínua de casos d'ús: el servei haurà de revisar i optimitzar periòdicament els casos de detecció i resposta en entorns de núvol, incorporant mètriques de fiabilitat i ajustos basats en lliçons apreses.

REQ-TCN-287. Playbooks d'auto-remediació amb baranes (guardrails): el servei haurà de disposar de procediments automatitzats d'auto-remediació que puguin aplicar mesures correctores en recursos de núvol, sempre sota el control de baranes de seguretat que evitin impactes operatius indesitjats.

REQ-TCN-288. Informes de maduresa i millora contínua: el servei haurà de generar informes que integrin resultats de hunting, validacions BAS, RCA i propostes concretes d'auto-remediació segura.

Activitats a realitzar per part de l'adjudicatari

- Desenvolupar activitats de hunting en entorns multicloud per descobrir tècniques avançades com account hopping o shadow admins.
- Realitzar validacions periòdiques de deteccions i respostes mitjançant exercicis controlats de BAS cloud.
- Reconstruir incidents complexos mitjançant anàlisi de causa arrel automatitzada amb gràfics de dependències.
- Revisar i millorar de manera contínua els casos d'ús i regles de detecció.

- Implementar i mantenir playbooks d'auto-remediació sota l'aplicació de guardrails de seguretat.
- Elaborar informes executius i tècnics amb resultats, lliçons apreses i recomanacions de millora contínua.

Resultats esperats

- Capacitat d'anticipar-se a compromisos avançats en entorns multicloud.
- Confirmació periòdica de l'eficàcia dels mecanismes de detecció i resposta al núvol.
- Reconstrucció automatitzada d'incidents que permeti entendre l'origen i propagació en serveis i identitats.
- Millora contínua dels casos d'ús i de les estratègies de detecció i resposta al núvol.
- Implementació d'auto-remediació guiada i segura mitjançant guardrails.
- Evolució constant de la seguretat del núvol municipal, adaptant-se a nous entorns i tecnologies.

4.1.38 Paquet P24-A – Monitoratge i detecció d'incidents a tecnologies emergents i especialitzades (nivell inicial)

El paquet P24-A té per objectiu establir un servei bàsic de monitoratge d'alertes i detecció d'incidents en horari 24x7 sobre les tecnologies emergents i especialitzades utilitzades per l'Ajuntament i les entitats dependents, incloent entorns d'operació tecnològica (OT) i dispositius connectats (IoT). Aquest nivell inicial proporciona visibilitat sobre la infraestructura crítica, els dispositius connectats i les anomalies més elementals, garantint la coordinació amb els equips operatius sota criteris de seguretat funcional.

El paràmetre quantificador d'aquest servei seran paquets de 50 actius de l'entitat contractant objecte del servei. Els actius podran ser dispositius OT i IOT; el número de sistemes i models d'IA, i el número de sistemes de gestió de claus criptogràfiques (KMS, HMS, PKI, key vaults, etc).

El paquet P24 inclou el llicenciament i els serveis d'administració i operació de les solucions SIEMaaS i SOARaaS integrant les solucions de protecció de tecnologies emergents i especialitzades (OT, IoT, IA i criptografia) de que disposi l'entitat contractant, així com la resta de solucions (Threat Hunting, BAS, Threat Intel, etc) necessàries per prestar el servei.

Tanmateix, el paquet P24 no inclou el llicenciament de les solucions de protecció de tecnologies emergents i especialitzades.

Funcionalitats que ha de suportar el servei

REQ-TCN-289. Ingesta d'alertes OT/IoT: el servei haurà d'incorporar i normalitzar les alertes i esdeveniments passius generats pels sistemes i dispositius OT/IoT, incloent sensors, PLCs i passarel·les de comunicació.

REQ-TCN-290. Ingesta d'alertes de sistemes criptogràfics: el servei haurà d'incorporar i normalitzar les alertes i esdeveniments generats pels sistemes criptogràfics (PKI, KMS, HSM, key vaults, etc) per exemple quan es detectin accessos no autoritzats a claus mestres o break-glass accounts,.

REQ-TCN-291. Inventari i seguiment de canvis: el servei haurà de mantenir un inventari actualitzat dels dispositius OT/IoT monitorats i registrar els canvis detectats en la seva configuració o estat.

REQ-TCN-292. Inventari de sistemes i algorismes criptogràfics: el servei haurà de mantenir un inventari actualitzat dels sistemes de gestió de claus criptogràfiques on-premise i on-cloud (PKI, KMS, HSM, key vaults, etc), dels algorismes criptogràfics que fa servir l'entitat, identificant quins són obsolets i vulnerables, i dels certificats digitals emesos o custodiats per l'entitat identificant la seva data d'expiració.

REQ-TCN-293. Casos d'ús bàsics de seguretat: el servei haurà de detectar esdeveniments elementals com la incorporació de nous dispositius a la xarxa, l'ús de protocols de comunicació no habituals o la connexió de dispositius no autoritzats. També haurà de detectar intents d'accés no autoritzats a claus mestres o break-glass-accounts.

REQ-TCN-294. Coordinació amb operació: el servei haurà d'actuar en coordinació amb els equips operatius responsables dels entorns OT/IoT, assegurant que qualsevol acció correctora o de contenció respecti els criteris de seguretat funcional i no comprometi la continuïtat del servei.

REQ-TCN-295. Classificació i triatge inicial: el servei haurà de revisar i classificar les alertes rebudes, establint-ne la gravetat i escalant-les quan sigui necessari al procés de gestió d'incidents.

REQ-TCN-296. Informes periòdics OT/IoT: el servei haurà de generar informes amb un resum de dispositius inventariats, incidents detectats i recomanacions bàsiques de millora.

REQ-TCN-297. Informes periòdics de criptografia: el servei haurà de generar informes que resumeixin, entre d'altres, la taxa de rotació de claus, el número i el percentatge de claus d'alta criticitat .emmagatzemades en mòduls de seguretat de maquinari (HSM) o en serveis de gestió de claus (KMS o key vaults), el percentatge d'algorismes criptogràfics obsolets i vulnerables, i el percentatge de certificats expirats en ús que encara no han estat renovats.

REQ-TCN-298. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per integrar fonts d'alerta de noves tecnologies emergents, com sensors intel·ligents avançats, sistemes de control distribuït o entorns d'intel·ligència artificial aplicada a l'operació.

Activitats a realitzar per part de l'adjudicatari

- Configurar i posar en marxa la ingesta d'alertes passives de dispositius OT/IoT.
- Elaborar i mantenir un inventari actualitzat amb seguiment dels canvis detectats.
- Definir i aplicar casos d'ús bàsics de seguretat en entorns OT/IoT.
- Coordinar les accions de resposta amb els equips d'operació sota criteris de seguretat funcional.
- Revisar i classificar alertes segons la seva gravetat i escalar-les quan sigui necessari.
- Generar informes periòdics diferenciats per a responsables tècnics i executius.

Resultats esperats

- Visibilitat mínima sobre els dispositius i entorns OT/IoT municipals.
- Capacitat de detectar i notificar incidents elementals com nous dispositius, protocols inusuals o canvis no autoritzats.
- Coordinació efectiva amb operacions per garantir respostes segures sense comprometre la continuïtat.
- Informes periòdics que permetin avaluar l'estat i seguretat dels entorns OT/IoT.
- Preparació per evolucionar cap al nivell avançat (P24-B), amb deteccions contextuals i resposta remota inicial.

4.1.39 Paquet P24-B – Monitoratge i detecció d'incidents a tecnologies emergents i especialitzades (nivell avançat)

El paquet P24-B té per objectiu proporcionar un nivell avançat de monitoratge d'alertes, detecció d'incidents i resposta inicial en horari 24x7 sobre els entorns OT/IoT i altres tecnologies emergents utilitzades per l'Ajuntament, ampliant les capacitats establertes al nivell bàsic. Aquest nivell introdueix la correlació d'esdeveniments operacionals amb informació d'IT, la detecció d'intrusions específiques d'OT i l'anàlisi de riscos associats a noves tecnologies com la intel·ligència artificial i el *cryptomining*.

Aquest paquet incorpora tots els requisits establerts en el P24-A i els amplia amb les següents funcionalitats:

REQ-TCN-299. Correlació d'esdeveniments OT/IT: el servei haurà de correlacionar esdeveniments operacionals de control industrial (com PLCs o consoles d'enginyeria) amb esdeveniments d'IT, per identificar compromisos híbrids que afectin tant la part operativa com la corporativa.

REQ-TCN-300. Detecció d'intrusions específiques d'OT: el servei haurà de detectar intents d'intrusió propis d'entorns OT, com canvis no autoritzats en PLCs, modificacions en receptes de processos o execució de codi en dispositius de control.

REQ-TCN-301. Detecció d'ús indegut de tecnologies emergents: el servei haurà d'identificar l'ús indegut de models d'intel·ligència artificial (per exemple, manipulació de sistemes autònoms) i activitats de *cryptomining* en infraestructures OT/IoT.

REQ-TCN-302. Resposta inicial segura en entorns OT/IoT: el servei haurà de poder executar o sol·licitar mesures de contenció inicial que no comprometin la seguretat funcional, com aplicar llistes de bloqueig dinàmiques o segmentar temporalment la xarxa per aïllar dispositius compromesos.

REQ-TCN-303. Informes ampliats d'OT/IoT: el servei haurà de generar informes que incloguin anomalies detectades, correlacions amb esdeveniments d'IT, mesures de contenció aplicades i recomanacions de millora.

REQ-TCN-304. Ingesta d'alertes de sistemes d'IA: el servei haurà d'incorporar i normalitzar les alertes i esdeveniments generats pels sistemes d'IA quan es detectin atacs al model o a les dades, per exemple atacs d'enverinament de les dades durant la fase d'entrenament, d'evasió de l'adversari durant la fase d'inferència, d'injecció de prompt, de jailbreaking, de robatori de models o de dades d'entrenament, o atacs de denegació de servei.

REQ-TCN-305. Inventari de sistemes i models d'IA : el servei haurà d'inventariar el número i el tipus de sistemes i de models d'IA que fa servir l'entitat, tant els desplegats a la pròpia entitat com els consumits com a servei (p.e. SaaS). També haurà d'identificar la criticitat i el risc dels sistemes i dels models, la diversitat dels frameworks emprats, el volum i la velocitat d'ingesta de dades, i els requisits de compliment aplicables.

REQ-TCN-306. Adaptabilitat a noves plataformes: el servei haurà d'estar preparat per integrar fonts d'alerta i capacitats de resposta de noves tecnologies emergents, com sistemes de control distribuït basats en IA o xarxes industrials de nova generació.

Activitats a realitzar per part de l'adjudicatari

- Correlacionar esdeveniments operacionals OT amb informació d'IT.
- Detectar intrusions i modificacions no autoritzades en dispositius de control industrial.
- Identificar l'ús indegut de tecnologies emergents com IA o *cryptomining*.
- Executar o sol·licitar accions de contenció inicial segures, com llistes de bloqueig o segmentació de xarxa.
- Elaborar informes ampliats amb incidents, correlacions i recomanacions específiques.

Resultats esperats

- Capacitat de detectar compromisos avançats que afectin simultàniament OT i IT.
- Identificació d'intrusions específiques d'entorns de control industrial.
- Detecció d'ús indegut de tecnologies emergents en l'àmbit municipal.
- Possibilitat de contenir incidents inicialment sense comprometre la seguretat funcional.
- Informes ampliats que facilitin la millora contínua de la seguretat en entorns OT/IoT.
- Preparació per evolucionar cap al nivell òptim (P24-C), amb hunting, validació contínua i alineament amb estàndards internacionals com IEC-62443.

4.1.40 Paquet P24-C – Monitoratge i detecció d'incidents a tecnologies emergents i especialitzades (nivell òptim)

El paquet P24-C té per objectiu assolir un nivell òptim de monitoratge d'alertes, detecció d'incidents i resposta en horari 24x7 sobre els entorns OT/IoT i altres tecnologies emergents utilitzades per l'Ajuntament, establint capacitats avançades de *hunting*, validació contínua i aprenentatge orientat a la millora dels processos operatius. Aquest nivell permet anticipar-se a compromisos complexos en entorns industrials, validar de manera recurrent l'eficàcia de les deteccions i alinear la resposta amb estàndards internacionals de seguretat.

Aquest paquet incorpora tots els requisits establerts en el P24-B i els amplia amb les següents funcionalitats:

REQ-TCN-307. Hunting específic OT/IoT: el servei haurà de dur a terme activitats recurrents de *hunting* orientades a detectar cadenes d'atac pròpies d'entorns industrials i de control, basades en vectors coneguts i en hipòtesis de compromís no reflectides en alertes prèvies.

REQ-TCN-308. Validació contínua de deteccions en zones OT: el servei haurà de validar periòdicament l'eficàcia dels mecanismes de detecció en entorns OT mitjançant simulacions segures o exercicis de *Breach and Attack Simulation (BAS)* adaptats a la realitat industrial.

REQ-TCN-309. Anàlisi de causa arrel automatitzada (RCA): el servei haurà de reconstruir incidents OT/IoT de manera semi o totalment automatitzada, mapant els vectors i les fases de l'atac contra estàndards de referència com IEC-62443 i el marc MITRE ATT&CK for ICS.

REQ-TCN-310. Lliçons apreses i millora operativa: el servei haurà de generar informes de lliçons apreses per a cada incident crític, amb recomanacions de reforç de seguretat (hardening) i mesures operatives que puguin ser integrades pels equips responsables de l'explotació.

REQ-TCN-311. Informes de maduresa i evolució contínua: el servei haurà de proporcionar informes executius i tècnics amb resultats de hunting, validacions, RCA i lliçons apreses, establint fulls de ruta per a l'evolució de la seguretat OT/IoT.

REQ-TCN-312. Adaptabilitat a noves tecnologies: el servei haurà d'estar preparat per integrar fonts i mecanismes de detecció en plataformes emergents de control industrial, IA aplicada a processos o nous estàndards de seguretat funcional.

Activitats a realitzar per part de l'adjudicatari

- Desenvolupar activitats de *hunting* específic en entorns OT/IoT.
- Realitzar simulacions segures o exercicis BAS per validar deteccions en zones industrials.
- Reconstruir incidents OT/IoT mitjançant RCA automatitzada amb mapatge a estàndards.
- Elaborar informes de lliçons apreses i recomanacions de millora per a equips operatius.
- Generar informes periòdics amb resultats i propostes de fulls de ruta d'evolució.

Resultats esperats

- Capacitat d'anticipar-se a compromisos avançats en entorns OT/IoT.
- Confirmació recurrent de l'eficàcia de les deteccions en zones industrials.
- Reconstrucció sistemàtica i automatitzada dels incidents segons marcs internacionals (IEC-62443, MITRE ATT&CK for ICS).
- Millora progressiva de la seguretat i resiliència dels entorns OT/IoT gràcies a les lliçons apreses.
- Evolució constant del servei i adaptació a noves tecnologies industrials i emergents.

4.1.41 Paquet P25-A – Monitoratge i detecció d'incidents a hipervisors i plataformes de virtualització (nivell inicial)

El **paquet P25-A** té per objectiu establir un **servei bàsic de monitoratge i detecció d'incidents** en horari 24x7 als entorns d'hipervisors i plataformes de virtualització de l'Ajuntament, que allotgen sistemes i aplicacions corporatives essencials. Aquest servei proporciona una visibilitat inicial sobre l'activitat dels entorns virtualitzats i permet detectar de manera primerenca anomalies o comportaments potencialment maliciosos que puguin afectar la integritat o disponibilitat dels recursos virtuals.
El servei es fonamenta en la recopilació de telemetria essencial dels hipervisors i de les consoles d'administració, la seva integració dins del CROC-OSAP i la generació d'alertes bàsiques correlacionades amb altres dominis tecnològics.

El paràmetre quantificador d'aquest servei serà el número de nodes que suportin els hipervisors i les plataformes de virtualització de l'entitat contractant objecte del servei.

El paquet P25 inclou el llicenciament i els serveis d'administració i operació de les solucions SIEMaaS i SOARaaS integrant la telemetria essencial i les solucions de protecció d'hipervisors i de plataformes de virtualització de que disposi l'entitat contractant, així com la resta de solucions (Threat Hunting, BAS, Threat Intel, etc) necessàries per prestar el servei.

Tanmateix, el paquet P25 no inclou el llicenciament de les solucions de protecció d'hipervisors i de plataformes de virtualització.

Funcionalitats que ha de suportar el servei

REQ-TCN-313. Integració de telemetria bàsica d'hipervisors. L'adjudicatari haurà de garantir la recopilació i integració al CROC-OSAP dels registres principals dels hipervisors (accés, gestió, arrencada/aturada de màquines virtuals, canvis de configuració, ús de recursos, etc.).

REQ-TCN-314. Visibilitat sobre consoles d'administració. El servei haurà d'incorporar la captació d'esdeveniments provinents de les consoles d'administració de la virtualització, incloent intents d'autenticació, modificacions de polítiques o canvis de permisos.

REQ-TCN-315. Correlació d'incidents bàsica. L'adjudicatari haurà d'implementar regles bàsiques de correlació per identificar patrons anòmals, accés indegut o comportament irregular dins els entorns virtualitzats.

REQ-TCN-316. Monitoratge de disponibilitat i ús de recursos. El servei haurà d'oferir visibilitat sobre l'estat operatiu dels hipervisors i l'ús dels recursos virtuals (CPU, memòria, disc, xarxa), amb notificacions davant sobrecàrregues o anomalies de rendiment que puguin indicar un incident.

REQ-TCN-317. Gestió i escalat d'incidents. Els incidents detectats hauran de ser registrats i gestionats mitjançant l'eina de tiqueting corporativa, amb notificació al personal tècnic municipal i escalat segons la seva severitat.

REQ-TCN-318. Informes periòdics de monitoratge. L'adjudicatari haurà d'elaborar informes periòdics (com a mínim trimestrals) que incloguin volum d'alertes, tipologia d'incidents, temps de detecció i recomanacions de millora.

Activitats a realitzar per part de l'adjudicatari

- Parametritzar i mantenir regles bàsiques de correlació per a la detecció d'incidents comuns.

- Supervisar la disponibilitat i rendiment dels entorns virtualitzats i comunicar anomalies detectades.
- Registrar i gestionar les alertes generades, assegurant el seu seguiment i resolució.
- Elaborar informes periòdics amb indicadors d'activitat i estat de seguretat dels entorns monitorats.

Resultats esperats

- Existència d'una **capacitat bàsica de monitoratge i detecció d'incidents** als entorns d'hipervisors i virtualització.
- Visibilitat inicial sobre esdeveniments crítics i activitats d'administració dels hipervisors.
- Correlació elemental d'incidents amb altres dominis tecnològics gestionats pel servei CROC-OSAP.
- Reducció del temps de detecció d'anomalies i millora de la capacitat de resposta inicial.
- Base de partida per evolucionar cap als nivells **avançat (P25-B)** i **òptim (P25-C)**, amb una cobertura més àmplia i mecanismes avançats d'anàlisi i correlació.

4.1.42 Paquet P25-B – Monitoratge i detecció d'incidents a hipervisors i plataformes de virtualització (nivell avançat)

El **paquet P25-B** té per objectiu oferir un **servei avançat de monitoratge i detecció d'incidents** als entorns d'hipervisors i plataformes de virtualització de l'Ajuntament, millorant la visibilitat, la correlació i la capacitat de detecció sobre activitats anòmales o malicioses. Aquest nivell amplia les funcionalitats bàsiques del servei inicial, incorporant anàlisi comportamental, detecció d'activitats laterals i correlació d'esdeveniments entre múltiples dominis tecnològics.

El servei permet detectar de manera proactiva intents de compromís de consoles d'administració, alteracions en les màquines virtuals, desviacions de configuració o patrons de comportament no habituals, reforçant així la seguretat i disponibilitat dels entorns virtualitzats crítics de l'Ajuntament.

Funcionalitats que ha de suportar el servei

REQ-TCN-319. Recollida ampliada de telemetria. El servei haurà d'ampliar la telemetria recollida dels hipervisors i orquestradors de virtualització, incloent dades de xarxa, processos interns i operacions administratives avançades, garantint la seva integració dins del servei.

REQ-TCN-320. Correlació avançada d'incidents. L'adjudicatari haurà d'implantar regles de correlació avançades que permetin identificar patrons complexos d'activitat, com accessos simultanis sospitosos, moviments laterals o manipulacions coordinades de configuració.

REQ-TCN-321. Detecció comportamental. El servei haurà d'incorporar tècniques de detecció basades en comportament (UEBA o equivalent) per identificar desviacions respecte a patrons normals d'ús dels hipervisors, consoles o màquines virtuals.

REQ-TCN-322. Validació d'integritat i configuració. L'adjudicatari haurà d'implementar mecanismes de detecció de canvis no autoritzats a la configuració dels hipervisors, repositoris de màquines virtuals o perfils d'usuari, amb notificació immediata al CROC-OSAP.

REQ-TCN-323. Supervisió de la seguretat de les APIs. El servei haurà de monitorar les crides a les APIs d'administració i automatització per detectar usos indeguts o anomalies, incloent intents de desplegament no autoritzat o accés a recursos sensibles.

REQ-TCN-324. Informes i mètriques d'eficiència. L'adjudicatari haurà d'elaborar informes mensuals que recullin volum d'alertes, incidents gestionats, temps mitjà de detecció (MTTD) i recomanacions de millora basades en tendències observades.

Activitats a realitzar per part de l'adjudicatari

- Configurar i mantenir regles de detecció comportamental sobre usuaris, sistemes i processos de virtualització.
- Supervisar l'activitat de consoles, APIs i entorns d'administració d'hipervisors.
- Analitzar incidents i emetre informes tècnics amb recomanacions de mitigació.
- Coordinar-se amb el Servei per a la resposta i escalat dels incidents detectats.
- Proporcionar informes mensuals amb mètriques, resultats i tendències del servei.

Resultats esperats

- Prestació d'un **servei avançat i proactiu de detecció d'incidents** en entorns d'hipervisors i virtualització.
- Major visibilitat i capacitat de correlació entre dominis de seguretat.
- Identificació primerenca de desviacions de comportament o canvis no autoritzats.
- Reducció del temps mitjà de detecció (MTTD) i millora de la resposta coordinada.

- Evolució del servei cap a una cobertura integral de detecció, base per al nivell òptim (P25-C).

4.1.43 Paquet P25-C – Monitoratge i detecció d'incidents a hipervisors i plataformes de virtualització (nivell òptim)

El **paquet P25-C** té per objectiu oferir un **servei òptim de monitoratge i detecció d'incidents** en entorns d'hipervisors i plataformes de virtualització, capaç d'identificar de forma intel·ligent, automatitzada i predictiva qualsevol activitat anòmala o maliciosa que pugui afectar els sistemes virtuals de l'Ajuntament. Aquest nivell consolida la plena integració dels entorns de virtualització dins de l'ecosistema de detecció i resposta del CROC-OSAP, incorporant tecnologies d'anàlisi avançada, aprenentatge automàtic i correlació multidomini.

El servei proporciona **una visibilitat completa i en temps real** de la seguretat dels entorns virtualitzats, permetent anticipar incidents, reduir els temps de detecció i millorar la resposta coordinada amb la resta de dominis de seguretat operativa.

Funcionalitats que ha de suportar el servei

REQ-TCN-325. Detecció basada en intel·ligència artificial. El servei haurà d'incorporar models d'intel·ligència artificial i aprenentatge automàtic (ML) capaços d'identificar patrons d'activitat anòmals, desviacions de configuració i amenaces emergents que no siguin detectables per regles estàtiques.

REQ-TCN-326. Validació d'integritat i traçabilitat completa. L'adjudicatari haurà de mantenir mecanismes d'auditoria que permetin reconstruir la seqüència completa d'esdeveniments associats a un incident, assegurant la integritat de les evidències i la seva disponibilitat per a anàlisi forense.

REQ-TCN-327. Enriquiment amb intel·ligència d'amenaces. El servei haurà d'integrar fonts d'intel·ligència d'amenaces (Threat Intelligence) per contextualitzar alertes i identificar actors, tàctiques i tècniques associades a atacs sobre entorns virtualitzats.

REQ-TCN-328. Quadre de comandament i mètriques avançades. L'adjudicatari haurà de proporcionar un quadre de comandament dinàmic que mostri mètriques de detecció,

tendències, temps mitjà de detecció (MTTD), temps mitjà de resposta (MTTR) i índex de falsos positius, així com recomanacions de millora contínua.

Activitats a realitzar per part de l'adjudicatari

- Aplicar models d'IA per detectar desviacions o patrons d'amenaça desconeguts.
- Emetre informes i mètriques avançades d'eficiència, cobertura i millora del servei.

Resultats esperats

- Prestació d'un **servei òptim i intel·ligent de detecció d'incidents** en entorns d'hipervisors i virtualització.
- Capacitat de detecció automatitzada, predictiva i multidomini amb reducció significativa del temps mitjà de detecció (MTTD).
- Traçabilitat i registre exhaustiu d'incidents amb suport per a anàlisi forense i millora contínua.
- Enriquiment constant amb intel·ligència d'amenaces actualitzada i context operatiu.

4.1.44 Paquet P26-A – Monitoratge i detecció d'incidents a contenidors i orquestradors (nivell inicial)

El **paquet P26-A** té per objectiu establir un **servei inicial de monitoratge i detecció d'incidents** en horari 24x7 en els entorns de contenidors i orquestradors de l'Ajuntament, com ara Kubernetes, OpenShift o plataformes equivalents. Aquest servei proporciona la primera capa de visibilitat sobre l'activitat d'aquests entorns, permetent identificar anomalies operatives, configuracions indegudes i comportaments sospitosos que puguin afectar la disponibilitat o integritat dels serveis desplegats.

El servei forma part del conjunt de capacitats de detecció del CROC-OSAP i garanteix que les plataformes de contenidors quedin sota supervisió centralitzada, amb telemetria bàsica integrada i notificació d'incidents mitjançant el sistema de tiqueting corporatiu.

El paràmetre quantificador d'aquest servei serà el número de nodes que suportin els entorns de contenidors i sistemes d'orquestració de l'entitat contractant objecte del servei.

El paquet P25 inclou el llicenciament i els serveis d'administració i operació de les solucions SIEMaaS i SOARaaS integrant la telemetria essencial i les solucions de protecció de contenidors i d'orquestradors de que disposi l'entitat contractant, així com la resta de solucions (Threat Hunting, BAS, Threat Intel, etc) necessàries per prestar el servei.

Tanmateix, el paquet P25 no inclou el llicenciament de les solucions de protecció de contenidors i d'orquestradors.

Funcionalitats que ha de suportar el servei

REQ-TCN-329. Integració de telemetria bàsica de contenidors i orquestradors. L'adjudicatari haurà de garantir la recepció dels principals esdeveniments dels nodes i clústers (arrencada i aturada de pods, canvis de configuració, errors de desplegament o d'imatge, etc.).

REQ-TCN-330. Visibilitat del pla de control. El servei haurà d'incorporar la captació d'esdeveniments provinents de les consoles d'administració i APIs dels orquestradors, incloent autenticacions, canvis de rols i modificacions de polítiques.

REQ-TCN-331. Correlació bàsica d'incidents. S'hauran d'aplicar regles bàsiques de correlació per identificar patrons elementals d'activitat anòmala, com errors reiterats, desplegaments no autoritzats o execució d'imatges desconegudes.

REQ-TCN-332. Supervisió de l'estat dels clústers i nodes. El servei haurà de monitorar l'estat general dels clústers i nodes de contenidors, generant alertes per caigudes, saturacions o anomalies de rendiment que puguin tenir origen en un incident de seguretat.

REQ-TCN-333. Gestió d'incidents i escalat. Els incidents detectats hauran de registrar-se al sistema de tiqueting corporatiu, amb notificació als responsables designats i escalat segons la seva severitat i impacte.

REQ-TCN-334. Informes bàsics de monitoratge. L'adjudicatari haurà d'elaborar informes periòdics, com a mínim trimestrals, amb el resum d'alertes, tipologia d'incidents i recomanacions de millora de configuració o supervisió.

Activitats a realitzar per part de l'adjudicatari

- Parametritzar regles bàsiques de detecció i correlació d'esdeveniments.
- Supervisar l'estat operatiu dels clústers i nodes, comunicant anomalies detectades.
- Gestionar i registrar les alertes generades, assegurant el seu seguiment i tancament.
- Elaborar informes de servei amb estadístiques d'activitat i recomanacions tècniques.

Resultats esperats

- Prestació d'un **servei bàsic de monitoratge i detecció** sobre contenidors i orquestradors municipals.
- Visibilitat inicial dels esdeveniments crítics i de l'activitat d'administració dels entorns.
- Correlació elemental amb altres dominis de detecció.
- Reducció dels temps de detecció d'anomalies i millora de la resposta inicial.
- Base de partida per evolucionar cap als nivells **avançat (P26-B)** i **òptim (P26-C)**, amb anàlisi comportamental, correlació avançada i detecció intel·ligent.

4.1.45 Paquet P26-B – Monitoratge i detecció d'incidents a contenidors i orquestradors (nivell avançat)

El **paquet P26-B** té per objectiu oferir un **servei avançat de monitoratge i detecció d'incidents** sobre els entorns de contenidors i orquestradors de l'Ajuntament, ampliant la visibilitat, la correlació i la profunditat analítica respecte del nivell inicial. Aquest servei permet identificar de forma proactiva comportaments anòmals, configuracions indegudes o intents de compromís en els clústers de contenidors, els nodes i els components d'orquestració, garantint la integritat i disponibilitat dels serveis municipals desplegats en aquests entorns.

El servei reforça la integració dels sistemes de contenidors dins del Servei, amb capacitat per correlacionar esdeveniments entre dominis tecnològics, detectar amenaces avançades i reduir els temps de detecció i resposta.

Funcionalitats que ha de suportar el servei

REQ-TCN-335. Recollida ampliada de telemetria. L'adjudicatari haurà de garantir la recepció d'esdeveniments addicionals dels clústers i orquestradors (com operacions de desplegament, execució de pods, ús de secrets, canvis de configuració o anomalies en pipelines) dins del Servei.

REQ-TCN-336. Correlació avançada d'incidents. El servei haurà d'incloure regles de correlació avançades que permetin identificar patrons complexos, com desplegaments no autoritzats, ús de credencials compartides, modificacions de polítiques o moviments laterals entre contenidors.

REQ-TCN-337. Detecció de comportament. El servei haurà d'aplicar tècniques de detecció basades en comportament per identificar desviacions respecte als patrons habituals d'ús dels contenidors, processos i components d'orquestració.

REQ-TCN-338. Validació d'integritat de configuracions. L'adjudicatari haurà d'implantar mecanismes per detectar canvis no autoritzats en manifestos, imatges o fitxers de configuració dels entorns monitorats, notificant immediatament qualsevol alteració.

REQ-TCN-339. Supervisió de les APIs d'orquestració. El servei haurà de monitorar les crides a les APIs dels orquestradors i repositoris d'imatges per detectar usos indeguts, execucions no controlades o anomalies d'autenticació.

REQ-TCN-340. Informes i mètriques del servei. L'adjudicatari haurà d'elaborar informes mensuals amb volum d'alertes, tipus d'incidents, temps mitjà de detecció (MTTD), recomanacions i propostes de millora.

Activitats a realitzar per part de l'adjudicatari

- Configurar la integració avançada de fonts de telemetria.
- Actualitzar i mantenir regles de correlació per a la detecció d'activitats complexes o coordinades.
- Analitzar i validar anomalies de comportament i canvis de configuració no autoritzats.
- Supervisar l'activitat d'APIs i components d'orquestració, detectant usos indeguts.
- Generar informes mensuals amb mètriques, tendències i recomanacions.

Resultats esperats

- Prestació d'un **servei avançat de detecció d'incidents** als entorns de contenidors i orquestradors.
- Major visibilitat i capacitat de correlació amb altres dominis tecnològics.
- Identificació primerenca de desviacions, manipulacions o desplegaments no autoritzats.
- Reducció del temps mitjà de detecció (MTTD) i millora de la resposta coordinada amb el CROC-OSAP.
- Base consolidada per evolucionar cap al nivell **òptim (P26-C)**, orientat a l'automatització i detecció intel·ligent.

4.1.46 Paquet P26-C – Monitoratge i detecció d'incidents a contenidors i orquestradors (nivell òptim)

El **paquet P26-C** té per objectiu proporcionar un **servei òptim i intel·ligent de monitoratge i detecció d'incidents** en entorns de contenidors i orquestradors (Kubernetes, OpenShift o equivalents), garantint la detecció proactiva, automatitzada i contextual d'amenaces complexes o avançades que puguin afectar els serveis municipals desplegats.

Aquest nivell incorpora tecnologies d'**intel·ligència artificial, anàlisi predictiva i correlació multidomini**, integrades dins del Servei, per aconseguir una detecció anticipada i una resposta coordinada amb la resta d'àrees de seguretat operativa. El servei ofereix una visibilitat completa, en temps real, sobre la seguretat dels entorns de contenidors i assegura la seva protecció davant tècniques d'evasió, moviments laterals o manipulacions d'imatges i configuracions.

Funcionalitats que ha de suportar el servei

REQ-TCN-341. Orquestració i automatització de detecció. L'adjudicatari haurà de desplegar processos d'orquestració (SOAR) que automatitzin la detecció, validació i notificació d'incidents als entorns de contenidors i orquestradors, garantint una resposta immediata i eficient.

REQ-TCN-342. Detecció intel·ligent basada en IA. El servei haurà d'incorporar models d'intel·ligència artificial i aprenentatge automàtic (ML) capaços d'identificar patrons d'activitat anòmals, correlacions no evidents i tècniques avançades d'atac (com execució lateral, enverinament de pipelines o manipulació d'imatges).

REQ-TCN-343. Detecció d'anomalies en cadena de subministrament. El servei haurà d'identificar anomalies o compromisos en repositoris d'imatges, components o pipelines de construcció, detectant manipulacions en dependències o execucions no autoritzades.

REQ-TCN-344. Enriquiment amb intel·ligència d'amenaces. El servei haurà d'integrar fonts de Threat Intelligence per contextualitzar les deteccions, identificant tàctiques i tècniques d'atac (TTPs) específiques contra entorns de contenidors i orquestradors.

REQ-TCN-345. Quadre de comandament i mètriques avançades. L'adjudicatari haurà de proporcionar un quadre de comandament dinàmic amb mètriques de detecció, tendències d'alertes, temps mitjà de detecció (MTTD), temps mitjà de resposta (MTTR) i recomanacions de millora contínua del servei.

Activitats a realitzar per part de l'adjudicatari

- Aplicar models d'IA i ML per detectar activitats anòmales o amenaces desconegudes.
- Automatitzar els fluxos de detecció i notificació mitjançant orquestració.
- Garantir la traçabilitat completa dels incidents i conservar evidències per a investigació forense.
- Elaborar informes i mètriques d'eficiència, cobertura i evolució del servei.

Resultats esperats

- Prestació d'un **servei òptim i intel·ligent de detecció d'incidents** sobre contenidors i orquestradors.
- Capacitat predictiva i automatitzada per identificar amenaces complexes o desconegudes.
- Traçabilitat i conservació d'evidències per a investigacions posteriors.
- Enriquiment constant amb intel·ligència d'amenaces i millora contínua del servei.
- Consolidació d'una **capacitat de detecció proactiva i resilient**, essencial per garantir la seguretat dels entorns de desplegament d'aplicacions municipals.

4.1.47 Paquet P27 – Resposta a incidents

El paquet P27 té per objectiu establir un servei bàsic de resposta a incidents de seguretat que permeti al CROC municipal gestionar, contenir i documentar de manera immediata els incidents confirmats. Aquest nivell assegura que qualsevol esdeveniment crític pugui ser atès sense retard, establint un protocol de resposta i garantint la continuïtat dels serveis públics. Aquest nivell garanteix que l'Ajuntament i les seves entitats dependents disposin d'una capacitat permanent de detecció, contenció, anàlisi i recuperació davant incidents de seguretat, amb cobertura completa i sense límits en el nombre d'incidents gestionats. A més, incorpora serveis especialitzats de forense, suport legal i eliminació d'actius fraudulents, amb disponibilitat ampliada i adaptativa segons l'evolució de l'amenaça. L'assistència haurà de ser presencial, si escau.

El paràmetre quantificador d'aquest servei seran paquets de 40h (5 jornades) de resposta a incidents de seguretat i d'anàlisi forense pericial o judicial.

El paquet P27 inclou el llicenciament i els serveis d'administració i operació de les plataformes que requereixi l'equip de resposta a incidents i l'equip d'analistes forenses per recollir i custodiar proves digitals, i per analitzar incidents complexos.

Tanmateix, el paquet P27 no inclou el llicenciament de les solucions de detecció i resposta a incidents.

Funcionalitats que ha de suportar el servei

REQ-TCN-346. Procés de gestió d'incidents. El servei haurà de disposar d'un protocol establert per a la recepció, registre, classificació i resposta a incidents detectats pel CROC i mantenir-lo actualitzat, aplicant la guia CCN-STIC-817 i l'eina de registre d'incidents indicada per l'entitat contractant.

REQ-TCN-347. Contenció immediata. El servei haurà de contemplar accions de contenció bàsica, com aïllar un dispositiu compromès o suspendre un compte sospitós, assegurant que l'impacte no s'estengui.

REQ-TCN-348. Gestió integral d'incidents. El servei haurà de cobrir un nombre il·limitat d'incidents, amb capacitat de resposta 24x7 i disponibilitat immediata d'equips especialitzats. El servei haurà de cobrir totes les fases d'un incident, des de la detecció, anàlisi i contenció inicial fins a la mitigació i tancament, amb protocols estandarditzats i alineats amb bones pràctiques internacionals.

REQ-TCN-349. Coordinació multidimensional. Els incidents hauran de ser gestionats assegurant que totes les alertes i registres estiguin correlacionats i contextualitzats. El servei haurà de coordinar-se també amb l'equip de resposta a incidents municipal, i amb altres actors externs (proveïdors crítics, CERTs sectorials i nacionals).

REQ-TCN-350. Anàlisi tècnica avançada. El servei haurà d'incloure capacitats per analitzar incidents complexos (moviments laterals, escalat de privilegis, exfiltració de dades, atacs híbrids IT/OT).

REQ-TCN-351. Suport proactiu en la mitigació. El servei haurà d'oferir recomanacions tècniques immediates i donar suport directe als equips municipals per aplicar mesures correctives.

REQ-TCN-352. Actuacions especialitzades mensuals sense restriccions predefinides. El servei haurà d'incloure:

- **Anàlisis forenses avançades sense límit predefinit**, amb cadena de custòdia completa i validesa judicial.

- **Suport legal sense restriccions**, incloent coordinació amb autoritats reguladores, cossos policials i assessoria estratègica en crisis de seguretat.

REQ-TCN-353. Coordinació multidimensional. El servei haurà de coordinar-se de manera fluida amb altres actors externs (proveïdors crítics, CERTs sectorials i nacionals).

REQ-TCN-354. Horari de servei: 24x7. Les persones que integrin el servei hauran de ser operatives de 0h a 24h de dilluns a diumenge per tal d'atendre incidents de seguretat de criticitat alta o superior

REQ-TCN-355. Documentació operativa: el servei haurà de mantenir actualitzada la documentació relativa als procediments establert de resposta davant d'incidents.

REQ-TCN-356. Matriu de contactes: el servei haurà de mantenir actualitzada i posar a disposició de l'entitat contractant una matriu de contactes d'emergència que inclogui tant els serveis de resposta a incidents del proveïdor com els contactes dels responsables i dels equips tècnics de l'entitat contractant amb els que s'haurà de coordinar la resposta als incidents.

REQ-TCN-357. Gestió de tiquets: el servei haurà de fer servir l'eina de gestió de tiquets (ITSM) de l'entitat per a la notificació, suport i seguiment de la gestió d'incidents. En cas que la comunicació inicial de l'incident es faci per via telefònica, el servei haurà de documentar l'incident a l'eina ITSM de l'entitat contractant.

REQ-TCN-358. Comunicació inicial. Els incidents hauran de ser notificats de manera clara i ràpida als responsables municipals quan impliquin serveis crítics o informació sensible.

REQ-TCN-359. Escalat a l'equip de resposta municipal. Els incidents que superin la capacitat de gestió del nivell inicial hauran de ser escalats a l'equip de resposta municipal o a equips especialitzats designats.

REQ-TCN-360. Registre i traçabilitat. Totes les accions realitzades durant la resposta hauran de ser registrades amb detall, garantint la traçabilitat i possibilitant una revisió posterior.

REQ-TCN-361. Informes tècnics i executius avançats. Cada incident haurà de generar informes diferenciats, amb detalls tècnics exhaustius (cronologia de l'incident, accions de

contenció adoptades i recomanacions inicials de mitigació) per als equips operatius i una visió executiva per als responsables de decisió.

REQ-TCN-362. Informes estratègics i predictius. En cas que l'entitat contractant ho sol·liciti els informes hauran d'anar més enllà de la descripció tècnica, incloent anàlisi de tendències, prediccions sobre vectors emergents i recomanacions d'inversió estratègica.

REQ-TCN-363. Millora contínua basada en lliçons apreses. El servei haurà d'incloure sessions periòdiques de revisió d'incidents (post-mortem), orientades a extreure lliçons apreses i reforçar els controls preventius i de detecció. Cada incident i simulacre haurà de generar recomanacions accionables per millorar la detecció, la contenció i la recuperació, integrades dins del full de ruta de seguretat municipal.

Activitats a realitzar per part de l'adjudicatari

- Rebre i registrar tots els incidents detectats.
- Gestionar tots els incidents detectats o notificats, independentment de la seva complexitat i del volum.
- Dur a terme accions especialitzades de forense i suport legal sense límits mensuals preestablerts.
- Coordinar simulacres mensuals i sessions de preparació davant crisis semestrals.
- Classificar la gravetat i l'impacte inicial.
- Executar mesures bàsiques de contenció immediata.
- Notificar els incidents crítics als responsables municipals.
- Coordinar-se, quan sigui necessari, amb l'equip de resposta municipal o amb tercers especialitzats.
- Elaborar informes tècnics, executius i estratègics amb recomanacions orientades a la resiliència.
- Coordinar-se amb autoritats i organismes externs per garantir una resposta integral.
- Integrar de manera contínua els aprenentatges en els processos de seguretat municipal.

Resultats esperats

- Procés establert i operatiu per gestionar incidents de seguretat.
- Capacitat de contenció immediata per reduir l'impacte sobre els serveis municipals.
- Comunicació fluida i ràpida amb responsables municipals.
- Registre i traçabilitat de totes les actuacions.
- Capacitat òptima de resposta a incidents, amb cobertura integral i permanent.
- Eliminació de dominis, comptes i plataformes fraudulentes sense límits preestablerts.

- Anàlisis pericials judicials forenses i suport legal complet, que reforcen la capacitat de l'Ajuntament en procediments legals.
- Simulacres mensuals que asseguren la preparació contínua dels equips municipals.
- Informes estratègics i predictius que connecten la resposta a incidents amb la planificació de la seguretat a llarg termini.
- Evolució cap a un model resilient i adaptatiu, alineat amb la NIS2, l'ENS i les directrius del CCN i CERT de referència.

4.1.48 Paquet P28-A – Recuperació post-incident (nivell inicial)

El paquet P28-A té per objectiu establir una capacitat bàsica i estructurada que garanteixi que, en cas que l'Ajuntament necessiti activar processos de recuperació post-incident, tots els equips, procediments, eines i mecanismes de verificació estiguin degudament preparats, actualitzats i validats.
Aquest nivell inicial defineix els fonaments que permeten assegurar que la recuperació podrà ser executada per l'Ajuntament o pels serveis corresponents de manera repetible, segura i alineada amb els processos de resposta.

El servei inclou la integració amb les solucions SIEMaaS i SOARaaS i la monitorització continuada de l'estat de les còpies de seguretat existents a l'entitat contractant. També incorpora la verificació periòdica de la seva integritat i disponibilitat i la realització de proves bàsiques de continuïtat del servei, però **no inclou en cap cas l'execució directa de processos de restauració ni el llicenciament, administració o operació de les solucions de backup**.

El paràmetre quantificador d'aquest servei seran el número de serveis crítics de l'entitat contractant objecte del servei.

Funcionalitats que ha de suportar el servei

REQ-TCN-364. Plans bàsics de recuperació. El servei haurà de garantir l'existència, disponibilitat i actualització de plans mínims de recuperació post-incident per als serveis crítics, documentats i revisats periòdicament. Aquests plans han de definir com l'Ajuntament recuperarà el servei.

