Plaça de la Vila, 1
08172 Sant Cugat del Vallès
T. 935 657 000
santcugat.cat

Codi de verificació	5R2058465W5805340IIY
Procediment: N488 Contractació de serveis	
Expedient: 17295/2025	Document: 302226/2025

PLEC DE PRESCRIPCIONS TÈCNIQUES DE CONTRACTACIÓ DE SERVEIS

Primer. Objecte del contracte

L'objecte d'aquesta licitació és la contractació d'un servei gestionat de ciberseguretat (MSSP) que doni resposta a les necessitats actuals de l'Ajuntament de Sant Cugat del Vallès, mitjançant la incorporació d'un servei de seguretat avançada, juntament amb els serveis especialitzats de desplegament, configuració, migració, explotació i millora contínua, segons les prescripcions establertes en aquest plec.

L'objectiu principal és garantir un model de seguretat modern, integral i eficient, alineat amb l'Estratègia Nacional de Ciberseguretat. Aquest model ha de proporcionar:

- Seguretat i resiliència de les xarxes i sistemes d'informació i comunicacions municipals.
- Desenvolupament d'una cultura organitzativa compromesa amb la ciberseguretat i l'impuls de les capacitats tècniques i humanes.

El servei gestionat de ciberseguretat permetrà disposar d'una servei unificat que integri funcions de gestió d'esdeveniments i informació de seguretat (SIEM), resposta automatitzada davant incidents (SOAR), anàlisi basada en intel·ligència artificial i visibilitat centralitzada dels actius i riscos. Aquest tipus de solució proporciona detecció avançada d'amenaces, correlació d'activitat sospitosa, automatització de respostes, informes contextualitzats i monitorització 24x7, millorant de forma substancial la capacitat de resposta i anticipació davant incidents.

Aquest enfocament permet a l'Ajuntament desplegar una ciberseguretat eficaç sense necessitat de construir infraestructures pròpies complexes ni sobrecarregar els recursos interns, delegant en un proveïdor especialitzat la gestió, manteniment i evolució tecnològica del servei.

El projecte també dona suport a la necessitat d'invertir en eines i processos destinats a assegurar un elevat nivell de protecció sobre els sistemes municipals, tenint en compte el paper clau que tenen en el funcionament econòmic, social i administratiu de la ciutat. La interrupció o compromís d'aquests sistemes podria tenir un impacte significatiu que superaria l'àmbit estrictament local.

D'altra banda, l'homogeneïtzació de criteris i estàndards en matèria de seguretat entre administracions és una peça clau per reduir vulnerabilitats estructurals. A través d'aquest projecte, es reforça l'adopció de bones pràctiques, alineades amb normatives nacionals i europees.

A més, el servei contractat ha de reforçar les capacitats municipals en prevenció, detecció, contenció i resposta davant ciberincidents. L'equilibri entre els riscos reals i els recursos aplicats per gestionar-los ha de ser estable i suficient, garantint la qualitat i continuïtat dels serveis públics digitals.

Aquest reforç s'ha d'estendre a totes les àrees de l'Ajuntament, simplificant l'ecosistema tecnològic i optimitzant recursos. L'objectiu és avançar cap a una ciberseguretat transversal, escalable i sostenible, basada en solucions intel·ligents i automatitzades.

Finalment, el projecte posa al centre la protecció de les dades personals i dels drets digitals de la ciutadania. Aquest compromís no només respon a exigències legals, sinó a una responsabilitat institucional fonamentada en l'ètica pública. En un context de sofisticació creixent de les amenaces i disponibilitat d'eines d'atac al mercat il·lícit, la protecció efectiva de la informació ha de sustentar-se en sistemes avançats, serveis especialitzats i capacitats de resposta contínua.

Donat que els tractaments d'informació es duen a terme mitjançant equips informàtics, s'emmagatzemen en suports digitals i es transmeten per xarxes, la protecció integral de tots els components del sistema d'informació és una prioritat estratègica. L'exposició constant a amenaces internes i externes reforça la necessitat d'un servei com el previst en aquest projecte.

Segon. Característiques tècniques dels serveis o prestacions

En la determinació de les prescripcions, s'han tingut en compte els arts. 124 a 128 de la LCSP sobre definicions i regles per a l'establiment de prescripcions tècniques.

L'objecte del contracte és la implantació i explotació d'un servei gestionat de seguretat (MSSP – Managed Security Services Provider) que substitueixi l'actual prestació i ampliï les capacitats de ciberseguretat de l'Ajuntament de Sant Cugat del Vallès, amb cobertura proactiva, preventiva i reactiva.

Aquest servei haurà de cobrir les àrees clau de la ciberseguretat corporativa i garantir:

- Servei unificat de ciberseguretat, amb integració de telemetria provinent d'endpoints, xarxa, identitat, correu electrònic, sistemes i entorns al núvol, amb correlació contextual per a cada incident detectat.