REQ-TCN-365. Preparació per a la restauració controlada de sistemes. El servei haurà d'assegurar que els procediments, les eines i les còpies de seguretat verificades necessàries per a una restauració eventual estiguin documentades, accessibles i validades, perquè puguin ser utilitzades per l'Ajuntament o pel proveïdor de backup quan sigui necessari.

REQ-TCN-366. Coordinació amb resposta a incidents. Els processos de preparació per a la recuperació hauran d'estar alineats amb les activitats de contenció i erradicació executades pel CROC, per assegurar que, en cas d'activació de la recuperació, no existeixin riscos de reinfecció o persistència de l'amenaça

REQ-TCN-367. Proves bàsiques de continuïtat. El servei haurà d'incloure com a mínim **una prova anual de recuperació** en entorns controlats, destinada a validar els procediments i mecanismes que farien possible la recuperació.

REQ-TCN-368. Monitoratge continuat de l'estat del backup. S'haurà de disposar d'un sistema de monitoratge 24x7 que permeti detectar errors, intents d'accés no autoritzats o fallades en els processos de còpia, i generar alertes integrades amb el CROC-OSAP per a la seva gestió immediata.

REQ-TCN-369. Verificació de l'estat de les còpies de seguretat. El servei haurà de comprovar periòdicament l'estat, integritat i accessibilitat de les còpies de seguretat proporcionades per l'Ajuntament o pels proveïdors corresponents, validant que siguin aptes per a la restauració en cas d'incident. Les incidències o errors detectats hauran de ser reportats mitjançant l'eina de tiqueting per al seu seguiment.

Activitats a realitzar per part de l'adjudicatari

- Definir conjuntament amb l'Ajuntament els serveis que requereixen plans bàsics de recuperació.
- Documentar, revisar i mantenir vigents els plans i procediments de suport a la recuperació.
- Validar que les eines i processos necessaris per a una eventual recuperació estan disponibles i operatius.
- Coordinar-se amb el CROC per assegurar l'alineació entre preparació, contenció i erradicació.
- Conduir almenys una prova anual de validació de procediments, documentant resultats i millores.

- Verificar l'estat, consistència i integritat de les còpies de seguretat destinades a una futura activació de recuperació.
- Emetre informes tècnics i executius sobre l'estat de preparació per a la recuperació, riscos detectats i recomanacions.

Resultats esperats

- Existència de plans de recuperació bàsics i operatius per a serveis crítics.
- Garantia que els equips, eines i procediments necessaris per recuperar serveis estan preparats.
- Coordinació fluida entre resposta i recuperació, reduint riscos de reinfecció.
- Validació documentada de l'estat de les còpies de seguretat emprades en cada recuperació.
- Major consciència organitzativa sobre els temps reals de recuperació.
- Base sòlida per evolucionar cap als nivells avançats (P28-B i P28-C), que incorporaran processos més sofisticats i mecanismes de resiliència.

4.1.49 Paquet P28-B – Recuperació post-incident (nivell avançat)

El paquet P28-B té per objectiu consolidar i ampliar les capacitats establertes al nivell inicial (P28-A), assegurant que, en escenaris d'incident complexos, l'Ajuntament disposi de tots els elements necessaris per executar una recuperació estructurada, segura i eficient.
Aquest nivell avançat se centra en l'evolució dels plans, la validació automatitzada de les còpies, la preparació de processos en entorns híbrids i la realització de proves periòdiques que garanteixin que els mecanismes de recuperació són viables i fiables quan s'hagin d'activar.

El servei prepara la recuperació, però no realitza cap acció directa de restauració, que correspon sempre a l'Ajuntament.

Funcionalitats que ha de suportar el servei

REQ-TCN-370. Plans avançats de continuïtat i recuperació. Els plans hauran de contemplar escenaris d'interrupció complexos, integrant serveis crítics interconnectats, entorns híbrids (locals i al núvol) i càrregues virtualitzades. Aquests plans definiran com s'hauria d'executar la recuperació, però no impliquen l'execució operativa.

REQ-TCN-371. Validació automatitzada de còpies. El servei haurà d'integrar-se amb les plataformes de backup corporatives per executar comprovacions automàtiques diàries de la integritat i restaurabilitat de les còpies, incloent validacions per checksum, proves de muntatge virtual i simulacions de restauració parcial. El servei haurà de recopilar evidències de l'execució del pla de DRP (Pla de Recuperació de Desastres) i garantir que s'està realitzant correctament.

REQ-TCN-372. Proves periòdiques de recuperació. S'hauran de realitzar **proves semestrals de recuperació**, orientades a validar procediments, dependències i seqüències necessàries per a una futura recuperació real.

REQ-TCN-373. Coordinació amb proveïdors externs. Quan es tracti de serveis externalitzats o allotjats en terceres parts, el servei haurà de garantir la coordinació amb aquests proveïdors per assegurar que els plans, procediments i eines necessàries per recuperar serveis estan alineats, disponibles i verificats.

REQ-TCN-374. Informes de lliçons apreses. Cada prova o validació avançada haurà de generar un informe detallat amb les lliçons apreses, desviacions, riscos detectats i oportunitats de millora dels processos de recuperació

REQ-TCN-375. Reducció dels temps de recuperació. Els processos de preparació hauran de demostrar una millora mesurable en els objectius previstos de temps de recuperació (RTO) i de pèrdua potencial de dades (RPO), en comparació amb el nivell inicial, com a indicador de maduresa del procés.

Activitats a realitzar per part de l'adjudicatari

- Dissenyar i mantenir plans avançats de recuperació i continuïtat per a serveis municipals.
- Verificar periòdicament la integritat de les còpies de seguretat i corregir desviacions.
- Prestar el servei de verificació automatitzada diària de les còpies de seguretat i mantenir-ne l'històric de resultats
- Coordinar i executar proves semestrals de recuperació amb implicació dels equips municipals.
- Coordinar-se amb proveïdors externs per assegurar que els processos de recuperació són viables en entorns híbrids.
- Documentar resultats, lliçons apreses i recomanacions per a la millora contínua dels procediments.
- Emetre informes tècnics i executius per a responsables operatius i de direcció.

Resultats esperats

- Existència de plans avançats que cobreixen escenaris complexos i entorns híbrids.
- Validació fiable, automatitzada i regular de les còpies de seguretat.
- Millora dels objectius previstos de recuperació (RTO/RPO), com a exercici de preparació.
- Preparació reforçada davant incidents d'alt impacte que requereixin recuperacions sofisticades.
- Consolidació d'una cultura de millora contínua basada en resultats, proves i lliçons apreses.
- Integració completa de la informació de preparació per a la recuperació amb el CROC i els quadres de comandament municipals.
- Evolució cap al nivell òptim (P28-C), que permetrà exercicis integrals i mecanismes de recuperació predictiva i automatitzada.

4.1.50 Paquet P28-C – Recuperació post-incident (nivell òptim)

El paquet P28-C té per objectiu assolir el màxim nivell de maduresa en la preparació per a la recuperació post-incident, establint un model integral, automatitzat i predictiu que garanteixi que l'Ajuntament està plenament preparat per recuperar serveis fins i tot en escenaris de màxima gravetat o interrupció catastròfica.

Aquest nivell consolida la resiliència operativa municipal i assegura que tots els mecanismes necessaris per activar la recuperació estiguin disponibles, validades, coordinats i integrats amb la gestió de crisi i amb els procediments de resposta del CROC.

El servei no executa la recuperació, sinó que assegura que l'Ajuntament pot fer-la, perquè els procediments, eines, sistemes i equips estan preparats, supervisats i verificats.

Funcionalitats que ha de suportar el servei

REQ-TCN-376. Recuperació integral i automatitzada. El servei haurà d'assegurar que existeixen mecanismes d'orquestració i automatització que permetrien una recuperació ràpida i segura amb mínima intervenció manual, en cas que l'Ajuntament decideixi activar el procés. Aquests mecanismes hauran d'estar provats, documentats i coordinats amb les infraestructures municipals i amb els proveïdors de backup.

REQ-TCN-377. Exercicis de simulació integrals. S'hauran de realitzar **simulacres trimestrals de recuperació**, incloent-hi serveis crítics, dependències municipals i proveïdors externs, reproduint escenaris realistes d'interrupció massiva.

REQ-TCN-378. Capacitats de recuperació en temps real. Quan sigui tècnicament factible, el servei haurà verificar mecanismes de replicació immediata per als serveis crítics, així com validar periòdicament que els objectius previstos de RTO i RPO gairebé nuls són assolibles.

REQ-TCN-379. Alineament amb protocols de cibercrisi. El servei haurà d'estar completament integrat amb els protocols de crisi, cibercrisi i resposta del CROC municipal, assegurant que, en cas d'activació de recuperació, totes les peces organitzatives estan coordinades i preparades.

REQ-TCN-380. Millora contínua i predicció de riscos. Els resultats de cada simulacre i incident real hauran d'alimentar mecanismes de millora contínua, incorporant capacitats predictives per anticipar futurs riscos i optimitzar la resposta.

REQ-TCN-381. Quadres de comandament estratègics. Els responsables municipals hauran de disposar de dashboards estratègics amb informació immediata sobre l'estat de preparació per a la recuperació, indicadors de resiliència i evolució dels objectius previstos de RTO i RPO..

Activitats a realitzar per part de l'adjudicatari

- Dissenyar, documentar i validar els mecanismes d'automatització que permetrien una recuperació integral.
- Coordinar i executar simulacres trimestrals amb equips municipals i proveïdors crítics, en escenaris controlats.
- Verificar la viabilitat tècnica de mecanismes de replicació i recuperació immediata quan sigui factible.
- Integrar tots els procediments de preparació dins dels protocols de crisi i cibercrisi de l'Ajuntament.
- Elaborar informes predictius, estratègics i tècnics amb recomanacions de millora.
- Proporcionar quadres de comandament estratègics amb visió de la preparació per a la recuperació i la resiliència global.

Resultats esperats

- Preparació òptima per assolir RTO i RPO pràcticament nuls en els serveis més crítics quan s'activi la recuperació real.

- Realització regular de simulacres que validen i milloren la resiliència municipal.
- Integració completa dels processos de preparació amb els protocols de crisi, cibercrisi i el CROC.
- Disponibilitat d'informes predictius que orienten decisions estratègiques i inversions en resiliència.
- Evolució cap a un model de seguretat resilient, adaptatiu, proactiu i alineat amb la Directiva NIS2, l'ENS i les guies del CCN.
- Capacitat municipal consolidada per activar una recuperació integral amb risc mínim i màxima coherència operativa.

4.1.51 Paquet P29-A – Capacitació i conscienciació (nivell inicial)

El paquet P29-A té per objectiu establir les bases d'un programa de sensibilització en ciberseguretat, assegurant que el personal municipal disposi d'uns coneixements mínims per reconèixer riscos habituals i aplicar bones pràctiques bàsiques en l'ús dels sistemes d'informació. Aquest nivell inicial busca reduir la superfície d'atac derivada del factor humà i consolidar un comportament preventiu bàsic entre els usuaris.

El paràmetre quantificador d'aquest servei serà el número d'usuaris interns de l'entitat contractant objecte del servei.

El paquet P29 inclou els serveis d'administració i operació de les capacitats tecnològiques de l'entitat per simular ciberatacs, desplegar campanyes de comunicació i conscienciació, i també el llicenciament i els serveis de formació en línia i presencial. La formació s'haurà d'oferir com a mínim en català i castellà.

Tanmateix, el paquet P29 no inclou el llicenciament de les solucions de simulació de ciberatacs,

Funcionalitats que ha de suportar el servei

REQ-TCN-382. Campanyes bàsiques de sensibilització. El servei haurà de desplegar campanyes de comunicació i conscienciació amb contingut adaptat a la realitat municipal (pòsters, butlletins, guies breus).

REQ-TCN-383. Formació inicial en línia. El servei haurà de proporcionar cursos digitals bàsics, accessibles a tot el personal, amb continguts sobre phishing, gestió de contrasenyes i ús segur del correu electrònic.

REQ-TCN-384. Sessions introductòries presencials o virtuals. Es realitzaran sessions breus per grups d'usuaris, orientades a explicar riscos habituals i resoldre dubtes. S'oferiran com a mínim 24 sessions presencials anuals amb 25 alumnes per sessió.

REQ-TCN-385. Materials de bones pràctiques. El servei haurà d'elaborar documents senzills amb recomanacions concretes per al dia a dia (gestió de dispositius mòbils, ús d'aplicacions col·laboratives, protecció de dades personals).

REQ-TCN-386. Avaluació inicial de coneixements. El servei haurà de dur a terme una enquesta o prova bàsica per mesurar el nivell de conscienciació dels usuaris i establir una línia de base.

Activitats a realitzar per part de l'adjudicatari

- Definir conjuntament amb l'Ajuntament el pla de campanyes i formació bàsica.
- Elaborar i difondre materials de sensibilització adaptats al context municipal.
- Organitzar cursos en línia i sessions breus per a grups d'usuaris.
- Mesurar el nivell de coneixement dels participants mitjançant proves bàsiques.
- Generar informes amb els resultats i recomanacions de millora.

Resultats esperats

- Augment de la consciència bàsica en matèria de seguretat entre el personal municipal.
- Disponibilitat de materials i guies pràctiques per a l'ús quotidià.
- Primera línia de defensa reforçada davant riscos habituals com phishing i errors humans.
- Línia de base establerta per mesurar l'evolució en nivells més avançats (P29-B i P29-C).

4.1.52 Paquet P29-B – Capacitació i conscienciació (nivell avançat)

El paquet P29-B té per objectiu consolidar i ampliar la sensibilització en seguretat establerta al nivell inicial (P29-A), introduint tècniques més immersives i especialitzades. Aquest nivell avançat busca que els treballadors municipals siguin capaços de detectar i reaccionar davant

atacs més sofisticats, reduint la probabilitat d'èxit de campanyes de phishing, enginyeria social i altres vectors basats en el factor humà.

Funcionalitats que ha de suportar el servei

REQ-TCN-387. Simulacions periòdiques de phishing. El servei haurà de dur a terme simulacions regulars d'atacs de phishing i enginyeria social per avaluar la capacitat de resposta dels usuaris i identificar àrees de millora.

REQ-TCN-388. Tallers pràctics especialitzats. Es realitzaran tallers temàtics (per exemple, protecció de dades, ús segur de plataformes col·laboratives, gestió d'incidents interns) amb exercicis pràctics i casos reals.

REQ-TCN-389. Campanyes interactives de conscienciació. El servei haurà d'incloure campanyes multimèdia més avançades (vídeos interactius, newsletters digitals, pòdcasts interns) adaptades a perfils específics d'usuaris.

REQ-TCN-390. Avaluacions periòdiques de coneixements. Es duran a terme proves en línia després de cada acció formativa per mesurar el progrés i adaptar els continguts a les necessitats detectades.

REQ-TCN-391. Informes de maduresa en conscienciació. El servei haurà de generar informes periòdics amb mètriques sobre el nivell de consciència del personal, la taxa d'èxit en simulacions de phishing i recomanacions de millora contínua.

Activitats a realitzar per part de l'adjudicatari

- Dissenyar i executar simulacions de phishing adaptades al context municipal.
- Organitzar tallers pràctics presencials o virtuals amb exercicis basats en incidents reals.
- Desenvolupar i difondre campanyes interactives adaptades als perfils d'usuari.
- Avaluar el coneixement i el comportament dels treballadors després de cada activitat.
- Generar informes de maduresa i recomanacions per optimitzar el programa de conscienciació.

Resultats esperats

- Major capacitat dels treballadors per identificar i evitar atacs de phishing i enginyeria social.
- Personal municipal format en bones pràctiques específiques i aplicables al seu dia a dia.

- Increment progressiu dels índexs de maduresa en conscienciació.
- Reducció significativa de l'exposició al risc associat al factor humà.
- Base sòlida per evolucionar cap al nivell òptim (P29-C), que integrarà programes continus i avaluacions regulars a escala global.

4.1.53 Paquet P29-C – Capacitació i conscienciació (nivell òptim)

El paquet P29-C té per objectiu assolir el màxim nivell de maduresa en la capacitació i conscienciació en seguretat, establint un programa permanent, adaptatiu i alineat amb els riscos emergents. Aquest nivell garanteix que el conjunt del personal municipal adquireixi i mantingui hàbits de seguretat sòlids, amb una cultura organitzativa on la ciberseguretat sigui part natural de l'activitat diària.

Funcionalitats que ha de suportar el servei

REQ-TCN-392. Programes continus de formació. El servei haurà de desplegar formacions contínues i modulars, amb itineraris adaptats per rols i nivells de responsabilitat, incloent personal tècnic, directiu i operatiu.

REQ-TCN-393. Simulacions avançades i campanyes realistes. El servei haurà de realitzar mensualment simulacions de phishing i enginyeria social avançada, amb escenaris realistes i complexos que integrin múltiples canals (correu, trucades, missatgeria instantània).

REQ-TCN-394. Exercicis de seguretat a escala organitzativa: les proves hauran d'incloure escenaris de compromís d'usuaris VIP, atacs a la cadena de subministrament i proves de resiliència dels serveis públics essencials. El servei haurà d'incloure com a mínim **un simulacre semestral** de resposta a incidents i crisi, adaptat a escenaris d'alt impacte i coordinat amb equips municipals i terceres parts.

REQ-TCN-395. Avaluacions regulars i mètriques de progrés. Es duran a terme avaluacions trimestrals del nivell de consciència, amb mètriques clau (taxa de clics en phishing simulat, temps de notificació d'incidents, índex de resposta adequada).

REQ-TCN-396. Programes de conscienciació immersius. El servei haurà d'incloure activitats immersives com jocs de rol, escape rooms digitals i exercicis de crisi simulada per fomentar l'aprenentatge pràctic i col·laboratiu.

REQ-TCN-397. Quadres de comandament estratègics. Els responsables municipals hauran de disposar de dashboards amb visibilitat en temps real sobre l'estat de la conscienciació, evolució de les mètriques i comparatives històriques.

REQ-TCN-398. Integració amb el pla director de seguretat. El programa de capacitació haurà d'estar plenament alineat amb el pla director de seguretat i amb els objectius estratègics municipals en matèria de ciberresiliència.

Activitats a realitzar per part de l'adjudicatari

- Desenvolupar i mantenir un programa continu de capacitació amb itineraris adaptatius.
- Dissenyar i executar simulacions realistes d'enginyeria social i phishing avançat.
- Realitzar avaluacions periòdiques i elaborar informes amb mètriques d'evolució.
- Coordinar activitats immersives per reforçar l'aprenentatge pràctic.
- Proporcionar quadres de comandament estratègics per a la direcció municipal.
- Assegurar l'alineament permanent del programa amb els objectius del pla director de seguretat.

Resultats esperats

- Consolidació d'una cultura organitzativa de seguretat madura i resilient.
- Personal municipal capaç de reconèixer i reaccionar ràpidament davant tècniques d'enginyeria social avançada.
- Disponibilitat de mètriques fiables que permetin mesurar i demostrar el progrés en conscienciació.
- Integració de la formació i la sensibilització dins de l'estratègia de seguretat municipal.
- Reducció sostinguda del risc derivat del factor humà i preparació òptima davant nous vectors d'amenaça.

4.1.54 Paquet P30-A – Governança i compliment (nivell inicial)

El paquet P30-A té per objectiu establir una primera capa de governança en matèria de seguretat de la informació, gestió de riscos i ciberresiliència, assegurant que l'Ajuntament disposi de visibilitat bàsica sobre el nivell de compliment i els riscos associats. Aquest nivell inicial posa les bases per generar una supervisió mínima, documentar la situació actual i iniciar un procés estructurat de millora dins del marc operatiu d'un CROC (Centre de Riscos i Operacions de Ciberresiliència).

El paràmetre quantificador d'aquest servei serà el número d'usuaris interns de l'entitat contractant objecte del servei.

El paquet P30 inclou els serveis d'elaboració i actualització dels quadres de comandament i informes de seguiment (operatius, tàctics i estratègics).

Funcionalitats que ha de suportar el servei

REQ-TCN-399. Quadres de comandament bàsics. El servei haurà de proporcionar panells amb els principals indicadors de seguretat i risc (incidents, vulnerabilitats obertes, nivells de parxes aplicats), accessibles als responsables municipals. El servei haurà de proporcionar com a mínim els següents indicadors clau de forma agregada per criticitat, classificació i tipus d'incident d'acord a la guia CCN-STIC-817:

- MTTD – Mean Time To Detect
  - Temps promig que triga el CROC en detectar una amenaça (incident, vulnerabilitat, etc) des de que esdevé el primer indici.
- MTTC – Mean Time To Contain
  - Temps promig que triga el CROC en fer la primera tasca de contenció per mitigar l'amenaça des de que s'ha detectat.
- MTTR - Mean Time To Resolve
  - Temps promig que triga el CROC en resoldre la situació i recuperar completament la normalitat del servei des de que l'amenaça s'ha detectat.
- FPR - False Positive Rate
  - Taxa de falsos positius: percentatge d'alertes que resulten no ser incidents reals.
- FNR – False Negative Rate
  - Taxa de falsos negatius: percentatge d'incidents reals que no són detectats pel CROC en temps i forma.
- Número d'incidents de seguretat gestionats

    - Número total d'incidents detectats, investigats i resolts en un període.
- Acumulat de tiquets de servei oberts
    - Número de tiquets de servei (alertes, incidents, peticions, etc) oberts en mans del CROC pendents de resolució.
- Taxa d'escalat d'alertes i d'incidents
    - Percentatge d'alertes i d'incidents que requereixen escalat a equips tècnics de l'entitat contractant
- Cobertura de detecció
    - Percentatge de tècniques MITRE ATT&CK cobertes per casos d'ús i regles de detecció.

REQ-TCN-400. Informes de seguiment. El servei haurà de generar informes periòdics amb l'estat de seguretat i compliment, destacant les principals desviacions respecte a marcs com l'ENS, la NIS2 i les guies del CCN.

REQ-TCN-401. Registre de riscos bàsic. El servei haurà d'incloure un catàleg inicial de riscos de seguretat de la informació, basat en incidents registrats i en els resultats d'auditories o escanejos de vulnerabilitats, classificant-los segons probabilitat i impacte.

REQ-TCN-402. Traçabilitat mínima de controls. El servei haurà de permetre identificar quins controls de seguretat bàsics estan implementats i quins manquen, establint un primer mapa de cobertura i la seva relació amb els riscos associats.

REQ-TCN-403. Canal de report bàsic. El servei haurà de facilitar un mecanisme senzill perquè els responsables municipals puguin reportar desviacions, incidències o nous riscos relacionades amb el compliment.

Activitats a realitzar per part de l'adjudicatari

- Configurar i mantenir quadres de comandament bàsics de seguretat i risc.
- Generar informes periòdics amb les principals mètriques i exposició al risc.
- Elaborar i actualitzar un registre bàsic de riscos.
- Mapar els controls de seguretat existents i identificar les principals mancances.
- Facilitar un mecanisme de report per a responsables municipals.

Resultats esperats

- Visibilitat inicial sobre el nivell de seguretat i compliment normatiu.
- Disponibilitat d'indicadors bàsics per a la direcció municipal.
- Primer registre de riscos que permet establir prioritats de millora.

- Mapa inicial de controls de seguretat i cobertura.
- Base sòlida per evolucionar cap als nivells avançat i òptim (P30-B i P30-C), on s'incorporaran seguiments més detallats, auditories, plans estratègics de governança i gestió de riscos.

4.1.55 Paquet P30-B – Governança i compliment (nivell avançat)

El paquet P30-B té per objectiu ampliar i consolidar les capacitats establertes en el nivell inicial (P30-A), introduint mecanismes més madurs de seguiment, control, gestió de riscos i millora contínua. Aquest nivell garanteix que l'Ajuntament disposi d'una supervisió estructurada, amb mètriques fiables, plans de millora específics i un alineament més estret amb els requisits normatius i de governança corporativa, dins del marc operatiu d'un CROC (Centre de Riscos i Operacions de Ciberresiliència)..

Funcionalitats que ha de suportar el servei

REQ-TCN-404. Quadres de comandament avançats. El servei haurà de proporcionar panells enriquits amb indicadors clau de seguretat, compliment i risc, segmentats per àmbits (tecnològic, organitzatiu, normatiu) i amb capacitat de comparativa històrica.

REQ-TCN-405. Seguiment d'indicadors de compliment. El servei haurà de monitorar el grau de compliment amb els marcs normatius aplicables (ENS, NIS2, guies CCN), i el nivell d'exposició al risc establint percentatges de cobertura i alertes sobre desviacions.

REQ-TCN-406. Plans de millora operativa. El servei haurà d'elaborar i mantenir plans de millora derivats d'auditories, exercicis de resposta a incidents i anàlisis de riscos, amb calendarització i responsables assignats.

REQ-TCN-407. Coordinació amb processos de gestió de riscos. El servei haurà d'assegurar que els resultats de governança alimentin el registre de riscos municipal i els plans de tractament associats, garantint la seva traçabilitat dins del CROC

REQ-TCN-408. Informes executius i tècnics de seguiment. El servei haurà de lliurar informes regulars que combinin una visió executiva (nivell de compliment, desviacions, prioritats, riscos identificats) amb un detall tècnic de les àrees de millora.

REQ-TCN-409. Sessions de revisió periòdiques. El servei haurà d'organitzar reunions periòdiques amb responsables municipals per revisar resultats, validar prioritats de tractament de riscos i acordar ajustos als plans de millora.

Activitats a realitzar per part de l'adjudicatari

- Configurar i mantenir quadres de comandament avançats de seguretat i compliment.
- Monitorar i reportar el nivell de compliment i l'exposició al risc respecte als marcs normatius aplicables.
- Elaborar i fer el seguiment de plans de millora calendaritzats i prioritzats.
- Correlacionar els resultats de governança amb el registre i tractament de riscos.
- Lliurar informes executius i tècnics amb recomanacions accionables.
- Conduir sessions periòdiques de revisió amb responsables municipals.

Resultats esperats

- Visibilitat completa i estructurada sobre el nivell de seguretat i compliment normatiu.
- Existència de plans de millora concrets, amb responsables i terminis establerts.
- Millora progressiva i mesurable dels nivells de compliment.
- Integració directa de la governança amb els processos de gestió de riscos.
- Major capacitat de decisió estratègica gràcies a informes diferenciats per perfils tècnics i executius.
- Base sòlida per evolucionar cap al nivell òptim (P30-C), que consolidarà fulls de ruta estratègics i una visió global de gestió de riscos i resiliència corporativa.

4.1.56 Paquet P30-C – Governança i compliment (nivell òptim)

El paquet P30-C té per objectiu assolir el màxim nivell de maduresa en governança, compliment i gestió de riscos, establint un model estratègic, proactiu i plenament integrat amb la direcció municipal. Aquest nivell garanteix que la gestió de la seguretat i dels riscos associats estigui alineada amb les prioritats de l'Ajuntament, reforçada per auditories externes i per fulls de ruta que asseguren la millora contínua i la resiliència corporativa dins d'un marc del CROC (Centre de Riscos i Operacions de Ciberresiliència).

Funcionalitats que ha de suportar el servei

REQ-TCN-410. Fulls de ruta estratègics. El servei haurà de definir i mantenir fulls de ruta plurianuals que alineïn els objectius de seguretat i gestió de riscos amb els de l'Ajuntament, incorporant inversions prioritzades i objectius de maduresa.

REQ-TCN-411. Quadres de comandament estratègics. Els responsables municipals hauran de disposar de dashboards estratègics que mostrin en temps real el nivell de compliment, l'evolució de riscos i l'impacte de les millores implantades.

REQ-TCN-412. Auditories externes de validació. El servei haurà de contemplar auditories externes anuals realitzades per entitats independents, que validin el nivell de compliment, la maduresa dels processos de gestió de riscos i la maduresa dels processos de governança.

REQ-TCN-413. Integració amb la direcció municipal. Els processos de governança hauran de formar part de les dinàmiques de decisió estratègica de la direcció municipal, facilitant la presa de decisions **basada en el risc i l'impacte operatiu**.

REQ-TCN-414. Millora contínua i benchmark internacional. El servei haurà de garantir la revisió i actualització contínua de processos, utilitzant com a referència bones pràctiques i estàndards internacionals, i comparant el nivell de maduresa amb entorns similars.

REQ-TCN-415. Informes estratègics anuals. El servei haurà de generar informes anuals amb una visió executiva i tècnica, incloent la situació actual, l'evolució dels riscos de seguretat, les fites assolides i les recomanacions per mantenir i millorar la resiliència.

Activitats a realitzar per part de l'adjudicatari

- Dissenyar i mantenir fulls de ruta estratègics de seguretat alineats amb els objectius municipals.
- Configurar i mantenir quadres de comandament estratègics per a la direcció municipal.
- Coordinar i facilitar auditories externes anuals.
- Participar en sessions de decisió estratègica de la direcció municipal.
- Actualitzar processos i controls segons benchmark internacional i lliçons apreses.
- Elaborar informes estratègics anuals amb recomanacions concretes d'inversió i mitigació de riscos.

Resultats esperats

- Governança òptima, amb processos completament alineats amb l'estratègia municipal i el marc de gestió de riscos.
- Transparència i visibilitat estratègica per a la direcció i responsables polítics.
- Validació independent del nivell de compliment, maduresa i gestió de riscos.
- Millora contínua sostinguda gràcies a referències internacionals i comparatives sectorials.
- Capacitat d'anticipar riscos i orientar inversions estratègiques en seguretat.
- Resiliència corporativa i operativa consolidada dins del marc del CROC, alineada amb els marcs NIS2, ENS i directrius del CCN.

5. Descripció dels serveis a prestar per l'adjudicatari de Lot 2

A continuació es detallen els serveis que haurà de prestar l'adjudicatari del Lot 2 en el marc dels contractes basats derivats del present Acord Marc. El Lot 2 té per finalitat exclusiva proporcionar serveis d'avaluació independent, validació, verificació tècnica i control qualitatiu sobre les capacitats, processos, configuracions i resultats del CROC (Centre de Riscos i Operacions de Ciberresiliència), amb plena independència respecte dels serveis operatius prestats en la resta de lots.

En primer lloc, es descriuen els **serveis generals obligatoris**, aplicables a qualsevol contracte basat del Lot 2. Aquests serveis constitueixen la base comuna que garanteix la imparcialitat, la coherència metodològica i la traçabilitat de totes les activitats d'avaluació. L'adjudicatari haurà de proporcionar, com a mínim, la direcció i el seguiment dels treballs, la documentació tècnica i funcional generada, la coordinació amb l'equip d'operacions de l'entitat municipal, l'elaboració d'informes d'avaluació i validació, i l'assessorament necessari per permetre a l'Ajuntament entendre l'impacte, la qualitat i l'eficàcia de les capacitats operatives avaluades. Igualment, haurà d'assegurar la correcta gestió del canvi en els processos d'avaluació i la traçabilitat de totes les actuacions realitzades.

Tot seguit, es descriuen els **serveis específics del Lot 2**, que podran ser sol·licitats de forma independent en cada contracte basat. Aquests serveis cobreixen la verificació de configuracions, la revisió de procediments operatius, l'avaluació de capacitats de detecció, resposta i resiliència, la realització de proves de qualitat i robustesa, la validació de resultats operatius, l'anàlisi de mètriques, l'avaluació de la qualitat del servei prestat en altres lots, i qualsevol altra activitat orientada al control independent i a la millora contínua del CROC.

Per la seva naturalesa de **servei d'avaluació i validació independent**, tots els treballs del Lot 2 hauran de ser prestats de manera autònoma respecte dels serveis operatius i sense cap interferència amb els processos del CROC i OSAP, assegurant la neutralitat, l'objectivitat i la fiabilitat dels resultats.

5.1 Serveis generals inclosos

De manera transversal a tots els contractes basats derivats del present Acord Marc, es defineix un conjunt de serveis generals que l'adjudicatari del **Lot 2** haurà de prestar obligatòriament en qualsevol servei d'avaluació, verificació o validació independent del CROC i OSAP. Aquests serveis generals constitueixen l'eix metodològic i de qualitat del Lot 2 i tenen com a objectiu garantir la imparcialitat, la rigorositat tècnica, la traçabilitat i la coherència de totes les activitats de revisió i control.

Els serveis generals inclouen les activitats següents:

- **Direcció global del servei contractat**, amb la coordinació i el seguiment de totes les tasques previstes en cada contracte basat, assegurant la interlocució fluida amb la direcció de projecte de les entitats adherides i la coordinació entre tots els agents implicats, siguin tècnics, funcionals, operatius o proveïdors externs.
- **Planificació, supervisió i seguiment del projecte**, incloent l'elaboració i manteniment del pla de treball, amb cronograma, fites, dependències, identificació de riscos, mecanismes de control i informes de seguiment, garantint la comunicació regular amb els responsables municipals designats.
- **Gestió mitjançant eines corporatives**, amb l'ús obligatori de les eines de gestió de projectes determinades per les entitats adherides, mantenint tota la informació degudament registrada i actualitzada i assegurant la traçabilitat completa de les accions i decisions.
- **Presa i validació de requisits funcionals i tècnics**, amb la recollida, documentació i validació conjunta amb els responsables municipals, aportant estimacions d'esforç, impactes operatius i consideracions tècniques o econòmiques.

- **Generació i actualització de documentació tècnica**, que haurà d'incloure com a mínim:
    - Documentació tècnica i funcional relacionada amb les activitats de revisió i validació.
    - Registre de resultats, evidències, proves aplicades i conclusions.
    - Documentació de canvis, validacions, decisions i control de versions.
    - Manuals o guies que facilitin la interpretació i l'aplicació dels criteris d'avaluació.
- **Reporting i seguiment executiu**, amb l'emissió d'informes periòdics sobre l'estat dels treballs, els resultats preliminars, les desviacions detectades, l'anàlisi de riscos i les recomanacions de millora. S'haurà d'elaborar una memòria de tancament en finalitzar cada contracte basat.
- **Gestió de la qualitat**, mitjançant la revisió metodològica de totes les activitats d'avaluació, l'ús d'estàndards i bones pràctiques reconegudes, l'auditoria interna dels processos aplicats, i la formulació de recomanacions orientades a la millora contínua de les capacitats operatives del CROC-OSAP.
- **Gestió del tancament del projecte**, que haurà d'incloure la validació final dels resultats, el lliurament complet de la documentació, l'explicació tècnica de les conclusions, la revisió conjunta amb els responsables municipals i, si escau, l'aixecament de l'acta de conformitat.

Aquests serveis generals són de compliment obligatori i s'han d'incloure de manera inherent en qualsevol contracte basat derivat del Lot 2, amb independència de la naturalesa, abast o finalitat de l'activitat d'avaluació.

5.1.1 Requisits tècnics generals del servei

Els requisits tècnics generals definits a continuació són d'aplicació obligatòria a qualsevol servei contractat en el marc del present Acord Marc per al **Lot 2**, i constitueixen les condicions mínimes que ha de complir el servei d'avaluació, verificació i validació proposat pel licitador.

Aquests requisits tenen com a objectiu assegurar la **coherència tècnica, la rigorositat metodològica, l'eficiència en l'execució de les avaluacions i el compliment normatiu** del servei dins de l'ecosistema digital municipal. Tots ells seran objecte de valoració i verificació tant en el procés de licitació com durant l'execució dels contractes basats.

Per cadascun dels requeriments, el licitador haurà d'indicar en una **matriu de conformitat** (veure Annex 2) el seu grau de compliment segons les opcions següents:

- "**Compleix**"
- "**No compleix**"
- "**No aplica**"

REQ-TCN-416. Servei industrialitzat d'avaluació. El servei haurà d'estar basat en un model industrialitzat, capaç d'incorporar de manera homogènia metodologies, criteris i casos d'ús a les diferents tecnologies presents a les entitats municipals. gualment, haurà de permetre incorporar noves metodologies o pràctiques desenvolupades en altres clients de l'adjudicatari, garantint que l'Ajuntament es beneficiï de la millora contínua i de l'efecte d'escala propi d'un servei madur.

REQ-TCN-417. Plataforma com a servei per a l'avaluació. El servei haurà de proporcionar, de manera gestionada i sota modalitat de servei, una plataforma que doni suport als processos d'avaluació, verificació i reporting, incloent la gestió d'evidències, el seguiment de troballes, la traçabilitat de les revisions i l'emissió d'informes, amb capacitat d'escalabilitat horitzontal quan s'incrementi l'abast o el nombre de serveis avaluats.

REQ-TCN-418. Incorporació progressiva d'intel·ligència artificial. El servei haurà d'integrar funcionalitats basades en intel·ligència artificial i aprenentatge automàtic per millorar l'anàlisi de dades, la priorització de riscos, la detecció de patrons i la identificació de desviacions significatives en els resultats de les avaluacions. Haurà d'incloure un pla d'evolució que permeti incrementar la maduresa d'aquestes capacitats durant la vigència del contracte.

REQ-TCN-419. Automatització de processos d'avaluació. El servei haurà d'incorporar automatismes per a la gestió de processos d'avaluació i validació, des de la recollida d'evidències fins a la generació d'informes o quadres de comandament. Els fluxos d'automatització hauran d'estar documentats, ser revisables per les entitats contractants i poder evolucionar al llarg del contracte.

REQ-TCN-420. Escalabilitat i modularitat. El servei haurà de ser escalable per cobrir increments en el nombre de serveis, sistemes o entitats municipals avaluades, i modular per permetre afegir nous àmbits d'avaluació o nous tipus de proves sense impactar el funcionament ordinari del servei.

REQ-TCN-421. Compliment normatiu. El servei haurà de garantir el compliment de la Directiva NIS2, l'Esquema Nacional de Seguretat i les guies tècniques del CCN que resultin aplicables a l'activitat d'avaluació, i assegurar que les dades i evidències analitzades es custodien exclusivament en centres de dades ubicats dins de la Unió Europea..

REQ-TCN-422. Transparència i traçabilitat. El servei haurà de disposar de mecanismes que permetin als responsables municipals consultar, en temps adequat, l'estat de cada avaluació, les troballes identificades, les recomanacions emeses i les accions de seguiment, garantint la traçabilitat completa des de la recollida d'evidències fins a les conclusions finals.

REQ-TCN-423. Evolució i millora contínua. El licitador haurà de presentar un pla d'evolució del servei, revisat almenys anualment, que inclogui l'adopció de noves metodologies d'avaluació, millores en els processos d'anàlisi, l'ús d'IA i eines avançades, i l'optimització dels temps i esforços requerits, garantint la millora contínua del servei durant tota la vigència del contracte.

REQ-TCN-424. Integració amb plataforma ITSM i eines corporatives de l'entitat. El servei haurà de poder integrar-se amb la plataforma ITSM (IT Service Management) o amb les eines corporatives que determini l'entitat contractant, a fi de registrar, documentar i gestionar les peticions d'avaluació, les troballes, les recomanacions i el seu seguiment, sense que això suposi cap cost addicional per a l'entitat.

REQ-TCN-425. Documentació operativa. El servei haurà de documentar mitjançant protocols, metodologies i procediments totes les activitats d'avaluació i validació que es realitzin durant l'execució del contracte. Aquesta documentació haurà de ser revisada periòdicament i aprovada per l'autoritat competent abans de la seva entrada en vigor. Tota la documentació generada serà propietat de l'entitat contractant i, un cop finalitzat el servei, s'haurà de garantir el lliurament de la documentació i la destrucció de qualsevol còpia en mans del proveïdor, excepte que la normativa disposi el contrari.

REQ-TCN-426. Personal especialitzat: El servei haurà de disposar de personal especialitzat en cadascun dels àmbits d'avaluació (seguretat, operacions, governança, compliment, etc.), i

aquest personal haurà de comptar amb certificacions reconegudes nacional o internacionalment que acreditin el coneixement i l'experiència necessaris per a l'execució de les tasques.

REQ-TCN-427. Procediment d'emergència: El servei haurà de disposar dels recursos necessaris i d'un procediment d'actuació en cas que, durant una avaluació, es detecti una vulnerabilitat crítica o una situació de risc greu que requereixi comunicació i atenció immediata amb l'entitat contractant. Aquest procediment haurà de detallar els mitjans de contacte, les persones responsables i els passos a seguir fins a la transferència formal de la gestió a l'equip corresponent de l'Ajuntament. La comunicació inicial haurà de realitzar-se, com a mínim, de forma telefònica, establint contacte directe i immediat amb els responsables designats de l'entitat contractant, sense que l'obertura d'un tiquet o qualsevol altre mecanisme asíncron es consideri suficient en aquests casos d'emergència.

REQ-TCN-428. Certificació de Conformitat amb l'ENS: Els sistemes d'informació i els processos que emprin les organitzacions adjudicatàries per a la prestació del servei hauran de disposar de la certificació de conformitat amb l'Esquema Nacional de Seguretat per a categoria MITJANA o superior, o bé evidenciar l'adient adopció del conjunt mínim de mesures de seguretat recollides a la guia CCN-STIC-896, amb el compromís formal d'obtenir la certificació en un termini no superior a 12 mesos si encara no es disposa de la mateixa.

REQ-TCN-429. Atracció, promoció i retenció del talent: el servei haurà de demostrar que implementa mesures per atraure, promocionar i retenir el talent, especialment el talent femení, fomentant la igualtat de gènere en el sector de la ciberseguretat.

REQ-TCN-430. Ús de ciberintel·ligència en les avaluacions: El servei haurà de ser capaç d'incorporar fonts de ciberintel·ligència (per exemple, indicadors d'amenaces, campanyes actives, vulnerabilitats crítiques) en els seus processos d'avaluació i validació, a fi de contextualitzar millor els riscos i ajustar les recomanacions a l'escenari d'amenaces vigent.

REQ-TCN-431. Comunicació tècnica amb l'entitat contractant: El servei haurà d'elaborar les propostes de comunicació tècnica relatives als resultats de les avaluacions, les troballes crítiques i les recomanacions de millora, que hauran de ser sempre validades amb l'entitat contractant abans de fer-se arribar als equips afectats o a altres interlocutors.

5.1.2 Paquet P31 – Avaluació i millora contínua

El paquet P31 té per objectiu establir un servei d'avaluació i millora contínua del servei que acompanyi al CROC i l'ajudi a evolucionar madurant i incrementant les seves capacitats a nivell de governança, prevenció, protecció, detecció, contenció, resposta i recuperació davant de ciberincidents. Aquest paquet incorpora pràctiques de Red Team, validació contínua de controls de seguretat, exercicis de simulació híbrida (Purple Team) i exercicis de seguretat a escala organitzativa.

El paràmetre quantificador d'aquest servei serà el número d'usuaris interns de l'entitat contractant objecte del servei.

El paquet P31 inclou el llicenciament i els serveis d'administració i operació de les solucions per fer una supervisió i avaluació contínua del servei CROC, així com el llicenciament i els serveis de RedTeam i PurpleTeam.

Funcionalitats que ha de suportar el servei

REQ-TCN-432. Supervisió i avaluació contínua del CROC: El servei haurà de proporcionar una avaluació contínua del nivell de maduresa del CROC a escala estratègica (anual), tàctica (trimestral) i operativa (setmanal), incloent indicadors clau de rendiment (KPI), indicadors clau de risc (KRI) i mètriques de qualitat del servei (SLA i SLO).
Les avaluacions hauran d'abastar, com a mínim, els dominis de Negoci, Persones, Processos, Tecnologia i Serveis, i presentar-se en quadres de comandament multinivell amb vista actual, evolució històrica i tendències.

REQ-TCN-433. Mapa de ruta de maduresa: elaborar i presentar, com a mínim trimestralment, un mapa de maduresa per dominis (Negoci, Persones, Processos, Tecnologia i Serveis) i per subdominis (p.e. governança, gestió del coneixement, gestió de vulnerabilitats, anàlisi forense, SIEM, etc) del CROC, identificant la situació actual (AS-IS), la situació objectiu (TO-BE) i les mancances més significatives (GAPs) presentant propostes i recomanacions d'accions concretes que permetin suplir les carències per arribar a la situació objectiu desitjada per l'entitat contractant.

REQ-TCN-434. Avaluació integrada de maduresa: El servei haurà d'avaluar periòdicament la maduresa del CROC mitjançant un marc d'avaluació integrat que combini:

- un model estructurat de maduresa del CROC reconegut internacionalment (SOC-CMM, NIST CSF, MITRE SOC Assessments o equivalents), i

- una avaluació tècnica de les capacitats de detecció i resposta basada en la matriu MITRE ATT&CK, identificant cobertures, mancances i oportunitats de millora.

L'avaluació integrada haurà d'incloure:

- puntuacions quantitatives i qualitatives per domini i subdomini,
- cobertura de tècniques ATT&CK i correlació amb casos d'ús operatius del CROC,
- comparatives històriques,
- identificació de GAPs prioritzats segons risc i amenaça real, i
- recomanacions concretes per avançar cap al nivell de maduresa objectiu.

Aquesta avaluació haurà d'incloure puntuacions quantitatives i qualitatives, comparatives històriques i recomanacions de millora vinculades al mapa de maduresa del requeriment anterior.

REQ-TCN-435. Integració amb el servei de GRC i amb el Pla Director de Seguretat. El servei ha d'estar plenament integrat amb el servei de GRC de l'entitat contractant, el Pla Director de Seguretat de l'Ajuntament de Barcelona i els objectius estratègics municipals en matèria de ciberresiliència.

REQ-TCN-436. Exercicis de Red Team a escala municipal: El servei haurà d'incloure simulacions d'atac realistes, persistents i multidimensionals, orientades a validar les capacitats de detecció, resposta i contenció del CROC. Aquestes simulacions hauran de reproduir tàctiques, tècniques i procediments d'actors amenaçadors avançats (APT), mantenint un entorn controlat i documentat. El servei haurà de garantir la realització de quatre (4) exercicis Red Team anuals, distribuïts de manera que cobreixin diferents escenaris, superfícies d'atac i capacitats operatives del CROC.

REQ-TCN-437. Validació contínua de controls de seguretat: el servei haurà d'incloure la verificació periòdica i automatitzada de l'eficàcia dels controls tècnics desplegats, amb proves que en validin la resiliència davant vectors d'atac actuals, identificant debilitats, desviacions o ineficiències, i proposant mesures correctores.

REQ-TCN-438. Exercicis de simulació híbrida (Purple Team): el servei haurà d'incloure exercicis coordinats entre equips de Red Team i Blue Team per optimitzar els casos de detecció i resposta, generant aprenentatge immediat i millora contínua.

REQ-TCN-439. Millora contínua i benchmark internacional. El servei haurà de garantir la revisió i actualització contínua de processos, utilitzant com a referència bones pràctiques i estàndards internacionals, i comparant el nivell de maduresa amb entorns similars.

REQ-TCN-440. Auditories periòdiques de serveis, processos i procediments del CROC. El servei auditarà periòdicament (com a mínim mensualment) els serveis, processos i procediments del CROC per tal de validar que en tots els casos es segueix el PNT (procediment normalitzat de treball) adient, es mesura l'eficàcia i eficiència dels casos d'ús i playbooks, i es compleixen els estàndards de qualitat definits. Aquestes auditories hauran d'incloure evidències, conclusions i recomanacions.

REQ-TCN-441.. Independència i absència de conflictes d'interès. El servei haurà d'assegurar, documentar i demostrar la seva independència operativa i organitzativa respecte de qualsevol proveïdor que presti serveis operatius del CROC (incloent Lots 1 i 3). Això inclou prohibició de compartir equips, eines, dades o processos que puguin comprometre l'objectivitat de les avaluacions.

Activitats a realitzar per part de l'adjudicatari

- Supervisar i avaluar de forma contínua el servei del CROC de l'entitat.
- Proporcionar quadres de comandament multinivell amb agrupació estratègica, tàctica i operativa.
- Elaborar i mantenir el mapa de ruta de maduresa del CROC de l'entitat.
- Integrar les activitats i recomanacions amb el servei de GRC i el Pla Director de Seguretat.
- Realitzar auditories periòdiques dels serveis, processos i procediments del CROC.
- Realitzar una avaluació integrada de maduresa del CROC mitjançant models reconeguts (p. ex. SOC-CMM/NIST CSF) i l'anàlisi basada en MITRE ATT&CK.
- Aplicar mecanismes de validació contínua de controls
- Planificació i coordinació d'exercicis de Red Team i Purple Team amb l'Ajuntament, establint objectius clars, regles de joc i mecanismes de supervisió.

Resultats esperats

- Visibilitat a nivell estratègic, tàctic i operatiu del nivell de maduresa del CROC.
- Millora contínua de la maduresa del CROC d'acord al mapa de ruta.
- Alineament i retroalimentació amb GRC i Pla Director de Seguretat.
- Millora en l'eficàcia i 'eficiència dels serveis, processos i procediments del CROC.

- Increment de la resiliència municipal gràcies a exercicis Red Team/Purple Team i auditories periòdiques.
- Disposar de resultats objectius, mesurables i comparables gràcies a les avaluacions SOC-CMM/NIST CSF, l'anàlisi MITRE ATT&CK i la validació contínua.

6. Descripció dels serveis a prestar per l'adjudicatari de Lot 3

A continuació es detallen els serveis que haurà de prestar l'adjudicatari en el marc dels contractes basats derivats del present Acord Marc per al desplegament, l'operació i l'evolució dels **serveis i eines avançades de protecció (OSAP).**

En primer lloc, es descriuen els serveis generals obligatoris, aplicables a qualsevol contracte basat derivat d'aquest acord, independentment del paquet funcional contractat. Aquests serveis constitueixen la base comuna que garanteix la coherència, la integració i la qualitat tècnica de totes les prestacions OSAP. L'adjudicatari haurà de proporcionar, com a mínim, la direcció i el seguiment dels projectes, la documentació tècnica i funcional, la formació operativa als equips municipals quan sigui requerida i la coordinació amb l'equip d'operacions de l'entitat municipal. Igualment, haurà d'assegurar la correcta gestió del canvi, la supervisió continuada de les activitats i la traçabilitat de totes les actuacions realitzades.

Tot seguit, es descriuen els **paquets funcionals específics contractables de forma independent**, i que constitueixen les unitats mínimes de prestació dels serveis OSAP. Cada paquet cobreix funcionalitats concretes relacionades amb l'operació, administració, configuració, actualització, optimització i evolució de les eines avançades de protecció.

Per la seva naturalesa modular i complementària, els diferents paquets es poden combinar lliurement en els contractes basats, i hauran de ser prestats de forma homogènia, garantint així la continuïtat operativa i l'alineament amb l'estratègia global de seguretat definida per l'Ajuntament de Barcelona.

6.1 Serveis generals inclosos

De manera transversal a tots els contractes basats que es derivin del present Acord Marc, es defineix un conjunt de serveis generals que l'adjudicatari haurà de prestar obligatòriament com a part de l'execució de qualsevol paquet funcional relacionat amb els serveis d'Operació de Serveis i eines Avançades de Protecció (OSAP).

Aquests serveis generals constitueixen l'eix de suport operatiu, coordinació i control de qualitat dels projectes, i tenen com a objectiu garantir l'homogeneïtat, la traçabilitat i la integració de totes les actuacions que es desenvolupin en el marc d'aquest Acord Marc. Inclouen les activitats següents:

- **Direcció global del servei contractat**, amb la coordinació i el seguiment de totes les tasques previstes en cada contracte basat, assegurant la interlocució fluida amb la direcció de projecte de les entitats adherides i la coordinació entre tots els agents implicats, siguin tècnics, funcionals, operatius o proveïdors externs.

- **Planificació, supervisió i seguiment del projecte**, incloent l'elaboració i manteniment del pla de treball, amb cronograma, fites, dependències, identificació de riscos, mecanismes de control i informes de seguiment, garantint la comunicació regular amb els responsables municipals designats.

- **Gestió mitjançant eines corporatives**, amb l'ús obligatori de les eines de gestió de projectes determinades per les entitats adherides, mantenint tota la informació degudament registrada i actualitzada i assegurant la traçabilitat completa de les accions i decisions.

- **Presa i validació de requisits funcionals i tècnics**, amb la recollida, documentació i validació conjunta amb els responsables municipals, aportant estimacions d'esforç, impactes operatius i consideracions tècniques o econòmiques.

- **Generació i actualització de documentació tècnica**, que haurà d'incloure com a mínim:

    - Documentació funcional i tècnica de les solucions de seguretat desplegades.

    - Procediments d'operació i manuals d'usuari.

    - Documentació de canvis, incidències, configuracions aplicades i control de versions.

    - Registre formal de decisions, validacions i lliuraments.

- **Reporting i seguiment executiu**, amb l'emissió d'informes periòdics sobre l'estat del projecte, l'evolució de la implantació, l'estat de la plataforma, les mètriques de servei i d'ús, així com l'elaboració d'una memòria de tancament amb valoració i propostes de millora.

- **Gestió de la qualitat**, mitjançant el control de l'execució del servei per garantir el compliment dels requisits establerts, la realització de proves i revisions, l'execució d'auditories de qualitat, la proposta de millores i l'alineament amb les millors pràctiques del sector.

- **Gestió del tancament del projecte**, que haurà d'incloure el lliurament complet de la documentació, el traspàs formal del servei a l'equip d'operacions de l'entitat municipal, la valoració final del servei prestat i, si escau, l'aixecament de l'acta de conformitat.

Aquests serveis generals són de compliment obligatori i s'han d'incloure de manera inherent en l'execució de qualsevol paquet funcional contractat dins d'aquest Acord Marc, amb independència de la seva naturalesa, abast o finalitat.

De manera transversal a tots els paquets funcionals contractats en el marc del Lot 3, l'adjudicatari haurà de garantir la capacitat d'actuar de forma coordinada, integrada i simultània sobre totes les eines i serveis de protecció **en funció dels paquets contractats**. Aquest requisit és essencial per assegurar la coherència de les polítiques de seguretat, la uniformitat de les configuracions i l'eficàcia de les mesures de protecció aplicades en l'àmbit municipal.

Així mateix, les eines i serveis OSAP hauran de permetre que el CROC, com a servei responsable de la detecció i la resposta a incidents de seguretat, pugui ordenar i executar les mesures de contenció que corresponguin. L'adjudicatari haurà de disposar dels mecanismes tècnics i procedimentals necessaris per aplicar de manera immediata i diligent aquestes mesures sobre totes les eines i plataformes que administra.

Aquesta capacitat multieina implica que les actuacions de configuració, administració, optimització, actualització, gestió de polítiques, revisió de paràmetres i resolució d'incidències es puguin aplicar de manera homogènia a totes les solucions OSAP vigents en funció dels paquets contractats, evitant discrepàncies, desalineaments i comportaments divergents entre productes o plataformes de seguretat.

En concret, l'adjudicatari haurà de garantir:

- **Coherència global de polítiques i configuracions**, aplicant criteris unificats, patrons comuns i controls consistents en totes les eines OSAP gestionades en funció dels paquets contractats, independentment del fabricant o tecnologia.

- **Aplicació coordinada de canvis**, assegurant que qualsevol modificació aprovada (polítiques, signatures, regles de protecció, paràmetres d'inspecció, mecanismes de control, perfils d'usuari o configuracions d'integració) s'implementi de manera sincronitzada a totes les eines afectades en funció dels paquets contractats.

- **Visió centralitzada de l'estat i salut de les eines**, proporcionant informes comparats, quadres de comandament unificats i evidències que permetin validar la coherència tècnica entre totes les plataformes OSAP operades en funció dels paquets contractats.

- **Gestió transversal d'incidències**, de manera que els esdeveniments que tinguin impacte en més d'una eina, servei o plataforma puguin ser tractats conjuntament, evitant resolucions parcials o desalineades dins l'àmbit dels paquets contractats.

- **Traçabilitat completa de totes les actuacions**, mantenint el registre detallat i unificat de les modificacions, actualitzacions, intervencions i tasques operatives realitzades sobre cada eina OSAP, amb capacitat d'auditoria i reconstrucció històrica d'acord amb els paquets contractats.

- **Automatització progressiva de tasques repetitives o multieina**, mitjançant l'ús d'eines corporatives, connectors, scripts o mecanismes proporcionats pels fabricants, sempre que sigui tècnicament viable i d'acord amb les eines incloses en els paquets contractats, per reduir errors i incrementar l'eficiència operativa.

6.1.1 Requisits tècnics generals del servei

Els requisits tècnics generals definits a continuació són d'aplicació obligatòria a qualsevol paquet funcional d'OSAP contractat en el marc del present Acord Marc i constitueixen les condicions mínimes que ha de complir el servei proposat pel licitador.

Aquests requisits tenen com a objectiu assegurar la **coherència tècnica, l'escalabilitat, l'eficiència operativa, l'optimització contínua i el compliment normatiu** del servei dins de l'ecosistema digital municipal. Tots ells seran objecte de valoració i verificació tant en el procés de licitació com durant l'execució dels contractes basats.

Per cadascun dels requeriments, el licitador haurà d'indicar en una **matriu de conformitat** (veure Annex 2) el seu grau de compliment segons les opcions següents:

- "**Compleix**"
- "**No compleix**"
- "**No aplica**"

REQ-TCN-442. Servei industrialitzat. El servei haurà d'estar basat en un model industrialitzat, d'administració i operació d'eines de protecció, capaç d'aplicar casos d'ús, bones pràctiques i automatismes de manera homogènia sobre totes les tecnologies contractades per les entitats municipals. Així mateix, haurà de permetre la incorporació de nous casos d'ús desenvolupats en altres clients de l'adjudicatari, aprofitant l'efecte d'escala i la millora contínua.

REQ-TCN-443. Plataforma com a servei. El servei haurà de proporcionar una plataforma gestionada que centralitzi la monitorització, l'orquestració, la governança de configuracions i la gestió operativa de les eines OSAP, incloent-hi repositori de registres, revisions de salut i mecanismes d'auditoria..

REQ-TCN-444. Incorporació progressiva d'intel·ligència artificial. Les capacitats d'IA i aprenentatge automàtic hauran d'estar integrades per millorar la detecció d'anomalies operatives, l'optimització de configuracions i l'automatització de tasques repetitives, amb un pla d'evolució revisat anualment.

REQ-TCN-445. Automatització de processos. El servei haurà d'incorporar fluxos d'automatització aplicats a l'administració i operació de les eines de protecció (validacions, aplicació de polítiques, sincronització multieina, etc.), documentats i revisables per l'entitat contractant.

REQ-TCN-446. Optimització de recursos. L'adjudicatari haurà de demostrar, mitjançant evidències anuals, la reducció progressiva de l'esforç manual gràcies a automatismes i optimitzacions, mantenint el mateix nivell de cobertura i qualitat del servei OSAP.

REQ-TCN-447. Escalabilitat i modularitat. El servei haurà de ser escalable en nombre d'usuaris, dispositius, aplicacions i serveis municipals, i modular per incorporar noves eines o tecnologies OSAP sense afectació de l'operació existent.

REQ-TCN-448. Independència de la ubicació. La protecció i el monitoratge hauran de ser consistents tant per a usuaris i dispositius dins de la xarxa corporativa com per a aquells que treballin en mobilitat o des de fora de les dependències municipals.

REQ-TCN-449. Compliment normatiu. El servei haurà de garantir el compliment de la Directiva NIS2, l'Esquema Nacional de Seguretat i les guies tècniques del CCN, i assegurar que

les dades del servei es mantinguin exclusivament en centres de dades ubicats dins la Unió Europea.

REQ-TCN-450. Disponibilitat i rendiment. El servei haurà de garantir una disponibilitat mínima del 99,999% sota acords de nivell de servei (SLA) i uns temps de resposta que preservin l'experiència de l'usuari.

REQ-TCN-451. Transparència i traçabilitat. El servei haurà de disposar d'una consola de gestió accessible per als responsables municipals, que permeti consultar en temps real l'estat de les eines OSAP, les polítiques aplicades i els canvis executats.

REQ-TCN-452. Evolució i millora contínua. El licitador haurà de presentar un pla d'evolució del servei OSAP, incloent noves funcionalitats, optimització basada en IA, integració de noves eines i ajust de procediments.

REQ-TCN-453. Integració amb plataforma ITSM de l'entitat. El servei haurà d'integrar-se completament amb la plataforma ITSM (IT Service Management) de l'entitat contractant per tal de registrar, documentar i gestionar les alertes operatives, els incidents, les peticions de servei, les peticions de canvi, etc, sense que això suposi cap cost addicional per a l'entitat.

REQ-TCN-454. Documentació operativa. El servei haurà de documentar mitjançant protocols i procediments operatius de seguretat totes les activitats que es realitzin durant l'execució del contracte. Aquests protocols i procediments operatius de seguretat hauran de ser revisats periòdicament pel servei i aprovats per l'autoritat competent abans de la seva entrada en vigor. Tota la documentació operativa generada serà propietat de l'entitat contractant i un cop finalitzat el servei s'ha de garantir el lliurament de la documentació generada i validada, i la destrucció de la documentació en mans del proveïdor. El servei haurà de disposar de procediments d'actuació per a l'actualització de les eines, així com els processos de marxa enrere davant d'errors o incidències. El servei també haurà de disposar de procediments d'operació i escalat d'incidents a especialistes i fabricants. El servei haurà de mantenir actualitzada la documentació relativa a l'administració i operació de les diferents solucions objecte del servei.

REQ-TCN-455. Personal especialitzat: El servei haurà de disposar de personal altament especialitzat en cadascun dels àmbits funcionals i tecnològics inclosos en el servei. Aquest personal haurà de comptar amb certificacions professionals, nacionals o internacionals, que acreditin de manera verificable el coneixement i l'experiència requerits per a l'administració i operació de les eines de protecció.

REQ-TCN-456. Procediment d'emergència: El servei haurà de disposar dels recursos necessaris i d'un procediment formalitzat d'actuació en cas d'emergència, operatiu en horari 24x7. Aquest procediment haurà de detallar els mecanismes de notificació i escalat, les persones responsables i les accions immediates a emprendre davant una situació que requereixi intervenció urgent.

La comunicació inicial haurà de realitzar-se obligatòriament, com a mínim, mitjançant un canal telefònic, atès que es tracta d'un escenari d'emergència.

REQ-TCN-457. Certificació de Conformitat amb l'ENS: tots els mitjans, sistemes i recursos empleats per l'organització prestadora de SSG per tal de prestar cadascun dels diferents àmbits del servei hauran de disposar de la Certificació de Conformitat amb l'Esquena Nacional de Seguretat (RD 311/2022, de 3 de maig) per a categoria MITJANA o superior, o bé evidenciar l'adient adopció d'un conjunt mínim de 36 mesures de seguretat (recollides a l'apartat 5.1 de la guia CCN-STIC-896) que resultin d'aplicació a cada cas concret i que inclouran el compromís formal d'obtenir la Conformitat amb l'ENS en un termini no superior a 12 mesos. En cas de disposar de serveis al núvol per prestar els SSG, el proveïdor de serveis al núvol on s'allotgi part de la infraestructura dels SSG de ciberseguretat haurà de disposar dels seus sistemes d'informació certificats en categoria ALTA de l'ENS.

REQ-TCN-458. Atracció, promoció i retenció del talent: el servei haurà de demostrar que implementa mesures per atraure, promocionar i retenir el talent, especialment el talent femení, fomentant la igualtat de gènere en el sector de la ciberseguretat.

REQ-TCN-459. Elaboració propostes de comunicació tècnica a l'usuari relativa al servei: El servei haurà d'elaborar propostes de comunicació tècnica i operativa dirigides a l'usuari final relatives a l'estat, canvis o afectacions de les eines administrades. Aquestes comunicacions hauran de ser valides prèviament amb l'entitat contractant i es distribuiran exclusivament a través dels canals oficials de l'Ajuntament.

REQ-TCN-460. Capacitat d'integració amb qualsevol dels productes i serveis del CPSTIC: el servei haurà de suportar la operació i administració complerta de qualsevol dels productes i serveis inclosos dins el Catàleg de Productes i Serveis STIC (CPSTIC) detallats a la guia CCN-STIC-105, i de qualsevol de les solucions de ciberseguretat que ofereix el CCN-CERT.

REQ-TCN-461. Administració i operació sondes artificials de simulació d'usuaris: el servei haurà d'administrar, operar i mantenir les sondes artificials de simulació d'usuaris que permeten detectar de forma proactiva incidències a les xarxes de comunicacions a les seus que l'organisme contractant defineixi com critiques o necessàries.

REQ-TCN-462. Kit bàsic de material de gestió d'avaries greus: El servei haurà de disposar d'un estoc bàsic de cablejat i d'interfases SFP, SFP+ i XFP per tal de recuperar el servei en cas d'avaria greu d'un element de cablejat o d'una interfase SFP, SFP+ o XFP en algun dels actius objecte del servei.

REQ-TCN-463. Monitorització general dels sistemes objecte del contracte: El servei haurà de monitorar de forma continuada l'estat, disponibilitat i funcionament de tots els sistemes inclosos en el contracte, detectant anomalies, errors o degradacions i executant les accions preventives o correctives necessàries.

REQ-TCN-464. Gestió de llicències, casos de suport i garanties esteses de fabricant dels sistemes objecte del contracte: el servei haurà de gestionar les llicències, casos de suport i les garanties esteses de fabricant de tots els sistemes objecte del contracte sota la seva administració i operació.

REQ-TCN-465. Realització i validació còpies de seguretat de configuració dels sistemes objecte del servei: el servei haurà de realitzar i comprovar periòdicament les còpies de seguretat de la configuració dels elements que conformen la infraestructura de seguretat i de les eines de protecció.

REQ-TCN-466. Documentació procediments d'actuació: el servei haurà de disposar de procediments d'actuació per a l'actualització de les eines, així com els processos de marxa enrere davant d'errors o incidències. El servei també haurà de disposar de procediments d'operació i escalat d'incidents a especialistes i fabricants.

REQ-TCN-467. Auditoria de configuració de les solucions de protecció: el servei haurà d'auditar periòdicament (com a mínim semestralment) la configuració de les solucions de protecció, verificant que compleixen les millors pràctiques, les guies del CCN i els estàndards municipals de seguretat.

REQ-TCN-468. Servei d'implantació de paquet: el servei haurà d'oferir a l'entitat contractant la possibilitat d'implantar cadascun dels paquets de servei de forma individual, integrant les capacitats humanes, de processos i tecnològiques de l'entitat dins l'àmbit de servei del paquet en qüestió, en el termini màxim de 90 dies. En cas que durant el cicle de vida del servei l'entitat contractant substitueixi (p.e. canvi de EDR) o incorpori una nova capacitat tecnològica (p.e. afegir NDR) dins l'àmbit de servei del mateix paquet, aquest canvi s'haurà de gestionar com una ampliació del paquet.

REQ-TCN-469. Servei d'ampliació de paquet: el servei haurà d'oferir a l'entitat contractant la possibilitat d'ampliar l'abast de cadascun dels paquets de servei de forma individual, integrant les capacitats humanes, de processos i tecnològiques de l'entitat dins l'àmbit de servei del paquet en qüestió prèviament implantat, en el termini màxim de 30 dies. En cas que durant el cicle de vida del servei l'entitat contractant substitueixi o incorpori una nova capacitat tecnològica dins l'àmbit de servei del mateix paquet, aquest canvi s'haurà de gestionar també com una ampliació del paquet.

REQ-TCN-470. Servei d'explotació de paquet: el servei haurà d'oferir a l'entitat contractant un servei recurrent mensual d'explotació de cadascun dels paquets de servei de forma individual, integrant les capacitats humanes, de processos i tecnològiques de l'entitat dins l'àmbit de servei del paquet en qüestió. En cas que durant el cicle de vida del servei l'entitat contractant substitueixi o incorpori una nova capacitat tecnològica dins l'àmbit de servei del mateix paquet que sigui inclosa dins la mateixa família de productes (p.e. EDR) del catàleg CPSTIC (guia CCN-STIC-105), el servei d'explotació haurà d'assumir sense cost addicional l'explotació d'aquesta nova capacitat tecnològica un cop ampliat el paquet. En cas que durant el cicle de vida del servei l'entitat contractant incorpori una nova capacitat tecnològica dins l'àmbit de servei del mateix paquet que no sigui inclosa dins la mateixa família de productes (p.e. SWG) del catàleg CPSTIC (guia CCN-STIC-105), el cost del servei recurrent mensual d'explotació serà incrementat en el número d'unitats contractades del mateix paquet o subpaquet.

6.1.2 Paquet P5 – Protecció de llocs de treball i dispositius mòbils

El paquet P5 té per objectiu establir un servei integral de govern i protecció en horari 24x7 dels dispositius finals —ordinadors d'escriptori, portàtils, estacions virtuals i dispositius mòbils— com a element fonamental del pla de defensa municipal. El servei es concep com una capa avançada de control, detecció i resposta que articula la protecció en temps real dels dispositius amb la governança centralitzada i l'orquestració amb el CROC municipal.

Aquest servei combina l'administració d'agents de protecció avançada, el control d'integritat del dispositiu, la gestió centralitzada de polítiques de seguretat, la capacitat de resposta immediata i continguda i la seva integració amb plataformes de correlació i orquestració. L'enfocament és preventiu i reactiu alhora, garantint que qualsevol punt final es converteixi en una extensió del sistema de seguretat corporatiu.

El paràmetre quantificador d'aquest servei serà el número d'usuaris interns de l'entitat contractant objecte del servei.

El paquet P5 inclou els serveis d'administració i operació de les solucions de protecció de llocs de treball i dispositius mòbils (de forma descriptiva però no limitativa: EPP, EDR, XDR, MTD, protecció navegació, etc) de que disposi l'entitat contractant, així com la resta de solucions necessàries per prestar el servei. Als efectes de valorar l'esforç requerit pel servei, s'ha d'estimar que tots els usuaris disposen d'estació de treball corporativa i que un terç disposen de terminal mòbil corporatiu.

Tanmateix, el paquet P5 no inclou el llicenciament de les solucions de protecció de llocs de treball i dispositius mòbils.

Funcionalitats que ha de suportar el servei

REQ-TCN-471. Administració i operació de solucions de protecció avançada. El servei haurà de gestionar de forma completa les solucions de protecció avançada desplegades on-premise i al núvol, així com els agents de seguretat instal·lats als dispositius per protegir usuaris i dispositius en tot moment (protecció de la navegació, etc), incloent-hi la seva configuració òptima, l'actualització de signatures i motors heurístics, l'activació de mòduls de prevenció d'explotació, control de processos i vigilància de la memòria.

REQ-TCN-472. Gestió centralitzada de polítiques de seguretat. Haurà de permetre definir i desplegar polítiques de seguretat uniformes a tot el parc de dispositius, amb capacitat de segmentació per grups funcionals, definició de llistes d'aplicacions autoritzades o bloquejades, control granular de permisos i traçabilitat completa de les modificacions.

REQ-TCN-473. Control d'integritat i estat de seguretat. Els dispositius hauran de ser sotmesos a comprovacions de seguretat abans i durant la seva connexió als serveis corporatius, incloent-hi verificació de firmware, arrencada segura, xifratge complet del disc, estat de pegats i compliment de la configuració de seguretat.

REQ-TCN-474. Prevenció i detecció d'explotacions. El servei haurà de disposar de mecanismes contra tècniques d'injecció de codi, abús de memòria, escalada de privilegis i persistència il·lícita, així com capacitat per bloquejar processos maliciosos en execució i revertir canvis de registre o configuració.

REQ-TCN-475. Capacitat de contenció i aïllament. El servei haurà de permetre aïllar remotament un dispositiu de la xarxa en temps real, mantenint la seva visibilitat telemètrica, bloquejar processos, neutralitzar sessions actives i revertir canvis no autoritzats, tot sota protocols documentats i validats pel CROC.

REQ-TCN-476. Orquestració amb plataformes de detecció i resposta automatitzada des del CROC. La telemetria dels dispositius haurà d'alimentar motors d'anàlisi i correlació centralitzats, permetent generar casos de seguretat unificats, enriquir la informació amb context de xarxa i aplicació, i executar respostes coordinades en múltiples capes tecnològiques com aïllament de nodes, bloqueig de processos o reversió de canvis.

REQ-TCN-477. Govern de la seguretat mòbil. El servei haurà de cobrir el cicle complet de gestió de dispositius mòbils: enrolament segur, segmentació de dades corporatives, control d'aplicacions instal·lades, detecció de manipulacions del sistema i possibilitat d'aplicar esborrats remots selectius o totals en cas de pèrdua o compromís.

REQ-TCN-478. Integració amb processos de gestió de vulnerabilitats. El servei haurà de generar informació precisa sobre l'estat de pegats i configuracions dels dispositius, correlacionant-la amb els processos de gestió de vulnerabilitats per permetre una priorització segons el risc i l'exposició real.

REQ-TCN-479. Compliment normatiu i sobirania de dades. La informació generada pel servei —telemetria, registres i informes— haurà de ser gestionada sota els requisits de la normativa europea vigent, assegurant que el seu emmagatzematge i processament es realitza exclusivament en infraestructures ubicades a la Unió Europea.

REQ-TCN-480. Informes i mètriques de rendiment. El servei haurà de produir informes periòdics amb indicadors clau com la cobertura del parc de dispositius, el temps mitjà de detecció i contenció, la taxa de reincidència en incidents i el nivell de compliment de polítiques, aportant una visió operativa i executiva.

Activitats a realitzar per part de l'adjudicatari

- Implantar, configurar i mantenir els agents de protecció en tot el parc de dispositius.
- Definir i governar polítiques de seguretat, incloent-hi excepcions justificades i auditables.
- Monitorar i verificar l'estat de seguretat i integritat dels dispositius.
- Executar accions de resposta i contenció seguint protocols establerts pel CROC.

- Integrar la telemetria dels dispositius en les plataformes centrals de detecció i correlació del CROC.
- Donar suport als processos de gestió de vulnerabilitats amb dades contextualitzades dels endpoints.
- Elaborar informes tècnics i estratègics per avaluar l'eficàcia del servei i recomanar millores.

Resultats esperats

- Parc de dispositius governat i protegit sota un model centralitzat, robust i verificable.
- Reducció dràstica de la superfície d'atac i millora de la capacitat de contenció davant incidents.
- Integració fluïda amb el CROC per a detecció i resposta coordinades en temps real.
- Garantia de compliment normatiu i sobirania de les dades recollides.
- Visibilitat estratègica de l'estat de seguretat dels dispositius mitjançant mètriques i indicadors objectius.

6.1.3 Paquet P6 – Protecció de servidors i càrregues de treball

El paquet P6 té per objectiu establir un servei integral de protecció en horari 24x7 dels servidors físics, màquines virtuals, contenidors i càrregues de treball desplegades en entorns híbrids (centres de dades municipals i plataformes al núvol). Aquest servei proporciona un marc avançat de bastionat, monitoratge i governança de la seguretat, assegurant que totes les càrregues crítiques disposin de controls coherents i consistents independentment de la seva ubicació.
La seva finalitat és reduir la superfície d'exposició dels sistemes, reforçar la resiliència davant atacs i garantir la integració completa amb els processos de detecció i resposta operats des del CROC municipal.

El paràmetre quantificador d'aquest servei serà el número de servidors i càrregues de treball de l'entitat contractat objecte del servei.

El paquet P6 inclou els serveis d'administració i operació de les solucions de protecció de servidors i càrregues de treball (de forma descriptiva però no limitativa: EPP, EDR, XDR, protecció navegació, etc) de que disposi l'entitat contractant, així com la resta de solucions necessàries per prestar el servei.

Tanmateix, el paquet P6 no inclou el llicenciament de les solucions de protecció de servidors i càrregues de treball.

Funcionalitats que ha de suportar el servei

REQ-TCN-481. Administració i operació de solucions de protecció avançada. El servei haurà de gestionar de forma completa les solucions de protecció avançada desplegades on-premise i al núvol, així com els agents de seguretat instal·lats als servidors per protegir-los en tot moment (protecció de la navegació, etc), incloent-hi la seva configuració òptima, l'actualització de signatures i motors heurístics, l'activació de mòduls de prevenció d'explotació, control de processos i vigilància de la memòria.

REQ-TCN-482. Bastionat de sistemes. El servei haurà d'aplicar processos de configuració segura en servidors físics i virtuals, desactivant serveis innecessaris, aplicant controls d'accés restrictius, monitorant processos en execució i assegurant el registre complet d'esdeveniments.

REQ-TCN-483. Hardening de màquines virtuals i contenidors. Les càrregues virtualitzades i basades en contenidors hauran de ser sotmeses a pràctiques estrictes de reforç, incloent-hi control de permisos, integritat d'imatges, seguretat en l'orquestració i revisió periòdica de vulnerabilitats.

REQ-TCN-484. Monitoratge del comportament de càrregues de treball. El servei haurà de supervisar en temps real l'activitat de processos, serveis i connexions de xarxa associats als servidors i contenidors, detectant desviacions respecte a patrons normals i alertant d'anomalies potencialment malicioses.

REQ-TCN-485. Gestió de seguretat en entorns híbrids. El servei haurà de garantir que els mateixos controls de bastionat, monitoratge i protecció s'apliquen de manera uniforme en centres de dades locals i en plataformes al núvol, independentment del proveïdor.

REQ-TCN-486. Control d'integritat i protecció contra manipulació. Els servidors i càrregues de treball hauran de ser verificats periòdicament per detectar canvis no autoritzats en configuracions, fitxers crítics i binaris del sistema.

REQ-TCN-487. Aplicació de controls de seguretat per a càrregues crítiques. El servei haurà d'incorporar controls específics per a entorns altament sensibles, com bases de dades, serveis

de directori i aplicacions corporatives, assegurant la seva protecció reforçada i la segregació de funcions.

REQ-TCN-488. Integració amb processos de gestió de vulnerabilitats. Els servidors i càrregues de treball hauran de remetre informació d'estat de pegats, configuracions i desviacions de seguretat a les plataformes de gestió de vulnerabilitats municipals, per facilitar la priorització i la correcció ràpida.

REQ-TCN-489. Orquestració i resposta automatitzada des del CROC. El servei haurà d'integrar la telemetria i els esdeveniments generats pels servidors i càrregues amb el CROC, permetent correlació avançada i execució de respostes automatitzades com aïllament de nodes, bloqueig de processos o reversió de canvis.

REQ-TCN-490. Compliment i traçabilitat. El servei haurà d'assegurar que totes les activitats de bastionat, monitoratge i resposta queden documentades, auditables i alineades amb els marcs regulatoris vigents, amb residència de dades garantida dins de la Unió Europea.

Activitats a realitzar per part de l'adjudicatari

- Dissenyar i implantar les configuracions de bastionat per a servidors físics, virtuals i contenidors.
- Monitorar de manera contínua el comportament de càrregues de treball i generar alertes davant anomalies.
- Revisar i reforçar de manera periòdica les imatges de màquines virtuals i contenidors.
- Integrar les dades dels servidors i càrregues amb el CROC per a correlació i resposta.
- Donar suport als processos de gestió de vulnerabilitats amb dades detallades de sistemes i serveis.
- Generar informes executius i tècnics sobre l'estat de la seguretat dels servidors i workloads, amb recomanacions de millora.

Resultats esperats

- Servidors i càrregues de treball bastionats i governats sota un model uniforme i coherent.
- Detecció proactiva d'anomalies i intents de compromís en entorns físics, virtuals i al núvol.
- Reducció de riscos derivats de configuracions insegures o vulnerabilitats no corregides.
- Resposta orquestrada i immediata des del CROC davant incidents en servidors i workloads.
- Compliment normatiu i traçabilitat completa de totes les accions aplicades.

- Millora sostinguda de la postura de seguretat municipal mitjançant processos de reforç i revisió contínua.

.

6.1.4 Paquet P7 – Protecció d'identitat i accessos

El paquet P7 té per objectiu establir un servei de govern i protecció en horari 24x7 de les identitats digitals i dels mecanismes d'accés als sistemes municipals, assegurant que els usuaris, els dispositius i els serveis utilitzen canals d'autenticació i autorització robustos, adaptatius i supervisats en temps real pel CROC. La identitat es concep com el nou perímetre de seguretat, i aquest servei garanteix la seva integritat mitjançant controls avançats i una gestió basada en el risc.

El paràmetre quantificador d'aquest servei serà el número d'usuaris interns de l'entitat contractant objecte del servei.

El paquet P7 inclou els serveis d'administració i operació de les solucions de protecció d'identitats i accessos (de forma descriptiva però no limitativa: ITDR, MFA, PAM, UEBA, plataformes AAA, VPN, ZTNA, etc) de que disposi l'entitat contractant, així com la resta de solucions necessàries per prestar el servei.

Tanmateix, el paquet P7 no inclou el llicenciament de les solucions de protecció d'identitats i accessos.

Funcionalitats que ha de suportar el servei

REQ-TCN-491. Administració i operació dels sistemes de protecció, detecció i resposta d'amenaces a les identitats. El servei haurà d'administrar i operar els sistemes de protecció, detecció i resposta d'amenaces a les identitats (ITDR), els sistemes protecció MFA, les polítiques d'accés condicional i els sistemes de protecció de comptes privilegiats (PAM).

REQ-TCN-492. Administració i operació de plataformes AAA. El servei haurà d'administrar i operar les plataformes AAA (Authentication, Authorization and Accounting) que fan servir protocols estàndard com Radius o Tacacs+ per gestionar l'accés remot dels usuaris a la xarxa, o bé per gestionar l'accés d'usuaris administradors a l'equipament de xarxa respectivament. El servei també haurà de gestionar la integració d'aquestes plataformes AAA amb el Directori Actiu, directori LDAP o el serveis d'identitat de l'entitat.

REQ-TCN-493. Control d'accés sense perímetre. El servei haurà d'administrar i operar les plataformes d'accés remot VPN i ZTNA, i haurà de permetre l'accés segur de les persones usuàries a serveis corporatius independentment de la seva ubicació, basant-se en l'estat de seguretat del dispositiu, la identitat i el context d'accés.

REQ-TCN-494. Gestió de certificats de lloc web amb Autoritat Certificadora. El servei haurà gestionar l'alta, la baixa i la renovació dels certificats de lloc web amb l'Autoritat Certificadora (CA) que en cada cas determini l'entitat contractant.

REQ-TCN-495. Gestió d'accés privilegiat. El servei haurà de controlar i monitorar l'ús de credencials privilegiades, establint mecanismes d'autorització temporal, traçabilitat completa de les sessions i revisió periòdica dels permisos atorgats.

REQ-TCN-496. Autenticació multifactor adaptativa. Els mecanismes d'accés hauran d'incloure mètodes de verificació addicionals basats en el context (localització, dispositiu, hora, comportament), permetent adaptar el nivell d'exigència segons el risc de cada accés.

REQ-TCN-497. Federació i accés únic. El servei haurà de permetre integrar sistemes interns i externs sota un model d'autenticació unificada, reduint la necessitat de múltiples credencials i reforçant la seguretat de les connexions amb tercers.

REQ-TCN-498. Monitoratge i detecció d'anomalies d'identitat. El servei haurà de vigilar l'ús de credencials en temps real per identificar patrons sospitosos, intents de compromís o anomalies com accés simultani des de localitzacions incompatibles.

REQ-TCN-499. Governança basada en el risc. Els permisos i privilegis hauran de ser atorgats i revisats seguint principis de mínima assignació, amb processos d'aprovació i revocació automatitzats, vinculats a rols funcionals i riscos associats.

REQ-TCN-500. Orquestració i resposta automatitzada des del CROC. El servei haurà d'integrar la telemetria i els esdeveniments generats pels sistemes de gestió i de protecció de les identitats i els accessos que hauran d'alimentar els processos de correlació i resposta del CROC, permetent detectar moviments laterals, abús de credencials o escalades il·lícites de privilegis mitjançant correlació avançada i l'execució de respostes automatitzades com reinici de contrasenya, desactivació d'identitats i de comptes d'usuari, entre d'altres.

REQ-TCN-501. Informes de compliment i auditories. El servei haurà de generar informes detallats sobre l'estat dels comptes, l'ús de privilegis, les sessions d'accés i les anomalies detectades, amb capacitat d'alimentar els processos d'auditoria interna i externa.

Activitats a realitzar per part de l'adjudicatari

- Gestionar els directoris corporatius i les plataformes d'identitat, assegurant-hi l'actualització constant.
- Definir i aplicar polítiques d'accés privilegiat, amb sessions controlades i registrades.
- Implantar i operar mecanismes d'autenticació multifactor adaptatius.
- Configurar la federació d'identitat i els mecanismes d'accés únic per a sistemes interns i externs.
- Monitorar l'ús de credencials i detectar anomalies de comportament en temps real.
- Integrar els esdeveniments d'identitat dins els processos de detecció i resposta del CROC.
- Generar informes executius i tècnics amb indicadors de compliment i riscos associats a identitats.

Resultats esperats

- Identitats digitals governades de manera centralitzada i coherent.
- Reducció del risc d'abús de privilegis i credencials compromeses.
- Millora de l'experiència d'usuari amb accés unificat i segur.
- Detecció immediata d'anomalies en l'ús de credencials i accessos.
- Integració de la seguretat de la identitat dins els fluxos del CROC, amb resposta ràpida i contextualitzada.
- Compliment normatiu i capacitat d'auditoria reforçada sobre la gestió d'identitats i accessos.

6.1.5 Paquet P8 – Protecció d'informació i dades

El paquet P8 té per objectiu establir un servei integral de govern i protecció en horari 24x7 de la informació municipal, tant en repòs com en trànsit i ús, assegurant que les dades sensibles estiguin correctament identificades, classificades i protegides amb controls preventius i reactius. El servei es concep com un element central per evitar la pèrdua, exfiltració o manipulació de dades, reforçar la governança criptogràfica i integrar les dades dins dels processos de detecció i resposta del CROC municipal.

El paràmetre quantificador d'aquest servei serà el número d'usuaris interns de l'entitat contractant objecte del servei.

El paquet P8 inclou els serveis d'administració i operació de les solucions de protecció de la informació i les dades (de forma descriptiva però no limitativa: DLP, DSPM, etc) de que disposi l'entitat contractant, així com la resta de solucions necessàries per prestar el servei.

Tanmateix, el paquet P8 no inclou el llicenciament de les solucions de protecció de la informació i les dades.

Funcionalitats que ha de suportar el servei

REQ-TCN-502. Classificació i etiquetatge de dades. El servei haurà de permetre identificar i classificar la informació segons el seu nivell de sensibilitat i criticitat, aplicant etiquetes visibles i metadades que condicionin el seu ús i protecció.

REQ-TCN-503. Prevenció de pèrdua de dades. El servei haurà d'implantar mecanismes per monitorar i controlar la transferència de dades sensibles a través de correu electrònic, dispositius extraïbles, serveis al núvol i canals de comunicació corporatius.

REQ-TCN-504. Protecció de dades en ús i en repòs. La informació emmagatzemada o processada haurà de ser protegida mitjançant controls de xifratge, restricció d'accés i verificació d'integritat, incloent mecanismes de control per a entorns compartits o externs.

REQ-TCN-505. Governança criptogràfica. El servei haurà de gestionar el cicle de vida de claus i certificats, incloent-hi la generació, distribució, emmagatzematge segur i revocació, i haurà de garantir la integració amb mòduls de seguretat de maquinari quan correspongui.

REQ-TCN-506. Monitoratge i detecció d'anomalies de dades. El servei haurà de supervisar l'accés, ús i transferència d'informació per detectar patrons sospitosos, intents d'exfiltració o manipulació, amb alertes integrades al CROC.

REQ-TCN-507. Integració amb processos de gestió de riscos. Les dades classificades hauran d'alimentar els processos de governança de riscos, facilitant la priorització de mesures de protecció i el compliment dels requisits normatius.

REQ-TCN-508. Informes i mètriques de seguretat de dades. El servei haurà de generar informes sobre l'estat de protecció de la informació, incidents relacionats amb dades i índexs de compliment de polítiques de seguretat.

Activitats a realitzar per part de l'adjudicatari

- Implantar mecanismes de classificació i etiquetatge de dades corporatives.
- Definir i aplicar polítiques de prevenció de pèrdua de dades en canals crítics.
- Administrar mecanismes de xifratge i control d'integritat en informació en repòs i en ús.
- Gestionar claus criptogràfiques i certificats, garantint la seva protecció i disponibilitat.
- Monitorar l'ús i transferència de dades, integrant alertes en el CROC per a resposta immediata.
- Generar informes periòdics i recomanacions de millora per a la protecció de dades sensibles.

Resultats esperats

- Dades municipals classificades i protegides d'acord amb la seva criticitat.
- Reducció de riscos d'exfiltració, pèrdua o manipulació de dades.
- Governança robusta del cicle de vida de claus i certificats criptogràfics.
- Detecció immediata d'anomalies en l'ús i transferència d'informació.
- Integració de la seguretat de la informació dins els processos del CROC i de la governança de riscos.
- Compliment normatiu garantit i disponibilitat d'evidències auditables.