- La solució proposada haurà de disposar d'una capacitat centralitzada per a la recol·lecció, anàlisi i correlació d'esdeveniments de seguretat procedents de múltiples fonts, amb gestió diferenciada de dades segons el seu ús operatiu. Concretament, es requerirà la gestió de:
  - Log calent, accessible en temps real per a detecció immediata d'incidents, investigació ràpida i resposta operativa contínua.
  - Log fred, orientat a l'emmagatzematge a llarg termini amb accés optimitzat per a anàlisi forense, seguiment històric, auditoria i compliment normatiu.

- Utilització d'intel·ligència artificial (IA) i aprenentatge automàtic (ML) per millorar la detecció primerenca d'amenaces, identificar comportaments anòmals i prioritzar alertes segons el risc real per a l'organització.

- Automatització de resposta a incidents mitjançant capacitats SOAR (Security Orchestration, Automation and Response), amb accions automatitzades o guiades per reduir temps de contenció i resolució.

- Integració amb el sistema corporatiu de ticketing per a la gestió completa i traçable dels incidents des del seu registre fins al tancament, amb assignació d'accions i seguiment integrat.

- Quadres de comandament personalitzables i exportables, amb visualització consolidada dels indicadors de seguretat, estat d'alertes, compliment normatiu i anàlisi de tendències.

- Detecció i anàlisi contínua de vulnerabilitats, amb verificació del compliment de polítiques de seguretat, proposta de mesures correctores i suport a la seva implantació.

- Contextualització de l'activitat digital, incorporant la visió dels usuaris, recursos, serveis i aplicacions per a una detecció més precisa i una reducció significativa de falsos positius.

- Monitoratge continu i en temps real dels esdeveniments de seguretat, amb capacitat de resposta 24/7 i cobertura de tot l'abast tecnològic de l'organització.

- Servei complet de resposta a incidents de ciberseguretat, incloent anàlisi forense, suport legal i tècnic, recuperació davant desastres i tractament post-incident.

- Emissió d'informes periòdics de seguretat, amb mètriques, estadístiques, evolució de les amenaces i recomanacions de millora adaptades.

- Informes tècnics específics per a cada incident, incloent traces de detecció, mesures aplicades i línies temporals, amb termini màxim de lliurament de 7 dies naturals.

- El servei haurà de complir amb el nivell mitjà de l'Esquema Nacional de Seguretat (ENS)

- El MSSP haurà de garantir una prestació eficaç, escalable i adaptada a l'evolució del risc, amb capacitat de suport estratègic i tècnic a la gestió de la ciberseguretat municipal.

En el cicle de vida de la prestació dels serveis implantats distingim tres fases:

- Fase 0: Transició del servei actual al MSSP
- Fase 1: Implantació, parametrització.
- Fase 2: Prestació dels serveis.
- Fase 3: Supervisió, Coordinació i Lliurament de Documentació
- Fase 4: Serveis a demanda

Fase 0: Transició del servei actual al MSSP

Amb l'objectiu de garantir una transició ordenada i sense interrupcions en la prestació dels serveis de ciberseguretat, es defineix una Fase 0 prèvia i vinculada a la Fase 1 (implantació). Aquesta fase es concep com a període de coexistència entre el servei actual (CUGAT-SOC) i el nou servei gestionat de seguretat (MSSP), amb la finalitat de disposar d'un punt de partida estable i verificat abans de la plena implantació.

Actualment, l'Ajuntament compta amb 129 casos d'ús (CdU) i 8 tipus de fonts d'informació (Active Directory, Servidors de fitxers, Office 365, Firewall, Xarxa sense fils, Endpoints, Seguretat web i Infraestructura de xarxa), desplegades en un total de 22 dispositius, amb una ingesta diària aproximada de 100 GB/dia de logs. La magnitud i la criticitat d'aquest entorn exigeixen una transició progressiva i controlada.

La planificació de la transició estableix uns mínims clars i obligatoris:

- Primer mes: ha d'estar implantat com a mínim el 50% de les fonts i CdU actuals, prioritzant els sistemes més crítics (Active Directory, Firewalls, Office 365, Endpoints i serveis de xarxa bàsics), amb validació de fluxos de logs i configuracions inicials.

- Segon mes: ha d'estar implantat el 100% de les fonts i CdU, completant la migració de totes les integracions i validant la correlació, els casos d'ús i la resposta a incidents.

És important destacar que la Fase 0 i la Fase 1 comparteixen període d'execució, ja que la transició i la implantació són processos interdependents. En aquest marc, les activitats de la Fase 0 constitueixen el fonament perquè la Fase 1 es pugui desplegar amb garanties. Per això, subfases com la Fase 1.1.1 (Gestió del risc i de la superfície d'atac), la Fase 1.1.2 (Índex del risc) i la Fase 1.1.3 (Valoració contínua del risc) s'han de desenvolupar en paral·lel a la transició, aprofitant la integració progressiva de fonts i CdU, de manera el servei gestionat de ciberseguretat (MSSP) pugui començar a generar visibilitat i indicadors de risc des del primer mes i disposar de la totalitat de la informació al finalitzar el segon mes.