6.1.6 Paquet P9 – Protecció de correu i entorns de col·laboració

El paquet P9 té per objectiu establir un servei integral de protecció en horari 24x7 del correu electrònic i de les plataformes de col·laboració corporatives, incloent serveis de missatgeria, compartició de fitxers i entorns de treball col·lectius. El servei busca reduir la superfície d'atac vinculada a aquests canals, prevenir fraus digitals com el phishing i el compromís de comptes de correu, i garantir la seguretat i integritat de les comunicacions institucionals.

Aquest servei actua com a capa avançada de defensa davant els vectors d'atac més utilitzats pels actors amenaçadors i integra la seva operació amb els processos de monitoratge, correlació i resposta del CROC municipal.

El paràmetre quantificador d'aquest servei serà el número d'usuaris interns de l'entitat contractant objecte del servei.

El paquet P9 inclou els serveis d'administració i operació de les solucions de protecció del servei de correu electrònic i dels entorns de col·laboració (de forma descriptiva però no

limitativa: Email and Collaboration Security Platforms, etc) de que disposi l'entitat contractant, així com la resta de solucions necessàries per prestar el servei.

Tanmateix, el paquet P9 no inclou el llicenciament de les solucions de protecció del servei de correu i dels entorns de col·laboració.

Funcionalitats que ha de suportar el servei

REQ-TCN-509. Filtrat avançat de correu electrònic. El servei haurà d'aplicar mecanismes de filtratge per detectar i bloquejar correus fraudulents, programari maliciós incrustat i contingut no desitjat, amb actualització contínua de regles i signatures.

REQ-TCN-510. Prevenció de suplantació d'identitat. El servei haurà de validar l'autenticitat dels remitents mitjançant l'aplicació de protocols d'identificació de domini, per prevenir intents de suplantació i atacs de compromís de correu empresarial.

REQ-TCN-511. Anàlisi d'adjunts i enllaços. Els fitxers i enllaços continguts en missatges hauran de ser analitzats amb tècniques estàtiques i dinàmiques en entorns aïllats, per detectar comportaments maliciosos abans que arribin a l'usuari final.

REQ-TCN-512. Protecció d'entorns de col·laboració. El servei haurà de supervisar i protegir plataformes corporatives de treball compartit, com sistemes de missatgeria instantània i espais de documents, evitant la difusió de contingut maliciós o l'accés no autoritzat a informació sensible.

REQ-TCN-513. Monitoratge d'activitat d'usuari. El servei haurà de detectar patrons anòmals en l'ús del correu i les plataformes de col·laboració (com descàrregues massives, compartició indeguda o accessos sospitosos), amb integració d'alertes al CROC.

REQ-TCN-514. Protecció de dominis institucionals. Haurà d'incloure mecanismes per vigilar i protegir dominis municipals contra usos indeguts, intents de registre fraudulent o creació de dominis similars orientats al frau digital.

REQ-TCN-515. Informes i mètriques de seguretat. El servei haurà de generar informes regulars sobre volum de correu analitzat, incidents bloquejats, intents de suplantació detectats i estat de seguretat de les plataformes de col·laboració.

Activitats a realitzar per part de l'adjudicatari

- Configurar i administrar les passarel·les segures de correu electrònic i col·laboració.
- Monitorar de manera contínua el trànsit de correu i l'activitat en entorns de col·laboració.
- Analitzar adjunts i enllaços amb tecnologies avançades de detecció.
- Detectar i bloquejar intents de suplantació i correus fraudulents.
- Protegir els dominis institucionals i notificar intents d'ús fraudulent.
- Integrar telemetria i alertes dins del CROC per a correlació i resposta.
- Elaborar informes tècnics i executius amb recomanacions de millora.

Resultats esperats

- Comunicacions corporatives protegides contra phishing, programari maliciós i intents de suplantació.
- Entorns de col·laboració corporativa governats i protegits contra accessos no autoritzats i propagació d'amenaces.
- Integració amb el CROC que permeti correlació d'incidents i resposta coordinada.
- Protecció proactiva dels dominis institucionals i reducció del risc de frau digital.
- Informes i mètriques que proporcionin visibilitat estratègica i capacitat de decisió sobre la seguretat del correu i la col·laboració.

6.1.7 Paquet P10a – Protecció de xarxes i serveis de telecomunicacions

El paquet P10a té per objectiu establir un servei integral de protecció en horari 24x7 de la infraestructura de xarxa i de les telecomunicacions municipals, centrant-se en les plataformes i solucions de seguretat de xarxa, i **excloent expressament la gestió, administració i operació de routers, switches, controladores Wi-Fi i punts d'accés inalàmbrics**, que es recullen al paquet P10b.

Aquest servei es fonamenta en la governança de les comunicacions digitals mitjançant controls de filtratge, segmentació lògica, inspecció i detecció, assegurant que el trànsit circuli de manera segura i controlada. El servei és independent de la gestió de la infraestructura física de xarxa, sobre la qual opera de manera complementària.

El servei s'integra plenament amb el CROC, que rep la telemetria i els esdeveniments generats per la infraestructura de xarxa, i permet activar respostes orquestrades davant incidents.

El paràmetre quantificador d'aquest servei serà el número d'usuaris interns de l'entitat contractant objecte del servei.

El paquet P10a inclou els serveis d'administració i operació de les solucions de protecció de les xarxes i dels serveis de telecomunicacions (de forma descriptiva però no limitativa: NGFW, IPS/IDS, DDI, NDR, NAC, etc) de que disposi l'entitat contractant, així com la resta de solucions necessàries per prestar el servei.

Queden fora de l'abast del paquet P10a els equips físics d'infraestructura de xarxa, incloent routers, switches, controladores de xarxa inalàmbrica, punts d'accés Wi-Fi i la resta d'electrònica de xarxa associada.

Tanmateix, el paquet P10a no inclou el llicenciament de les solucions de protecció de les xarxes i dels serveis de telecomunicacions.

Funcionalitats que ha de suportar el servei

REQ-TCN-516. Administració i operació de tallafocs avançats (NGFW: Next Generation Firewall). El servei haurà de gestionar tallafocs capaços d'aplicar polítiques de filtratge per aplicació, usuari i contingut, amb actualització dinàmica de regles i capacitat de registrar tots els esdeveniments de trànsit.

REQ-TCN-517. Administració i operació de sistemes de detecció i prevenció d'intrusions. El servei haurà de gestionar sistemes de detecció i prevenció d'intrusions incloent-hi la seva configuració òptima, el monitoratge constant del trànsit i correlació d'esdevenimens amb el SIEM, i l'actualització contínua de signatures i regles IDS/IPS de forma coordinada amb el CROC.

REQ-TCN-518. Administració i operació de sistemes de prevenció d'amenaces. El servei haurà de gestionar sistemes de prevenció d'amenaces incloent-hi la seva configuració òptima, la gestió de signatures i regles IPs per blocar exploits i malware, la configuració de seguretat DNS amb sinkholing i controls avançats per detectar hosts infectats, la integració amb NGFW, SIEM i SOAR per correlar esdeveniments de seguretat, automatitzar i orquestrar la resposta, incloent com a mínim mòduls anti-bot, anti-virus, protecció de vulnerabilitats, i sandboxing o deep learning per detectar amenaces de dia zero.

REQ-TCN-519. Administració i operació de sistemes DDI (DNS, DHCP, IPAM). El servei haurà de gestionar els sistemes DDI (DNS, DHCP i IPAM) de l'entitat, tant en entorns on-premise com

en entorns híbrids i multicloud. La gestió de DNS haurà de garantir una configuració correcta de zones autoritatives i inverses, activar DNS Firewall amb polítiques RPZ per blocar dominis maliciosos, implementar DNSSEC per garantir integritat i autenticitat de les respostes, i monitorar consultes amb analítica i auditories periòdiques. La gestió de DHCP haurà de definir àmbits (scopes) amb polítiques clares i evitar sobreassignacions, i farà auditora logs leases i opcions DHCP per detectar anomalies. La gestió d'IPAM mantindrà un inventari d'adreces IP i VLANs, automatitzarà assignacions i subxarxes per reduir conflictes, integrarà IPAM amb sistemes de seguretat per detectar dispositius no autoritzats, i generarà informes periòdics per planificació.

REQ-TCN-520. Segmentació dinàmica de xarxes. El servei haurà de proposar i aplicar , si escau, tècniques de segmentació per separar entorns crítics, industrials i corporatius, garantint que només el trànsit autoritzat pugui circular entre segments, i que la seva configuració sigui revisada i auditada periòdicament.

REQ-TCN-521. Inspecció de trànsit xifrat. El servei haurà d'analitzar el trànsit xifrat per detectar amenaces, aplicant tècniques de descodificació controlada, inspecció i rexifratge, tot garantint la privadesa i el compliment normatiu.

REQ-TCN-522. Monitoratge de protocols i fluxos de xarxa. El servei haurà de supervisar protocols crítics i patrons de trànsit, identificant anomalies, comportaments inusuals o intents de comunicació amb entorns maliciosos.

REQ-TCN-523. Integració amb el CROC. Els dispositius i plataformes de xarxa hauran de generar telemetria i registres que alimentin el CROC, permetent correlació d'incidents, detecció d'amenaces i resposta coordinada.

REQ-TCN-524. Informes i mètriques de seguretat de xarxa. El servei haurà de generar informes periòdics que incloguin volum de trànsit processat, intents d'intrusió bloquejats, anomalies detectades i estat de compliment de les polítiques de segmentació.

Activitats a realitzar per part de l'adjudicatari

- Configurar i administrar els tallafocs, passarel·les i plataformes de seguretat de xarxa.
- Definir i aplicar polítiques de segmentació i control d'accés.
- Monitorar el trànsit xifrat i aplicar mecanismes d'inspecció quan sigui necessari.
- Protegir aplicacions i serveis exposats contra atacs habituals i avançats.
- Recollir i integrar la telemetria de xarxa dins dels sistemes del CROC.

- Generar informes tècnics i executius amb indicadors de seguretat i recomanacions de millora.

Resultats esperats

- Xarxes corporatives i municipals protegides sota un model segmentat i governat.
- Reducció de riscos derivats de trànsit maliciós, connexions no autoritzades o atacs sobre serveis exposats.
- Integració fluïda amb el CROC, amb capacitat de detecció i resposta ràpida davant incidents de xarxa.
- Compliment normatiu en el tractament del trànsit i la gestió de registres.
- Visibilitat completa sobre l'estat de la seguretat de les comunicacions municipals.

6.1.8 Paquet P10b – Gestió i protecció de la infraestructura física de xarxa

El paquet P10b té per objectiu establir el servei d'administració, operació i protecció en horari 24x7 de la **infraestructura física de xarxa** de l'entitat contractant, incloent routers, switches, controladores Wi-Fi, punts d'accés inalàmbrics i la resta d'electrònica de xarxa associada.

Aquest servei complementa el paquet P10a i garanteix la disponibilitat, la seguretat, la resiliència i la correcta configuració de la xarxa municipal en tots els seus segments (corporatius, serveis, IoT, entorns industrials, etc.).

El servei inclou totes les activitats necessàries per assegurar el funcionament continu de la infraestructura de xarxa, la seva integritat, la seva actualització segura, la configuració alineada amb el model d'arquitectura corporativa i la integració amb el CROC, de manera que la xarxa física també aporti telemetria i visibilitat contextual per a la detecció i resposta a incidents.

El paràmetre quantificador d'aquest servei serà **el nombre d'unitats d'infraestructura física de xarxa a gestionar**, incloent routers, switches, controladores i punts d'accés inalàmbrics.

El paquet P10b inclou la gestió i operació de la infraestructura existent de l'entitat, així com la integració de nous dispositius que s'incorporin durant la vigència del contracte, d'acord amb els procediments definits per l'Ajuntament.

Tanmateix, el paquet P10b no inclou el subministrament, compra o llicenciament dels dispositius o controladores de xarxa.

Funcionalitats que ha de suportar el servei

REQ-TCN-525. Administració integral de routers corporatius.
L'adjudicatari haurà d'administrar els routers corporatius garantint que els protocols de routing utilitzats (com OSPF, BGP o equivalents) es configuren, mantenen i supervisen adequadament, assegurant-ne l'estabilitat i la correcta propagació de rutes. Igualment haurà d'assegurar la configuració, verificació i manteniment dels mecanismes de redundància existents, incloent-hi el basculament controlat i la detecció de possibles desviacions o rutes anòmales. També haurà de gestionar la implementació de VRFs i de polítiques de control del pla de control, aplicar actualitzacions de firmware de manera segura i coordinada amb el CROC i validar periòdicament que la taula de rutes no presenta anomalies que puguin indicar problemes de seguretat, configuració o rendiment.

REQ-TCN-526. Administració i operació de switches d'accés, distribució i core.
L'adjudicatari haurà de gestionar els switches en totes les seves capes, assegurant una configuració correcta de VLANs, segments lògics i trunks, i mantenint en tot moment una topologia estable mitjançant l'ús adequat dels protocols de spanning tree. Igualment haurà de vigilar l'estabilitat dels enllaços agregats, assegurar una aplicació coherent de llistes de control d'accés i filtres de trànsit i garantir l'aplicació de configuracions de qualitat de servei d'acord amb les necessitats municipals. També haurà de mantenir un registre complet i traçable de tots els canvis, verificant regularment la coherència entre dispositius i entorns.

REQ-TCN-527. Gestió avançada de la xarxa inalàmbrica.
L'adjudicatari haurà de gestionar les controladores Wi-Fi i tots els punts d'accés associats assegurant la configuració correcta dels SSIDs, mecanismes d'autenticació i polítiques d'accés. També haurà d'optimitzar la radiofreqüència ajustant canals i potències per minimitzar interferències, detectar punts d'accés no autoritzats i donar resposta immediata a anomalies en els processos d'associació i autenticació. Igualment haurà d'analitzar de manera contínua la densitat d'usuaris, l'ús espectral i el rendiment de cada punt d'accés amb l'objectiu de garantir un servei eficient i segur.

REQ-TCN-528. Gestió segura i governada de configuracions.
L'adjudicatari haurà de mantenir un procés formal per a la gestió de configuracions que asseguri el control de versions, la validació prèvia als desplegaments, la comparació entre

configuracions actuals i previses i la disponibilitat de mecanismes de recuperació ràpida en cas d'error. Aquest procés haurà de permetre detectar desviacions respecte als estàndards corporatius, generar alertes en cas de canvis no autoritzats i garantir que qualsevol desplegament es realitza de manera governada i documentada.

REQ-TCN-529. Gestió de vulnerabilitats i actualitzacions.
L'adjudicatari haurà de monitorar de manera contínua les vulnerabilitats identificades pels fabricants o organismes de referència i avaluar-ne l'impacte sobre l'entorn municipal. Haurà de coordinar amb el CROC la priorització de pegats i actualitzacions, assegurar que el firmware dels dispositius es desplega de manera segura i supervisada i validar la continuïtat dels serveis un cop finalitzat el procés. Així mateix haurà de mantenir un inventari permanentment actualitzat de versions, dates d'End of Support i End of Life i proposar accions de renovació quan correspongui.

REQ-TCN-530. Monitoratge i detecció d'anomalies en infraestructura.
L'adjudicatari haurà de monitorar en tot moment l'estat i el rendiment de routers, switches i punts d'accés, incloent-hi ports, enllaços, taules MAC i ARP, consum de recursos i patrons de trànsit. Això inclou la detecció d'anomalies com ara flapping, saturacions, increments inusuals de trànsit, inconsistències en ARP o comportaments que puguin indicar atacs interns. També haurà de generar alertes predictives basades en l'evolució de paràmetres crítics que permetin actuar de manera preventiva.

REQ-TCN-531. Integració de telemetria amb el CROC.
L'adjudicatari haurà de garantir que tots els dispositius generen i transmeten al CROC els esdeveniments, fluxos i registres necessaris per a la detecció i resposta a incidents, incloent-hi logs de control, alertes de seguretat, fluxos NetFlow o equivalents i informació d'estat. Aquesta integració s'haurà de mantenir activa, coherent i actualitzada, i qualsevol canvi que afecti la telemetria haurà d'estar justificat, documentat i alineat amb els requisits del model operatiu del CROC.

REQ-TCN-532. Controls de seguretat L2/L3 en infraestructura.
L'adjudicatari haurà d'aplicar i supervisar mesures de protecció específiques per prevenir atacs interns en les capes 2 i 3. Això inclou la configuració adequada de mecanismes com DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, Port Security, proteccions contra tempestes de broadcast i control dels protocols susceptibles d'abús. També haurà de revisar periòdicament l'estat dels ports, detectar-ne usages anòmals i corregir desviacions que puguin comprometre la seguretat de la xarxa.

REQ-TCN-533. Gestió del cicle de vida i inventari d'infraestructura.
L'adjudicatari haurà de mantenir un inventari complet, actualitzat i verificable de tots els dispositius gestionats, incloent ubicació, rol, model, versió de firmware, estat de suport i dependències. Haurà de garantir un etiquetatge adequat, mantenir diagramació actualitzada, detectar dispositius que arriben al final del seu cicle de vida i proposar accions de renovació amb antelació suficient per evitar situacions de risc o interrupció del servei.

REQ-TCN-534. Alineament amb l'arquitectura corporativa.
L'adjudicatari haurà de garantir que la infraestructura física de xarxa s'ajusta al model d'arquitectura corporativa, aplicant i mantenint la segmentació, la topologia i els rols definits per l'Ajuntament. A més haurà de coordinar-se amb el CROC i amb els equips tècnics municipals en projectes d'evolució de xarxa i verificar constantment que les configuracions dels dispositius compleixen els estàndards de seguretat, qualitat i coherència establerts. Davant qualsevol desviació haurà de proposar mesures correctores o d'optimització.

Activitats a realitzar per part de l'adjudicatari

- Configurar, administrar i operar routers, switches i dispositius inalàmbrics.
- Definir, desplegar i verificar configuracions d'infraestructura en entorns d'accés, distribució i core.
- Aplicar controls de seguretat L2/L3 i mecanismes de protecció d'infraestructura.
- Gestionar incidències, alertes i degradacions de rendiment.
- Executar actualitzacions de firmware i pegats de seguretat.
- Gestionar SSIDs, RF i configuracions de la xarxa Wi-Fi.
- Mantenir un inventari complet i actualitzat de dispositius.
- Integrar la telemetria amb els sistemes del CROC.
- Elaborar informes tècnics i executius amb recomanacions de millora.
- Participar en auditories, revisions i exercicis de resiliència quan correspongui.

Resultats esperats

- Infraestructura de xarxa estable, segura i alineada amb els estàndards de l'Ajuntament.
- Reducció d'incidències derivades de configuracions errònies, vulnerabilitats o fallades d'equipament.
- Millora de la visibilitat i detecció d'amenaces gràcies a la telemetria integrada amb el CROC.
- Compliment dels requisits normatius aplicables a la infraestructura crítica municipal.
- Disponibilitat i rendiment òptim dels serveis de xarxa cablejada i inalàmbrica.
- Traçabilitat completa de tots els canvis i configuracions realitzats.

6.1.9 Paquet P11 – Protecció d'aplicacions i APIs

El paquet P11 té per objectiu establir un servei de protecció integral en horari 24x7 de les aplicacions municipals, incloent portals web, aplicacions mòbils, sistemes interns i interfícies de programació. El servei cobreix des de la fase de desenvolupament fins a l'execució en producció, assegurant que les aplicacions siguin dissenyades, desplegades i operades sota criteris de seguretat robustos, i que estiguin monitorades en temps real pel CROC per detectar i respondre a intents d'explotació.

Aquest servei combina controls preventius, detecció en execució i integració amb processos de desenvolupament segur, amb la finalitat de reduir el risc d'exposició i garantir la confiança en els serveis digitals municipals.

El paràmetre quantificador d'aquest servei serà el número d'aplicacions de l'entitat contractant objecte del servei.

El paquet P11 inclou els serveis d'administració i operació de les solucions de protecció de les aplicacions i APIs (de forma descriptiva però no limitativa: solucions per publicar i equilibrar la càrrega d'aplicacions, AntiDDoS, tallafocs d'aplicació "WAF", tallafocs d'aplicació i d'API "WAAP", etc) de que disposi l'entitat, així com la resta de solucions necessàries per prestar el servei.

Tanmateix, el paquet P11 no inclou el llicenciament de les solucions de protecció de les aplicacions i les APIs (interfícies de programació d'aplicacions).

Funcionalitats que ha de suportar el servei

REQ-TCN-535. Revisió de configuracions i bastionat d'aplicacions i APIs. El servei haurà de garantir que totes les aplicacions i els seus entorns d'execució compleixin amb guies de configuració segura, eliminant serveis innecessaris, reforçant permisos i aplicant polítiques de control d'accés granular.

REQ-TCN-536. Administració i operació de solucions de control del lliurament d'aplicacions. El servei haurà d'administrar i operar les solucions de control del lliurament d'aplicacions (ADC: Application Delivery Controller) que faci servir l'entitat per publicar i equilibrar la càrrega de les aplicacions, accelerar-les, aplicar mecanismes de seguretat addicionals, o fer SSL offloading, si escau.

REQ-TCN-537. Proves de seguretat automatitzades. Les aplicacions hauran de ser sotmeses a escanejos periòdics de vulnerabilitats i proves automatitzades que detectin fallades conegudes i desviacions respecte als estàndards de seguretat.

REQ-TCN-538. Integració en processos de desenvolupament. El servei haurà d'integrar controls de seguretat dins dels fluxos de construcció i desplegament de programari, assegurant que les vulnerabilitats siguin identificades i corregides abans de l'arribada a producció.

REQ-TCN-539. Protecció d'aplicacions web i serveis exposats. El servei haurà de protegir portals públics i aplicacions municipals contra atacs de denegació de servei, injeccions i altres vectors d'explotació, assegurant la seva disponibilitat i integritat.

REQ-TCN-540. Protecció d'interfícies i serveis d'aplicació. Les interfícies de programació i serveis exposats hauran de disposar de controls específics per detectar i bloquejar intents d'injecció, manipulació de dades i abús de funcionalitats.

REQ-TCN-541. Monitoratge de microserveis i entorns distribuïts. El servei haurà de supervisar aplicacions basades en microserveis, controlant la seva comunicació, permisos i fluxos interns, i detectant patrons anòmals que puguin indicar compromís.

REQ-TCN-542. Protecció en temps real davant atacs. Les aplicacions hauran de disposar de mecanismes que permetin identificar i neutralitzar atacs en execució, com intents d'injecció de codi, escalada de privilegis o denegació de servei.

REQ-TCN-543. Integració amb el CROC. Els esdeveniments de seguretat generats per les aplicacions hauran de ser transmesos al CROC, per permetre la correlació amb altres vectors d'atac i la resposta orquestrada en temps real.

REQ-TCN-544. Informes i mètriques de seguretat d'aplicacions. El servei haurà de generar informes periòdics que incloguin vulnerabilitats detectades, incidents bloquejats, desviacions de configuració i estat global de la seguretat de les aplicacions.

Activitats a realitzar per part de l'adjudicatari

- Revisar i bastionar configuracions d'aplicacions i entorns d'execució.
- Executar proves periòdiques de seguretat, automatitzades i manuals.
- Integrar controls de seguretat dins dels processos de desenvolupament i desplegament.
- Monitorar interfícies i serveis d'aplicació per detectar anomalies i intents d'explotació.

- Supervisar i reforçar la seguretat de microserveis i entorns distribuïts.
- Integrar esdeveniments i alertes dins els sistemes del CROC.
- Generar informes tècnics i executius amb indicadors i recomanacions de millora.

Resultats esperats

- Aplicacions municipals protegides durant tot el seu cicle de vida.
- Reducció de riscos derivats de vulnerabilitats de programari i configuracions insegures.
- Capacitat de detecció i resposta en temps real davant atacs contra aplicacions.
- Integració plena amb els processos del CROC i correlació amb altres vectors d'incident.
- Visibilitat estratègica sobre l'estat de seguretat de les aplicacions municipals.

6.1.10 Paquet P12 – Protecció d'entorns al núvol

El paquet P12 té per objectiu establir un servei integral de protecció en horari 24x7 dels entorns municipals allotjats al núvol, incloent infraestructures, plataformes i aplicacions en escenaris públics, privats i híbrids. L'objectiu és garantir que la configuració dels serveis, les càrregues de treball i les dades allotjades compleixin amb estàndards de seguretat robustos i que estiguin monitorades de manera contínua pel CROC.

Aquest servei proporciona governança de la seguretat al núvol mitjançant controls de configuració, protecció de càrregues, detecció d'anomalies i integració completa amb els processos de detecció i resposta.

El paràmetre quantificador d'aquest servei serà el número de càrregues de treball al núvol de l'entitat contractant objecte del servei.

El paquet P12 inclou els serveis d'administració i operació de les solucions de protecció d'entorns i serveis al núvol (de forma descriptiva però no limitativa: CNAPP, CSPM, CWPP, CIEM, IaS Scanning, etc) de que disposi l'entitat, així com la resta de solucions necessàries per prestar el servei.

Tanmateix, el paquet P12 no inclou el llicenciament de les solucions de protecció d'entorns i serveis al núvol.

Funcionalitats que ha de suportar el servei

REQ-TCN-545. Configuració segura de tenants. El servei haurà de garantir que totes les instàncies i entorns municipals al núvol compleixin amb pràctiques recomanades de seguretat, incloent-hi permisos mínims, segmentació de recursos i protecció de credencials.

REQ-TCN-546. Monitoratge de configuracions i desviacions. El servei haurà de revisar de manera contínua els entorns al núvol per detectar configuracions incorrectes, exposicions innecessàries o desviacions respecte als estàndards establerts.

REQ-TCN-547. Governança de càrregues de treball. El servei haurà de protegir les aplicacions i serveis desplegats al núvol, aplicant controls específics per a màquines virtuals, contenidors i serveis gestionats, assegurant-ne la integritat i l'aïllament.

REQ-TCN-548. Supervisió de trànsit i activitats sospitoses. El servei haurà de monitorar el comportament dels recursos al núvol per identificar patrons anòmals, com moviments laterals, escalades de privilegis o accés no autoritzat a dades.

REQ-TCN-549. Protecció de dades allotjades. La informació emmagatzemada o processada al núvol haurà d'estar protegida mitjançant controls de xifratge, restriccions d'accés i verificació d'integritat, amb capacitat de revocació immediata en cas de compromís.

REQ-TCN-550. Integració amb el CROC. Els esdeveniments i registres generats pels entorns al núvol hauran d'alimentar els processos de detecció i resposta del CROC, garantint la correlació amb incidents de xarxa, aplicació i identitat.

REQ-TCN-551. Informes i mètriques de seguretat al núvol. El servei haurà de generar informes periòdics amb llistat de desviacions corregides, incidents detectats i estat global de la seguretat dels entorns al núvol.

Activitats a realitzar per part de l'adjudicatari

- Configurar i revisar de manera periòdica els tenants i recursos municipals al núvol.
- Detectar i corregir desviacions en configuracions i permisos.
- Monitorar i protegir les càrregues de treball desplegades en entorns híbrids.
- Supervisar trànsit i activitats anòmales per a detecció primerenca d'incidents.
- Integrar registres i esdeveniments dins els sistemes del CROC.
- Elaborar informes tècnics i executius amb indicadors i recomanacions de millora.

Resultats esperats

- Entorns municipals al núvol configurats i governats sota criteris de seguretat robustos.

- Reducció de riscos derivats de configuracions incorrectes o permisos excessius.
- Protecció de càrregues de treball i dades davant intents d'explotació i accessos indeguts.
- Integració fluïda amb els processos del CROC i resposta coordinada davant incidents.
- Visibilitat estratègica sobre la seguretat i l'evolució dels entorns al núvol municipals.

6.1.11 Paquet P13 – Protecció de tecnologies emergents i especialitzades (OT, IoT, IA i criptografia)

El paquet P13 té per objectiu establir un servei de protecció avançada en horari 24x7 per a aquells àmbits tecnològics emergents i especialitzats que presenten riscos específics per a l'Ajuntament, incloent sistemes industrials, dispositius connectats, plataformes d'intel·ligència artificial i entorns criptogràfics. Aquest servei garanteix que les tecnologies innovadores adoptades per l'entitat es despleguin sota criteris de seguretat robustos i que quedin integrades dins dels mecanismes de monitoratge i resposta del CROC.

Aquest paquet cobreix tant la protecció preventiva com la detecció i la resposta davant incidents en aquests entorns, assegurant que les noves superfícies d'exposició quedin sota control i alineades amb les pràctiques internacionals de seguretat.

El paràmetre quantificador d'aquest servei seran paquets de 50 actius de l'entitat contractant objecte del servei. Els actius podran ser dispositius OT i IOT; el número de sistemes i models d'IA, i el número de sistemes de gestió de claus criptogràfiques (de forma descriptiva però no limitativa: KMS, HMS, PKI, key vaults, etc).

El paquet P13 inclou els serveis d'administració i operació de les solucions de protecció de tecnologies emergents i especialitzades (OT, IoT, IA i criptografia) , així com la resta de solucions necessàries per prestar el servei.

Tanmateix, el paquet P13 no inclou el llicenciament de les solucions de protecció de tecnologies emergents i especialitzades.

Funcionalitats que ha de suportar el servei

REQ-TCN-552. Protecció de sistemes industrials i de control. El servei haurà d'aplicar mesures de bastionat, monitoratge i detecció d'anomalies sobre protocols industrials i infraestructures de control, evitant manipulacions i assegurant la continuïtat operativa.

REQ-TCN-553. Supervisió de dispositius connectats. El servei haurà de garantir la seguretat de sensors, càmeres i dispositius IoT, incloent la detecció de vulnerabilitats, configuracions insegures i comportaments anòmals.

REQ-TCN-554. Seguretat d'entorns d'intel·ligència artificial. El servei haurà d'avaluar riscos específics en models d'aprenentatge automàtic, com atacs adversarials, manipulació de dades d'entrenament i biaixos explotables, establint controls de mitigació.

REQ-TCN-555. Preparació per a l'era post-quàntica. El servei haurà d'analitzar i reforçar els mecanismes criptogràfics utilitzats, avaluant la seva resiliència davant amenaces quàntiques i proposant estratègies de migració a algoritmes resistents.

REQ-TCN-556. Integració amb el CROC. Totes les plataformes i dispositius d'aquests entorns hauran de generar telemetria que alimenti els processos de detecció i resposta del CROC, amb correlació d'incidents que afectin entorns híbrids.

REQ-TCN-557. Informes tècnics i estratègics. El servei haurà de generar informes que recullin vulnerabilitats, incidents i recomanacions de millora, incloent fulls de ruta específics per a l'evolució segura d'aquestes tecnologies.

Activitats a realitzar per part de l'adjudicatari

- Configurar i bastionar sistemes industrials i dispositius connectats.
- Monitorar protocols i fluxos específics de tecnologies OT i IoT.
- Avaluar riscos en models i plataformes d'intel·ligència artificial.
- Revisar i proposar millores en els mecanismes criptogràfics existents.
- Integrar registres i telemetria dins els sistemes del CROC.
- Elaborar informes tècnics i estratègics amb recomanacions i plans de migració.

Resultats esperats

- Sistemes industrials, dispositius IoT i plataformes d'IA protegits i sota monitoratge continu.
- Reducció de riscos derivats de configuracions insegures o vulnerabilitats en tecnologies emergents.
- Estratègia definida de preparació criptogràfica per a l'era post-quàntica.
- Integració completa d'aquests entorns dins del CROC, amb detecció i resposta coordinada.

- Visibilitat estratègica i tècnica sobre la seguretat de tecnologies emergents i especialitzades.

6.1.12 Paquet P14 – Protecció d'hipervisors i plataformes de virtualització

El paquet P14 té per objectiu establir un servei de protecció avançada en horari 24x7 per als entorns d'hipervisors i plataformes de virtualització que allotgen sistemes crítics de l'Ajuntament. Aquest servei garanteix que la infraestructura virtualitzada, tant en entorns de CPD com híbrids o al núvol, estigui degudament bastionada, monitorada i protegida contra amenaces que puguin comprometre la seva integritat, disponibilitat o rendiment.

El servei proporciona una cobertura completa que inclou prevenció, detecció i resposta davant d'incidents en els entorns d'hipervisors, assegurant la segregació adequada entre màquines virtuals, la protecció dels recursos compartits i la integritat dels mecanismes d'administració. A més, assegura que les plataformes de virtualització s'integrin plenament dins dels processos de detecció, resposta i recuperació operats pel CROC-OSAP.

El paràmetre quantificador d'aquest servei serà el número de nodes que suportin els hipervisors i les plataformes de virtualització de l'entitat contractant objecte del servei.

El paquet P14 inclou els serveis d'administració i operació de les solucions de protecció d'hipervisors i de plataformes de virtualització, així com la resta de solucions necessàries per prestar el servei.

Tanmateix, el paquet P14 no inclou el llicenciament de les solucions de protecció d'hipervisors i de plataformes de virtualització.

Funcionalitats que ha de suportar el servei

REQ-TCN-558. Bastionat i control d'accés als hipervisors.. El servei haurà de garantir que tots els hipervisors estiguin configurats segons bones pràctiques de seguretat, amb credencials robustes, autenticació multifactor i control d'accés basat en rols per evitar administracions no autoritzades.

REQ-TCN-559. Protecció del pla de gestió i de la consola d'administració. L'adjudicatari haurà de desplegar mesures de protecció sobre les consoles de gestió incloent mecanismes de xifrat de comunicacions, registre d'operacions i detecció d'activitats anòmales.

REQ-TCN-560. Monitoratge d'activitat i integritat. El servei haurà de proporcionar monitoratge continu de l'activitat dels hipervisors i màquines virtuals, detectant desviacions, manipulacions no autoritzades o intents de compromís de l'entorn virtualitzat.

REQ-TCN-561. Protecció de comunicacions internes i tràfic est-oest. El servei haurà d'implantar controls de segmentació i inspecció del tràfic intern entre màquines virtuals (tràfic est-oest), evitant moviments laterals i propagació de programari maliciós dins del mateix host o clúster.

REQ-TCN-562. Gestió de vulnerabilitats i pegats. L'adjudicatari haurà d'identificar i gestionar de forma proactiva les vulnerabilitats associades als hipervisors i components de virtualització, planificant i executant pegats de seguretat d'acord amb els procediments de canvi establerts per l'Ajuntament.

REQ-TCN-563. Integració amb el CROC-OSAP. El servei haurà d'integrar els registres i la telemetria dels hipervisors i de les plataformes de virtualització dins dels sistemes de correlació i detecció del CROC, assegurant-ne la supervisió centralitzada i la resposta coordinada davant incidents.

REQ-TCN-564. Informes tècnics i de maduresa. El servei haurà de generar informes periòdics que recullin vulnerabilitats, incidències i recomanacions de millora, incloent l'avaluació de maduresa de la seguretat dels entorns virtualitzats i un full de ruta d'evolució.

Activitats a realitzar per part de l'adjudicatari

- Configurar i bastionar els hipervisors i consoles d'administració segons guies de seguretat i estàndards reconeguts.
- Monitorar l'activitat i la integritat dels entorns de virtualització, detectant anomalies i alertes crítiques.
- Gestionar vulnerabilitats, pegats i actualitzacions dels components de virtualització.
- Implementar controls de segmentació del tràfic intern entre màquines virtuals.
- Integrar logs i esdeveniments dins de la plataforma de monitorització del servei de CROC i col·laborar en la resposta a incidents.
- Elaborar informes tècnics i estratègics amb recomanacions de millora i estat de maduresa del servei.

Resultats esperats

- Entorns d'hipervisors i plataformes de virtualització degudament protegits, bastionats i monitorats.
- Reducció del risc de compromís dels sistemes virtuals i dels moviments laterals entre màquines.
- Visibilitat completa de l'activitat dels entorns virtuals dins del servei.
- Manteniment proactiu de la seguretat mitjançant gestió de vulnerabilitats i pegats.
- Millora de la maduresa i la resiliència dels entorns virtualitzats municipals.
- Integració efectiva dels entorns de virtualització dins del model global de seguretat operativa i resposta de l'Ajuntament.

6.1.13 Paquet P15 – Protecció de contenidors i orquestradors

El **paquet P15** té per objectiu establir un **servei de protecció avançada** en horari 24x7 **per als entorns de contenidors i sistemes d'orquestració** (com Kubernetes, OpenShift o equivalents) utilitzats per a l'execució d'aplicacions i serveis municipals. Aquest servei assegura que la infraestructura basada en contenidors es desplegui i operi sota criteris estrictes de seguretat, minimitzant la superfície d'exposició i prevenint vulnerabilitats o configuracions insegures que puguin comprometre la continuïtat dels serveis.

El servei actua sobre tot el cicle de vida del contenidor —des del desenvolupament fins a la posada en producció— i cobreix la seguretat de les imatges, dels nodes, dels components d'orquestració i dels processos de pipeline associats, garantint que els entorns de virtualització lleugera quedin protegits dins del marc global de seguretat de l'Ajuntament.

El paràmetre quantificador d'aquest servei serà el número de nodes que suportin els entorns de contenidors i sistemes d'orquestració de l'entitat contractant objecte del servei.

El paquet P15 inclou els serveis d'administració i operació de les solucions de protecció de contenidors i orquestradors, així com la resta de solucions necessàries per prestar el servei.

Tanmateix, el paquet P15 no inclou el llicenciament de les solucions de protecció de contenidors i orquestradors.

Funcionalitats que ha de suportar el servei

REQ-TCN-565. Bastionat d'entorns de contenidors i orquestradors. El servei haurà de garantir que els nodes, clústers i components d'orquestració estiguin configurats seguint bones pràctiques de seguretat, amb control d'accés basat en rols (RBAC), ús de secrets xifrats i comunicacions segures entre components.

REQ-TCN-566. Seguretat de les imatges de contenidors. L'adjudicatari haurà d'implantar un servei de revisió, validació i signatura d'imatges, analitzant-les abans del desplegament per detectar vulnerabilitats conegudes o configuracions insegures, i bloquejant l'execució d'imatges no validades o sense firma autoritzada.

REQ-TCN-567. Supervisió de la cadena de subministrament. El servei haurà de controlar els components que intervenen en la creació i publicació de contenidors (repositoris, artefactes, dependències, pipelines de CI/CD), prevenint l'ús de biblioteques o codi compromès i assegurant la integritat del procés de compilació.

REQ-TCN-568. Protecció del pla de control i dels secrets. L'adjudicatari haurà d'aplicar mesures de seguretat específiques al pla de control dels orquestradors, limitant-ne l'exposició pública, aplicant verificació d'autenticitat, rotació periòdica de claus i protecció criptogràfica dels secrets.

REQ-TCN-569. Gestió de vulnerabilitats i pegats. El servei haurà d'identificar vulnerabilitats en entorns de contenidors i gestionar l'aplicació de pegats o actualitzacions dels components afectats, d'acord amb els procediments de canvi de l'Ajuntament.

REQ-TCN-570. Integració amb processos corporatius. El servei haurà de garantir la coherència amb les polítiques de seguretat i gestió de riscos de l'Ajuntament, coordinant-se amb el Servei de CROC- per a la notificació d'incidències o desviacions detectades durant les tasques de manteniment preventiu.

REQ-TCN-571. Informes de seguretat i recomanacions. L'adjudicatari haurà d'elaborar informes periòdics amb l'estat de seguretat dels entorns, vulnerabilitats identificades, actualitzacions aplicades i recomanacions de millora contínua.

Activitats a realitzar per part de l'adjudicatari

- Configurar i bastionar nodes, clústers i components d'orquestració segons guies i estàndards reconeguts.
- Validar i signar imatges de contenidors abans del seu desplegament en entorns municipals.

- Supervisar i protegir els pipelines i repositoris utilitzats en la construcció d'imatges.
- Implementar mecanismes de protecció del pla de control i dels secrets d'orquestració.
- Gestionar de manera preventiva vulnerabilitats i actualitzacions dels components.
- Elaborar informes tècnics i estratègics amb recomanacions de millora i estat de maduresa del servei.

Resultats esperats

- Plataformes de contenidors i orquestradors degudament bastionades i protegides.
- Reducció de vulnerabilitats derivades de configuracions o imatges insegures.
- Control i integritat garantits de la cadena de subministrament i dels pipelines associats.
- Pla de control i secrets protegits sota mecanismes de seguretat robustos.
- Manteniment preventiu continu i alineat amb les polítiques de seguretat corporatives.
- Millora de la maduresa de seguretat en els entorns de desenvolupament i desplegament d'aplicacions.

7. Fases de prestació del Servei

La prestació dels serveis objecte del present Acord Marc es realitzarà exclusivament mitjançant la formalització de contractes basats per part de les entitats adherides. Per garantir la continuïtat operativa, la correcta habilitació del servei i el traspàs ordenat del coneixement quan sigui necessari, la prestació del servei s'estructurarà en **tres fases diferenciades**:

1. **Fase de Transició.** Aquesta fase **només s'aplicarà en aquelles entitats adherides que ja tinguin un servei similar en vigor**. En aquests casos, el nou adjudicatari rebrà tota la informació i documentació necessàries procedents de l'entitat contractant i de l'adjudicatari sortint, que continuarà prestant el servei i mantenint els ANS vigents durant aquest període. La fase tindrà una durada màxima de **90 dies naturals** i té per objectiu garantir una activació segura i sense discontinuïtats. En les entitats que **no disposin de cap servei previ**, no es realitzarà fase de transferència i el contracte basat passarà directament a la fase d'execució.

2. **Fase d'Execució del contracte basat**. Un cop finalitzada (o no aplicable) la fase de transferència, l'adjudicatari assumirà la responsabilitat tècnica i operativa del servei, l'aplicació immediata dels ANS i totes les activitats vinculades al desplegament, posada en funcionament, suport, manteniment, evolució i seguiment dels serveis contratats.

3. **Fase de Devolució del servei**. En finalitzar la vigència del contracte basat, l'adjudicatari haurà de garantir una transició ordenada, amb traspàs de coneixement, continuïtat operativa i manteniment dels ANS durant tot el període de devolució establert.

7.1 Fase de transició del servei

La fase de transició s'aplicarà exclusivament a les entitats adherides que disposin d'un servei similar en vigor. La seva finalitat és facilitar un traspàs ordenat entre l'adjudicatari sortint i el nou adjudicatari, garantint la continuïtat operativa i el manteniment dels ANS vigents durant tot el període de transició.

La durada de la fase de transició serà, en tot cas, **de 90 dies naturals**, i **no podrà ser objecte de pròrroga, ni condicionar l'inici de la prestació del servei per part del nou adjudicatari**. En finalitzar aquest termini, **el nou adjudicatari estarà obligat a assumir plenament el servei**, amb la informació disponible, independentment de l'estat dels treballs de traspàs.

a) Obligacions durant la fase

Durant aquests 90 dies:

- L'adjudicatari rebrà de BIT i del proveïdor sortint tota la informació, documentació i configuracions disponibles en el moment de la transició.
- El proveïdor sortint mantindrà íntegrament la prestació del servei i els ANS vigents.
- L'adjudicatari haurà d'assimilar la informació rebuda i preparar els seus equips, eines i processos per operar el CROC.
- L'adjudicatari haurà d'habilitar tots els accessos, canals i eines corporatives necessaris per a la prestació del servei.

b) Caràcter no suspensiu

La fase de transició **no té caràcter habilitant ni suspensiu**. Això implica que:

- **La manca o parcialitat d'informació no impedeix ni pot retardar l'inici del servei.**
- L'adjudicatari assumeix el servei en finalitzar els 90 dies, fins i tot si considera que el traspàs no és complet.
- Qualsevol desviació, mancança o necessitat addicional d'informació formarà part de les activitats ordinàries de la fase d'execució i no podrà ser utilitzada per justificar retards, excepcions o penalitzacions al servei.

c) Lliurament del Pla d'Activació Operativa

Durant la fase, l'adjudicatari haurà de lliurar un Pla d'Activació Operativa amb:

- model d'operació,
- rols i responsabilitats,
- calendaris interns,
- mecanismes de seguiment.

Aquest pla **no condicionarà l'inici del servei** i podrà ser ajustat durant la primera etapa de la fase d'execució.

d) Entitats sense servei previ

Per a les entitats adherides que **no disposin d'un servei previ**, la fase de transició **no serà d'aplicació** i el contracte basat entrarà directament en fase d'execució.

7.2 Fase d'execució del contracte basat

La fase d'execució s'inicia amb l'adjudicació de cada contracte basat i abasta totes les activitats vinculades al desplegament, posada en funcionament, suport, manteniment, evolució i seguiment dels serveis CROC contractats.

Des del primer dia, i sense períodes d'adaptació, l'adjudicatari haurà d'assumir de manera immediata:

- La responsabilitat tècnica i operativa completa del paquet funcional contractat.
- L'aplicació íntegra i immediata dels Acords de Nivell de Servei (ANS) definits al contracte.
- L'ús obligatori de les eines corporatives que defineixi l'entitat contractant per al seguiment, monitoratge, control i comunicació del servei.
- La coordinació continuada amb l'equip de seguretat i operacions de l'entitat contractatnt per garantir una implantació correcta i una gestió eficient del servei.

Aquesta fase pot incloure períodes de validació pilot, d'implantació progressiva o d'evolució funcional segons el tipus de paquet contractat, tal com es detalla a l'apartat 4 del present plec.

Addicionalment, l'adjudicatari haurà de proposar i mantenir **mecanismes d'evolució contínua** dels serveis, incloent-hi aspectes:

- **tecnològics** (millores, actualitzacions i noves capacitats),
- **econòmics** (optimització i racionalització de costos),
- **de governança** (model de control i presa de decisions),
- **de servei** (nous procediments, ampliacions i integracions),
- **i d'incorporació de noves funcionalitats del CROC** quan esdevinguin necessàries.

Aquests mecanismes hauran d'incloure informació detallada sobre:

- pautes i criteris d'activació,
- instruments de seguiment i quadres de comandament,

- integració de les necessitats dels usuaris, tant de forma reactiva com proactiva,
- compromisos temporals d'execució i posterior validació.

L'entitat contractant podrà requerir que part o la totalitat del personal assignat per l'adjudicatari presti els seus serveis de forma presencial quan les activitats associades als serveis CROC **no puguin garantir-se amb els mateixos nivells de qualitat, seguretat o eficàcia en modalitat remota**.

La presencialitat s'exigirà quan sigui necessària per garantir la correcta prestació del servei, la seguretat de les operacions o la coordinació directa amb els equips de l'entitat contractant. La determinació del percentatge, durada i personal afectat correspon a l'entitat contractant i no generarà cap cost addicional.

Es consideraran, **com a mínim**, els següents casos d'ús:

1. Suport en la resolució d'incidents crítics

La presencialitat serà obligatòria quan la naturalesa de l'incident requereixi:

- accés a consoles, sistemes o dades disponibles exclusivament des de la xarxa interna,
- intervenció directa en infraestructures locals o equipament físic,
- coordinació immediata i col·laboració estreta amb l'equip de seguretat i operacions de l'entitat contractant,
- accés a informació sensible o restringida no accessible de forma remota.

Inclou incidents de compromís actiu, interrupcions greus de serveis crítics, fallades en components de seguretat i qualsevol cas que afecti les capacitats de detecció o resposta.

2. Participació en simulacres, exercicis o proves de ciberresiliència

La presencialitat serà requerida quan:

- l'exercici impliqui treball sobre entorns interns o equipament local,
- es validin fluxos crítics o actuacions que necessiten coordinació estreta entre equips,

- es realitzin proves integrades amb components físics, laboratoris interns o entorns restringits.

Això inclou simulacres CROC, exercicis de continuïtat operativa, proves de restabliment i sessions postmortem.

3. Operació, manteniment o manipulació de components tècnics que requereixin accés local

Es requerirà treball presencial quan les activitats associades al servei impliquin accés físic a:

- sondes, equipament de xarxa, appliances de seguretat, sistemes situats en DMZ o dependències corporatives,
- maquinari o consoles que no poden ser operades en remot,
- laboratoris interns o equips situats en segments de xarxa no accessibles de forma remota.

4. Realització de serveis del Lot 3 que requereixin accés físic a equipament (a discreció de l'entitat contractant)

Quan els serveis o activitats inclosos en el **Lot 3** requereixin accés físic a dispositius, equips o infraestructures, **l'entitat contractant podrà exigir la presencialitat del personal de l'adjudicatari** per garantir una execució segura i correcta.

Aquesta decisió correspon únicament a l'entitat contractant i es farà en funció de:

- la naturalesa del servei,
- el nivell de seguretat associat,
- la necessitat de validació, supervisió o intervenció local,
- la criticitat del component o sistema.

7.3 Fase de devolució del servei

L'adjudicatari haurà d'incloure un **Pla de Devolució del Servei** que descrigui de manera clara i exhaustiva totes les obligacions, activitats i responsabilitats que correspondran a les parts implicades, així com els termes i condicions en què es durà a terme la devolució del servei CROC. El pla haurà de garantir en tot moment la continuïtat operativa, la preservació del coneixement i l'absència de qualsevol impacte negatiu sobre les entitats adherides.

El Pla de Devolució haurà de complir, com a mínim, els següents principis i continguts:

- **Termini d'execució**: la devolució haurà de completar-se en un període màxim de **3 mesos**, sense possibilitat de pròrroga ni afectació sobre el calendari del nou contracte basat.
- **Període de traspàs i suport actiu:** l'adjudicatari haurà de garantir un període continuat de **3 mesos de traspàs i transferència de coneixement**, durant el qual proporcionarà suport actiu al nou adjudicatari o a l'equip designat per l'entitat contractant, assegurant la correcta operació, supervisió i governança del servei CROC.
- **Transferència de coneixement i d'informació:** el Pla haurà d'incloure una metodologia completa de traspàs de tots els elements necessaris per operar el servei, incloent, com a mínim:
    - Formació, suport i documentació sobre procediments operatius: gestió d'incidents, informes, fluxos d'escalat i protocols de resposta.
    - Lliurament complet de **tota la informació disponible relacionada amb la prestació del servei per part de les entitats contractants**. Tota aquesta informació haurà d'entregar-se en **format exportable, estructurat i llegible**, i amb el nivell de detall necessari per permetre la continuïtat i traçabilitat del servei. Inclou:
        - l'històric de logs generats pel servei,
        - l'històric complet d'incidències, alertes, problemes i riscos,
        - qualsevol altre registre operatiu necessari.
    - Accés a totes les plataformes, configuracions, documentació operativa, informes i materials necessaris per mantenir el servei.

  - Formació pràctica tutelada, en què el personal designat per les entitats adherides realitzi les tasques pròpies sota supervisió fins a assolir autonomia operativa.

- **Transferència de contractes, serveis i garanties:** l'adjudicatari haurà de facilitar tot el suport necessari per al traspàs, a les entitats adherides o a terceres parts designades, dels serveis subcontractats, contractes de manteniment, llicències i garanties vigents, mantenint en tot moment la cobertura i la funcionalitat pactades.

- **Gestió de responsabilitats i resolució de problemes:** el Pla haurà d'establir un mecanisme clar per definir responsabilitats, gestionar incidències durant la devolució i coordinar-se amb el nou adjudicatari i altres proveïdors, assegurant una resolució eficient i evitant qualsevol interrupció del servei.

- **Manteniment íntegre de la qualitat del servei:** durant tot el període de devolució i traspàs, l'adjudicatari haurà de continuar complint **tots els Acords de Nivell de Servei (ANS)**. La devolució no podrà comportar cap degradació, interrupció ni reducció de les capacitats de detecció, resposta, monitoratge o operació del CROC.

- **Impacte mínim sobre les entitats adherides:** la devolució haurà de dur-se a terme sense requerir una dedicació significativa de recursos propis per part de les entitats adherides. La càrrega principal de les activitats de traspàs recaurà en l'adjudicatari sortint i en el nou adjudicatari.

8. Model de relació

Per a la correcta execució del present Acord Marc i dels contractes basats derivats, s'ha dissenyat un model de relació específic per al govern del mateix Acord Marc i un model de relació per als contractes basats.

Pel que fa a l'Acord Marc, s'estableix que hi haurà d'existir un **Comitè de Seguiment de l'Acord Marc**, responsable de vetllar pel compliment dels objectius generals, coordinar les entitats adherides i garantir la coherència global del servei CROC.

Pel que fa als contractes basats, es defineixen tres nivells de govern:

- **Comitè de Direcció**: òrgan estratègic encarregat d'alinear el servei amb les necessitats i prioritats de l'entitat contractant.
- **Comitè de Seguiment**: òrgan de control i gestió que vetlla pel compliment dels compromisos del contracte, incloent-hi ANS, gestió de riscos i millores proposades.
- **Comitè Operatiu**: espai tècnic per al seguiment diari de la prestació del CROC, la coordinació d'incidents, la planificació de canvis i la resolució de problemes operatius.

Les empreses licitadores hauran de presentar una **proposta de model de relació** tant per a l'Acord Marc com per als contractes basats, que cobreixi com a mínim els requeriments d'aquest plec i desenvolupi el que s'indica en els apartats següents. Aquesta proposta haurà de descriure com es garanteix la participació activa de les parts, la periodicitat de les reunions i els mecanismes de coordinació i escalat en cas d'incidències o conflictes.

8.1 Model de relació Acord Marc

Per a l'Acord Marc, s'estableix un òrgan de govern: el **Comitè de Seguiment de l'Acord Marc**. Aquest òrgan es formalitzarà una vegada finalitzat el procés d'homologació i perdurarà durant tota la vigència de l'Acord Marc.

Aquest comitè estarà format per la persona o persones que BIT designi per aquesta funció i el responsable de contracte del proveïdor seleccionat. En cas necessari, es podran incorporar altres perfils experts en seguretat o en contractació per reforçar la governança.

Les principals funcions del Comitè de Seguiment de l'Acord Marc són:

- Llançament de l'Acord Marc.
- Seguiment i control de l'estat dels contractes basats.
- Gestió dels canvis en l'abast del marc.

- Alineació dels serveis amb l'estratègia de seguretat i transformació digital de l'Ajuntament.
- Revisió de riscos transversals associats al CROC i propostes de mitigació.

El comitè s'executarà a través de dos tipus de reunions:

- **Reunió de llançament (Kick-Off)**: es realitzarà un cop seleccionat el proveïdor i formalitzat l'Acord Marc. L'objectiu és donar visibilitat al proveïdor seleccionat dels futurs projectes i iniciatives, traslladar les necessitats estratègiques i formalitzar l'inici del servei.
- **Reunions de seguiment periòdiques**: es realitzaran de forma trimestral sempre que existeixi un contracte basat actiu. Addicionalment, qualsevol de les parts podrà convocar-les sota demanda. En aquestes reunions participaran l'empresa seleccionada, independentment de si té contractes basats adjudicats o no, i els responsables designats per BIT.

Les principals funcions de les reunions de seguiment seran:

- Presentar el quadre de comandament amb l'estat dels contractes basats.
- Proposar noves millores i oportunitats.
- Proposar i resoldre modificacions i canvis en l'abast dels contractes.
- Presentar riscos associats al funcionament general de l'Acord Marc i les propostes de mitigació.
- Informar sobre l'estat genèric de seguiment dels ANS dels contractes basats en execució, en format agregat.

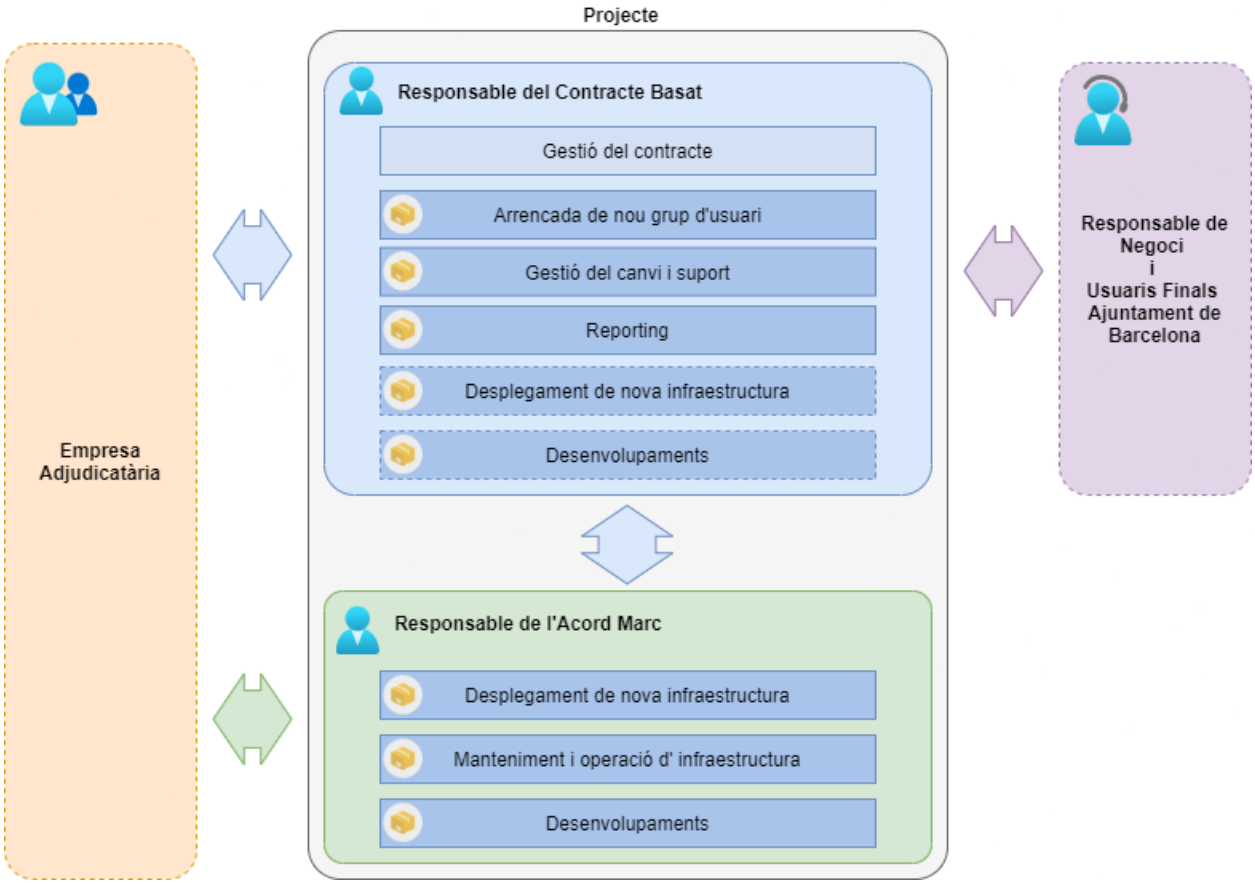
El proveïdor seleccionat, independentment de quan es convoquin les reunions de seguiment i de si té contractes basats adjudicats o no, haurà de presentar de forma **trimestral un informe executiu** a la Direcció de BIT. Aquest informe haurà d'incloure:

- Relació de contractes basats des de l'inici de l'Acord Marc.
- Estat actual dels contractes (actius, finalitzats o en preparació).
- Quadre resum de compliment d'ANS en format agregat.
- Detall de la facturació associada a cadascun dels contractes.

8.2 Model de relació dels contractes basats

El model de relació de cadascun dels contractes basats estarà estructurat en dos subnivells:

- El conduït pel **Responsable del Contracte Basat**, designat per cada entitat contractant.
- El conduït pel **Responsable de l'Acord Marc**, amb una visió global i transversal sobre tots els contractes actius.



Responsable del Contracte Basat

El Responsable designat per cada entitat contractant assumirà la direcció directa del contracte i actuarà com a interlocutor principal amb l'adjudicatari. Les seves funcions principals seran:

- Gestionar i fer el seguiment integral del contracte.
- Coordinar-se amb els equips tècnics i funcionals interns per garantir un desplegament correcte dels serveis CROC.

- Validar el model de desplegament i donar suport a la planificació de la incorporació progressiva de serveis i funcionalitats de seguretat.
- Supervisar la gestió del canvi i donar suport als usuaris i responsables funcionals afectats per la implantació.
- Analitzar l'ús i l'eficiència del servei, revisar els informes de reporting i proposar millores específiques.
- En cas d'ampliacions funcionals o integracions amb serveis propis, fer el seguiment del calendari, l'execució, els lliuraments i la posada en producció.

Responsable de l'Acord Marc

Aquest rol tindrà una visió global i actuarà com a garant de la coherència en la prestació del CROC entre totes les entitats adherides. Les seves funcions principals seran:

- Gestionar de manera transversal el marc contractual, en coordinació amb les entitats adherides i amb l'adjudicatari.
- Supervisar la prestació global del servei per garantir-ne l'homogeneïtat tècnica i metodològica.
- Avaluar, conjuntament amb l'adjudicatari, les necessitats d'ampliació o optimització dels serveis comuns i de les plataformes compartides.
- Fer el seguiment del manteniment i l'evolució dels components transversals del CROC (SIEM/SOAR, canals de resposta, eines de reporting).
- Coordinar l'impacte dels canvis o desenvolupaments impulsats des d'una entitat per assegurar-ne la compatibilitat amb el model general.

Per a cada contracte basat s'estableixen tres òrgans de govern diferenciats, que es constituiran un cop formalitzada l'adjudicació:

- **Comitè de Direcció**: òrgan d'alineació estratègica i presa de decisions a nivell de direcció.
- **Comitè de Seguiment**: òrgan de gestió i control del servei, amb responsabilitat sobre els ANS i la millora contínua.
- **Comitè Operatiu**: òrgan tècnic i de treball per a la coordinació diària, la resolució d'incidents i la planificació de canvis.

Les funcions, responsabilitats i periodicitat de cada comitè es detallen als apartats següents.

8.3 Comitè de direcció

El Comitè de Direcció és l'òrgan encarregat de la supervisió estratègica de cada contracte basat i de la presa de decisions que afectin de manera rellevant els objectius, l'abast o les condicions generals de la prestació del servei de CROC.

Aquest comitè es convocarà sempre sota demanda, a petició de qualsevol de les parts implicades (l'entitat contractant, l'Institut Municipal Barcelona Innovació i Tecnologia –BIT–, o l'adjudicatari), amb un preavís mínim de cinc (5) dies laborables.

Composició mínima

El Comitè de Direcció estarà integrat, com a mínim, per:

- El responsable del contracte basat designat per l'entitat contractant.
- El responsable del projecte designat per BIT.
- Altres representants de BIT que es considerin oportuns en funció de l'abast o la complexitat del servei.
- Els representants de l'empresa adjudicatària responsables de la direcció i coordinació del servei.

Funcions principals

Les funcions específiques d'aquest comitè inclouen:

- Revisar l'estat general del contracte basat, incloent l'evolució del calendari, la planificació i el compliment de les fites establertes.
- Avaluar propostes d'ampliació o reducció de l'abast, sempre que siguin compatibles amb les condicions del contracte.
- Analitzar el compliment dels Acords de Nivell de Servei (ANS) i aplicar les penalitzacions que corresponguin en cas d'incompliments.
- Gestionar riscos estratègics, conflictes o incidències que puguin comprometre la continuïtat o la qualitat del servei, així com identificar oportunitats de millora.
- Conduir les sessions de llançament del projecte (Kick-Off) o de reorientació estratègica, si escau.

Obligacions de l'adjudicatari

Sempre que sigui convocat el Comitè de Direcció, l'adjudicatari haurà de presentar un **resum executiu de l'estat del contracte**, que inclogui com a mínim:

- L'estat de la planificació, calendari i fites assolides o pendents.
- Principals riscos identificats i les accions correctores o mitigadores proposades.
- Valoració dels ANS amb indicació de possibles desviacions.
- Si escau, justificació de les propostes de canvi d'abast i el seu impacte funcional, temporal i econòmic.

A més, l'adjudicatari tindrà la responsabilitat d'aixecar **acta formal de cada reunió** del Comitè de Direcció, amb el resum dels acords presos, els compromisos adquirits i els punts oberts pendents de resolució.

8.4 Comitè de seguiment

El Comitè de Seguiment és l'òrgan encarregat del control i la supervisió operativa de cada contracte basat. Té com a objectiu principal vetllar pel correcte funcionament del servei CROC, el compliment dels compromisos establerts i la identificació d'àrees de millora contínua.

Aquest comitè es reunirà amb caràcter **trimestral**, sense perjudici de reunions extraordinàries que puguin ser convocades a petició de qualsevol de les parts en cas d'incidents crítics, desviacions significatives o canvis rellevants en el servei.

Composició mínima

El Comitè de Seguiment estarà integrat, com a mínim, per:

- El responsable del contracte basat designat per l'entitat contractant.
- Els representants tècnics i funcionals de l'entitat vinculats al servei CROC.
- Els responsables de gestió de l'adjudicatari encarregats del contracte.
- Altres persones de BIT que es considerin necessàries en funció de la naturalesa del servei o de les incidències a tractar.

Funcions principals

Les funcions específiques d'aquest comitè inclouen:

- Fer el seguiment del compliment dels Acords de Nivell de Servei (ANS) i revisar el quadre de comandament del contracte.

- Analitzar els informes periòdics sobre incidents, vulnerabilitats, respostes, investigacions forenses i altres activitats del CROC.
- Identificar desviacions respecte als compromisos adquirits i establir les mesures correctores corresponents.
- Avaluar l'eficàcia dels mecanismes de resposta, gestió de vulnerabilitats i mesures preventives implantades.
- Coordinar la integració amb altres serveis o contractes actius per garantir coherència i sinergies.
- Valorar i aprovar les propostes de millora contínua i d'evolució funcional.
- Identificar riscos operatius i definir conjuntament accions de mitigació.

Obligacions de l'adjudicatari

L'adjudicatari haurà de presentar a cada reunió del Comitè de Seguiment:

- El quadre de comandament actualitzat amb indicadors de compliment dels ANS.
- Llistat d'incidents registrats en el període, amb especial atenció als crítics i a la seva resolució.
- Estat de les activitats de gestió de vulnerabilitats i campanyes de monitoratge.
- Relació de riscos identificats i propostes de mesures correctores.
- Recomanacions de millora i innovacions que puguin aportar valor al servei.

A més, l'adjudicatari haurà d'aixecar **acta formal de cada reunió**, incloent-hi els acords presos, els compromisos adquirits i els punts oberts pendents de resolució.

8.5 Comitè operatiu

El Comitè Operatiu és l'òrgan encarregat de la coordinació tècnica i de la gestió diària del servei CROC. Té com a objectiu garantir la correcta prestació dels serveis contractats, assegurar la resolució àgil d'incidents i coordinar els treballs tècnics i funcionals associats a la detecció, resposta i prevenció de ciberamenaces.

Aquest comitè es reunirà amb caràcter **mensual**, o amb la freqüència necessària segons el volum d'activitat, la criticitat dels serveis o la gravetat dels incidents registrats.

Composició mínima

El Comitè Operatiu estarà integrat, com a mínim, per:

- Els responsables tècnics de l'entitat contractant relacionats amb el CROC.
- Els tècnics i gestors operatius designats per l'adjudicatari.
- Altres perfils especialitzats (per exemple, experts en forense, vulnerabilitats o resposta a incidents) quan la naturalesa dels temes a tractar ho requereixi.

Funcions principals

Les funcions específiques d'aquest comitè inclouen:

- Revisar l'activitat diària del CROC i l'estat dels incidents oberts.
- Coordinar la resolució d'incidents i la seva correcta documentació.
- Planificar i prioritzar les activitats de monitoratge, detecció, resposta i gestió de vulnerabilitats.
- Coordinar les activitats d'anàlisi forense i de threat hunting quan sigui necessari.
- Fer seguiment de les tasques pendents derivades dels Comitès de Direcció i Seguiment.
- Compartir lliçons apreses i recomanacions de seguretat derivades d'incidents o exercicis de simulació.
- Coordinar els canvis tècnics que afectin el CROC i garantir que es realitzin de manera controlada i segura.

Obligacions de l'adjudicatari

L'adjudicatari haurà de presentar a cada reunió del Comitè Operatiu:

- Estat detallat dels incidents oberts i tancats en el període, incloent-hi la seva classificació, temps de resposta i resolució.
- Informe de vulnerabilitats detectades i estat de les tasques de correcció o mitigació.
- Propostes de millora operativa i tècnica, incloent-hi recomanacions basades en noves amenaces o tendències identificades.
- Estat dels canvis tècnics planificats i valoració del seu impacte en el servei.

L'adjudicatari tindrà la responsabilitat d'aixecar **acta formal de cada reunió**, amb els acords presos, les tasques assignades i els punts oberts pendents de resolució.

Estandardització de lliurables

BIT es reserva la facultat d'establir un **format normalitzat d'informes i lliurables de seguiment** aplicable a tots els contractes derivats d'aquest Acord Marc, amb independència dels paquets CROC o OSAP contractats.

Aquesta mesura té com a objectius principals:

- Facilitar la comparabilitat entre diferents contractes basats i adjudicataris.
- Optimitzar la gestió global del servei, permetent una visió agregada dels resultats.
- Assegurar l'homogeneïtat en la qualitat, el contingut i la presentació dels lliurables de seguiment operatiu i estratègic.

Els informes estandarditzats hauran d'incloure, com a mínim:

- Estat actual dels contractes basats i paquets actius.
- Grau de compliment dels Acords de Nivell de Servei (ANS).
- Relació d'incidents i vulnerabilitats més rellevants, amb especial atenció als crítics i a les accions de resolució.
- Riscos identificats i accions de mitigació en curs.
- Propostes de millora i evolució dels serveis prestats.

Quan sigui necessari, BIT podrà actualitzar el format i contingut d'aquests informes per adaptar-los a nous requeriments de seguretat, normatius o de governança. L'adjudicatari estarà obligat a utilitzar aquests formats en tots els lliurables que corresponguin.

9. Equip de treball per l'homologació i per la contractació basada

Per garantir la qualitat tècnica, la continuïtat operativa i l'eficiència en l'execució dels contractes basats derivats d'aquest Acord Marc, l'empresa adjudicatària haurà de disposar d'un equip de treball estable, altament qualificat i dimensionat adequadament a les necessitats de cada paquet funcional que es contracti.

9.1 Equip de treball mínim per l'homologació del Lot 1

Aquest apartat defineix els rols mínims i els equips de treball que haurà de posar a disposició l'adjudicatari del **Lot 1 – Serveis del Centre de Riscos i Operacions de Ciberresiliència**, responsables de l'execució dels serveis de detecció, resposta, recuperació, governança, conscienciació i suport avançat inclosos en els paquets definits en l'apartat 3.3.1, d'acord amb la descripció funcional de cadascun d'ells.

L'equip haurà d'estar dimensionat per garantir la correcta prestació del conjunt dels serveis i haurà de ser capaç d'integrar-se operativament amb:

- El CROC municipal, que manté la capacitat de decisió i la supervisió estratègica.
- L'equip d'operacions de l'entitat municipal.
- Els equips tècnics, funcionals i de desenvolupament de les entitats dependents.
- Els proveïdors tecnològics que donin suport als serveis o plataformes monitorades.

En cap cas el model proposat per l'adjudicatari podrà limitar o impedir que des del CROC municipal es puguin executar o iniciar mesures de contenció directa sobre els dominis tecnològics o les plataformes integrades en els paquets del Lot 1.

Per poder ser homologat en aquest lot, l'empresa proposada haurà de disposar amb el perfils o rols mínims obligatoris establerts per a tots els paquets del lot; el mínim obligatori transversal a tot el lot i els específics de cada paquet.

9.1.1 Rols mínims obligatoris per al Lot 1

L'adjudicatari haurà de designar un **Coordinador/a del servei CROC operatiu**, que actuarà com a interlocutor únic amb el CROC municipal i exercirà, com a mínim, les funcions següents:

a) Supervisar de manera global l'execució dels serveis associats als paquets P1, P2, P3, P4 i P16 a P30;
b) Assegurar l'alineament operatiu amb el CROC municipal i amb l'equip d'operacions de l'entitat municipal;
c) Liderar la gestió operativa, qualitat i millora contínua del servei;
d) Coordinar els escalats i el seguiment de les incidències;
e) Verificar la correcta integració dels informes, mètriques i quadres de comandament;
f) Dirigir i supervisar la implantació i evolució dels paquets contractats;
g) Garantir la disponibilitat dels perfils especialitzats quan els paquets contractats així ho requereixin.

Aquest rol és **l'únic perfil obligatori i mínim** de manera transversal a tots els paquets per a l'homologació dels serveis del Lot 1. El Coordinador/a del servei CROC operatiu haurà de disposar d'experiència demostrable mínima de 5 anys en serveis de ciberseguretat operativa, gestió d'incidents i coordinació amb centres de seguretat (SOC/CERT/CSIRT) a organitzacions de complexitat i volumetria equiparable a l'Ajuntament de Barcelona, i haurà de participar de manera regular en les reunions de seguiment i comitès que es defineixin conjuntament amb el CROC municipal.

9.1.2 Perfils mínims exigibles en funció dels paquets contractats en contractació basada

Els perfils assignats a cada paquet de servei contractable tindran caràcter mínim obligatori en funció del tipus de paquet contractat en cada basat i podran ser prestats tant per persones físiques com mitjançant sistemes automatitzats o agents autònoms basats en intel·ligència artificial.

En el cas de perfils prestats per persones físiques, aquestes hauran d'acreditar una experiència professional mínima de dos (2) anys en l'exercici de funcions de naturalesa equivalent a les objecte del servei, en organitzacions de complexitat, criticitat i volumetria equiparables a l'Ajuntament de Barcelona.

En el cas de perfils no humans, no serà exigible un requisit d'antiguitat temporal. No obstant això, aquests hauran d'estar degudament validats per a ús productiu, amb garanties de maduresa operativa, traçabilitat, fiabilitat, control, auditabilitat i supervisió humana, restant en tot cas sota la responsabilitat plena del contractista pel que fa al seu funcionament, resultats i actuacions. En tots els supòsits, els perfils (humans o no humans) hauran d'estar

integrats dins els mecanismes de governança, seguiment i control definits en el contracte basat.

9.1.2.1 Paquet P1. Gestió de vulnerabilitats i exposició

Quan el paquet **P1** sigui contractat, l'adjudicatari haurà de disposar dels perfils següents, segons correspongui:

- **Especialista en gestió de vulnerabilitats i escaneig d'exposició**, responsable de l'anàlisi, priorització i seguiment de vulnerabilitats en sistemes, aplicacions i serveis.
- **Perfil d'anàlisi funcional** per a la revisió d'informes, contextualització de riscos i suport a la planificació de remediació.

9.1.2.2 Paquet P2. Auditories tècniques i proves de seguretat

Per a la contractació del paquet **P2**, l'adjudicatari haurà d'aportar perfils amb capacitat demostrada en:

- **Auditoria tècnica de seguretat**, incloent-hi proves de penetració, anàlisi de configuracions i revisió de superfícies d'atac.
- **Especialistes en proves de seguretat d'aplicacions**, revisió de codi (si s'inclou en el servei), explotació controlada i validació de vulnerabilitats.
- **Analista de resultats d'auditoria**, per a la consolidació d'informes i la comunicació de conclusions a l'equip municipal.

9.1.2.3 Paquet P3. Serveis d'intel·ligència d'amenaces

Quan el paquet **P3** sigui contractat, s'hauran d'aportar els perfils següents:

- **Analista d'intel·ligència d'amenaces (CTI)**, amb capacitat per a l'anàlisi tàctica, operativa i estratègica de fonts d'intel·ligència.
- **Especialista en correlació d'indicadors i contextualització d'amenaces**, encarregat de la integració de feeds, IoC, TTP i informació rellevant al SIEM, SOAR o sistemes equivalents.
- **Perfil de redacció d'informes CTI**, per a la generació de productes d'intel·ligència orientats a la presa de decisions.

9.1.2.4 Paquet P4. Inventari i classificació d'actius

Quan el paquet **P4** sigui contractat, l'adjudicatari haurà de posar a disposició perfils amb competències en:

- **Especialista en inventari i classificació d'actius**, responsable de la gestió de catàlegs d'actius, modelització de dependències i actualització de registres.
- **Analista de classificació i criticitat**, encarregat d'aplicar criteris de classificació, taxonomia d'actius i avaluació del nivell d'importància i dependència amb els serveis crítics.

9.1.2.5 Paquet P16. Monitoratge i detecció en llocs de treball i dispositius mòbils

Quan el paquet **P16** sigui contractat, l'adjudicatari haurà de posar a disposició:

- **Especialista en EDR/XDR**, responsable de la configuració, manteniment i validació de deteccions en endpoints i dispositius mòbils.
- **Analistes N1/N2 de detecció**, amb capacitat per analitzar alertes, correlacionar esdeveniments i identificar comportaments anòmals.
- **Perfil de resposta inicial sobre endpoint**, encarregat de proposem accions de contenció i mesures correctores.

9.1.2.6 Paquet P17. Monitoratge i detecció en servidors i càrregues de treball

Quan es contracti el paquet **P17**, es requeriran:

- **Especialista en seguretat de servidors i plataformes de virtualització**, capaç de supervisar i mantenir sensors, agents i telemetries.
- **Analista N2 especialitzat en detecció sobre servidors**, per a l'anàlisi de patrons, correlació avançada i interpretació de telemetries de càrregues.
- **Perfil de suport a la resposta en servidors**, per a recomanacions de contenció i mesures de remediació.

9.1.2.7 Paquet P18. Monitoratge i detecció en identitats i accessos

Quan el paquet **P18** sigui contractat, l'adjudicatari haurà de disposar de:

- **Especialista en identitats i accés (IAM/IGA)** amb coneixement de telemetries de comportament, alertes de compromís i riscos associats.
- **Analistes N1/N2 de detecció en identitats**, responsables de la revisió d'activitats sospitoses, autenticacions anòmales i correlació amb altres dominis.
- **Perfil de suport a les mesures de contenció i bloqueig d'identitats compromeses**.

9.1.2.8 Paquet P19. Monitoratge i detecció sobre dades i informació

Quan el paquet **P19** sigui contractat, caldrà aportar:

- **Especialista en protecció de dades i DLP**, encarregat de la configuració, monitoratge i revisió d'esdeveniments relacionats amb la fuga de dades i l'accés indegut.
- **Analista N2 especialitzat en detecció orientada a dades**, per a la validació d'incidents, revisió de patrons d'exfiltració i correlació amb altres dominis.
- **Perfil de suport a plans de contenció i protecció de la informació**.

9.1.2.9 Paquet P20. Monitoratge i detecció en correu i col·laboració

Quan el paquet **P20** sigui contractat, l'adjudicatari haurà de disposar de:

- **Especialista en seguretat de correu i plataformes de col·laboració**, responsable d'analitzar deteccions i configuracions avançades (phishing, malware, spoofing, etc.).
- **Analistes N1/N2 de detecció en correu**, per a la revisió d'alertes i correlació amb altres dominis.
- **Perfil d'investigació funcional de casos associats a usuaris**, quan sigui necessari.

9.1.2.10 Paquet P21. Monitoratge i detecció en xarxa

Per a la contractació del paquet **P21**, es requerirà:

- **Especialista en xarxes i NDR**, responsable de regles, signatures, deteccions basades en comportament i telemetries de trànsit.

- **Analista N2 especialitzat en domini de xarxa**, per interpretar patrons de moviment lateral, escanejos, anomalies i connexions sospitoses.
- **Perfil de suport a la contenció en xarxa** (segmentació, bloqueigs i mesures equivalents).

9.1.2.11 Paquet P22. Monitoratge i detecció en aplicacions i APIs

Quan el paquet **P22** sigui contractat:

- **Especialista en WAF/WAAP i seguretat d'aplicacions**, responsable de regles, signatures i deteccions avançades en aplicacions i APIs.
- **Analista N2 especialitzat en telemetries d'aplicació**, per a la revisió d'anomalies, patrons d'abús i correlació amb registres d'aplicació.
- **Perfil de suport a la revisió d'incidents d'aplicació**.

9.1.2.12 Paquet P23. Monitoratge i detecció en serveis al núvol

Quan el paquet **P23** sigui contractat, l'adjudicatari haurà d'aportar:

- **Especialista en seguretat al núvol (CNAPP/CSPM)**, responsable d'alertes, configuracions crítiques i detecció de riscos.
- **Analista N2 especialitzat en entorns multicloud**, per correlació i investigació d'incidents.
- **Perfil de suport a recomanacions de contenció en entorns cloud**.

9.1.2.13 Paquet P24. Monitoratge i detecció en OT/IoT i tecnologies emergents

Quan el paquet **P24** sigui contractat:

- **Especialista OT/IoT**, amb capacitat per interpretar alertes en entorns industrials, IoT, sensors i tecnologies emergents.
- **Analista especialitzat en telemetries de protocols industrials i IoT**, per a la validació i investigació d'incidents.
- **Perfil de coordinació amb equips d'infraestructura i manteniment d'OT/IoT**.

9.1.2.14 Paquet P25. Monitoratge i detecció en hipervisors i plataformes de virtualització

Per al paquet **P25**:

- **Especialista en virtualització i hipervisors**, responsable del monitoratge de plataformes i deteccions associades.
- **Analista N2 especialitzat en entorns virtuals**, per correlació i validació de deteccions.
- **Perfil de suport a accions de contenció en entorns virtuals**.

9.1.2.15 Paquet P26. Monitoratge i detecció en contenidors i orquestradors

Quan **P26** sigui contractat:

- **Especialista en seguretat de contenidors i Kubernetes/OpenShift**, responsable de regles, deteccions i configuració.
- **Analista N2 amb coneixement de plataformes cloud-native**, per investigació i correlació de deteccions.
- **Perfil tècnic de suport a mesures de contenció en orquestradors**.

9.1.2.16 Paquet P27. Resposta a incidents

Quan el paquet **P27** sigui contractat:

- **IR Lead (Incident Response Lead)**.
- **Analistes d'Incident Response N2/N3**, per a la investigació tècnica.
- **Perfil de forense digital**, per a la gestió d'evidències.
- **Suport legal/regulatori**, quan es requereixi notificació ENS/NIS2.

9.1.2.17 Paquet P28-A/B/C. Recuperació post-incident

Per als paquets **P28-A, P28-B i P28-C**:

- **Especialista en continuïtat (BCP/DRP)**, per al suport a plans, proves i validacions.

- **Especialista en restauració i resiliència**, responsable de validar la recuperació tècnica dels serveis afectats.

9.1.2.18 Paquet P29. Conscienciació en seguretat

Quan el paquet **P29** sigui contractat:

- **Consultor/a de conscienciació i formació**, responsable de campanyes, simulacions i activitats divulgatives.
- **Especialista en disseny de continguts i exercicis de phishing**, quan correspongui.

9.1.2.19 Paquet P30. Governança, risc i compliment

Quan el paquet **P30** sigui contractat, l'adjudicatari haurà d'aportar:

- **Consultor/a de governança, risc i compliment (GRC)**.
- **Especialista en mètriques, quadres de comandament i informes estratègics**, responsable de KPI, KRI i informes executius.
- **Perfil de suport a la maduresa, qualitat i millora contínua del servei**.

9.1.3 Criteris de dimensionament

El dimensionament dels perfils requerits es determinarà atenent els paràmetres quantificadors de cada paquet i haurà de garantir:

a) La cobertura operativa adequada per als paquets contractats;
b) La disponibilitat i especialització dels perfils necessaris sense imposar equips mínims addicionals;
c) La plena integració amb el CROC municipal i la seva capacitat de contenció directa;
d) L'adaptació del dimensionament a l'evolució del servei contractat;
e) La disponibilitat de recursos per reforçar el servei en cas d'incident crític.
f) El compliment dels acords de nivell de servei aplicables.

En tot cas, el dimensionament proposat per l'adjudicatari haurà de ser **justificat documentalment en les ofertes dels contractes basats**, indicant la dedicació estimada per perfil, tasca i paquet funcional, i restarà subjecte a validació i revisió per part del CROC municipal i dels responsables de l'entitat contractant al llarg de la vigència del contracte.

9.1.4 Requisits addicionals

- Els perfils requerits hauran de participar en simulacres, exercicis de cibercrisi i proves de recuperació.
- S'haurà de garantir l'elaboració d'informes tècnics, operatius i estratègics derivats dels paquets contractats.
- Tots els perfils hauran de complir els requisits de confidencialitat, competència i experiència establerts al plec.
- L'adjudicatari haurà de garantir la continuïtat operativa dels perfils clau, preveient mecanismes de substitució en cas de vacances, baixes o rotació, de manera que no es vegi afectada la qualitat ni la disponibilitat del servei.

9.2 Equip de treball mínim per l'homologació del Lot 2

Aquest apartat defineix els rols mínims i els equips de treball que haurà de posar a disposició l'adjudicatari del **Lot 2 – Serveis d'avaluació independent, verificació i control qualitatiu del CROC**, responsables de l'execució dels serveis d'avaluació, validació, verificació tècnica, auditories i millora contínua descrits a l'apartat 5, d'acord amb la descripció funcional de cadascun dels paquets contractats.

L'equip haurà d'estar dimensionat per garantir la correcta prestació del conjunt dels serveis d'avaluació, i haurà de ser capaç de coordinar-se amb:

- El CROC municipal i els seus òrgans de governança.
- L'equip d'operacions de l'entitat municipal i els responsables de GRC.
- Els equips tècnics, funcionals i de desenvolupament de les entitats dependents.
- Els proveïdors que prestin serveis operatius CROC-OSAP, únicament a efectes de recollida d'evidències i validació de resultats.

En tot cas, **l'equip del Lot 2 haurà de mantenir en tot moment la seva independència organitzativa i operativa** respecte dels serveis prestats en la resta de lots, d'acord amb els requisits d'absència de conflictes d'interès definits al plec.

Per poder ser homologat en aquest lot, l'empresa proposada haurà de disposar amb el perfils o rols mínims obligatoris establerts per a tots els paquets del lot; el mínim obligatori transversal a tot el lot i els específics de cada paquet.

9.2.1 Rols mínims obligatoris per al Lot 2

L'adjudicatari haurà de designar un **Coordinador/a del servei d'avaluació independent del CROC**, que actuarà com a interlocutor únic amb el CROC municipal i amb els responsables designats per les entitats adherides, i que exercirà, com a mínim, les funcions següents:

a) Supervisar de manera global l'execució dels serveis associats als paquets del Lot 2
b) Assegurar la **independència, imparcialitat i absència de conflictes d'interès** en totes les activitats d'avaluació, de conformitat amb els requisits definits al plec.
c) Vetllar per l'alineament metodològic amb els marcs de referència aplicables (ENS, NIS2, guies CCN, models de maduresa, etc.) i amb el Pla Director de Seguretat de l'Ajuntament.
d) Coordinar la planificació, l'execució i el seguiment de les avaluacions, auditories, exercicis i proves associades als contractes basats.
e) Dirigir la gestió de la qualitat del servei, garantint la coherència metodològica, la traçabilitat de les evidències i la consistència dels informes emesos.
f) Coordinar la comunicació amb els responsables municipals, incloent comitès de seguiment, presentació de resultats i sessions d'explicació de conclusions.
g) Garantir la disponibilitat dels perfils especialitzats necessaris per a cada paquet o abast concret, d'acord amb les característiques del contracte basat.

Aquest rol és **l'únic perfil obligatori i mínim** de manera transversal a tots els paquets per a l'homologació dels serveis del Lot 2. El Coordinador/a del servei d'avaluació independent haurà de disposar d'experiència demostrable mínima de 5 anys en serveis de ciberseguretat (SOC/CERT/CSIRT o equivalents) a organitzacions de complexitat i volumetria equiparable a l'Ajuntament de Barcelona, i haurà de participar de manera regular en les reunions de seguiment i comitès que es defineixin conjuntament amb el CROC municipal.

9.2.2 Perfils mínims exigibles en funció dels paquets contractats en contractació basada

Els perfils assignats a cada paquet de servei contractable tindran caràcter mínim obligatori en funció del tipus de paquet contractat en cada basat i podran ser prestats tant per persones físiques com mitjançant sistemes automatitzats o agents autònoms basats en intel·ligència artificial.

En el cas de perfils prestats per persones físiques, aquestes hauran d'acreditar una experiència professional mínima de dos (2) anys en l'exercici de funcions de naturalesa equivalent a les objecte del servei, en organitzacions de complexitat, criticitat i volumetria equiparables a l'Ajuntament de Barcelona.

En el cas de perfils no humans, no serà exigible un requisit d'antiguitat temporal. No obstant això, aquests hauran d'estar degudament validats per a ús productiu, amb garanties de maduresa operativa, traçabilitat, fiabilitat, control, auditabilitat i supervisió humana, restant en tot cas sota la responsabilitat plena del contractista pel que fa al seu funcionament, resultats i actuacions. En tots els supòsits, els perfils (humans o no humans) hauran d'estar integrats dins els mecanismes de governança, seguiment i control definits en el contracte basat.