Fase 1: Implantació, parametrització i explotació

L'objecte del present contracte és la contractació d'un Servei Gestionat de Seguretat que assumeixi de forma delegada, contínua i professional la gestió integral de la ciberseguretat de l'Ajuntament de Sant Cugat del Vallès.

El servei haurà de proporcionar una vigilància activa, proactiva i permanent (24x7) sobre els sistemes d'informació de l'organització, oferint capacitats avançades de detecció, anàlisi, resposta i prevenció d'incidents, així com la gestió de vulnerabilitats, el suport forense i el compliment normatiu vigent, especialment en el marc de l'Esquema Nacional de Seguretat (ENS).

El proveïdor haurà de disposar d'una infraestructura tecnològica pròpia, escalable i segura, amb capacitat per oferir:

- Monitoratge centralitzat d'esdeveniments de seguretat i gestió de logs, amb tractament de dades en calent i fred.

- Anàlisi avançada i correlació d'esdeveniments mitjançant sistemes intel·ligents.

- Resposta automatitzada i assistida a incidents de seguretat.

- Integració amb les eines de l'organització, especialment el sistema de ticketing corporatiu.

- Quadres de comandament, informes periòdics i indicadors de rendiment i risc.

- Servei de resposta davant d'incidents (CSIRT), suport forense (DFIR) i anàlisi de causes.

- Compliment amb els requeriments normatius aplicables.

Totes les comunicacions i materials derivats de la prestació hauran de complir els requisits lingüístics següents:

- **La documentació oficial** relacionada amb el servei (informes, manuals, procediments, memòries tècniques, etc.) s'haurà de lliurar obligatòriament en llengua catalana.

- **Les comunicacions urgents**, incloses les relatives a incidents de seguretat, actuacions sobrevingudes, alertes, notificacions crítiques o qualsevol acció immediata derivada del servei, hauran de dur-se a terme com a mínim en català o castellà, a elecció de l'organització, per garantir la comprensió i una resposta efectiva per part dels equips interns.

Aquest requisit és essencial per garantir l'operativitat i el correcte seguiment del servei dins del marc lingüístic i administratiu de l'organització.

Fase 1.1 – Servei unificat de Seguretat

Servei unificat de Seguretat de detecció i resposta gestionada en entorns complexos ha d'estar dissenyat per proporcionar una visió unificada, automatització intel·ligent i capacitat de resposta avançada davant amenaces. Aquesta solució ha de complir, com a mínim, els següents requisits generals:

- Model de servei en núvol (SaaS): El servei s'haurà de lliurar com a servei totalment gestionat.

- Residència de dades dins la Unió Europea: Tant la infraestructura com les dades associades han d'estar allotjades en centres de dades ubicats físicament dins del territori de la Unió Europea, garantint el compliment de la normativa aplicable en matèria de protecció de dades.

- Solució completa i integrada: El servei haurà d'incloure tots els mòduls i funcionalitats requerits de forma nativa i integrada, en la mesura que sigui possible.

- Gestió centralitzada: Totes les operacions de configuració, monitoratge i resposta s'hauran de poder realitzar des d'una d'administració accessible mitjançant navegador web.

- Control d'accés basat en rols (RBAC): El servei haurà d'oferir un sistema granular de permisos que permeti definir perfils d'accés diferenciats segons funcions i responsabilitats, garantint la traçabilitat i la separació de tasques.

- Propietat de les dades: Totes les dades generades, recollides, emmagatzemades o tractades durant la prestació del servei —incloent configuracions, casos d'ús, regles de correlació, informes, alertes, dashboards, scripts, automatitzacions i qualsevol altra informació resultant— seran propietat exclusiva de l'Ajuntament de Sant Cugat del Vallès.

- Accés permanent del responsable designat: El responsable que designi l'Ajuntament haurà de disposar, com a mínim, d'un accés permanent 24/7/365 en modalitat de lectura (read-only) a el servei i els seus components, amb la finalitat de garantir la transparència, seguiment i supervisió continuada del servei.

- Prohibició d'ús extern de la informació: L'empresa adjudicatària no podrà utilitzar, conservar, copiar ni transmetre les dades ni cap altra informació derivada del servei per a finalitats alienes al contracte, ni un cop finalitzada la seva vigència, excepte en el cas de requisits legals específics.

- Portabilitat i canvi de titularitat: La solució proposada haurà de garantir que, en cas de finalització del contracte, canvi d'adjudicatari o decisió de l'Ajuntament, es pugui realitzar la transferència completa del servei, les configuracions i totes les dades a un altre

proveïdor o a l'Ajuntament, sense restriccions tecnològiques ni dependències de l'empresa adjudicatària.

Aquest conjunt de requisits assegura que el servei compleixi amb els estàndards actuals en matèria de ciberseguretat, escalabilitat i governança operativa, facilitant una gestió eficient del servei de ciberseguretat gestionat (MSSP).

Fase 1.1.1 – Gestió del risc i de la superfície d'atac

El servei haurà d'incloure la gestió preventiva del risc i la identificació de la superfície d'atac de l'organització. Aquest ha de proporcionar una visió global i actualitzada dels actius exposats i del seu nivell de risc associat, facilitant així la presa de decisions estratègiques en matèria de ciberseguretat.

A tal efecte, es requereix que:

La solució no es basi exclusivament en la telemetria pròpia generada pels sensors de la seva arquitectura, sinó que també sigui capaç d'integrar-se amb altres plataformes i sistemes corporatius per enriquir l'anàlisi i obtenir una visió completa i contextualitzada.

El servei haurà de contemplar mecanismes per a la identificació contínua d'actius, vulnerabilitats i exposicions, així com la seva correlació amb riscos coneguts o potencials.

A continuació, es detallen les fonts mínimes amb les quals s'haurà de garantir la integració per a la recopilació i consolidació de dades de seguretat:

Fonts	Fabricant
Directori Actiu	Microsoft
EntraId	Microsoft
Servidor DNS	Microsoft
Servidor DHCP	Microsoft
Antivirus	Microsoft
Intune	Microsoft
Servidor de Correu on premise	Microsoft
Servidor de Correu cloud	Microsoft
Controladora Wifi	Ruckus
Switches Core	HP
Mòduls Firewall*	Checkpoint
NetScaler	Citrix
Servidores de fitxers	S.O Windows

*Els mòduls principals del Firewall son el següents: IPS, IDS, Anti-bot, Application Control, VPN, Firewall.

El proveïdor haurà d'acreditar la seva capacitat per integrar totes les fonts d'informació definides, així com prestar el servei corresponent, mitjançant la signatura d'un **acord de confidencialitat (NDA)** que garanteixi la protecció de la informació sensible gestionada.

L'emmagatzematge i la conservació dels logs recollits hauran de garantir una **retenció mínima de dos anys**, complint amb els requisits legals i operatius aplicables.

Així mateix, el servei haurà d'incloure:

La **definició i configuració d'un quadre de comandament** que permeti visualitzar i monitorar l'estat de totes les fonts d'informació integrades.

La **personalització i desenvolupament de casos d'ús específics**, incorporant mecanismes d'intel·ligència per a la detecció, correlació i resposta davant d'activitats anòmales o incidents de seguretat.

En finalitzar la fase d'instal·lació i desplegament de la solució, el proveïdor haurà de garantir **l'accés al servei** a l'equip tècnic de l'Ajuntament de Sant Cugat del Vallès, així com **la formació adequada sobre l'ús i administració de les eines implementades**.

Fase 1.1.2 - Índex del risc

La construcció de l'índex de risc a partir de diverses categories d'informació és essencial per obtenir una visió precisa, contextual i dinàmica de l'estat de seguretat de l'organització. Aquest enfocament multivariable permet identificar de forma més eficient els riscos reals que poden afectar diferents àrees, usuaris o serveis, i dona suport a la presa de decisions basada en l'impacte i la criticitat. A més, assegura que la resposta davant amenaces sigui proporcional i orientada a l'actiu més exposat o valuós, optimitzant els recursos del servei MSSP i millorant la detecció proactiva.

L'índex de risc s'haurà de construir tenint en compte, com a mínim, els aspectes següents, els quals permeten avaluar de manera integral l'estat de seguretat de la infraestructura, les configuracions i les activitats dels usuaris i dispositius:

- **Comptes compromesos:** La detecció de comptes que han estat filtrats, robats o utilitzats de forma sospitosa és clau per identificar vectors d'atac actius. Un compte comprom ès pot servir de porta d'entrada per a moviments laterals dins l'entorn i suposa un risc immediat per a la integritat de l'organització.

- **Detecció de vulnerabilitats:** Les vulnerabilitats no corregides en sistemes, aplicacions o dispositius constitueixen una de les principals vies d'explotació per part d'actors maliciosos. Incorporar aquesta informació en l'índex permet prioritzar la remediació segons l'impacte real.

- **Anàlisi de comportament:** L'ús d'eines de detecció basades en comportament permet identificar anomalies no detectables per signatures tradicionals. Activitat fora del patró habitual pot indicar un atac en curs, abús de privilegis o moviment lateral.

- **Activitat en aplicacions cloud:** L'ús massiu de serveis SaaS (com Teams, Exchange Online, SharePoint, etc.) ha desplaçat gran part de l'activitat fora del perímetre clàssic. Monitorar aquesta activitat és imprescindible per detectar exfiltracions, accessos sospitosos o comparticions indegudes.