9.2.2.1 Paquet P31. Avaluació i millora contínua

Quan el paquet P31 sigui contractat, l'adjudicatari haurà de disposar, segons l'abast del servei, de perfils amb les competències següents:

- **Consultor/a sènior de maduresa de CROC/SOC**, responsable de dissenyar i mantenir el model d'avaluació integrada, el mapa de maduresa, el full de ruta (roadmap) i les recomanacions estratègiques, utilitzant marcs de referència reconeguts (p. ex. SOC-CMM, NIST CSF, MITRE ATT&CK, ENS).
- **Especialista en Red Team** amb experiència en la definició, execució i documentació d'exercicis d'atac realistes i controlats a escala organitzativa, orientats a validar les capacitats de detecció, resposta i contenció del CROC.
- **Especialista en exercicis Purple Team**, encarregat de coordinar les activitats entre equips Red i Blue, optimitzar els casos de detecció i resposta, i transformar els resultats en millores operatives i tècniques.
- **Analista de dades i mètriques de seguretat**, responsable de la definició, càlcul i manteniment de KPI, KRI, indicadors de qualitat de servei, quadres de comandament multinivell i comparatives històriques.
- **Auditor/a de serveis i processos CROC-OSAP**, encarregat de la revisió periòdica de procediments, PNT, playbooks i fluxos operatius, així como de la verificació de la seva aplicació efectiva i eficàcia.
- **Consultor/a de governança, risc i compliment (GRC)**, responsable d'alinear els resultats de les avaluacions amb el Pla Director de Seguretat, el model de riscos i els requisits normatius (ENS, NIS2, CCN, etc.).

Aquests perfils podran ser exercits per persones diferents o acumulats en un nombre inferior de professionals, sempre que es demostri que es cobreixen de manera adequada totes les competències i responsabilitats, i que es manté la independència respecte dels equips operatius dels altres lots.

9.2.3 Criteris de dimensionament

El dimensionament dels perfils requerits per al Lot 2 es determinarà atenent, com a mínim, els paràmetres següents:

a) El nombre d'usuaris interns de l'entitat contractant objecte del servei i l'abast dels serveis CROC avaluats.
b) La freqüència i intensitat de les avaluacions (estratègiques, tàctiques i operatives), auditories, exercicis Red Team/Purple Team i activitats de validació contínua de controls.
c) La complexitat dels dominis tecnològics i organitzatius analitzats (serveis, plataformes, entitats adherides i proveïdors implicats).

El dimensionament haurà de garantir:

d) La capacitat d'executar les activitats d'avaluació, validació i millora contínua dins dels terminis acordats, sense afectar la independència del servei.
e) La disponibilitat i especialització dels perfils necessaris, sense imposar equips mínims addicionals més enllà del coordinador del servei, però assegurant en tot moment la cobertura de totes les competències requerides.
f) La plena separació funcional i operativa respecte dels equips i recursos que prestin serveis en els Lots 1 i 3, evitant qualsevol conflicte d'interès o interferència amb els processos operatius del CROC.
g) L'adaptació del dimensionament a l'evolució del servei contractat, permetent reforçar temporalment els recursos en períodes d'alta activitat (per exemple, en campanyes d'exercicis Red Team/Purple Team o en cicles d'auditoria intensiva).
h) El compliment dels acords de nivell de servei aplicables.

En tot cas, el dimensionament proposat per l'adjudicatari haurà de ser **justificat documentalment en les ofertes dels contractes basats**, indicant la dedicació estimada per perfil, tasca i paquet funcional, i restarà subjecte a validació i revisió per part del CROC municipal i dels responsables de l'entitat contractant al llarg de la vigència del contracte.

9.2.4 Requisits addicionals dels perfils del Lot 2

A més dels requisits generals del plec, els perfils adscrits al Lot 2 hauran de complir els criteris següents:

- Participar activament en **simulacres, exercicis de cibercrisi, Red Team i Purple Team**, així com en les sessions de revisió de resultats amb l'Ajuntament.
- Garantir l'elaboració d'**informes tècnics, operatius i estratègics** derivats de les avaluacions, en un format comprensible per a diferents nivells (tècnic, tàctic i direccional).
- Mantenir en tot moment els requisits de **confidencialitat, competència i experiència**, incloent certificacions reconegudes en ciberseguretat, auditoria, Red Team/Purple Team, GRC o marcs de maduresa, d'acord amb el que estableix el plec.
- Garantir la **continuïtat operativa dels perfils clau**, preveient mecanismes de substitució en cas de vacances, baixes o rotació, de manera que no es vegi afectada la qualitat ni la disponibilitat del servei.

9.3 Equip de treball mínim per l'homologació del Lot 3

Aquest apartat defineix els rols mínims i els equips de treball que haurà de posar a disposició l'adjudicatari del **Lot 3 – Serveis d'Operació, Administració i Evolució de les Eines Avançades de Protecció (OSAP)**, responsables de l'execució dels serveis descrits a l'apartat 6, incloent la implantació, configuració, administració, operació, optimització i evolució de les diferents solucions de seguretat associades als paquets funcionals contractats.

Els serveis del Lot 3 requereixen necessàriament la participació de **perfils d'operació i administració tècnica especialitzada**, responsables de gestionar de manera directa les plataformes OSAP, aplicar polítiques, executar canvis, realitzar actuacions de manteniment preventiu i reactiu, supervisar la salut i rendiment de les eines, i donar suport tècnic a les activitats de detecció i resposta coordinades amb el CROC.

L'equip haurà d'estar dimensionat per garantir la correcta prestació del conjunt dels serveis OSAP, i haurà de ser capaç de coordinar-se amb:

- El **CROC municipal**, com a servei responsable de la detecció i la resposta a incidents, especialment en l'execució de mesures de contenció, en la integració de telemetria i en l'orquestració de respostes automatitzades.

- L'**equip d'operacions de l'entitat municipal**, responsable del manteniment i gestió de les plataformes corporatives i dels serveis TIC associats.
- Les **entitats dependents i els seus equips tècnics**, per garantir l'alineament operatiu i la uniformitat de les polítiques de seguretat.
- Els **proveïdors externs** que prestin serveis tecnològics o de manteniment d'infraestructures corporatives, exclusivament a efectes de coordinació operativa, resolució d'incidències i integració de funcionalitats en el marc dels paquets contractats.

L'equip del Lot 3 haurà de mantenir en tot moment la seva **coherència operativa** respecte de la resta de lots, preservant la **coordinació necessària amb el CROC**, i garantint alhora l'**execució homogènia, multieina i coordinada** de totes les actuacions sobre les plataformes OSAP, d'acord amb els requisits definits al plec.

En tots els casos, l'adjudicatari haurà d'assegurar que l'equip disposa de la **capacitat tècnica, l'especialització i la disponibilitat** necessàries per prestar els serveis contractats amb qualitat, mantenint **traçabilitat completa**, **documentació actualitzada** i **alineament amb les millors pràctiques** i els estàndards municipals de seguretat.

Per poder ser homologat en aquest lot, l'empresa proposada haurà de disposar amb el perfils o rols mínims obligatoris establerts per a tots els paquets del lot; el mínim obligatori transversal a tot el lot i els específics de cada paquet.

9.3.1Rols mínims obligatoris per al Lot 3

L'adjudicatari haurà de designar obligatòriament un **Coordinador/a del servei OSAP**, que actuarà com a interlocutor únic amb el CROC municipal i amb els responsables designats per les entitats adherides. Aquest rol és l'únic perfil mínim obligatori per a la prestació dels serveis del Lot 3.

El Coordinador/a del servei OSAP assumirà, com a mínim, les funcions següents:

a) Dirigir i supervisar de manera global l'execució dels serveis OSAP, incloent tots els paquets funcionals contractats.
b) Coordinar les activitats de planificació, seguiment, reporting i control de qualitat associades a cada contracte basat.
c) Assegurar l'alineament tècnic, metodològic i procedimental amb el model operatiu del CROC, facilitant la integració de telemetria i la resposta coordinada davant incidents.

d) Garantir la coherència tècnica entre totes les eines OSAP operades, vetllant perquè s'apliquin criteris unificats de polítiques, configuracions i actualitzacions.
e) Coordinar la comunicació amb els responsables municipals designats, incloent la participació en comitès de seguiment, sessions de revisió i presentacions de resultats.
f) Assegurar la disponibilitat dels perfils tècnics especialitzats requerits per cada paquet funcional.
g) Verificar que la documentació tècnica, funcional, operativa i de tancament es genera, manté i lliura d'acord amb els requisits del plec.

Aquest rol és **l'únic perfil obligatori i mínim** de manera transversal a tots els paquets per a l'homologació dels serveis del Lot 3. El Coordinador/a del servei haurà d'acreditar experiència demostrable mínima de 5 anys en la direcció o coordinació de serveis d'operació i gestió d'eines avançades de protecció (EDR/XDR, WAF, NGFW, DLP, ITDR, CNAPP, etc.) i en la gestió operativa de plataformes de seguretat en entorns híbrids i multitecnologia a organitzacions de complexitat i volumetria equiparable a l'Ajuntament de Barcelona, i haurà de participar de manera regular en les reunions de seguiment i comitès que es defineixin conjuntament amb el CROC municipal.

9.3.2 Perfils mínims exigibles en funció dels paquets contractats en contractació basada

Els perfils assignats a cada paquet de servei contractable tindran caràcter mínim obligatori en funció del tipus de paquet contractat en cada basat i podran ser prestats tant per persones físiques com mitjançant sistemes automatitzats o agents autònoms basats en intel·ligència artificial.

En el cas de perfils prestats per persones físiques, aquestes hauran d'acreditar una experiència professional mínima de dos (2) anys en l'exercici de funcions de naturalesa equivalent a les objecte del servei, en organitzacions de complexitat, criticitat i volumetria equiparables a l'Ajuntament de Barcelona.

En el cas de perfils no humans, no serà exigible un requisit d'antiguitat temporal. No obstant això, aquests hauran d'estar degudament validats per a ús productiu, amb garanties de maduresa operativa, traçabilitat, fiabilitat, control, auditabilitat i supervisió humana, restant en tot cas sota la responsabilitat plena del contractista pel que fa al seu funcionament, resultats i actuacions. En tots els supòsits, els perfils (humans o no humans) hauran d'estar

integrats dins els mecanismes de governança, seguiment i control definits en el contracte basat.

En el cas de perfils no humans, no serà exigible un requisit d'antiguitat temporal. No obstant això, aquests hauran d'estar degudament validats per a ús productiu, amb garanties de maduresa operativa, traçabilitat, fiabilitat, control, auditabilitat i supervisió humana, restant en tot cas sota la responsabilitat plena del contractista pel que fa al seu funcionament, resultats i actuacions. En tots els supòsits, els perfils (humans o no humans) hauran d'estar integrats dins els mecanismes de governança, seguiment i control definits en el contracte basat.

9.3.2.1 Paquet P5. Protecció de llocs de treball i dispositius mòbils

Quan P5 sigui contractat, l'adjudicatari haurà d'aportar els perfils següents:

- Tècnic/s N3, especialistes en administració d'EPP/EDR/XDR, així com a dispositius de protecció de navegació (servidors proxies, etc), responsables de configuracions, polítiques, agents i actualitzacions.
- Tècnic/s N1/N2, responsables de la operació de les solucions desplegades, monitoratge, revisió d'estat i actuacions preventives.
- Perfil tècnic de suport a contenció en endpoints, per executar aïllaments, bloqueigs i accions correctores.

9.3.2.2 Paquet P6. Protecció de servidors i càrregues de treball

Quan P6 sigui contractat, l'adjudicatari haurà d'aportar els perfils següents:

- Tècnic/s N3, especialistes en administració de protecció de servidors, així com a dispositius de protecció de navegació (servidors proxies, etc), responsables de bastionat, agents i configuracions de seguretat.
- Tècnic/s N1/N2, responsables de la operació de les solucions desplegades, monitoratge i revisió d'anomalies.
- Perfil tècnic de suport a mesures de contenció i recuperació en servidors.

9.3.2.3 Paquet P7. Protecció d'identitat i accessos

Quan P7 sigui contractat, l'adjudicatari haurà d'aportar els perfils següents:

- Tècnic/s N3, especialistes en administració d'identitats i accessos (IAM/ITDR/MFA/PAM), així com plataformes AAA, VPN (U2S i L2L) i ZTNA, responsable de polítiques d'autenticació i permisos.
- Tècnic/s N1/N2, responsables de la operació de les solucions desplegades, gestió de certificats de lloc web, supervisió d'activitats i detecció d'anomalies.
- Perfil tècnic de suport a bloqueig i recuperació d'identitats compromeses.

9.3.2.4 Paquet P8. Protecció d'informació i dades

Quan P8 sigui contractat, l'adjudicatari haurà d'aportar els perfils següents:

- Administrador/a de DLP/DSPM, responsable de polítiques, regles, classificació i etiquetatge.
- Operador/a, per monitoratge de transferències i ús de la informació.
- Perfil tècnic de suport a mesures de contenció i protecció de dades

9.3.2.5 Paquet P9. Protecció de correu i entorns de col·laboració

Quan P9 sigui contractat, l'adjudicatari haurà d'aportar els perfils següents:

- Tècnic/s N3, especialistes en administració de plataformes de seguretat de correu i col·laboració, responsable de configuracions i regles.
- Tècnic/s N1/N2,, responsables de la operació d'equips i monitoratge, detecció i gestió d'incidències.
- Perfil tècnic de suport a contenció d'incidents de correu i plataformes col·laboratives..

9.3.2.6 Paquet P10a. Protecció de xarxes i serveis de telecomunicacions

Quan P10a sigui contractat, l'adjudicatari haurà d'aportar els perfils següents:

- Consultor/a sènior, amb perfil de arquitecte de comunicacions i sistemes, responsable de garantir que les solucions tecnològiques siguin segures, escalables i eficients.

- Tècnics N3, especialistes en administració de solucions de comunicacions i seguretat, incloent NGFW/IPS/NDR/DDI, responsables de configuracions i polítiques.
- Tècnics N1/N2, responsables de la operació de les plataformes de seguretat/comunicacions i monitoratge de trànsit, alertes i esdeveniments, així com la gestió d'incidències, problemes, peticions i canvis de primer nivell.
- Perfil tècnic de suport a contenció i segmentació.

9.3.2.7 Paquet P10b. Gestió i protecció de la infraestructura física de xarxa

Quan P10b sigui contractat, l'adjudicatari haurà d'aportar els perfils següents:

- Consultor/a sènior, amb perfil de arquitecte de comunicacions i sistemes, responsable de optimitzar i supervisar la infraestructura tecnològica que suporta els sistemes d'informació i les comunicacions.
- Tècnic/s N3, especialistes en administració de routers, switches i controladores Wi-Fi, responsable de configuracions, manteniment, actualitzacions i seguretat.
- Tècnic/s N1/N2,, responsables de la operació d'equips i monitoratge de ports, enllaços i dispositius, així com la gestió d'incidències, problemes, peticions i canvis de primer nivell.
- Perfil tècnic de suport a actuacions de recuperació i resolució d'incidències.

9.3.2.8 Paquet P11. Protecció d'aplicacions i APIs

Quan P11 sigui contractat, l'adjudicatari haurà d'aportar els perfils següents:

- Tècnic/s N3, especialistes en administració de WAF/WAAP/ADC/AntiDDoS, així com a solucions per balanceig de carrega, responsable de regles i configuracions.
- Tècnic/s N1/N2, responsables de la operació d'equips i monitoratge, detecció i revisió d'anomalies.
- Perfil tècnic de suport a contenció i reforç de configuracions d'aplicació.

9.3.2.9 Paquet P12. Protecció d'entorns al núvol

Quan P12 sigui contractat:

- Administrador/a de CNAPP/CSPM/CWPP/CIEM, responsable de configuracions i controls de seguretat.

- Operador/a, per monitoratge d'activitats i detecció d'anomalies.
- Perfil tècnic de suport a accions de contenció i correcció en entorns híbrids i multicloud.

9.3.2.10 Paquet P13. Protecció de tecnologies emergents i especialitzades (OT, IoT, IA i criptografia)

Quan P13 sigui contractat:

- Administrador/a de plataformes OT/IoT/IA/criptografia, responsable de configuracions i bastionat.
- Operador/a, per supervisió de telemetria i detecció d'anomalies.
- Perfil tècnic de suport a mesures de contenció en entorns OT/IoT/IA i criptogràfics.

9.3.2.11 Paquet P14. Protecció d'hipervisors i plataformes de virtualització

Quan P14 sigui contractat:

- Administrador/a d'hipervisors i virtualització, responsable de bastionat, configuracions i controls d'accés.
- Operador/a, per monitoratge i detecció d'activitat anòmala.
- Perfil tècnic de suport a contenció i recuperació en entorns de virtualització.

9.3.2.12 Paquet P15. Protecció de contenidors i orquestradors

Quan P15 sigui contractat:

- Administrador/a de Kubernetes/OpenShift i seguretat de contenidors, responsable de configuracions i regles.
- Operador/a, per monitoratge de clústers, imatges i pipelines.
- Perfil tècnic de suport a mesures de contenció en orquestradors i entorns cloud-native.

9.3.3Criteris de dimensionament

El dimensionament dels perfils requerits per a la prestació dels serveis del Lot 3 s'establirà atenent, com a mínim, els paràmetres següents:

a) **L'abast funcional dels paquets contractats**, incloent el nombre d'eines a administrar, la seva complexitat i els dominis tecnològics implicats (endpoints, servidors, xarxa, aplicacions, cloud, identitat, dades, OT/IoT, virtualització, contenidors, etc.).
b) **El volum d'actius i usuaris associats a cada paquet**, d'acord amb els paràmetres quantificadors definits en l'apartat 6 (usuaris, servidors, workloads, nodes de virtualització, càrregues cloud, dispositius OT/IoT, etc.).
c) **La intensitat operativa prevista**, incloent la freqüència de canvis, la gestió de polítiques, el volum d'incidències i alertes, l'aplicació de parches i actualitzacions, i les necessitats de monitoratge i optimització contínua.
d) **La necessitat de garantir operació multieina**, assegurant la coherència de configuracions i polítiques en tots els productes contractats.
e) **Els requisits de disponibilitat i resposta**, especialment en aquells serveis que puguin requerir actuacions immediates en coordinació amb el CROC, com ara contencions, bloqueigs, aïllaments o aplicació urgent de canvis de seguretat.

El dimensionament proposat haurà de garantir sempre:

f) **La cobertura operativa adequada**, assegurant que els administradors i operadors assignats puguin executar totes les tasques requerides sense retardar l'operativa del CROC.
g) **La disponibilitat i especialització suficients**, evitant dependències crítiques d'un únic perfil en cap paquet funcional.
h) **La capacitat de reforç temporal**, de manera que l'adjudicatari pugui aportar recursos addicionals en períodes d'alta càrrega operativa o en escenaris d'incident crític.
i) **La traçabilitat i control de qualitat**, garantint que totes les actuacions sobre les eines quedin registrades i puguin ser auditades.
j) **La integració amb el model operatiu del CROC**, assegurant que els perfils del Lot 3 treballin de manera coordinada amb els processos de detecció i resposta, sense generar interferències, desalineaments o riscos operatius.
k) El **compliment dels acords de nivell de servei** aplicables.

En tot cas, el dimensionament proposat per l'adjudicatari haurà de ser **justificat documentalment en les ofertes dels contractes basats**, indicant la dedicació estimada per

perfil, tasca i paquet funcional, i restarà subjecte a validació i revisió per part del CROC municipal i dels responsables de l'entitat contractant al llarg de la vigència del contracte.

9.3.4Requisits addicionals dels perfils del Lot 3

A més dels requisits generals establerts al plec, els perfils assignats al Lot 3 hauran de complir els criteris següents:

- **Participació en activitats de coordinació operativa amb el CROC**, incloent sessions periòdiques de revisió, comitès tècnics, i reunions de seguiment dels serveis OSAP.
- **Participació en simulacres, exercicis de cibercrisi i proves de contenció**, quan els paquets contractats tinguin implicació en processos de detecció, resposta o recuperació, especialment en les eines que suporten mesures de contenció directa.
- **Elaboració d'informes tècnics i operatius**, corresponents a les tasques d'administració, configuració, manteniment, actualització o optimització de les solucions.
- **Compliment d'experiència i certificacions**, acreditant coneixement pràctic de les tecnologies concretes operades (EDR, NGFW, WAF, CNAPP, etc.) i de les millors pràctiques aplicables a cada paquet funcional.
- **Disponibilitat de mecanismes de substitució**, garantint la continuïtat del servei en cas de vacances, baixes o rotació de personal, sense impactar l'operació dels paquets contractats.
- **Confidencialitat, independència i integritat professional**, assegurant que els administradors i operadors del Lot 3 compleixen els requisits de seguretat, confidencialitat i accés privilegiat establerts per l'Ajuntament.
- **Adherència als processos municipals de gestió del canvi**, de manera que qualsevol modificació sobre les solucions quedi validada, registrada, aprovada i integrada en els procediments corporatius de control, **adaptant-se en tot cas a l'horari de gestió del canvi definit per l'entitat contractant**.
- **Domini de les eines corporatives de gestió ITSM**, incloent-hi la gestió d'incidències, peticions, canvis, problemes i documentació operativa.
- **Capacitat de col·laboració amb tercers** (fabricants, suport especialitzat, integradors), sempre d'acord amb els procediments de seguretat municipals i sense comprometre la sobirania dels sistemes.

10. Condicions d'Execució

10.1 Durada de l'Acord Marc

La durada màxima del present Acord Marc serà de 4 anys d'ençà de la seva entrada en vigor.

El termini d'execució i els terminis o dates d'entregues parcials dels contractes basats de l'Acord Marc podran superar el termini de vigència de l'Acord Marc. En aquests casos, la vigència de les prescripcions de l'Acord Marc s'estendrà als períodes que comprendran la durada dels contractes basats.

10.2 Lloc de prestació del servei

La prestació dels serveis associats als **paquets funcionals del CROC (Centre de Riscos i Operacions de Ciberresiliència)** i **de l'OSAP (Operacions de Seguretat i Anàlisi de Protecció)** es realitzarà combinant modalitats **remotes i presencials**, segons les necessitats específiques de cada contracte basat i del tipus de servei prestat.

Prestació remota
Els serveis de caràcter **analític, estratègic o de governança**, incloent la gestió de riscos, el seguiment d'indicadors, la generació d'informes o la gestió de compliment, es realitzaran majoritàriament **de forma remota** des de les instal·lacions del contractista, mitjançant connexió segura amb les entitats contractants.
L'empresa adjudicatària haurà d'establir i mantenir una **connexió dedicada** entre els seus centres de treball i les dependències tècniques de les entitats adherides a l'Acord Marc, complint els següents requisits:

- No suposarà cap cost addicional per a les entitats contractants.
- Haurà de ser, com a mínim, una línia dedicada amb una amplada de banda mínima garantida de 100 Mbps.
- Caldrà disposar d'una connexió alternativa per garantir la redundància i la continuïtat del servei.
- La no prestació del servei per manca de connexió es considerarà una **falta greu** a efectes del compliment dels compromisos contractuals.

Prestació presencial
Els serveis **operatius o de supervisió directa** vinculats a l'àmbit **OSAP**, especialment aquells relacionats amb la monitorització, l'anàlisi de seguretat o la resposta coordinada davant

incidents, podran requerir la **presència física parcial o recurrent** de personal de l'empresa adjudicatària a les instal·lacions municipals o dels centres designats per l'Ajuntament.

L'empresa adjudicatària haurà de garantir aquesta presencialitat en els percentatges i terminis pactats en cada contracte basat, sense que això suposi cap increment del cost de prestació dels serveis.

Les entitats contractants es comprometen, en aquests casos, a proporcionar les condicions bàsiques per al desenvolupament de l'activitat presencial: espai de treball, connexió a xarxa, mobiliari i accés als serveis generals de l'oficina.

10.3 Serveis en remot

Atesa la naturalesa **distribuïda i col·laborativa** del model operatiu del CROC i el seu component **basat en dades i coneixement**, part significativa de les tasques de supervisió, gestió de riscos, governança i seguiment de ciberresiliència es desenvoluparan **en remot**, garantint sempre la qualitat, seguretat i traçabilitat dels processos.

Per assegurar aquesta eficiència, l'adjudicatari haurà de descriure i implementar un **model de prestació remota** que permeti l'execució òptima de totes les tasques assignades, amb capacitat d'adaptació a les diferents realitats de les entitats contractants.

El servei en remot haurà d'incloure, com a mínim, les característiques següents:

- Capacitat d'absorbir càrrega de treball variable, segons l'evolució dels contractes basats i dels requeriments de risc i governança.
- Flexibilitat i adaptabilitat a noves necessitats, mitjançant equips multidisciplinaris amb formació i certificacions actualitzades en gestió de riscos, seguretat de la informació, ciberresiliència i normativa aplicable.
- Disponibilitat de personal expert per cadascuna de les àrees funcionals del CROC i l'OSAP (riscos, governança, compliment, operacions de seguretat, monitoratge, informes executius, etc.).
- Procediments de contingència i garanties de continuïtat del servei, especialment per a la supervisió de serveis crítics o en cas d'incidents de seguretat.
- Capacitat completa de prestació operativa remota, incloent configuració, suport, seguiment d'indicadors, anàlisi, documentació i gestió de riscos.

- Capacitat d'executar auditories, revisions i gestió d'incidents de forma remota, garantint traçabilitat, confidencialitat i compliment normatiu.

Tots els serveis prestats en remot hauran d'estar **coordinats pel Cap de Servei del CROC-OSAP**, que actuarà com a interlocutor principal amb l'entitat contractant.

Aquesta figura serà responsable de garantir una comunicació fluïda, proactiva i efectiva, així com d'impulsar la **millora contínua, la coherència operativa i l'alineament estratègic** del servei amb els objectius i prioritats de cada projecte o entitat municipal.

10.4 Estructura organitzativa i RRHH

La prestació dels serveis derivats del present **Acord Marc** haurà de ser garantida per l'empresa adjudicatària mitjançant recursos propis o, si escau, a través de subcontractistes autoritzats, limitant-se sempre a **un únic nivell de subcontractació**. Atès que l'Acord Marc no comporta l'execució immediata dels serveis, sinó que aquesta es formalitza en els **contractes basats**, l'adjudicatari haurà d'acreditar **la capacitat organitzativa i tècnica suficient** per posar a disposició els recursos humans necessaris en cada contracte basat, d'acord amb els perfils i rols definits al plec.

En tots els casos, l'adjudicatari haurà d'assegurar que **el personal efectivament assignat a cada contracte basat** disposa de la qualificació, experiència i competències requerides per garantir una prestació adequada, segura i alineada amb els objectius operatius del **CROC** i de l'**OSAP**.

Els recursos humans que es posin a disposició en cada contracte basat hauran de respondre estrictament a les especificacions de perfils de l'**apartat 9 Equip de treball**, i hauran de demostrar tant **competències tècniques especialitzades** com **habilitats interpersonals** suficients per treballar en entorns d'alta exigència, col·laboració interinstitucional i elevada confidencialitat.

A títol orientatiu, el personal haurà de demostrar:

- Professionalitat, responsabilitat i compromís amb la qualitat del servei.
- Habilitats comunicatives, capacitat d'explicar conceptes tècnics i aptitud per a la negociació.

- Capacitat de treball col·laboratiu i coordinació amb equips diversos de les entitats adherides.
- Aptitud analítica per a la diagnosi, priorització i resolució eficient de problemes.
- Capacitat de treball sota pressió i en contextos crítics de servei o ciberincidents.
- Domini funcional del català, castellà i anglès, tant oral com escrit.
- Coneixement sòlid en gestió de riscos, seguretat de la informació, operacions de ciberresiliència i compliment normatiu (ENS, NIS2, ISO 27001, guies CCN).

Els licitadors hauran d'incloure en la seva oferta **un organigrama funcional orientatiu**, que descrigui la seva estructura de prestació en el marc de l'Acord Marc i que detalli:

- La capacitat organitzativa disponible per donar cobertura a qualsevol contracte basat.
- Les línies de dependència i responsabilitats operatives.
- La relació prevista amb els equips tècnics i de direcció de les entitats contractants.

Aquest organigrama tindrà caràcter **no vinculant**, però haurà de demostrar que l'adjudicatari disposa d'un model organitzatiu **àgil, escalable i transparent**, apte per satisfer els objectius i necessitats de qualsevol contracte basat.

Les entitats contractants podran sol·licitar, de manera motivada, la **substitució d'un recurs** adscrit a un contracte basat quan concorrin els supòsits següents:

- Incompliment dels requisits mínims exigits pel perfil.
- Detecció d'incidències reiterades en la qualitat del servei o actituds contràries al bon funcionament dels equips.
- Desajust entre les necessitats del contracte i les competències o disponibilitat del recurs.

La substitució haurà de fer-se efectiva en un **termini màxim de 15 dies naturals** des de la notificació formal, garantint la continuïtat del servei sense afectacions. Igualment, l'adjudicatari haurà de presentar, en un **termini màxim de 10 dies naturals**, un **pla d'acció correctiu** que expliqui les mesures previstes per corregir les causes que han motivat la substitució i evitar-ne la reiteració.

10.5 Horari de la prestació del servei

L'adjudicatari haurà de prestar els serveis definits en aquest Acord Marc de **dilluns a divendres**, en **horari laborable comprès entre les 8:00 h i les 18:00 h**, excepte en aquells casos en què s'estableixi un horari específic dins del contracte basat corresponent.

L'horari establert podrà ser modificat per les entitats contractants per adaptar-se a **necessitats operatives, de suport o de gestió de riscos**, sempre que aquestes modificacions siguin degudament notificades i coordinades mitjançant el procés formal de **gestió del canvi.**

Cobertura obligatòria

L'adjudicatari haurà de garantir la **cobertura contínua dels serveis**, incloent substitucions en cas de vacances, baixa per malaltia o absències justificades dels membres de l'equip. Aquestes substitucions hauran de preveure un període de transició mínim d'una setmana, per assegurar la **transferència de coneixement i la continuïtat del servei.**

L'incompliment d'aquesta cobertura es considerarà una **falta lleu** per cada setmana en què no es cobreixi adequadament el rol afectat.

Serveis fora d'horari habitual

En situacions excepcionals o prèviament planificades, es podrà requerir la prestació de serveis fora de l'horari indicat. Aquestes situacions inclouen, entre d'altres:

- Emergències de seguretat o situacions de **risc operatiu o reputacional greu.**
- Projectes crítics amb terminis inajornables o imposats per tercers.
- Actuacions preventives o correctives que impliquin afectació sobre **serveis municipals crítics**, i que s'executin fora d'horari per minimitzar impactes.
- Activitats de suport funcional o tècnic durant **operacions especials del CROC o de l'OSAP.**
- Gestió d'incidències o alertes amb **alt impacte o gravetat elevada.**

La prestació d'aquests serveis fora d'horari **no comportarà cap cost addicional** respecte al preu adjudicat del contracte basat i es considerarà **inclosa dins l'àmbit de cobertura habitual del servei.**

10.6 Eines i equipament personal per a la prestació del servei

Quan el personal de l'adjudicatari presti serveis **presencialment** en les instal·lacions de les entitats contractants, aquestes proporcionaran:

- Espai físic adequat per al desenvolupament de les tasques assignades.
- Accés a la infraestructura corporativa (servidors, eines corporatives, xarxa de comunicacions i entorns d'anàlisi) necessària per a la prestació del servei.
- Accés restringit a Internet mitjançant la xarxa local, limitat als llocs de treball que ho requereixin i als dominis essencials per a l'execució de les tasques.

En cap cas les entitats contractants proporcionaran:

- Ordinadors de sobretaula amb sistema operatiu i programari d'ofimàtica.
- Ordinadors portàtils, tauletes o altres dispositius personals.
- Línies de telefonia mòbil ni terminals associats.
- Accés a Internet via xarxa mòbil (3G/4G/5G).
- Altres recursos no especificats explícitament.

Responsabilitats de l'adjudicatari

L'empresa adjudicatària serà responsable de:

- **Subministrar tot el maquinari, programari, llicències i serveis necessaris** per a l'execució del servei durant la vigència del contracte, incloent-hi el manteniment i la substitució.
  Aquests recursos seran d'ús exclusiu per a la prestació dels serveis derivats de l'Acord Marc del **CROC i de l'OSAP**.
- **Acceptar i complir les polítiques de seguretat de la informació i de gestió de riscos** definides per les entitats contractants.
- Permetre que els dispositius siguin administrats, maquetats, supervisats i esborrats per l'equip tècnic que designi l'entitat corresponent, quan es requereixi per garantir la seguretat o la integritat de la informació.
- Assegurar que, un cop finalitzada la prestació del servei, es realitzi l'esborrat complet de la informació i configuració dels dispositius utilitzats, d'acord amb les instruccions dels serveis tècnics o de seguretat.
- **Garantir la separació d'entorns**, de manera que els dispositius utilitzats per a serveis de governança, anàlisi o gestió de riscos estiguin degudament aïllats dels entorns d'operació o monitoratge per mantenir la integritat i la confidencialitat de la informació.

Homogeneïtat d'equipament i adaptació tecnològica

L'adjudicatari haurà de presentar una **proposta homogènia de maquinari, programari i accessoris** que cobreixi les necessitats dels perfils involucrats, amb l'objectiu de garantir compatibilitat amb els sistemes de maquetat i optimitzar el servei de suport tècnic i d'operacions.
A més, caldrà adaptar-se als **processos de millora contínua i transformació tecnològica** de les entitats contractants, considerant les condicions següents:

- L'entitat podrà determinar la incorporació de noves eines, tecnologies o l'evolució de les ja existents, així com la seva forma d'implantació.
- L'adjudicatari haurà de participar de manera activa en la **planificació i execució dels projectes de transició tecnològica**, tant en l'àmbit de gestió de riscos com en el d'operacions de seguretat.
- No es reconeixerà cap cost addicional per l'adaptació dels recursos humans ni per la incorporació de noves eines tecnològiques necessàries per al servei.
- Els equips i eines utilitzats hauran d'estar **alineats amb les polítiques corporatives de seguretat, continuïtat i protecció de la informació** de l'Ajuntament i de les entitats adherides.

10.7 Seguretat Corporativa

Tant l'empresa adjudicatària com el personal de l'adjudicatari s'hauran de sotmetre a les polítiques i regulacions internes que estableix la Direcció de Seguretat Corporativa en matèria de seguretat de la informació, com a mínim i no limitant-se a:

- Permetre i facilitar la realització d'auditories de compliment de les normatives establertes pel Departament de Seguretat, internes o externes, sobre els sistemes d'informació vinculats a la prestació del servei, i garantir la possibilitat de traçabilitat de les accions fetes per l'auditor per facilitar el seguiment d'aquestes i els seus possibles impactes no desitjats.
- Facilitar l'accés en qualsevol moment als equips i mitjans tècnics emprats pel personal de l'adjudicatari en les oficines de les entitats contractants (sigui o no per l'exercici de la seva funció).
- Acceptar les normes i polítiques que estableix la Direcció de Seguretat tant en el moment de la seva incorporació com després de cada canvi important de les polítiques, normes o regulacions.

- Permetre l'administració i gestió dels equips i mitjans tècnics emprats per l'exercici de les seves funcions per part de l'equip que designin les entitats contractants per fer el desplegament de polítiques i controls de seguretat, actualització d'eines i manteniment d'aplicacions autoritzades i permisos d'accés a la informació.
- La custòdia per part de les entitats contractants dels equips, així com la informació resident d'aquests.
- Donar compliment a totes les normes, polítiques i marcs reguladors vigents durant el període del contracte (LOPDGDD i LSSI).
- A la finalització del contracte, l'adjudicatari quedarà obligat a l'entrega o destrucció en cas de ser sol·licitada, de qualsevol informació obtinguda o generada a conseqüència de la prestació del servei.

10.8 Pla de formació a usuaris de la plataforma

Els licitadors hauran d'incloure en la seva proposta un **Pla de Formació i Transferència de Coneixement** complet i detallat que asseguri la **capacitat operativa, la gestió del risc i la ciberresiliència** de tots els col·lectius implicats en la utilització, supervisió i operació dels serveis del **CROC (Centre de Riscos i Operacions de Ciberresiliència)** i de l'**OSAP (Operacions de Seguretat i Anàlisi de Protecció)**.

Aquest pla serà clau per garantir una **adopció adequada dels serveis**, una **explotació funcional i tècnica eficient** i una **governança municipal madura i sostenible** en matèria de seguretat i gestió de riscos.

Contingut mínim del Pla de Formació
El Pla de Formació haurà d'incloure com a mínim:

- **Metodologia de formació**, incloent formats, enfocaments pedagògics, sistemes d'avaluació i mecanismes de seguiment de la transferència de coneixement.
- **Calendari i planificació** de les sessions, adaptat a les diferents fases de desplegament i als col·lectius afectats.
- **Continguts formatius**, que inclouran:
    - Manuals d'usuari i guies funcionals dels serveis i eines del CROC i de l'OSAP.
    - Accés a entorns de prova o simulació per a sessions pràctiques i casos reals d'anàlisi.
    - Documentació estructurada de processos, procediments i fluxos operatius.
    - Base de coneixement corporativa, accessible via plataforma digital o entorn LMS, amb recursos disponibles en accés continu.

Abast de la formació

El pla haurà de contemplar, com a mínim, la formació per als àmbits següents:

- **Serveis CROC:** gestió de riscos, governança, compliment normatiu, anàlisi d'indicadors de seguretat i processos de millora contínua.
- **Serveis OSAP:** operacions de seguretat, monitoratge, resposta a incidents, administració d'eines de protecció i supervisió de serveis crítics.
- **Paquets de desplegament i suport postprojecte**, amb sessions específiques per a usuaris funcionals, equips tècnics, analistes i responsables de seguretat o resiliència.

Requisits específics de la formació

- **Formació preferentment virtual**, utilitzant eines corporatives de videoconferència compatibles amb els entorns municipals del CROC–OSAP.
- **Grups reduïts** (idealment entre 10 i 15 participants) per garantir la interacció i l'assimilació del coneixement.
- **Sessions teòrico-pràctiques**, orientades a casos d'ús reals i a l'aplicació pràctica de procediments de seguretat, risc i resposta.
- **Formació segmentada per col·lectius**, incloent:
  - Usuaris funcionals i administratius.
  - Personal tècnic i equips d'operació.
  - Responsables de seguretat, de compliment i de gestió de riscos.
- **Formació específica** sobre fluxos operatius, funcionalitats crítiques i **procediments de resposta i comunicació davant incidents o situacions de risc operatiu.**

Tot el material formatiu utilitzat durant les sessions serà **lliurat a l'entitat contractant en finalitzar la formació**, en **format digital i editable**, per a la seva **reutilització, actualització i difusió interna** dins del marc del CROC–OSAP i de les polítiques municipals de ciberresiliència.

10.9 Pla de Qualitat

L'adjudicatari haurà de definir i documentar, durant el primer mes de la vigència del contracte, segons els punts que s'indiquen a continuació, un Pla de Qualitat específic que asseguri la qualitat dels serveis oferts.

El Pla de Qualitat inclourà tots els requisits definits en el present plec per part de BIT.

BIT serà responsable de la implantació, seguiment i compliment dels estàndards de qualitat que contempla el present contracte. Per tal d'assegurar aquest compliment, els licitadors s'hauran de comprometre a contractar una auditoria interna amb periodicitat biennal per tal d'auditar que tots els procediments contemplats dins la norma ISO20000 i la certificació ITIL v3 són vigents i s'implanten d'acord amb els estàndards.

Els punts que s'indiquen a continuació seran els índexs que, com a mínim, ha d'emplenar l'adjudicatari:

- Cicle de Vida d'un servei:
    - Checkpoints.
    - Rols responsables de cada tasca o activitat.
- Gestió de la Configuració: Assegura que els canvis no afecten els nivells de qualitat del servei.
- Resolució dels problemes relatius a la gestió del servei.
- Control de la documentació:
    - Procediments que assegurin que la documentació s'ha actualitzat d'acord amb els canvis o peticions realitzades al llarg del cicle de vida del servei.
- Gestió de la documentació i dels requeriments del servei.
- Regles i procediments que garanteixin la millora contínua del servei.
- Planificació de les auditories internes que asseguren l'adequada documentació dels resultats i accions dutes a terme.
- Mètriques i indicadors.
- Pla de validació de la qualitat.
- Gestió de les responsabilitats relatives a l'actualització del Pla de Qualitat.
- Gestió de riscos que possibiliti una reducció o eliminació dels possibles impactes en el servei.
- Plans de continuïtat del servei que garanteixin que el servei podrà ser restaurat en cas de produir incidències en el mateix.
- Pla de formació que cobreixi les necessitats dels rols implicats en el servei.

Els rols responsables de l'execució de les activitats detallades en el Pla de Qualitat, l'Assegurament de la Qualitat i Auditories internes han d'estar reflectits en l'apartat corresponent a recursos.

Els licitadors han de presentar aquest Pla de Qualitat en el conjunt de documentació tècnica que es detalla al punt "Proposta Tècnica", amb el detall suficient que permeti la valoració de la seva viabilitat, coherència, realisme, estructura organitzativa.

10.10 Qualitat del servei i treballs realitzats

L'empresa adjudicatària haurà de definir, documentar i mantenir un **Pla de Qualitat específic** per a la prestació dels serveis, que asseguri el compliment dels requisits de qualitat establerts en aquest plec i garanteixi la millora contínua dels serveis prestats.

Aquest **Pla de Qualitat s'haurà de lliurar durant el primer mes d'execució de cada contracte basat**, i haurà de ser aprovat per l'òrgan responsable del contracte. El pla haurà d'aplicar-se a tots els serveis inclosos dins dels diferents paquets funcionals contractats, ja siguin pilots, ampliacions o suport postprojecte.

L'òrgan gestor del contracte o del present Acord Marc vetllarà per l'adequació, desplegament i seguiment dels estàndards de qualitat. Per garantir aquest compromís, l'adjudicatari es compromet a contractar una **auditoria interna biennal**, a càrrec seu, que avali el desplegament efectiu dels processos i controls, basant-se en estàndards reconeguts com **ISO 20000 i el marc de bones pràctiques ITIL v4**.

El Pla de Qualitat haurà d'incloure, com a mínim, els següents elements:

- **Cicle de vida del servei**:
  - Fites i checkpoints clau.
  - Assignació clara de rols i responsabilitats per cada fase.
- **Gestió de la configuració**: mecanismes per assegurar que els canvis no comprometen la qualitat del servei.
- **Resolució de problemes**: procediments per a la detecció, anàlisi i resolució eficient de problemes recurrents.
- **Control i actualització de la documentació**: sistemes per assegurar la traçabilitat, actualització i validesa dels documents tècnics i operatius.
- **Gestió de requisits**: sistemes per capturar, validar i integrar canvis o requisits addicionals al servei.
- **Millora contínua**: regles i processos orientats a optimitzar constantment la prestació dels serveis.
- **Auditories internes**: planificació, execució i documentació de les auditories periòdiques.
- **Mètriques i indicadors clau** (KPI): definició dels indicadors que permetin monitorar l'eficiència, qualitat i rendiment del servei.
- **Pla de validació de la qualitat**: procediments per validar si el servei s'ajusta als requisits establerts.
- **Gestió de responsabilitats**: identificació dels rols responsables de cada activitat del pla.
- **Gestió de riscos**: mesures preventives i correctives per minimitzar l'impacte de possibles incidències en la prestació del servei.

- **Pla de continuïtat del servei**: definició d'escenaris de contingència i restauració del servei.
- **Pla de formació**: programes formatius per garantir que tots els perfils implicats en l'execució del servei tenen els coneixements actualitzats i adequats.

Els **rols responsables de la implementació i seguiment del Pla de Qualitat** (incloent assegurament de la qualitat i auditories) hauran d'estar identificats en l'apartat corresponent a l'equip de treball proposat (veure apartat 7).
Els licitadors hauran d'incloure el Pla de Qualitat com a part de la **Proposta Tècnica**, amb el grau de detall necessari per a la seva avaluació, valorant especialment la seva viabilitat, coherència, realisme i adaptació a l'entorn municipal.

10.10.1 Auditories

10.10.1.1 Introducció

BIT en funció del desenvolupament del contracte pot exigir la realització, sense càrrec per les entitats contractants, d'auditories sobre el conjunt del seu treball des de la vessant de qualitat.

L'auditoria en cas que s'exigeixi ha de complir els següents requisits:

- Periodicitat: semestral
- Abast: totalitat del servei
- Serveis a auditar: compliment del contracte amb la qualitat desitjada.
- Equip: Empresa externa i independent.
- Resultat: informe d'auditoria.

10.10.1.2 Objectiu de les Auditories

L'objectiu de les Auditories i Revisions de Qualitat dels Serveis Contractats és proporcionar visibilitat i control a la Direcció de les entitats contractants, sobre el grau de compliment dels adjudicataris amb els aspectes formals del servei.