- **Esdeveniments de detecció d'amenaces:** Incloure alertes generades per EDRs, firewalls, gateways o altres sensors permet quantificar l'activitat maliciosa real observada, assignant pes a indicadors de compromís que ja han estat detectats per la infraestructura defensiva.

- La integració amb **Microsoft Defender for Endpoint** és fonamental per tenir visibilitat precisa de l'estat real dels dispositius i dels seus riscos de configuració. L'índex de risc haurà d'incloure informació derivada de la seva anàlisi:

- **Configuracions de comptes errònies o insegures:** Ús de comptes amb privilegis innecessaris, comptes locals habilitats sense control o absència de MFA suposen riscos crònics que cal quantificar i mitigar.

- **Configuracions d'aplicacions errònies o insegures:** Aplicacions amb permisos excessius, execució automàtica o sense control de versions poden facilitar l'explotació remota o l'execució de codi maliciós.

- **Configuracions de xarxa errònies o insegures:** Connexions innecessàries a xarxes públiques, ports oberts, serveis sense xifrat o exposició de serveis interns incrementen la superfície d'atac.

- **Recursos o serveis de xarxa exposats o mal configurats:** La publicació involuntària de recursos interns o la falta de segmentació pot permetre moviments laterals o accés no autoritzat des de fora de l'organització.

- **Configuració insegura del sistema operatiu:** Manca de paràmetres de seguretat bàsics (com protecció de registre, xifrat, control d'accés, etc.) debilita la postura de seguretat global de la màquina.

- **Controls de seguretat absents o desactivats:** Endpoints amb antivirus o EDR desactivat, sense protecció de memòria, sense detecció en temps real o sense actualitzacions incrementen exponencialment el risc de compromís.

Fase 1.1.3 - Valoració contínua del risc

La solució proposada haurà d'incorporar la valoració contínua del risc cibernètic, basat en l'anàlisi de la telemetria recollida de múltiples vectors d'informació dins l'organització. Aquest haurà de ser capaç de calcular i actualitzar de manera dinàmica un índex de risc agregat i segmentat, permetent una visibilitat clara i accionable sobre l'exposició real de l'entorn digital de l'organització.

Concretament, la solució haurà de proporcionar quadres d'indicadors de risc diferenciats per als següents àmbits:

- Situació global de la ciberseguretat de l'organització, oferint una visió consolidada i estratègica de l'estat de risc en temps real.

- Anàlisi per unitats organitzatives o departaments, amb capacitat de segmentació segons estructura jeràrquica o funcional de l'Ajuntament.

- Risc associat a usuaris i identitats digitals, amb detecció de comportaments anòmals, accés sospitós o ús indegut de credencials.

- Avaluació específica dels dispositius, tant endpoints com dispositius mòbils i servidors, amb identificació d'actius vulnerables o no conformes.

- Aplicacions i serveis en ús, incloent el risc vinculat a aplicatius corporatius, serveis web i entorns SaaS, especialment en contextos híbrids.

- Serveis en el núvol (cloud), amb detecció de configuracions insegures, permisos excessius o accés no autoritzat en entorns de núvol públic o privat.

- L'índex de risc s'haurà de generar de manera dinàmica i contínua, actualitzant-se automàticament davant de qualsevol canvi en la telemetria o els esdeveniments capturats pels sensors desplegats en els diferents vectors d'amenaces (usuaris, dispositius, serveis, xarxes, aplicacions, etc.).

- L'algoritme utilitzat per al càlcul del risc haurà de ser transparent, documentat i accessible, per garantir la seva comprensió i validació per part dels equips tècnics.

- El sistema haurà de disposar d'un quadre de comandament visual que representi gràficament els indicadors de risc de manera clara i intuïtiva, amb capacitat de desglossament per àrees funcionals, unitats organitzatives o tipus d'actius.

- La solució haurà de permetre la generació automatitzada d'informes executius de risc, que incloguin l'evolució temporal del risc, la identificació d'actius crítics, recomanacions prioritzades i alertes destacades.

- El servei haurà de realitzar un perfilat automàtic dels actius monitoritzats, assignant a cadascun d'ells un valor de criticitat calculat segons el seu context operatiu, exposició, vulnerabilitats i impacte potencial. Aquest valor haurà de ser editables manualment per tal d'adaptar-se a criteris de priorització específics.

- Aquest índex de risc haurà d'estar correlacionat amb dades d'intel·ligència d'amenaces, models d'amenaça contextualitzats i historial d'incidents detectats, de forma que permeti establir prioritats d'actuació i automatitzar la resposta davant exposicions crítiques.