Els aspectes més rellevants a verificar des del punt de vista d'Auditoria són:

- Verificació del compliment del Pla de Qualitat de Servei, de les condicions contractuals i dels procediments de treball establerts.
- Pla de Qualitat del Servei: fent especial èmfasi en els mecanismes d'assegurament de la qualitat proposats per l'adjudicatari per a les seves pròpies activitats (controls, revisions, proves, auditories internes de l'adjudicatari, etc.).

- Condicions contractuals: verificant, entre altres aspectes, el compliment dels requisits d'infraestructura (entorns, eines, comunicacions, etc.), requisits de personal i requisits de seguretat inclosos en el contracte.
- Procediments de treball: verificant el compliment del Model Operatiu i els procediments definits per a la prestació del servei (activitats, i lliurables).

Els aspectes més rellevants a verificar des del punt de vista d'una revisió són:

- Revisió del compliment i execució del Pla d'Acció proposat per a la seva esmena.

10.10.1.3 Procediment d'Auditoria

L'adjudicatari cooperarà en l'auditoria, responent immediatament a les informacions demanades per a l'execució d'aquesta, i auxiliant als auditors en el que considerin necessari.

Tota informació addicional o canvis de conducció d'un procés o com a resultat d'auditoria, serà considerada informació confidencial, segons els termes i condicions del Contracte.

La realització de l'auditoria en cap moment no eximirà l'adjudicatari del compliment dels compromisos derivats de la prestació dels serveis d'acord amb els termes inclosos en aquest Plec.

Els costos dels mitjans emprats per l'adjudicatari associats a les auditories no podran ser repercutits en cap cas a les entitats contractants.

10.10.1.4 Resultats de l'Auditoria

L'auditoria es realitzarà mitjançant revisions dels diferents aspectes que es contemplen en aquest plec, en el pla de qualitat del servei, formació, model de prestació del servei, així com qualsevol altre pla detallat en aquest plec. L'equip auditor buscarà la conformitat amb els aspectes establerts en aquests documents. Per a cada aspecte revisat existiran quatre possibles valoracions:

- Conformitat: si es compleix completament amb el que indica aquests documents.
- No Conformitat Major: si hi ha evidències d'incompliment de requisits relacionats amb la metodologia o els models de governança que incideixen directament en la prestació del servei (Documentació i Lliurables, Gestió de la Configuració, Traçabilitat, Gestió de Riscos i Problemes, Seguretat Físic-Lògica, etc.)

- No Conformitat Menor: si hi ha evidències d'incompliment de requisits no relacionats amb la metodologia o els models de governança i els procediments vigents en el moment d'execució de l'auditoria relatius als serveis d'aquest plec que incideixin directament en la qualitat del servei (organigrama, Responsabilitats, Rols, pla de recursos, Temes Laborals i Subcontractacions, Certificacions, Acords de Confidencialitat, Auditories internes de l'adjudicatari, comunicacions, etc.)
- Observació: addicionalment, s'inclouran com "observació" aquells fets identificats que afectin o puguin afectar, segons el parer de l'equip auditor, a la qualitat del servei, però que no suposin un incompliment formal dels compromisos establerts. Les observacions identificades en un informe d'Auditoria podrien derivar a No Conformitats en futures auditories si no s'esmenen.
- A la finalització de l'auditoria les parts revisaran les desviacions i/o observacions detectades respecte a l'acordat en el contracte. L'adjudicatari haurà d'establir un pla d'acció amb:
- Accions per assegurar que les desviacions i / o observacions detectades es corregeixin.
- Identificació de responsables i dates límit per l'execució de les accions.
- L'adjudicatari haurà de presentar a les entitats contractants el pla d'acció en el termini d'un mes des de la comunicació dels resultats finals de l'auditoria. Serà responsabilitat de l'adjudicatari la realització de les accions en els terminis establertes en el pla d'acció.

10.10.1.5 Resultats de la Revisió

Alternativament a les auditories completes, les entitats contractants podran realitzar una revisió de l'execució del pla d'acció proposat després dels resultats de l'auditoria del període anterior.

El mètode consistirà en la revisió del pla d'acció de cadascuna de les No Conformitats detectades i també es revisaran algunes de les observacions.

S'avaluarà amb una valoració entre 0 i 5 l'estat de l'acció corresponent, si l'acció s'obté un valor de 3 o més, es donarà com a vàlid el pla d'acció i per tant "tancada la No Conformitat".

10.11 Gestió de la documentació

El Servei, dins el marc de treball, posarà a disposició tots els documents de treball i consulta a través d'eines de treball col·laboratiu. Igualment s'haurà de traslladar aquesta documentació als diferents departaments de les entitats contractants que la puguin sol·licitar. Durant els

primers tres mesos de l'execució del contracte l'adjudicatari haurà de presentar una proposta al respecte.

10.12 Garantia dels treballs a la contractació basada

Ateses les característiques de l'objecte i abast dels treballs a realitzar per les empreses homologades, no s'estableix cap període de garantia un cop finalitzades les tasques establertes a la contractació basada.

11. Acords de Nivell de Servei (ANS) dels contractes basats

Per a la gestió i seguiment dels serveis prestats per l'adjudicatari dels contractes basats d'aquest acord marc, es defineixen una sèrie d'Acords de Nivell de Servei (ANS). Aquests permeten monitoritzar i avaluar la qualitat i la gestió dels serveis a través d'indicadors que parametritzen el grau de consecució acordat per a cada servei. El proveïdor adjudicatari serà responsable de portar el seguiment dels SLA i recollir la informació.

BIT o l'organisme contractant que correspongui es reserva el dret de determinar la forma en què el reporting d'ANS es dugui a terme tot buscant la millora en la gestió agregada de tots els contractes normalitzant la forma de recollir aquesta informació.

Els indicadors tindran la següent estructura en comú:

- Codi i Indicador: Codi i nom del propi indicador
- Descripció: definició de l'indicador i objecte de mesura.
- Càlcul: fórmula per al càlcul de l'indicador.
- Objectiu: llindar a partir del qual l'indicador compleix amb el nivell de servei acordat. Aquest valor s'indicarà específicament en cada un dels contractes en funció de les necessitats.
- Periodicitat: Període de temps pel càlcul de l'indicador.
- Penalització: Percentatge a descomptar de la factura mensual del servei en cas d'incompliment de l'ANS, amb el límit màxim del 10% del preu del contracte per a cada penalitat, i del 50% del preu del contracte en el seu conjunt, ambdós IVA exclòs.

El compliment dels ANS ha de ser revisat de manera mensual. En el Comitè de Seguiment s'haurà de realitzar una presentació de l'estat de compliment dels ANS, així com de les desviacions ocorregudes.

Els ANS es divideixen en dues tipologies:

- ANS per a la gestió del contracte prestat per l'adjudicatari. Fan referència a la gestió global del contracte.
- ANS de qualitat operativa dels serveis prestats per l'adjudicatari, que permeten mesurar la qualitat operativa del servei realitzat i la seva evolució en el temps.

Es mostren en els següents apartats els diferents ANS amb la seva descripció i mètode de càlcul als quals estaran sotmesos els contractes basats de l'agrupació corresponent. En cada un dels

contractes basats, en funció de les necessitats, s'especificaran els ANS aplicables al contracte amb la periodicitat i valor límit corresponent. En cas que una mateixa desviació afecti a l'incompliment de més d'un ANS, s'aplicarà l'ANS més restrictiu, en cap cas més d'un.

La imposició de penalitats serà acumulativa, no excloent i proporcional a l'import dels serveis afectats. Les penalitats s'aplicaran a la factura corresponent al trimestre on s'hagi produït l'incompliment dels ANS, o bé a les següents factures en cas que no hagi estat possible fer-lo a l'anterior. En aquest darrer cas, el càlcul de les penalitats es farà sobre la factura del mes en que s'hagi produït l'incompliment. Les penalitats relatives als incompliments produïts al darrer període de servei s'aplicaran sobre la darrera factura i, en cas que sigui insuficient, sobre la garantia depositada per l'adjudicatari.

11.1 ANS per a la gestió del contracte

En aquest grup d'ANS es defineixen els indicadors que apliquen a la gestió del contracte de forma genèrica principalment en el referent a la gestió de recursos humans.

De forma genérica, es defineixen els principals indicadors amb la seva fórmula de càlcul que apliquen:

- **Temps de reacció davant esdeveniment**: Es defineix el temps de reacció davant esdeveniment com el temps transcorregut des del moment en què en que es produeix l'esdeveniment, fins que queda es dona resposta al mateix.

  Els indicadors associats son:

Codi	Indicador ANS	Descripció	Càlcul	Objectiu	Periodicitat
GC_T.SUB	Temps de substitució d'un treballador adscrit al servei.	Dies que transcorren entre la comunicació (T_{Comun}) d'una substitució i la sortida del treballador ($T_{TecBaixa}$).	$T_{TecBaixa}$ - T_{Comun}	GC_T.SUB >= 10 dies laborables	Puntual
GC_T.SOL	Temps de solapament de treballadors quan es produeix una substitució d'un treballador adscrit al servei	Dies que treballen de forma conjunta el treballador que marxa i el de nova incorporació, on $T_{TecBaixa}$ és el darrer dia de treball del treballador que marxa, i T_{TecNou} és el primer dia de treball del nou treballador.	$T_{TecBaixa}$ - T_{TecNou}	GC_T.SOL > 15 dies	Puntual

GC_T.BAI	Temps de substitució d'una baixa imprevista d'un treballador adscrit al servei	Dies que transcorren des què es produeix una baixa imprevista i es substitueix, on $T_{TecBaixa}$ és el dia de la baixa imprevista, i T_{TecNou} és el primer dia de treball del nou treballador.	T_{TecNou} - $T_{TecBaixa}$	GC_T.BAI < 7 dies	Puntual
GC_T.IMP	Temps d'implantació d'un paquet de servei	Dies que transcorren entre la comunicació d'una sol·licitud d'implantació d'un paquet de servei (T_{ImpReq}) i la seva implantació efectiva ($T_{Implanta}$)	$T_{Implanta}$ - T_{ImpReq}	GC_T.IMP < 90 dies	Puntual
GC_T.AMP	Temps d'ampliació d'un paquet de servei	Dies que transcorren entre la comunicació d'una sol·licitud d'ampliació d'un paquet de servei (T_{AmpReq}) i la seva ampliació efectiva (T_{Amplia})	T_{Amplia} - T_{AmpReq}	GC_T.AMP < 30 dies	Puntual

11.2 ANS de qualitat operativa

En aquest grup d'ANS es defineixen els indicadors que apliquen a la qualitat operativa dels serveis prestats. Es dividiran en ANS transversals d'aplicació a tots els lots i ANS específics d'aplicació en el lot corresponent.

Es detallen a continuació els tipus de tasques i les definicions de les actuacions que poden ser objecte del servei (seguint el model ITIL):

- **Peticions de servei**: és una petició formal d'un usuari per a obtenir informació, assessorament, accés a un recurs, o un canvi estàndard dins del present lot.
- **Peticions de canvi**: és la proposta formal i documentada per a implementar un canvi no estàndard en un servei o infraestructura de TIC.
- **Incidències**: és la tasca que es genera quan es produeix una interrupció no planificada o reducció en la qualitat d'un servei de TIC, l'objectiu de gestió del qual és restaurar l'operativitat normal al més aviat possible per a minimitzar l'impacte en el negoci.
- **Incidents de seguretat**: és la tasca que es genera quan hi hagi indicacions d'una possible o potencial bretxa en la seguretat dels sistemes d'informació objecte de protecció del present lot, afectant la disponibilitat, traçabilitat, confidencialitat, disponibilitat o autenticitat dels sistemes d'informació.

- **Problemes**: és la tasca que es genera dins per tractar d'identificar les causes arrel que generen incidències, minimitzar l'impacte d'incidents inevitables i prevenir futurs incidents

La prioritat dels diferents tipus d'actuacions objecte del servei (incidències, peticions, etc) es calcularà en base a l'impacte i la urgència.

L'impacte mesura l'afectació al servei, al negoci o a la ciutadania en funció de l'abast, la criticitat, el nombre de persones usuàries afectades i l'impacte operatiu, legal i reputacional.

Nivell	Impacte: Descripció breu
Baix	Afectació **limitada i local**. No impacta serveis crítics ni a la ciutadania. Pot afectar usuaris puntuals o tasques internes amb alternatives temporals.
Mitjà	Afectació **rellevant però controlable**. Impacta un servei no crític o un servei crític de manera parcial. Pot afectar diversos usuaris o generar retard operatiu.
Alt	Afectació **greu o generalitzada**. Impacta serveis crítics, ciutadania, compliment normatiu, seguretat de la informació o la continuïtat del servei. Requereix comunicació i escalat immediat.

La urgència mesura la rapidesa amb que cal actuar per evitar que l'impacte sigui més gran o per complir compromisos (ANS).

Nivell	Urgència: Descripció breu
Baixa	L'actuació **pot esperar** sense que l'impacte empitjori. No hi ha risc immediat ni dependències crítiques de temps.
Mitjana	L'actuació s'ha de fer en **termini raonable**. Un retard pot augmentar l'impacte o afectar compromisos operatius o ANS.
Alta (Urgent)	Cal actuar **de manera immediata**. Un retard incrementa clarament l'impacte, el risc de propagació (en seguretat) o el dany al servei.

A partir de la combinació d'ambdós criteris es deriva la prioritat, detallada a la següent taula, que marcarà el temps màxim de resposta i de resolució.

Prioritat		Impacte		
		Alt	Mig	Baix
Urgència	Alta	1	2	3
	Mitjana	2	3	4
	Baixa	3	4	5

Prioritat:

1. Crítica
2. Molt Alta
3. Alta
4. Mitjana

5. Baixa

11.2.1 ANS de qualitat operativa transversals

A continuació es detallen els acords de nivell de servei exigits amb caràcter general per a tots els lots.

De forma generica, es defineixen els principals indicadors amb la seva formula de càlcul que apliquen en cada lot:

- **Disponibilitat**: Es defineix la disponibilitat com el percentatge de temps en el que el servei es troba plenament operatiu ($T_{Operatiu}$) en relació al temps total (T_{Total}).

  L'indicador associat és el següent i es defineixen els següents objectius per a cada servei:

Codi	Indicador ANS	Descripció	Càlcul	Objectiu	Periodicitat
%.DISP	Disponibilitat mínima del servei	Percentatge de temps que el servei és operatiu ($T_{Operatiu}$) respecte del temps de servei total (T_{Total}).	$T_{Operatiu}$ / T_{Total}	%.DISP >= 99,9%	Trimestral

- **Temps de recuperació en desastre**: Es defineix el temps de recuperació en desastre com la durada màxima acceptable que una aplicació, sistema o procés pot estar fora de servei després d'un incident sense causar danys significatius. El límit s'estableix en el DRP (Disaster Recovery Plan)

  El indicador associat es:

Codi	Indicador ANS	Descripció	Càlcul	Objectiu	Periodicitat
T.RTO	Temps de recuperació del servei en cas de desastre	Temps màxim per assolir com a mínim el 50% del servei ($T_{Recupera}$) a partir del moment del desastre (T_{Zero})	$T_{Recupera}$ - T_{Zero}	T.RTO < 2h	Puntual

- **Monitoratge de la capacitat dels equipaments**: Dins del monitoratge realitzat per l'empresa adjudicatària s'hauran de notificar quan la capacitat dels equipaments i infraestructura superi determinats llindars:

  El indicador associat es:

Codi	Indicador ANS	Descripció	Càlcul	Objectiu	Periodicitat
%.CAPA	Percentatge d'alertes de superació de capacitat notificades en termini	Percentatge d'alertes de superació de llindars de capacitat notificats abans de 60 minuts (N_{MonOK}) respecte del número total d'alertes de capacitat (N_{MonTot})	N_{MonOK} / N_{MonTot}	%.CAPA > 99,9%	Trimestral

- **Temps d'atenció**: Es defineix el temps d'atenció com el temps transcorregut des del moment en què una incidència o petició és notificada a l'equip del servei, utilitzant el procediment establert, fins que queda constància que la incidència o petició està sent atesa per l'equip del servei.

  Els indicadors associats son:

Codi	Indicador ANS	Descripció	Càlcul	Objectiu	Periodicitat
T.ATNP 1	Temps d'atenció de prioritat 1	Temps que transcorre des què es notifica la incidència o petició de prioritat 1 ($T_{NotificaP1}$) fins que es rep resposta i és atesa ($T_{AtencioP1}$)	$T_{AtencioP1}$ - $T_{NotificaP1}$	T.ATNP1 < 15 min	Puntual
T.ATNP 2	Temps d'atenció de prioritat 2	Temps que transcorre des què es notifica la incidència o petició de prioritat 2 ($T_{NotificaP2}$) fins que es rep resposta i és atesa ($T_{AtencioP2}$)	$T_{AtencioP2}$ - $T_{NotificaP2}$	T.ATNP2 < 30 min	Puntual
T.ATNP 3	Temps d'atenció de prioritat 3	Temps que transcorre des què es notifica la incidència o petició de prioritat 3 ($T_{NotificaP3}$) fins que es rep resposta i és atesa ($T_{AtencioP3}$)	$T_{AtencioP3}$ - $T_{NotificaP3}$	T.ATNP2 < 60 min	
T.ATNP 4	Temps d'atenció de prioritat 4	Temps que transcorre des què es notifica la incidència o petició de prioritat 4 ($T_{NotificaP4}$) fins que es rep resposta i és atesa ($T_{AtencioP4}$)	$T_{AtencioP4}$ - $T_{NotificaP4}$	T.ATNP2 < 90 min	
T.ATNP 5	Temps d'atenció de prioritat 5	Temps que transcorre des què es notifica la incidència o petició de prioritat 5 ($T_{NotificaP5}$) fins que es rep resposta i és atesa ($T_{AtencioP5}$)	$T_{AtencioP5}$ - $T_{NotificaP5}$	T.ATNP2 < 120 min	

%.ATNP 1	Percentatge d'atenció de prioritat 1	Percentatge de incidències i peticions de prioritat 1 ateses dins de termini ($N_{AtenOKP1}$) respecte del total d'atencions de prioritat 1 ($N_{AtenTotP1}$)	$N_{AtenOKP1}$ / $N_{AtenTotP1}$	%.ATNP1 > 99,9%	Trimestral
%.ATNP 2	Percentatge d'atenció de prioritat 2	Percentatge de incidències i peticions de prioritat 2 ateses dins de termini ($N_{AtenOKP2}$) respecte del total d'atencions de prioritat 2 ($N_{AtenTotP2}$)	$N_{AtenOKP2}$ / $N_{AtenTotP2}$	%.ATNP2 > 99,9%	Trimestral
%.ATNP 3	Percentatge d'atenció de prioritat 3	Percentatge de incidències i peticions de prioritat 3 ateses dins de termini ($N_{AtenOKP3}$) respecte del total d'atencions de prioritat 3 ($N_{AtenTotP3}$)	$N_{AtenOKP3}$ / $N_{AtenTotP3}$	%.ATNP3 > 99,9%	Trimestral
%.ATNP 4	Percentatge d'atenció de prioritat 4	Percentatge de incidències i peticions de prioritat 4 ateses dins de termini ($N_{AtenOKP4}$) respecte del total d'atencions de prioritat 4 ($N_{AtenTotP4}$)	$N_{AtenOKP4}$ / $N_{AtenTotP4}$	%.ATNP4 > 99,9%	Trimestral
%.ATNP 5	Percentatge d'atenció de prioritat 5	Percentatge de incidències i peticions de prioritat 5 ateses dins de termini ($N_{AtenOKP5}$) respecte del total d'atencions de prioritat 1 ($N_{AtenTotP5}$)	$N_{AtenOKP5}$ / $N_{AtenTotP5}$	%.ATNP5 > 99,9%	Trimestral

- **Temps de resolució:** Es defineix el temps de resolució com el temps transcorregut des del moment en què una incidència o petició és notificada a l'equip del servei, utilitzant el procediment establert, fins que es dona per tancada.
    - Per a aquelles peticions la resolució de les quals depengui de l'aprovació de l'organisme contractant, no computarà com a temps de resolució el temps d'espera fins que l'adjudicatari rebi aquesta aprovació.
    - Quan una incidència hagi de ser escalada a un proveïdor o equip extern a l'adjudicatari, no computarà com a temps de resolució el temps transcorregut des de l'escalat de la incidència fins a la seva devolució per part del proveïdor o equip extern.
    - Per a les peticions en les quals s'especifiqui un termini de resolució diferent, de forma acordada prèviament amb l'organisme contractant, s'aplicarà el termini especificat per a aquestes peticions.
    - L'organisme contractant podrà reobrir incidències i peticions a conseqüència de no haver-se realitzat de manera conforme, i en aquest cas per al temps de resolució de la incidència o petició s'inclourà el temps de resolució de les reobertures.

Els indicadors associats son:

Codi	Indicador ANS	Descripció	Càlcul	Objectiu	Periodicitat
T.RESINCP 1	Temps de resolució d'incidències de prioritat 1	Temps que transcorre des què es notifica la incidència de prioritat 1 ($T_{NotincP1}$) fins que és resolta ($T_{ResincP1}$)	$T_{ResincP1}$ – $T_{NotificaP1}$	T.RESINCP1 < 2h	Puntual
T.RESINCP 2	Temps de resolució d'incidències de prioritat 2	Temps que transcorre des què es notifica la incidència de prioritat 2 ($T_{NotincP2}$) fins que és resolta($T_{ResincP2}$)	$T_{ResincP2}$ - $T_{NotincP2}$	T.RESINCP2 < 4h	Puntual
T.RESINCP 3	Temps de resolució d'incidències de prioritat 3	Temps que transcorre des què es notifica la incidència de prioritat 3 ($T_{NotincP3}$) fins que és resolta($T_{ResincP3}$)	$T_{ResincP3}$ - $T_{NotincP3}$	T.RESINCP3 < 24h	
T.RESINCP 4	Temps de resolució d'incidències de prioritat 4	Temps que transcorre des què es notifica la incidència de prioritat 4 ($T_{NotincP4}$) fins que és resolta($T_{ResincP4}$)	$T_{ResincP4}$ - $T_{NotincP4}$	T.RESINCP4 < 48h	
T.RESINCP 5	Temps de resolució d'incidències de prioritat 5	Temps que transcorre des què es notifica la incidència de prioritat 5 ($T_{NotincP5}$) fins que és resolta($T_{ResincP5}$)	$T_{ResincP5}$ - $T_{NotincP5}$	T.RESINCP5 < 96h	
T.RESPET P1	Temps de resolució de petició de prioritat 1	Temps que transcorre des què es notifica la petició de prioritat 1 ($T_{NotpetP1}$) fins que és resolta($T_{RespetP1}$)	$T_{RespetP1}$ - $T_{NotpetP1}$	T.RESPETP1 < 2h	Puntual
T.RESPET P2	Temps de resolució de petició de prioritat 2	Temps que transcorre des què es notifica la petició de prioritat 2 ($T_{NotpetP2}$) fins que és resolta($T_{RespetP2}$)	$T_{RespetP2}$ - $T_{NotpetP2}$	T.RESPETP2 < 8h	Puntual
T.RESPET P3	Temps de resolució de petició de prioritat 3	Temps que transcorre des què es notifica la petició de prioritat 3 ($T_{NotpetP3}$) fins que és resolta($T_{RespetP3}$)	$T_{RespetP3}$ - $T_{NotpetP3}$	T.RESPETP3 < 48h	
T.RESPET P4	Temps de resolució de petició de prioritat 4	Temps que transcorre des què es notifica la petició de prioritat 4 ($T_{NotpetP4}$) fins que és resolta($T_{RespetP4}$)	$T_{RespetP4}$ - $T_{NotpetP4}$	T.RESPETP4 < 5d	
T.RESPET P5	Temps de resolució de petició de prioritat 5	Temps que transcorre des què es notifica la petició de prioritat 5 ($T_{NotpetP5}$) fins que és resolta($T_{RespetP5}$)	$T_{RespetP5}$ - $T_{NotpetP5}$	T.RESPETP5 < 10d	
%.RESINC P1	Percentatge de resolució	Percentatge d'incidències de prioritat 1 ateses dins de termini ($N_{ResincOKP1}$) respecte del total	$N_{ResincOKP1}$ / $N_{ResincTotP1}$	%.RESINCP1 > 99,9%	Trimestral

	d'incidències de prioritat 1	d'atencions de prioritat 1 ($N_{ResincTotP1}$)			
%.RESINCP2	Percentatge de resolució d'incidències de prioritat 2	Percentatge d'incidències de prioritat 2 ateses dins de termini ($N_{ResincOKP2}$) respecte del total d'atencions de prioritat 2 ($N_{ResincTotP2}$)	$N_{ResincOKP2}$ / $N_{ResincTotP2}$	%.RESINCP2 > 99,9%	Trimestral
%.RESINCP3	Percentatge de resolució d'incidències de prioritat 3	Percentatge d'incidències de prioritat 3 ateses dins de termini ($N_{ResincOKP3}$) respecte del total d'atencions de prioritat 3 ($N_{ResincTotP3}$)	$N_{ResincOKP3}$ / $N_{ResincTotP3}$	%.RESINCP3 > 99,9%	Trimestral
%.RESINCP4	Percentatge de resolució d'incidències de prioritat 4	Percentatge d'incidències de prioritat 4 ateses dins de termini ($N_{ResincOKP4}$) respecte del total d'atencions de prioritat 4 ($N_{ResincTotP4}$)	$N_{ResincOKP4}$ / $N_{ResincTotP4}$	%.RESINCP4 > 99,9%	Trimestral
%.RESINCP5	Percentatge de resolució d'incidències de prioritat 5	Percentatge d'incidències de prioritat 5 ateses dins de termini ($N_{ResincOKP5}$) respecte del total d'atencions de prioritat 1 ($N_{ResincTotP5}$)	$N_{ResincOKP5}$ / $N_{ResincTotP5}$	%.RESINCP5 > 99,9%	Trimestral
%.RESPETP1	Percentatge de resolució de peticions de prioritat 1	Percentatge de peticions de prioritat 1 ateses dins de termini ($N_{RespetOKP1}$) respecte del total d'atencions de prioritat 1 ($N_{RespetTotP1}$)	$N_{RespetOKP1}$ / $N_{RespetTotP1}$	%.RESPETP1 > 99,9%	Trimestral
%.RESPETP2	Percentatge de resolució de peticions de prioritat 2	Percentatge de peticions de prioritat 2 ateses dins de termini ($N_{RespetOKP2}$) respecte del total d'atencions de prioritat 2 ($N_{RespetTotP2}$)	$N_{RespetOKP2}$ / $N_{RespetTotP2}$	%.RESPETP2 > 99,9%	Trimestral
%.RESPETP3	Percentatge de resolució de peticions de prioritat 3	Percentatge de peticions de prioritat 3 ateses dins de termini ($N_{RespetOKP3}$) respecte del total d'atencions de prioritat 3 ($N_{RespetTotP3}$)	$N_{RespetOKP3}$ / $N_{RespetTotP3}$	%.RESPETP3 > 99,9%	Trimestral
%.RESPETP4	Percentatge de resolució de peticions de prioritat 4	Percentatge de peticions de prioritat 4 ateses dins de termini ($N_{RespetOKP4}$) respecte del total d'atencions de prioritat 4 ($N_{RespetTotP4}$)	$N_{RespetOKP4}$ / $N_{RespetTotP4}$	%.RESPETP4 > 99,9%	Trimestral
%.RESPETP5	Percentatge de resolució de peticions de prioritat 5	Percentatge de peticions de prioritat 5 ateses dins de termini ($N_{RespetOKP5}$) respecte del total d'atencions de prioritat 1 ($N_{RespetTotP5}$)	$N_{RespetOKP5}$ / $N_{RespetTotP5}$	%.RESPETP5 > 99,9%	Trimestral
%.REOINC	Percentatge d'incidències reobertes a causa de l'adjudicatari	Percentatge d'incidències resoltes incorrectament per l'adjudicatari i han estat reobertes ($N_{ResincKO}$) respecte el total d'incidències resoltes ($N_{ResincTot}$)	$N_{ResincKO}$ /$N_{ResincTot}$	%.REOINC < 3%	Trimestral

%.REOPET	Percentatge de peticions reobertes a causa de l'adjudicatari	Percentatge de peticions resoltes incorrectament per l'adjudicatari que han estat reobertes ($N_{RespetkO}$) respecte el total de peticions resoltes ($N_{RespetTot}$)	$N_{RespetKO}$ /$N_{RespetTot}$	%.REOPET < 5%	Trimestral

- **Lliurament efectiu de documentació:** Una documentació es considerarà efectivament lliurada quan l'organisme contractant aprovi el seu contingut després de la seva recepció dins del termini acordat entre l'organisme contractant i l'adjudicatari o en els previstos en aquest plec.

  Els indicadors associats son:

Codi	Indicador ANS	Descripció	Càlcul	Objectiu	Periodicitat
T.DOC	Temps de lliurament d'informes	Temps que transcorre des que se sol·licita documentació (T_{Req}) fins al lliurament de la documentació definitiva (T_{Doc}).	T_{Doc} - T_{Req}	T.DOC < 7 d	
%.DOC	Percentatge de lliurament d'informes en termini	Percentatge de documents efectivament lliurats dins de termini (N_{DocOK}), respecte del número total d'informes lliurats ($N_{DocTotal}$)	N_{DocOK} /N_{DocTot}	%.DOC > 99,9%	Trimestral

11.2.2 ANS de qualitat operativa aplicables al lot 1

A continuació es detallen els acords de nivell de servei exigits específicament per al lot 1 – Serveis del Centre de Riscos i Operacions de Ciberresiliència .

En aquest grup d'ANS s'ha establert un criteri de criticitat per als incidents de seguretat, diferenciant:

- Incident de prioritat crítica (P1): quan es confirma que la xarxa es troba sota atac prolongat i/o l'organisme contractant està sent compromès pels atacants i/o es troba sota un atac de virus a gran escala i/o s'ha identificat una bretxa de seguretat a gran escala que impactarà immediatament a la reputació de l'organisme contractant (incloent la fugida de documents confidencials i crítics de l'organisme contractant).
- Incident de prioritat molt alta (P2): quan es confirma un atac actiu i rellevant que afecta serveis o sistemes crítics de l'organisme contractant, amb un impacte operatiu important però encara contingut, i que requereix una intervenció immediata per evitar la seva escalada a un incident de prioritat crítica. Inclou, entre d'altres, atacs en curs

amb afectació parcial a sistemes crítics, compromisos confirmats amb capacitat de contenció, incidents amb alta probabilitat d'impacte reputacional, legal o operatiu a curt termini, o situacions que poden derivar ràpidament en una interrupció greu del servei si no es mitiguen amb urgència.

- Incident de prioritat alta (P3): quan es confirma que la xarxa es troba sota atac continuat i/o múltiples sistemes s'han vist compromesos per un virus i/o s'ha identificat una fuita d'informació que no suposi un impacte immediat a la reputació de l'organisme contractant i/o un atac imminent reportat als mitjans de comunicació contra l'organisme contractant.
- Incident de prioritat mitjana (P4): quan un servidor s'ha vist compromès per malware o compromès per un altre mitjà, s'han exposat unes úniques credencials d'usuari mitjançant malware o hacking i/o algun informe de qualsevol tipus d'amenaça que afecti a l'organisme contractant.
- Incident de prioritat baixa (P5): alerta sense impacte.

Monitoratge i detecció d'incidents de seguretat

Codi	Indicador ANS	Descripció	Càlcul	Objectiu	Periodicitat
L1_T.MONP1	Monitorització i detecció d'incidents de seguretat. Prioritat 1 (Crítica)	Temps entre que s'origina una alerta al sistema SIEM, es processa (verifica i categoritza) com a P1 i es notifica per al seu tractament.	$T_{TractaP1}$ - $T_{DetectaP1}$	L1_T.MONP1 < 5 min	
L1_T.MONP2	Monitorització i detecció d'incidents de seguretat. Prioritat 2 (Molt Alta)	Temps entre que s'origina una alerta al sistema SIEM, es processa (verifica i categoritza) com a P2 i es notifica per al seu tractament.	$T_{TractaP2}$ - $T_{DetectaP2}$	L1_T.MONP2 < 10 min	
L1_T.MONP3	Monitorització i detecció d'incidents de seguretat. Prioritat 3 (Alta)	Temps entre que s'origina una alerta al sistema SIEM, es processa (verifica i categoritza) com a P3 i es notifica per al seu tractament.	$T_{TractaP3}$ - $T_{DetectaP3}$	L1_T.MONP3 < 15 min	
L1_T.MONP4	Monitorització i detecció d'incidents de seguretat. Prioritat 4 (Mitjana)	Temps entre que s'origina una alerta al sistema SIEM, es processa (verifica i categoritza) com a P4 i es notifica per al seu tractament.	$T_{TractaP4}$ - $T_{DetectaP4}$	L1_T.MONP4 < 30 min	
L1_T.MONP5	Monitorització i detecció	Temps entre que s'origina una alerta al sistema SIEM,	$T_{TractaP5}$ - $T_{DetectaP5}$	L1_T.MONP5 < 60 min	

	d'incidents de seguretat. Prioritat 5 (Baixa)	es processa (verifica i categoritza) com a P5 i es notifica per al seu tractament.			
L1_%.MONP1	Percentatge d'alertes de prioritat 1 notificades dins de termini	Percentatge d'alertes de prioritat 1 notificades dins de termini ($N_{MonOKP1}$) respecte del total d'alertes de prioritat 1 ($N_{MonTotP1}$)	$N_{MonOKP1}$ / $N_{MonTotP1}$	L1_%.MONP1 > 99,9%	Trimestral
L1_%.MONP2	Percentatge d'alertes de prioritat 2 notificades dins de termini	Percentatge d'alertes de prioritat 2 notificades dins de termini ($N_{MonOKP2}$) respecte del total d'alertes de prioritat 2 ($N_{MonTotP2}$)	$N_{MonOKP2}$ / $N_{MonTotP2}$	L1_%.MONP2 > 99,9%	Trimestral
L1_%.MONP3	Percentatge d'alertes de prioritat 3 notificades dins de termini	Percentatge d'alertes de prioritat 3 notificades dins de termini ($N_{MonOKP3}$) respecte del total d'alertes de prioritat 3 ($N_{MonTotP3}$)	$N_{MonOKP3}$ / $N_{MonTotP3}$	L1_%.MONP3 > 99,9%	Trimestral
L1_%.MONP4	Percentatge d'alertes de prioritat 4 notificades dins de termini	Percentatge d'alertes de prioritat 4 notificades dins de termini ($N_{MonOKP4}$) respecte del total d'alertes de prioritat 4 ($N_{MonTotP4}$)	$N_{MonOKP4}$ / $N_{MonTotP4}$	L1_%.MONP4 > 99,9%	Trimestral
L1_%.MONP5	Percentatge d'alertes de prioritat 5 notificades dins de termini	Percentatge d'alertes de prioritat 5 notificades dins de termini ($N_{MonOKP5}$) respecte del total d'alertes de prioritat 5 ($N_{MonTotP5}$)	$N_{MonOKP5}$ / $N_{MonTotP5}$	L1_%.MONP5 > 99,9%	Trimestral
L1_%MONKO	Eficiència monitorització i detecció d'incidents de seguretat	Percentatge d'incident crítics reportats directament per personal del client al servei de SOC, sense ser detectats prèviament pel SOC	$N_{IncRepClient}$ /N_{IncTot}	L1_%MONKO < 1%	Trimestral

Informes de servei

Codi	Indicador ANS	Descripció	Càlcul	Objectiu	Periodicitat
L1_T.INF_INC 1	Incident Handling: informe inicial	Temps màxim de lliurament d'informe inicial d'impacte per incidents de prioritat P1, P2 o P3 des de la notificació de l'incident	$T_{InforInici}$ - T_{Notinc}	L1_T.DOC_INC <= 8 h	Puntual
L1_T. INF_INC2	Incident Handling: actualitzacions	Temps màxim transcorregut entre actualitzacions de reports d'investigacions per	$T_{NovaAct}$ - $T_{AnteriorAct}$	L1_T.SO3 < 4 h	Puntual

		incidents de prioritat P1, P2 o P3			
L1_T. INF_INC3	Incident Handling: informe final	Temps màxim de lliurament de l'informe definitiu d'incidents de prioritat P1, P2 o P3 des de la data de tancament de l'incident	$T_{NovaAct}$ - $T_{AnteriorAct}$	L1_T.SO3 < 8 h	Puntual
L1_T.INF_EVI	Incident Handling: informe evidències	Temps màxim d'entrega d'informe d'evidències	$T_{InforEviden}$ - T_{Notinc}	L1_T.DOC_EVI <= 7 d	Puntual

Altres

Codi	Indicador ANS	Descripció	Càlcul	Objectiu	Periodicidad
L1_T.PREV1	Preventiu: Pla de mitigació vulnerabilitat	Temps transcorregut entre la identificació d'una vulnerabilitat i la proposta de pla d'acció de mitigació	T_{Resp} - T_{Vul}	L1_T.PREV1 < 5 d	Puntual
L1_T.AUDI1	Auditoria Tècnica: Temps d'inici	Temps transcorregut entre la sol·licitud d'una auditoria tècnica i l'inici de la mateixa	T_{Resp} - T_{Sol}	L1_T.AUDI1 < 5 d	Puntual
L1_T.AUTO1	Grau d'automatització del servei	Incidents que s'han tractat via playbook automatitzat (N_{IncAut}) respecte el total d'incidents tractats (N_{IncTot}).	N_{IncAut} / N_{IncTot}	L1_T.AUTO1 > 75%	Trimestral

11.2.3 ANS de qualitat operativa aplicables al lot 2

No es defineixen acords de nivell de servei específicament per al lot 2 – Serveis d'avaluació independent, verificació i control qualitatiu del CROC. Apliquen tots els acords de nivell de servei transversals indicats a 11.2.1

11.2.4 ANS de qualitat operativa aplicables al lot 3

A continuació es detallen els acords de nivell de servei exigits específicament per al lot 3 – Serveis d'Operació, Administració i Evolució de les Eines Avançades de Protecció (OSAP). Pel que fa als acords de nivell de servei relacionats amb la gestió d'incidències i peticions, s'aplicaran els definits amb caràcter transversal al punt 11.2.1.

Informes de servei

Codi	Indicador ANS	Descripció	Càlcul	Objectiu	Periodicitat
L3_T.DOC_SEM	Termini lliurament informe setmanal del servei	Temps màxim d'entrega de l'informe setmanal sobre l'estat del serveis operats al lot3, respecte de la data de fi del període objecte de l'informe.	$T_{InforSetm} - T_{FiPeriode}$	L3_T.DOC_SEM > 7 d	Puntual
L3_T.DOC_MEN	Termini lliurament informe mensual del servei	Temps màxim d'entrega de l'informe mensual sobre l'estat del serveis operats al lot3, respecte de la data de fi del període objecte de l'informe.	$T_{InforMens} - T_{FiPeriode}$	L3_T.DOC_MEN > 30 d	Puntual

Gestió d'Incidències/Peticions de Servei

Codi	Indicador ANS	Descripció	Càlcul	Objectiu	Periodicitat
T.PRESP1	Temps de mobilització presencial a instal·lacions municipals de prioritat 1	Temps que transcorre des què es notifica la incidència o petició de prioritat 1 ($T_{NotiPresP1}$) fins que es rep resposta i s'arriba al lloc de treball de manera presencial ($T_{MobPresP1}$)	$T_{MobPresP1} - T_{NotiPresP1}$	T.PRESP1 < 45 min	Puntual
T.PRESP2	Temps de mobilització presencial a instal·lacions municipals de prioritat 2	Temps que transcorre des què es notifica la incidència o petició de prioritat 2 ($T_{NotiPresP2}$) fins que es rep resposta i s'arriba al lloc de treball de manera presencial ($T_{MobPresP2}$)	$T_{MobPresP2} - T_{NotiPresP2}$	T.PRESP2 < 60 min	Puntual
T.PRESP3	Temps de mobilització presencial a instal·lacions	Temps que transcorre des què es notifica la incidència o petició de prioritat 3 ($T_{NotiPresP3}$) fins que es rep	$T_{MobPresP3} - T_{NotiPresP3}$	T.PRESP3 < 90 min	

	municipals de prioritat 3	resposta i s'arriba al lloc de treball de manera presencial ($T_{MobPresP3}$)			
T.PRESP4	Temps de mobilització presencial a instal·lacions municipals de prioritat 4	Temps que transcorre des què es notifica la incidència o petició de prioritat 4 ($T_{NotiPresP4}$) fins que es rep resposta i s'arriba al lloc de treball de manera presencial ($T_{MobPresP4}$)	$T_{MobPresP4} - T_{NotiPresP4}$	T.PRESP4 < 120 min	
T.PRESP5	Temps de mobilització presencial a instal·lacions municipals de prioritat 5	Temps que transcorre des què es notifica la incidència o petició de prioritat 5 ($T_{NotiPresP5}$) fins que es rep resposta i s'arriba al lloc de treball de manera presencial ($T_{MobPresP5}$)	$T_{MobPresP5} - T_{NotiPresP5}$	T.PRESP5 < 24 h	
L3_T.DOC_GIC	Temps de lliurament d'informes d'incidències de prioritat 1	Temps màxim que transcorre des que se sol·licita un informe d'incidència crítica fins al lliurament definitius.	$T_{Doc\_GIC} - T_{Res\_GIC}$	L3_T.DOC_GIC < 8 h	Puntual
L3_T.DOC_GIN	Temps de lliurament d'informes d'incidències de prioritat 2/3/4/5	Temps màxim que transcorre des que se sol·licita un informe d'incidència no crítica fins al lliurament definitius.	$T_{Doc\_GIN} - T_{Res\_GIN}$	L3_T.DOC_GIN < 12 h	Puntual

Gestió de Peticions de Canvi

Codi	Indicador ANS	Descripció	Càlcul	Objectiu	Periodicitat
L3_T.ACT	Periodicitat mínima per actualitzacions de versió per equip.	Temps que transcorre entre actualitzacions per equip	$T_{ActNew} - T_{ActOld}$	L3_T.ACT <= 12 mesos	Puntual
L3_T.RFC	Temps màxim d'execució de canvi de versió per equip des de la petició	Temps que transcorre des què es notifica fins que s'executa	$T_{Exe} - T_{Not}$	L3_T.RFC <= 15 d	Puntual
L3_T.VUL	Temps de correcció de vulnerabilitats	Temps que transcorre des de la publicació de vulnerabilitats crítiques/molt crítiques d'equipament gestionat fins	$T_{Exe} - T_{Not}$	L3_T.VUL < 7 d	Puntual

		que s'actualitza a una nova versió que corregeix aquesta vulnerabilitat			

11.3 Model de penalitzacions

A cada definició d'ANS s'introdueix la penalització màxima sobre la facturació de la part que s'aplicarà. Es recull en les següents taules:

Gestió del contracte

Codi	Penalització màxima
GC_T.SUB	1% Facturació mensual.
GC_T.SOL	1% Facturació mensual.
GC_T.BAI	1% Facturació mensual.
GC_T.IMP	1% Facturació mensual.
GC_T.AMP	1% Facturació mensual.

Qualitat operativa transversal

Codi	Penalització màxima
%.DISP	1% Facturació mensual.
T.RTO	1% Facturació mensual.
%.CAPA	1% Facturació mensual.
T.ATNP1	1% Facturació mensual.
T.ATNP2	1% Facturació mensual.
T.ATNP3	N/A
T.ATNP4	N/A
T.ATNP5	N/A
%.ATNP1	1% Facturació mensual.
%.ATNP2	1% Facturació mensual.
%.ATNP3	1% Facturació mensual.
%.ATNP4	0,5% Facturació mensual.
%.ATNP5	0,5% Facturació mensual.
T.RESINCP1	1% Facturació mensual.
T.RESINCP2	1% Facturació mensual.
T.RESINCP3	N/A
T.RESINCP4	N/A
T.RESINCP5	N/A
%.RESINCP1	1% Facturació mensual.
%.RESINCP2	1% Facturació mensual.