Fase 1.1.4 - Valoració actius

La solució haurà d'incloure funcionalitats avançades de visibilitat, anàlisi i gestió contextual dels actius, fonamentals per garantir un servei de ciberseguretat gestionat (MSSP) eficaç, proactiu i basat en intel·ligència. En concret, es requerirà:

- Inventari automàtic d'aplicacions locals instal·lades als dispositius de l'organització. Aquesta funcionalitat és clau per mantenir una visibilitat completa de l'entorn, identificar aplicacions obsoletes o no autoritzades, i avaluar el risc associat a cada una d'elles basant-se en vulnerabilitats conegudes (per exemple, a través de bases CVE públiques) i en la seva funcionalitat. La possibilitat de sancionar o restringir aplicacions de risc permet reduir la superfície d'atac i aplicar polítiques de seguretat més estrictes.

- Modelatge de relacions entre actius, incloent usuaris, dispositius, aplicacions i serveis. Aquesta capacitat és essencial per detectar anomalies en el comportament dels sistemes o de les identitats, identificant patrons que podrien indicar accions malicioses, moviments laterals o intents d'evasió dins la xarxa. Permet una detecció més precoç i contextualitzada de possibles amenaces.

- Visibilitat externa dels actius exposats a Internet. És imprescindible que la solució ofereixi mecanismes per analitzar la superfície d'exposició digital de l'organització, identificant dominis públics, serveis accessibles, certificats insegurs o vulnerabilitats explotables. Aquesta visibilitat facilita la detecció de riscos previs a un atac, permetent actuar amb caràcter preventiu abans que un adversari els exploti.

Aquest conjunt de funcionalitats aporta una visió holística de l'estat de seguretat de l'organització, millora la capacitat de resposta davant incidents i redueix el temps de detecció i mitigació. Així mateix, contribueix a prioritzar les accions de correcció basant-se en el risc real dels actius i el seu impacte potencial en el negoci.

AJUNTAMENT DE SantCugat

Plaça de la Vila, 1
08172 Sant Cugat del Vallès
T. 935 657 000
santcugat.cat

Fase 1.1.5 - Intel·ligència artificial

La solució haurà d'incorporar intel·ligència d'amenaces amb capacitat per recollir, analitzar i correlacionar informació procedent de fonts internes i externes, amb l'objectiu de millorar la detecció proactiva de ciberamenaces. Aquesta informació ha d'incloure indicadors de compromís, tàctiques, tècniques i procediments, vulnerabilitats crítiques, actors amenaçadors actius i campanyes en curs.

La solució haurà de fer ús de tecnologies d'intel·ligència artificial i aprenentatge automàtic per analitzar aquesta informació de manera automatitzada i intel·ligent, amb la finalitat de:

- Detectar activitats malicioses amb més rapidesa i precisió.
- Reduir els falsos positius, millorant l'eficiència operativa del servei de seguretat gestionat.
- Prioritzar els riscos segons el seu impacte i el context organitzatiu.
- Proposar accions de resposta i mitigació automatitzades.

Aquestes capacitats d'intel·ligència s'han d'integrar de manera nativa amb la resta de funcionalitats de la solució per enriquir alertes, adaptar polítiques de seguretat i alimentar casos d'ús de forma dinàmica.

Importància de la intel·ligència artificial en un servei de seguretat gestionat (MSSP):

L'ús de la intel·ligència artificial és fonamental per afrontar l'elevada quantitat de dades, la sofisticació dels atacs i la necessitat de resposta ràpida. L'IA permet passar d'un model de seguretat reactiu a un model predictiu i automatitzat, amb capacitat de detecció primerenca, anàlisi contextual i actuació immediata.

Predicció automatitzada del camí d'atac:

La solució haurà d'incloure la capacitat de predir de manera automàtica el camí d'atac més probable, analitzant les dades recopilades pels sensors i mecanismes de monitoratge. Aquest mòdul utilitzarà tècniques d'intel·ligència artificial per:

- Identificar el vector d'entrada més probable i la seva progressió interna dins l'entorn,
- Estimar la probabilitat d'execució de l'atac,
- I proposar de forma automatitzada les accions de contenció i remediació més efectives.

Aquesta funcionalitat incrementa la capacitat de resposta preventiva i contextual davant amenaces complexes, afavorint una gestió eficient del risc i una millor resiliència cibernètica.

Fase 1.1.6 – Compliment

La solució haurà d'incloure gestió del compliment normatiu, que permeti identificar les mancances en les configuracions de seguretat de l'organització i mesurar el grau d'adequació a marcs normatius i estàndards reconeguts. Aquest mòdul és clau per garantir una alineació proactiva amb les obligacions reguladores i per facilitar la presa de decisions en matèria de ciberseguretat i governança TIC.

Plaça de la Vila, 1
08172 Sant Cugat del Vallès
T. 935 657 000
santcugat.cat

Aquest mòdul haurà de complir, com a mínim, els següents requisits:

- **Identificació d'incompliments** i desviacions en la configuració dels sistemes respecte als requisits d'un marc normatiu concret, indicant-ne la criticitat i les accions de correcció suggerides.

- **Visualització del progrés cap al compliment**, mitjançant indicadors i gràfics que reflecteixin l'evolució de l'estat de conformitat al llarg del temps.