%.RESINCP3	1% Facturació mensual.
%.RESINCP4	0,5% Facturació mensual.
%.RESINCP5	0,5% Facturació mensual.
T.RESPETP1	1% Facturació mensual.
T.RESPETP2	1% Facturació mensual.
T.RESPETP3	N/A
T.RESPETP4	N/A
T.RESPETP5	N/A
%.RESPETP1	1% Facturació mensual.
%.RESPETP2	1% Facturació mensual.
%.RESPETP3	1% Facturació mensual.
%.RESPETP4	0,5% Facturació mensual.
%.RESPETP5	0,5% Facturació mensual.
%.REOINC	1% Facturació mensual.
%.REOPET	1% Facturació mensual.
T.DOC	N/A
%.DOC	N/A

Qualitat operativa lot 1

Codi	Penalització màxima
L1_%.DISP.SVCS	4% Facturació mensual.
L1_%.DISP.PLAT	2% Facturació Mensual
L1_T.MONP1	2% Facturació Mensual
L1_T.MONP2	1% Facturació Mensual
L1_T.MONP3	1% Facturació Mensual
L1_T.MONP4	0,5% Facturació Mensual
L1_T.MONP5	0,5% Facturació Mensual
L1_%MONKO	2% Facturació Mensual
L1_T.INF_INC1	1% Facturació Mensual
L1_T.INF_INC2	1% Facturació Mensual
L1_T.INF_INC3	1% Facturació Mensual
L1_T.INF_EVI	0,5% Facturació Mensual
L1_T.PREV1	0,5% Facturació Mensual
L1_T.AUDI1	0,5% Facturació Mensual

Qualitat operativa lot 3

Codi	Penalització màxima
L3_T.DOC_SEM	0,2% Facturació mensual.
L3_T.DOC_MEN	0,2% Facturació mensual.
T.PRESP1	10% Facturació mensual.
T.PRESP2	4% Facturació mensual.
T.PRESP3	N/A
T.PRESP4	N/A
T.PRESP5	N/A
L3_T.DOC_GIC	0,5% Facturació mensual.
L3_T.DOC_GIN	0,5% Facturació mensual.
L3_T.ACT	1% Facturació mensual.
L3_T.RFC	1% Facturació mensual.
L3_T.VUL	1% Facturació mensual.

A més, al Plec de Clàusules Administratives Particulars d'aquest contracte s'especifiquen clàusules de penalitzacions addicionals per situacions relacionades amb els ANS descrits, i segons es consideren faltes lleus, greus o molt greus.

11.4 Modificació dels indicadors

Al llarg de la prestació del servei, davant qualsevol modificació dels indicadors i nivells de servei amb l'objectiu de donar un millor servei, l'organisme contractant, conjuntament amb l'adjudicatari, consensuaran i planificaran la seva introducció, així com el model de penalitzacions, si fos el cas.

Algunes de les causes que poden comportar aquestes modificacions són, per exemple: les variacions d'entorn tecnològic, d'entorn funcional i de condicions de negoci, els canvis d'abast i volum, així com les innovacions tecnològiques.

11.5 Millora del ANS

Durant l'execució del servei, l'organisme contractant pretén obtenir una millora del nivell de servei prestat per l'adjudicatari. Aquestes millores seran assolides com a conseqüència de l'execució de les activitats de millora contínua del servei, aplicades per l'adjudicatari.

Aquestes millores seran objectivades, definides i consensuades com a evolucions en el temps dels valors dels llindars assignats a un indicador de mesura o mètrica.

12. Facturació

En el marc del present Acord Marc per a la contractació de serveis del Centre de Riscos i Operacions de Ciberresiliència (CROC) i dels serveis d'Operació de Seguretat i Anàlisi de Protecció (OSAP), s'estableixen dos models de facturació diferenciats, en funció de la naturalesa i periodicitat dels serveis contractats en cada paquet funcional.

Models de facturació previstos:

- **Model de quota puntual.** Aquest model s'aplicarà als serveis orientats a la implantació inicial i a l'ampliació puntual de paquets o subpaquets de servei concrets amb calendarització definida. L'adjudicatari emetrà la factura un cop validada formalment la implantació o ampliació dels paquets o subpaquets de servei, d'acord amb la planificació establerta en el contracte basat corresponent.

- **Model de quota periòdica.** Aquest model s'aplicarà als serveis d'explotació mensual recurrent dels paquets o subpaquets de servei prèviament implantats o ampliats. La facturació es farà amb una periodicitat trimestral i per un import associat a la prestació regular del servei d'explotació de cadascun dels paquets de servei prèviament implantats o ampliats, en funció del paràmetre quantificador de cadascun dels paquets de servei i de les unitats objecte del servei. La quota periòdica de cadascun dels paquets de servei es meritarà a partir de la data en que hagi estat validada formalment la implantació o ampliació del paquet de servei respectiu. A la primera quota periòdica de cadascun dels paquets de servei es facturarà la part proporcional del temps transcorregut des de la data de meritació fins el darrer dia del mes en curs. A la darrera quota periòdica de cadascun dels paquets de servei es facturarà la part proporcional del temps transcorregut des de la data del primer dia del mes en curs fins la data de fi del servei.

Assignació del model segons el tipus de servei

Tipus de servei funcional	Model de facturació aplicable
Implantació de paquets de servei	Model de quota puntual
Ampliació de paquets de servei	Model de quota puntual
Explotació de paquets de servei	Model de quota periòdica

L'elecció del model de facturació per a cada contracte basat quedarà detallada en els documents corresponents a l'adjudicació del mateix i haurà de seguir el calendari i el pla de treball aprovat a la contractació basada.

12.1 Facturació de la implantació de paquets de servei

Aquest tipus de facturació s'aplicarà als serveis d'implantació de paquets de servei. La facturació es realitzarà en una única factura i **un cop realitzada i validada la implantació de paquets de servei per l'entitat contractant corresponent**.

La quota d'implantació d'un paquet o subpaquet de servei es calcularà en funció de l'import d'implantació unitari aplicable al paquet o subpaquet de servei en qüestió, multiplicat pel número d'unitats objecte de la implantació del servei, d'acord al paràmetre quantificador del servei. En cas que una entitat hagi implantat prèviament un subpaquet de servei amb un nivell de capacitats inferior, l'import unitari aplicable serà la diferència entre el nou import unitari aplicable i l'anterior.

En cada factura, s'haurà d'incloure el detall dels serveis prestats durant el període corresponent, així com la **relació d'indicadors ANS i les penalitzacions** aplicables, si escau, per incompliments detectats.

12.2 Facturació de l'ampliació de paquets de servei

Aquest tipus de facturació s'aplicarà als serveis d'ampliació de paquets de servei. La facturació es realitzarà en una única factura i **un cop realitzada i validada l'ampliació de paquets de servei per l'entitat contractant corresponent**.

La quota d'ampliació d'un paquet o subpaquet de servei es calcularà en funció de l'import d'ampliació unitari aplicable al paquet o subpaquet de servei, multiplicat pel número d'unitats objecte de l'ampliació del servei, d'acord al paràmetre quantificador del servei. En cas que durant el cicle de vida del servei l'entitat contractant substitueixi o incorpori una nova capacitat tecnològica dins l'àmbit de servei del mateix paquet la quota d'ampliació es

calcularà en funció de l'import unitari aplicable al paquet o subpaquet de servei, multiplicat pel número d'unitats objecte del servei, d'acord al paràmetre quantificador del servei.

En cada factura, s'haurà d'incloure el detall dels serveis prestats durant el període corresponent, així com la **relació d'indicadors ANS i les penalitzacions** aplicables, si escau, per incompliments detectats.

12.3 Facturació de l'explotació de paquets de servei

Aquest tipus de facturació s'aplicarà als serveis d'explotació de paquets de servei. La facturació es realitzarà **trimestralment i un cop vençut**, amb un import meritat mensualment un cop validada formalment l'explotació dels paquets o subpaquets de servei, d'acord amb la planificació establerta en el contracte basat **per l'entitat contractant corresponent**.

La quota d'explotació d'un paquet o subpaquet de servei es calcularà en funció de l'import d'explotació unitari aplicable al paquet o subpaquet de servei, multiplicat pel número d'unitats objecte del servei, d'acord al paràmetre quantificador del servei. En cas que durant el cicle de vida del servei l'entitat contractant substitueixi o incorpori una nova capacitat tecnològica dins l'àmbit de servei del mateix paquet que sigui inclosa dins la mateixa família de productes (p.e. EDR) del catàleg CPSTIC (guia CCN-STIC-105), el servei d'explotació haurà d'assumir sense cost addicional l'explotació d'aquesta nova capacitat tecnològica un cop ampliat el paquet. En cas que durant el cicle de vida del servei l'entitat contractant incorpori una nova capacitat tecnològica dins l'àmbit de servei del mateix paquet que no sigui inclosa dins la mateixa família de productes (p.e. UEM) del catàleg CPSTIC (guia CCN-STIC-105), el cost del servei recurrent mensual d'explotació serà incrementat en el número d'unitats contractades del mateix paquet o subpaquet.

En cada factura, s'haurà d'incloure el detall dels serveis prestats durant el període corresponent, així com la **relació d'indicadors ANS i les penalitzacions** aplicables, si escau, per incompliments detectats.

13. Procés de selecció

Els licitadors que es presentin hauran de poder prestar tots els serveis corresponents als paquets funcionals i serveis generals especificats al present plec. La selecció es resoldrà d'acord amb els criteris de valoració objectius i subjectius fixats en el plec de clàusules administratives que regula aquest Acord Marc i tenint en compte les restriccions descrites en els plecs. Es seleccionarà **1 única empresa** que s'encarregui de tots els serveis associats del present Acord Marc.

Un cop resolta la selecció i formalitzat l'Acord Marc, a mesura que sorgeixi la necessitat d'executar un projecte concret, es procedirà a l'adjudicació dels diferents contractes basats.

13.1 Procés de contractació de basats

Una vegada resolta la selecció d'**1 única empresa** i formalitzat l'Acord Marc, es procedirà al procés de contractació dels diferents contractes basats que puguin sorgir de l'acord marc en els termes i condicions previstos en el plec de clàusules administratives particulars.

14. Proposta Tècnica

Els licitadors presentaran la seva oferta tècnica de realització del contracte tant per fer comprensible la seva proposta com per facilitar i fer possible la seva valoració d'acord amb els criteris d'adjudicació assenyalats en el plec de clàusules administratives particulars que regeixen per aquesta contractació.

Cada licitador haurà de presentar la seva oferta en format electrònic, on tots els arxius han d'estar signats digitalment cadascun d'ells i en qualsevol dels formats admesos a la plataforma electrònica de conformitat amb l'establert al plec de clàusules administratives particulars. Les empreses licitadores hauran de presentar uns continguts mínims i estar obligatòriament estructurada de la forma següent:

La proposta tècnica es presentarà en dos sobres electrònics; el **sobre electrònic B**, on s'inclourà la documentació que haurà de ser valorada segons els criteris de judici de valor assenyalats en les clàusules del plec de clàusules administratives particulars, i el **sobre electrònic C**, que haurà de contenir la documentació que haurà de ser valorada segons els criteris avaluables de forma automàtica assenyalats al plec de clàusules administratives particulars que regeix per aquesta contractació. A l'interior de cada sobre s'ha d'incorporar una relació, en full independent, dels documents que hi conté ordenats numèricament, especialment en el **sobre electrònic B,** ja que aquest ha de respondre a les explicacions i compromisos sobre tots i cadascun dels criteris de valoració subjectius definits.

Es requereix utilitzar a l'oferta tipus de lletra Nimbus Roman, Liberation Sans, Calibri, Arial, Times New Roman o similar, de grandària 12 i interlineat simple.

14.1 Contingut sobre electrònic B

El sobre electrònic B inclourà la proposta tècnica per a l'execució dels serveis contemplats en aquest acord marc (casos d'us), d'acord amb els criteris de valoració definits en el plec de clàusules administratives i el plec de prescripcions tècniques.

La proposta tècnica haurà de presentar-se estructurada i redactada amb claredat, coherència i rigor, fent ús de taules, esquemes i elements gràfics quan sigui necessari per afavorir la comprensió.

Addicionalment a la proposta tècnica, que haurà de consistir en la resolució dels casos d'ús per la valoració dels criteris de judici de valor que consta al plec de clàusules administratives, les empreses licitadores hauran de presentar la següent documentació complementària. L'extensió màxima d'aquesta documentació per cada Lot no pot ser superior a 20 pàgines:

- **Resum executiu**

Resum per a la direcció dels continguts més significatius de la proposta del contracte.

- **Plantejament general**

S'exposa l'enteniment de les activitats que s'han de prestar i les línies principals de l'estratègia per dur-lo a terme, tenint en compte els requeriments exposats en el plec de prescripcions tècniques. Es detallarà tot el que es consideri interessant respecte a les metodologies de treball emprades.

- **Descripció del Model de relació de l'Acord Marc**

El licitant ha de proposar un model de relació que incloguin els mínims descrits en l'apartat corresponent del present plec i que permeti a BIT realitzar el govern global de totes les Agrupacions.

- **Descripció de l'estratègia d'execució dels serveis**

Aquest apartat haurà d'oferir una visió estratègica sobre com s'aborden els serveis objecte del contracte. Es valorarà que l'oferta presenti un enfocament sòlid, realista i alineat amb els objectius de l'Ajuntament i amb les característiques tècniques i organitzatives dels serveis descrits en el plec. La descripció haurà d'incloure:

- La visió general del model de prestació de serveis.
- La capacitat d'adaptació del servei a entorns municipals diversos.

- L'enfocament sobre governança tècnica i funcional, coordinació amb l'equip tècnic municipal i amb altres adjudicataris si escau.
- El plantejament per garantir la coherència, traçabilitat i integració dels serveis generals amb cada paquet funcional.
- L'estratègia per mantenir una qualitat homogènia en la prestació dels serveis al llarg del temps i entre col·lectius.
- **Resposta als requisits funcionals i tècnics**

L'empresa licitadora haurà d'actualitzar el document Excel de Taula de Requisits Tècnics específica de cada Lot per confirmar si compleix cadascun dels requisits funcionals i tècnics detallats. Aquest apartat no computa en el nombre màxim de pàgines sol·licitades.

14.2 Contingut Sobre electrònic C

En el **sobre electrònic C** s'inclourà la documentació que s'especifica en el plec de clàusules administratives particulars.

15. Clàusules generals de Seguretat

15.1 Seguretat dels sistemes d'informació, protecció de dades i compliment normatiu

BIT ha adoptat com a marc de referència per a la Seguretat dels Sistemes d'Informació el conjunt de bones pràctiques internacionalment reconegudes que desenvolupa la norma ISO-27002:2013.

El BIT, com a Organisme Autònom de caràcter administratiu de l'Administració Local depenent de l'Ajuntament de Barcelona, es troba subjecte al Principi de Legalitat i posa especial èmfasi en el compliment de les obligacions legals que es deriven de la Llei Orgànica 3/2018 de Protecció de Dades Personals i Garantia de Drets Digitals, de la Llei 39/2015 en tot allò que fa referència a l'accés dels ciutadans als serveis públics, així com de la resta de l'ordenament jurídic que sigui d'aplicació.

Pel que fa als aspectes propis de seguretat quan per l'objecte del contracte sigui d'aplicació, es tindrà especial cura de preveure que els productes finals compleixin amb el que estableix el

RD 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat en l'Àmbit de l'Administració Electrònica.

Les empreses licitadores s'obliguen a vetllar pel compliment de la legislació vigent aplicable a l'objecte del contracte i especialment pel que fa referència a la protecció de dades de caràcter personal.

A les diferents clàusules d'aquesta secció es fa referència a Ajuntament de Barcelona, Administració Municipal i BIT indistintament. De conformitat als seus estatuts s'ha d'entendre que BIT actua als efectes d'aquest contracte en nom i representació de l'Ajuntament de Barcelona i de l'Administració Municipal, pel que fa referència als fitxers, sistemes d'informació i/o infraestructures de les quals no sigui directament titular.

15.2 Responsable de seguretat

L'adjudicatari nomenarà un Responsable de Seguretat, el qual haurà de vetllar pel compliment dels següents requeriments:

- Actuar d'interlocutor únic per a tots els aspectes de seguretat del contracte.
- Garantir que tots els serveis prestats pel proveïdor a l'Ajuntament es realitzen d'acord al model i requeriments de seguretat establerts per BIT i seguint la normativa de seguretat vigent.
- Garantir i liderar dins la seva organització la correcta implantació dels nivells de seguretat i les seves corresponents mesures (tècniques, organitzatives i jurídiques), així com les directrius en matèria de seguretat establertes per BIT.
- Assegurar que tot el personal de l'adjudicatari que prestarà serveis a l'Ajuntament, passi per un pla de conscienciació i formació en matèria de seguretat.
- Informar al seu personal qualsevol obligació a què l'empresa estigui sotmesa per contracte, formar al seu personal en les polítiques i instruccions de l'Administració Municipal en cas que els sigui d'aplicació i fer signar al seu personal un document d'acceptació de les obligacions relatives a la seguretat de la informació i protecció de dades de caràcter personal de l'Administració Municipal.
- Mantenir actualitzada, i en tot moment disponible, una llista de les persones adscrites a l'execució del contracte on s'indicarà la data en què van rebre la formació en política i instruccions de l'Administració Municipal, així com el document d'acceptació de les obligacions relatives a la seguretat de la informació.

15.3 Condicions generals d'execució

BIT ha adoptat com a marc de referència per a la Seguretat dels Sistemes d'Informació el conjunt de bones pràctiques internacionalment reconegudes que desenvolupa la norma ISO-27002:2013.

BIT, com a Organisme Autònom de caràcter administratiu de l'Administració Local depenent de l'Ajuntament de Barcelona, es troba subjecte al Principi de Legalitat i posa especial èmfasi en el compliment de les obligacions legals que es deriven de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals i la normativa que la desenvolupa així com de la resta de l'ordenament jurídic que sigui d'aplicació.

Pel que fa als aspectes propis de seguretat quan per l'objecte del contracte sigui d'aplicació es tindrà especial cura de preveure que els productes finals compleixin amb el que estableix el RD 311/2022 de 3 de maig pel qual es regula l'Esquema Nacional de Seguretat en l'Àmbit de l'Administració Electrònica.

Les empreses licitadores s'obliguen a vetllar pel compliment de la legislació vigent aplicable a l'objecte del contracte i especialment pel que fa referència a la protecció de dades de caràcter personal

A les diferents clàusules d'aquesta secció es fa referència a l'Ajuntament de Barcelona, Administració Municipal i BIT indistintament. De conformitat amb els seus estatuts s'ha d'entendre que BIT actua als efectes d'aquest contracte en nom i representació de l'Ajuntament de Barcelona i de l'Administració Municipal, pel que fa referència als fitxers, sistemes d'informació i/o infraestructures de les quals no sigui directament titular.

15.4 Clàusula de propietat intel·lectual

La propietat intel·lectual dels treballs realitzats a l'empara d'aquest contracte pertany a l'Ajuntament de Barcelona de forma exclusiva. Els productes o subproductes basats, no podran ser utilitzats sense la deguda autorització prèvia.

L'accés a informació i/o productes protegits per la propietat intel·lectual, propietat de l'Ajuntament de Barcelona, necessaris per al desenvolupament del producte o servei contractat no pressuposa en cap cas la cessió d'aquesta.

L'empresa contractada accepta expressament que els drets d'explotació dels productes basats d'aquest plec corresponen única i exclusivament a l'Ajuntament de Barcelona. Així doncs, el contractat cedeix, amb caràcter d'exclusivitat, la totalitat dels drets d'explotació dels treballs objecte d'aquest plec, inclosos els drets de comunicació pública, reproducció,

transformació o modificació i qualsevol altre dret susceptible de cessió en exclusiva, d'acord amb la legislació sobre drets de propietat intel·lectual.

15.5 Confidencialitat

L'empresa contractada s'obliga a no difondre i a guardar el més absolut secret de tota la informació a la qual tingui accés en compliment del present contracte i a subministrar-la només al personal autoritzat per l'Administració Municipal.

Quan l'objecte del contracte sigui la construcció i/o el manteniment de Sistemes d'Informació i/o Infraestructures Tecnològiques, el deure de secret inclou els components tecnològics i mesures de seguretat tècniques implantades en els mateixos.

L'empresa contractada serà responsable de les violacions del deure de secret que es puguin produir per part del personal al seu càrrec. Així mateix, s'obliga a aplicar les mesures necessàries per a garantir l'eficàcia dels principis de mínim privilegi i necessitat de conèixer, per part del personal participant en el desenvolupament del contracte.

Un cop finalitzat el present contracte, l'empresa contractada es compromet a destruir amb les garanties de seguretat suficients o retornar tota la informació facilitada per l'Administració Municipal, així com qualsevol altre producte obtingut com a resultat del present contracte.

15.6 LOPDGDD

L'adjudicatari s'obliga a tractar les dades de caràcter personal a les quals tingui accés en ocasió del compliment dels contractes basats d'aquesta homologació d'acord amb les instruccions dictades per l'Ajuntament de Barcelona, sense que en cap cas les pugui aplicar ni utilitzar amb una finalitat diferent d'aquell compliment, ni comunicar-les, ni tan sols per a la seva conservació, a altres persones, i tindrà de conformitat amb la normativa aplicable en matèria de contractació la consideració d'encarregat del tractament.

1.- L'adjudicatari resta obligat al secret professional pel què fa a les dades de caràcter personal a les quals tingui accés en ocasió del compliment dels contractes basats en aquesta homologació, obligació que subsistirà, fins i tot, un cop el contracte s'hagi extingit, per finalització del seu termini o objecte, per resolució o per qualsevol altra causa legalment admesa o establerta en aquest contracte.

Així mateix, l'adjudicatari ha de guardar reserva respecte de les dades o antecedents dels quals hagi tingut coneixement en ocasió dels contractes basats d'aquesta homologació. En aquest sentit, la documentació i informació a la qual tingui accés l'adjudicatari té caràcter confidencial, i no podrà ser objecte de reproducció total o parcial per cap mitjà o suport. Per tant, no se'n podrà fer cap tractament ni edició, informàtica o no, ni transmissió a terceres

persones fora de l'estricte àmbit d'execució directa dels contractes basats d'aquesta homologació, ni tan sols entre la resta del personal que tingui o pugui tenir l'entitat que presta el servei objecte d'aquest.

Si l'accés a les dades es fa als locals de l'Ajuntament de Barcelona, o si es fa de forma remota exclusivament a suports o sistemes d'informació de l'Ajuntament, l'adjudicatari té prohibit incorporar les dades a d'altres sistemes o suports sense autorització expressa i haurà de complir amb les mesures de seguretat establertes en el document de seguretat del responsable del tractament.

En tot cas, i sens perjudici d'altres mesures a adoptar d'acord amb la normativa vigent en matèria de protecció de dades personals, només podran accedir a les esmentades dades de caràcter personal, informacions i documentació les persones estrictament imprescindibles pel desenvolupament de les tasques inherents al propi encàrrec. Totes elles seran advertides per l'adjudicatari del caràcter d'informació confidencial i reservada i del deure de secret als quals estan sotmeses, i aquell serà responsable del compliment d'aquestes obligacions per part del seu personal. Així mateix, s'obliga a realitzar la formació necessària al personal al seu càrrec que tingui accés a les dades personals, garantint el compliment de les obligacions derivades de la normativa de protecció de dades.

2.- L'adjudicatari/ària manifesta que té implantades les mesures de caràcter tècnic i organitzatiu necessàries per garantir la seguretat de les dades de caràcter personal a les quals tindrà accés en ocasió de l'execució dels contractes basats d'aquesta homologació, tot evitant-ne la seva alteració, pèrdua, tractament o accés no autoritzat, tenint en compte l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a què estan exposades, i en estricte compliment de la normativa vigent en matèria de protecció de dades de caràcter personal.

Per a cada contracte basat s'especificarà si les mesures de seguretat implantades per l'adjudicatari han de ser les corresponents **al nivell alt, mitjà o bàsic, segons es tractin dades personals a les aplicacions objecte dels contractes basats**, i són d'aplicació als fitxers, centres de tractament, locals, equips, sistemes, programes i persones que intervinguin en el tractament de les dades en els termes que estableix aquell reglament.

La finalitat del tractament d'aquestes dades estarà completament definida al contracte basat. Aquestes dades, que estan incloses en el/s tractament/s municipal/s explicitats a la Seu Electrònica de l'Ajuntament de Barcelona, requereixen per part de l'adjudicatari la implantació de les mesures de seguretat corresponents al nivell de seguretat de les dades.

L'adjudicatari mantindrà a disposició dels tècnics municipals còpia documentada de les mesures de seguretat aplicades.

A partir del 25 de maig, data d'exigibilitat del nou Reglament General de Protecció de Dades (Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016), l'empresa adjudicatària haurà d'implantar, sense cost addicional, les mesures de seguretat necessàries per minimitzar el risc de vulneració dels drets i llibertats dels ciutadans afectats, tot tenint en compte el nivell de classificació de les dades, els tractaments realitzats i l'estat de la tecnologia.

Quan el compliment d'un contracte basat es faci en el local de l'Ajuntament o l'accés sigui remot, l'adjudicatari s'obligarà a adoptar les mesures de seguretat previstes en el document de seguretat del fitxer municipal corresponent. En el cas que el servei sigui prestat en els locals del mateix adjudicatari, aleshores aquest haurà d'elaborar un document de seguretat, en els termes establerts en la normativa reglamentària sobre la protecció de dades de caràcter personal, o completar el que ja hagués elaborat, en el seu cas, tot identificant el fitxer o tractament i el responsable del mateix i incorporant les mesures de seguretat a implantar en relació amb aquest tractament.

Les resolucions dels procediments d'exercici dels drets LOPDGDD que puguin exercir els titulars de dades de caràcter personal corresponen a l'Ajuntament de Barcelona durant tota la vigència dels contractes basats.

En tot cas, l'adjudicatari haurà de posar en coneixement de l'Ajuntament de Barcelona, immediatament després de ser detectada, qualsevol sospita o constatació d'eventuals errors o incidències que poguessin produir-se en el sistema de seguretat de la informació.

3.- L'Ajuntament de Barcelona podrà designar, en qualsevol moment, durant la vigència dels contractes basats d'aquesta homologació, a personal intern o extern per a verificar que l'adjudicatari té implantades les mesures necessàries per garantir la seguretat de les dades de caràcter personal.

4.- Durant la vigència dels contractes basats d'aquesta homologació l'adjudicatari haurà de conservar qualsevol dada objecte de tractament, llevat que rebi indicacions en sentit contrari de l'Ajuntament de Barcelona.

5.- Una vegada executat un contracte basat d'aquesta homologació, l'adjudicatari haurà de destruir i/o retornar a l'Ajuntament de Barcelona, d'acord amb allò que s'estableixi legalment o les indicacions que li transmeti aquest, les dades de caràcter personal que hagin estat objecte de tractament per part d'aquell durant la vigència del mateix, juntament amb els suports o documents en què consti alguna dada de caràcter personal. El retorn de les dades a l'Ajuntament de Barcelona es durà a terme en el format i els suports utilitzats per l'adjudicatari pel seu emmagatzematge.

En el cas que, en finalitzar un contracte basat, les dades personals s'hagin de traspassar a un tercer, totes les dades i informació que, per la realització d'aquest traspàs de dades es posin

en coneixement de l'adjudicatari, seran considerades dades confidencials i l'adjudicatari en guardarà absoluta reserva. Aquesta confidencialitat i reserva s'estendrà a totes les dades i informacions lliurades, amb independència que tinguin o no el caràcter de dada personal.

En el cas que alguna previsió legal exigeixi la conservació de les dades, o de part d'elles, l'adjudicatari haurà de conservar-les, degudament bloquejades, per impedir-ne l'accés i el tractament en tant en quant puguin derivar-se responsabilitats de la seva relació amb l'Ajuntament de Barcelona.

6.- En el cas que destini les dades a les quals tingui accés a una finalitat diferent a l'establerta, o les comuniqui o les utilitzi incomplint les estipulacions del present contracte o les instruccions de l'Ajuntament de Barcelona, l'adjudicatari serà considerat responsable del tractament i respondrà personalment de les infraccions que hagi comès i de les possibles reclamacions que es puguin produir al respecte.

L'Ajuntament de Barcelona repercutirà en l'adjudicatari els costos corresponents a les sancions i/o indemnitzacions a què hagi de fer front que s'haguessin originat directa o indirectament pel deficient i/o negligent tractament de dades de caràcter personal realitzat per l'adjudicatari. En tot cas, l'adjudicatari s'obliga a mantenir indemne l'Ajuntament de Barcelona de totes les despeses o altres conseqüències negatives que se li puguin originar a causa dels esmentats tractaments, sancions i/o indemnitzacions.

L'adjudicatari s'obliga a comunicar a l'Ajuntament de Barcelona quins treballs seran objecte de subcontractació i quines seran les empreses que els realitzaran. Amb el permís exprés i escrit de l'Ajuntament de Barcelona, i actuant en nom i representació d'aquest, l'adjudicatari formalitzarà el corresponent contracte amb l'empresa o empreses subcontractades que, als efectes de l'aplicació de la normativa de protecció de dades, tindran la consideració d'encarregats de tractament de l'Ajuntament de Barcelona. Aquests contractes s'afegiran com annex al contracte administratiu que formalitza aquesta adjudicació.

El tractament de dades realitzat per part del subcontractat haurà de complir amb la normativa vigent en matèria de protecció de dades de caràcter personal, i, s'ajustarà així mateix a les obligacions assumides pel contractista i a les instruccions específiques que li doni l'Ajuntament de Barcelona al respecte.

15.7 Clàusula de comunicacions externes

L'empresa contractada disposarà dels mitjans materials i el maquinari necessari per a la connexió amb els Sistemes d'Informació de l'Administració Municipal, sent els costos de connexió a càrrec de l'empresa contractada.

La connexió és realitzarà seguint els protocols de seguretat per a les comunicacions externes establerts per l'Administració Municipal.

L'empresa contractada serà la responsable de custodiar correctament els certificats digitals lliurats per la interconnexió segura de xarxes i de demanar la seva revocació una vegada finalitzada la prestació del servei. Així mateix, serà responsable subsidiària de l'ús dels certificats personals individuals lliurats als seus empleats pel desenvolupament del producte o servei.

15.8 Clàusula de seguretat dels equips, programes i informació

L'empresa contractada es compromet a vetllar per la seguretat dels equips on es trobin instal·lats els programes, bases de dades i informació de l'Administració Municipal, així com per la seguretat en els canals de comunicació emprats. Per tant, prestarà els seus serveis guardant estrictament les mesures de seguretat necessàries, amb la finalitat d'evitar la pèrdua d'informació, així com danys, pèrdua o deteriorament dels programes i bases de dades utilitzades i que són propietat de l'Administració Municipal.

15.9 Clàusula de personal extern

El Cap responsable del contracte de l'empresa adjudicatària durà a terme de forma correcta la gestió del personal i els aspectes relacionats amb la seguretat de la informació.

L'empresa contractada està obligada a implantar els mecanismes i controls necessaris per a garantir la confidencialitat, privacitat, integritat i continuïtat de la informació de l'Administració Municipal, i, de donar-los a conèixer al seu personal.

El Cap responsable del contracte de l'empresa adjudicatària, abans de l'inici de la prestació del servei objecte d'un contracte basat d'aquesta homologació, haurà de notificar al seu personal qualsevol obligació a què l'empresa estigui sotmesa per contracte, formar al seu personal en la política i instruccions de l'Administració Municipal que els sigui d'aplicació, i fer signar al seu personal un document d'acceptació de les obligacions relatives a la seguretat de la informació i protecció de dades de caràcter personal de l'Administració Municipal.

L'empresa contractada haurà de mantenir disponible en tot moment la informació o treballs resultants de l'objecte del contracte, amb la finalitat de comprovar el compliment de les mesures i controls previstos en aquest apartat.

El responsable del contracte de l'empresa adjudicatària haurà de mantenir actualitzada, i en tot moment disponible, una llista de les persones adscrites a l'execució del contracte en què

s'indicarà la data en què van rebre la formació en política i instruccions de l'Administració Municipal, així com el document d'acceptació de les obligacions relatives a la seguretat de la informació.

El document d'acceptació de les obligacions signat per les persones adscrites a l'execució dels contractes basats d'aquesta homologació serà entregat al Cap responsable del contracte de l'Administració Municipal, abans de ser donats els permisos per accedir als Sistemes d'Informació de l'Administració Municipal o bé abans de ser facilitada la informació pel correcte compliment del servei contractat, i restarà en poder de l'empresa contractada que haurà de presentar-los quan siguin requerits per l'Administració Municipal.

15.10 Clàusula d'ús de programari lliure

BIT advoca per reduir el nombre de components de software amb llicència, i recomana per tant l'ús de components O*pen Source*.

Les solucions, sistemes, processos , metodologies que es defineixin hauran d'estar alineats, ser coherents amb les estratègies TIC de l'Ajuntament, que es poden concretar entre altres en:

- Transparència i participació
- Obertura al ciutadà.
- Agilitat i disseny centrat en l'experiència d'usuari
- Ús prioritari de Programari Lliure.
- Compartició i creació de solucions de forma col·laborativa amb comunitats i altres administracions.
- Interoperabilitat
- Dades obertes
- Aplicació d'estàndards oficials oberts i lliures, especialment en formats de dades i protocols

En tot el que es refereixi a la definició de programari lliure i estàndards oberts lliures s'aplicarà les definicions de la *Open Source Iniciative* (https://opensource.org/).

En concret, respecte a l'ús de programari lliure, s'haurà de prioritzar solucions de codi obert, o la construcció de noves solucions que es lliuraran mitjançant llicències obertes.

En els casos en què no es pugui construir la solució totalment amb mòduls de programari lliure o solucions noves a mida, s'intentarà dissenyar la solució de forma que contempli el màxim de peces o mòduls lliures.

Barcelona, a la data de signatura electrònica

Jorge Vicente López Portero
Cap del Departament de Seguretat Operativa

David Esteban Haro
Director de Serveis de Seguretat de la Informació

Annex I: Informació addicional i/o aclariments

Si és de l'interès dels licitadors sol·licitar informació per la presentació de l'oferta, BIT posarà a disposició les següents adreces de correu on els licitadors podran fer les seves consultes a la bústia bit_seg_oper@bcn.cat

En l'assumpte del correu indicar:

> Acord Marc de selecció per a la contractació de serveis CROC-OSAP
> *[**Número d'expedient del contracte**]*

S'atendran les sol·licituds d'informació fins a 3 dies laborables abans de la data límit de presentació d'ofertes.

Per tal que les empreses licitadores interessades a presentar oferta puguin aclarir els dubtes que els hi sorgeixin, BIT posa a la seva disposició la bústia de correu abans indicada per qüestions tècniques i la de BIT_gestio_contractacio@bcn.cat per consultes de caràcter administratiu.

Així mateix, s'indica que, inicialment, no es convocarà sessió informativa per a aquesta licitació. Malgrat això, si alguna de les empreses licitadores estigués interessada a realitzar-la, pot fer-ne la petició a través del correu BIT_gestio_contractacio@bcn.cat

Les consultes rebudes es respondran i es publicaran" al perfil del contractant de BIT:
https://contractaciopublica.gencat.cat/ecofin_pscp/AppJava/cap.pscp?reqCode=viewDetail&idCap=15990903

Annex II: Glossari

Per tal de facilitar la compressió de la terminologia emprada en aquest plec a continuació es presenta una llista dels termes i acrònims clau amb les seves respectives definicions. Aquestes definicions són d'aplicació exclusiva per a la interpretació d'aquest document:

- Esdeveniment de seguretat:
    - Qualsevol ocurrència observable en un sistema, servei, xarxa o infraestructura TIC que pot tenir una rellevància per a la seguretat. És una senyal, un succés o un canvi en l'estat del sistema que pot indicar una possible violació de la política de seguretat, una fallida en una salvaguarda o una situació prèviament desconeguda que podria ser pertinent per a la seguretat.
- Alerta de seguretat:
    - Notificació o avís que es genera de forma automàtica o manual quan es produeix un esdeveniment, o bé una sèrie d'esdeveniments, per alertar sobre una amenaça, un risc o un possible incident de seguretat que pugui comprometre la seguretat d'un sistema, xarxa, persona o organització.
- Incident de seguretat:
    - Una alerta de seguretat que ha estat confirmada com a una violació de la seguretat ja que ha compromès qualsevol de les dimensions de seguretat (confidencialitat, integritat, disponibilitat, autenticitat o traçabilitat) de la informació tractada o dels serveis prestats per un sistema TIC (Tecnologies de la Informació i Comunicació). Es cataloguen, registren i notifiquen d'acord amb allò especificat a l'ENS i a la guia CCN-STIC-817 de gestió de ciberincidents,
- CMDB (Configuration Management Database):
    - La base de dades de gestió de la configuració és un repositori central d'informació que emmagatzema i gestiona dades sobre tots els components de la infraestructura TIC d'una organització. Els components s'anomenen CI (Configuration Items) i poden ser qualsevol cosa que hagi de ser gestionada per a lliurar un servei TIC (maquinari, programari, documents, serveis, persones, etc). La clau d'una CMDB no és només l'inventari d'aquests components, sinó les relacions i dependències entre ells. En resum, és un component fonamental d'acord a les bones pràctiques de gestió de servei TIC (ITIL) i proporciona una visió integral i lògica de la infraestructura TIC de l'organització permeten una gestió estratègica, eficient i segura.
- SIEM (Security Information and Event Management)
    - És una solució de ciberseguretat que combina la gestió de la informació de seguretat i la gestió d'esdeveniments de seguretat en una única plataforma que

ofereix una visió centralitzada i en temps real de la postura de seguretat de l'organització, i facilita la detecció i l'anàlisi. És com un gran cervell que recopila esdeveniments de seguretat de múltiples fonts (dispositius d'usuari, servidors, aplicacions, sistemes de detecció i prevenció d'intrusions, serveis al núvol, IA, etc), els normalitza i emmagatzema, i els correla fent servir regles predefinides o algorismes d'aprenentatge automàtic per detectar alertes o incidents de seguretat.

- SOAR (Security Orchestration, Automation and Response)
    - Funcionalitat complementària al SIEM que facilita l'orquestració i automatització de la resposta a determinats incidents d'acord a un flux de treball predefinit, acordat i aprovat prèviament. Permet reduir el temps de resposta (MTTR: Mean Time To Respond) als incidents més simples i recurrents, alliberant .als analistes de seguretat per centrar-se en tasques més complexes i de més valor afegit.
- Respositori de logs centralitzat per a compliment i anàlisi forense
    - És una evolució del concepte de repositori de logs centralitzat que a més d'emmagatzemar les dades, garanteix la seva integritat i immutabilitat, la retenció adient, i l'accessibilitat per facilitar la cerca i generació d'informes a les persones autoritzades (auditors, analistes forenses, etc) per tal de donar compliment a la normativa aplicables (RGPD, LOPDPiGDD, ENS, NIS2, etc).
- EPP (Endpoint Protectioin Platform)
    - Solució de seguretat integral i centralitzada per a protegir dispositius finals (estacions de treball, portàtils, mòbils, servidors, etc) contra una amplia gama d'amenaces (programari maliciós, ransomware, etc) que combina vàries tecnologies com antivirus, antimalware avançat (basat en comportament i no només en signatures) i prevenció d'instrusions.
- EDR (Endpoint Detection and Response)
    - Solució de seguretat avançada per a protegir dispositius finals que recopila dades de manera constant sobre l'activitat del dispositiu (processos, comunicacions, arxius, etc) i utilitza anàlisi de comportament. intel·ligència artificial i Machine learning per identificar i alertar sobre activitats sospitoses o amenaces sofisticades que un EPP tradicional podria no detectar. Proporciona també visibilitat detallada i eines d'anàlisi forense per investigar la naturalesa i l'abast de l'amenaça. Ofereix al CROC capacitats de resposta ràpida i remediació de forma automàtica o manual (p.e. aïllar un equip, etc).
- XDR (eXtended Deteción and Response)

  - Plataforma de seguretat que correlaciona i analitza telemetria de múltiples fonts (endpoints, correu, identitats, xarxa, cloud, etc.) per detectar, investigar i respondre de manera unificada a amenaces avançades i multivector.
- MTD (Mobile Threat Detection)
  - Solució de seguretat per a dispositius mòbils que detecta i alerta sobre amenaces com aplicacions malicioses, comportaments sospitosos, vulnerabilitats del sistema operatiu o riscos de xarxa, protegint dades i accessos corporatius en smartphones i tauletes.
- CVSS (Common Vulnerability Scoring System)
  - És un estàndard de facto de la indústria, marc lliure i obert, per avaluar la gravetat de les vulnerabilitats dels sistemes TIC, assignant una puntuació que varia de 0 (gens crítica) a 10 (molt crítica). Hi ha diferents versions d'aquest marc que fan servir mètodes de càlcul de la criticitat cada cop més refinats. La versió 3.1 de l'any 2019 és la més usual, i la més recent és la versió 4.0 de l'any 2023.

Annex III: Descripció basat inicial

1. Basat inicial

El present annex descriu, amb caràcter **orientatiu i no exhaustiu**, els principals elements que es preveu que formin part del **primer contracte basat** que l'Institut Municipal Barcelona Innovació i Tecnologia (BIT) té la **voluntat d'impulsar** a l'empara del present Acord Marc, amb la finalitat de **garantir la continuïtat, estabilitat i evolució dels serveis de ciberseguretat operativa actualment prestats**.

Aquesta descripció no genera cap dret ni obligació de contractació, i el contingut definitiu del contracte basat s'establirà en el corresponent expedient, d'acord amb les necessitats reals del servei, la disponibilitat pressupostària i el marc normatiu aplicable.

2. Capacitats tecnològiques

La informació relativa a les **capacitats tecnològiques objecte del servei**, així com al **tipus, abast i vigència de les llicències actualment desplegades**, serà facilitada de manera **segura i confidencial** a les empreses licitadores que ho sol·licitin formalment.

L'accés a aquesta informació quedarà condicionat, amb caràcter previ, a la **signatura de l'acord de confidencialitat preceptiu (NDA)**, atesa la naturalesa sensible i crítica de la informació associada als sistemes de seguretat municipals.

3. Volumetries

Els ens dependents o vinculats a l'Ajuntament de Barcelona que, de manera voluntària, es podrien adherir al present Acord Marc es troben detallats al portal institucional https://ajuntament.barcelona.cat/ca/organitzacio-municipal/ens-dependents, i s'agrupen en les categories següents: **Societats Mercantils Municipals, Consorcis, Fundacions i Associacions**.

El dimensionament estimat del CROC impulsat per BIT, i recollit a la **Matriu de Valoració**, inclou la volumetria corresponent als usuaris de l'Ajuntament de Barcelona, així com la dels **organismes autònoms locals** i les **entitats públiques empresarials dependents**.

Pel que fa a la situació actual de les plataformes de monitoratge i correlació d'esdeveniments:

- La plataforma **QRadar** disposa actualment d'aproximadament **47 TB** ocupats en entorn *on-premise* corresponents a logs i índexs.

- La plataforma **ELK** disposa d'aproximadament **130 TB** ocupats en entorn *cloud* i **24 TB** en entorn *on-premise*, també corresponents a logs i índexs.

En relació amb l'àmbit OT i IoT, el portal https://connecta.bcn.cat/connecta-catalog-web/stats/ ofereix estadístiques de la plataforma municipal de sensors i actuadors (Sentilo), que actualment identifica **més de 29.000 sensors actius**. Addicionalment, la solució **Microsoft Defender for Endpoint** ha identificat **més de 7.000 dispositius OT i IoT addicionals**.
Tanmateix, **no és possible concretar en aquest moment** el nombre total de dispositius OT i IoT desplegats a la ciutat, ni la seva distribució física, ni el nombre exacte de *IoT Gateways* existents.

A títol estrictament orientatiu, es proposa estimar anualment els volums següents:

- Aproximadament **2.500 alertes de seguretat** que superen la fase inicial de triatge i requereixen una anàlisi aprofundida.
- Uns **250 incidents de seguretat**, dels quals al voltant de **40** poden tenir la consideració d'incidents significatius susceptibles de requerir l'activació del servei de resposta a incidents (IRT).
- Aproximadament **250 peticions de servei**.
- Aproximadament **250 peticions de canvi** sobre els actius administrats i operats pel servei.

Aquestes estimacions tenen caràcter merament orientatiu i podran ser ajustades en funció de l'evolució real del servei.

4. Altres consideracions

Els contractes basats que s'adjudiquin durant la vigència de l'Acord Marc **podran continuar vigents fins al seu venciment**, encara que l'Acord Marc hagi finalitzat, d'acord amb el que estableix la normativa de contractació pública.

La **durada mínima de contractació de cada paquet funcional** serà d'**un (1) any**, sense perjudici de les durades superiors que es puguin establir en els contractes basats concrets.