- **Generació d'informes automatitzats** alineats amb les principals normatives i estàndards de seguretat com a mínim amb ENS (Esquema Nacional de Seguretat).

- **Capacitat de definir marcs normatius personalitzats**, reutilitzant controls existents o definint-ne de nous segons les necessitats específiques del sector públic.

- **Integració amb la resta de les dades (*Fase 1.1 – Servei unificat de Seguretat*)**, per tal que les dades de configuració, detecció de vulnerabilitats i riscos alimentin el mòdul de compliment i permetin una supervisió unificada.

Aquesta gestió te com objectiu facilitar les auditories i reduir el risc de sancions o exposicions derivades d'incompliments, així com per consolidar un model de ciberseguretat orientat a la millora contínua i a la rendició de comptes.

Fase 2: Prestació dels serveis.

Aquest servei vindrà suportat pel personal adscrit al **Servei Gestionat de Seguretat** de l'adjudicatari. Els serveis de gestió de la seguretat inclouran les següents funcions:

- Monitorització de seguretat, detecció primerenca d'incidents i amenaces
- Detecció, anàlisi i gestió de vulnerabilitats
- Manteniment, revisió, administració i reporting de la infraestructura
- Gestió i resposta a incidents de seguretat de la informació (CSIRT)
- Interlocutor únic del proveïdor responsable de servei

Fase 2.1.- Monitorització de seguretat, detecció primerenca d'incidents i amenaces

El servei de monitoratge de seguretat es fonamenta en el servei unificat de seguretat, que actua com a eix central per a la recopilació, anàlisi i gestió dels esdeveniments de seguretat de tota la infraestructura tecnològica de l'Ajuntament de Sant Cugat del Vallès.

L'objectiu principal és garantir la detecció precoç i la resposta eficient davant qualsevol amenaça, violació o comportament anòmal, mitjançant l'anàlisi contínua dels logs, esdeveniments i alertes generats per les fonts d'informació integrades al servei.

Aquest servei de monitoratge haurà de complir, com a mínim, amb les condicions següents:

- Estar plenament integrat en servei de seguretat gestionada (MSSP), com a base per a la ingestió massiva, correlació i anàlisi d'esdeveniments en temps real.

- Realitzar la monitorització en modalitat 24x7x365, garantint la cobertura permanent i sense interrupcions de tot el conjunt de vectors de risc.

- Detecció, identificació, classificació i categorització automàtica dels incidents, amb recollida estructurada de totes les evidències necessàries per a la seva anàlisi posterior.

- Notificació immediata als responsables de l'Ajuntament per mitjans com correu electrònic, SMS o trucada, amb un resum inicial de l'incident detectat i la seva gravetat. El canal i la prioritat de notificació es determinaran segons el nivell de criticitat i impacte.

- Correlació intel·ligent d'esdeveniments i anàlisi avançada que consideri totes les fonts d'informació disponibles, per facilitar la contenció, remediació i recuperació d'actius afectats, així com per valorar l'impacte en serveis compromesos o dependents.

- Proposta i execució de protocols de resposta a incidents, amb plans de mitigació i remediació dissenyats conjuntament amb l'Ajuntament.

- Automatització de respostes davant incidents mitjançant accions predefinides (playbooks), amb execució ràpida de mesures de bloqueig i contenció per a determinades alertes validades.

- Obertura automàtica de tiquets per a la gestió dels incidents, amb integració amb la solució de gestió de tiquets utilitzada per l'Ajuntament.

- Capacitats d'orquestració i automatització de respostes (SOAR) sobre les principals tecnologies de seguretat integrades al servei.

- Resposta automatitzada i manual en horari 24/7, amb accions de remediació davant infeccions, accessos no autoritzats o compromisos detectats.

- Incorporació de fonts d'indicadors de compromís (IoC) provinents de repositoris públics, privats i propis de l'adjudicatari.

- Coordinació de la resposta a incidents: manteniment actiu del cas fins al seu tancament complet, amb participació directa de l'equip tècnic de l'adjudicatari, incloent el desplaçament físic si és necessari, assumit dins del servei ofert.

Aquest servei haurà d'estar alineat amb els requeriments funcionals i tècnics establerts prèviament pel servei, garantint una visió centralitzada, integradora i intel·ligent del panorama de seguretat de l'Ajuntament.

Fase 2.2 – Detecció, anàlisi i gestió de vulnerabilitats

Amb l'objectiu de disposar d'una visibilitat completa sobre l'estat de seguretat dels sistemes i garantir un tractament eficaç del cicle de vida de les vulnerabilitats, la solució proposada haurà d'incloure un mecanisme integrat per a la detecció proactiva, anàlisi, gestió i seguiment de vulnerabilitats en els sistemes i serveis de l'Ajuntament de Sant Cugat del Vallès.

Aquest mecanisme ha de complir amb els següents requisits mínims:

- Identificació automatitzada de vulnerabilitats: El sistema haurà de realitzar escanejos recurrents i sistemàtics utilitzant eines especialitzades proporcionades per l'adjudicatari per a detectar vulnerabilitats conegudes i potencials en infraestructures, dispositius, aplicacions i serveis cloud.

- Classificació i priorització intel·ligent: Les vulnerabilitats detectades s'hauran de categoritzar segons el seu nivell de criticitat, impacte i risc associat, incorporant informació actualitzada sobre amenaces (Threat Intelligence).

- Filtratge de falsos positius: La solució haurà de disposar de mecanismes per a validar i eliminar automàticament o manualment les deteccions errònies, per tal d'evitar la dedicació de recursos innecessaris.

- Definició i execució de protocols de resposta: S'hauran d'establir i aplicar accions correctives o preventives per a la mitigació de vulnerabilitats, que podran ser executades manualment o de forma automatitzada mitjançant playbooks dins el servei.

- Seguiment i verificació de mesures aplicades: La solució haurà de permetre fer un control exhaustiu del desplegament i efectivitat de les accions correctives, verificant que les vulnerabilitats han estat resoltes completament.

- Traçabilitat i informes: S'haurà de generar un registre complet del cicle de vida de cada vulnerabilitat, incloent-hi data de detecció, responsable, accions aplicades i estat final, així com informes periòdics sobre l'evolució i tancament de vulnerabilitats.

Aquest procés ha d'estar totalment integrat dins del serve de gestió de seguretat (MSSP) i formar part de les capacitats bàsiques de detecció i resposta contínua del servei.

Fase 2.2.1 – Mesures Avançades de Detecció, Simulació i Avaluació de Riscos

Amb l'objectiu de reforçar la postura de ciberseguretat de l'Ajuntament de Sant Cugat del Vallès, el servei haurà d'incloure un conjunt d'actuacions proactives i avançades que permetin la detecció precoç d'amenaces, l'avaluació contínua del nivell d'exposició i la capacitació dels usuaris. Aquestes actuacions hauran d'incloure, com a mínim, els següents serveis:

- **Cerca proactiva d'amenaces (Threat Hunting):** Activitats orientades a la detecció d'activitats anòmales o malicioses a través de tècniques d'anàlisi de comportament, telemetria i informació contextualitzada. Aquesta pràctica permet identificar atacs avançats que poden passar desapercebuts pels sistemes tradicionals.

- **Intel·ligència d'amenaces (Threat Intelligence):** Recollida, anàlisi i aplicació d'informació sobre indicadors de compromís (IOC – Indicadors de Compromís), tècniques, tàctiques i procediments (TTP) emprats per actors d'amenaça. Aquesta informació ha d'estar integrat al servei per millorar les capacitats de detecció i resposta.

- **Simulacres de phishing:** Es duran a terme dos simulacres anuals adreçats al personal de l'Ajuntament, amb l'objectiu de conscienciar i avaluar la resposta davant intents de suplantació d'identitat. Les campanyes han d'incloure escenaris reals, informes de resultats i propostes de millora o formació específica.

- **Proves d'intrusió controlades (Pentestings):** Es realitzaran com a mínim dues proves anuals: una prova externa (dirigida a serveis o sistemes exposats públicament a Internet) i una prova interna (orientada a identificar vulnerabilitats dins de la xarxa corporativa i serveis interns). Els resultats han de ser presentats en un informe amb evidències, avaluació de risc i mesures correctores recomanades.

- **Escaneig de vulnerabilitats perimetrals i d'entorns interns:** Realització periòdica d'anàlisis tècniques sobre actius exposats a Internet i sistemes interns per identificar vulnerabilitats, serveis en risc, configuracions insegures o programari obsolet. Aquests escaneigs han d'integrar-se amb les eines de gestió de vulnerabilitats del servei per mantenir un control actualitzat de la superfície d'atac.

AJUNTAMENT DE SantCugat

Plaça de la Vila, 1
08172 Sant Cugat del Vallès
T. 935 657 000
santcugat.cat

Fase 2.3 – Resposta incidents

La necessitat d'un servei de resposta a incidents (Incident Response) és fonamental dins d'un servei MSSP (Servei Gestionat de Seguretat) per les raons següents:

- **Contenció i mitigació ràpida d'amenaces:** Quan es produeix un incident de seguretat, una resposta immediata i estructurada és clau per evitar-ne l'expansió i reduir l'impacte sobre els sistemes i la informació.

- **Reducció de danys i temps d'inactivitat:** Un bon servei de resposta permet recuperar l'activitat normal en el menor temps possible, minimitzant les pèrdues econòmiques i operatives.

- **Anàlisi i comprensió de l'incident:** Identificar l'origen, el vector d'atac i els sistemes afectats és essencial per aplicar mesures correctives i evitar que es repeteixi.

- **Compliment normatiu i legal:** L'ENS (Esquema Nacional de Seguretat), el RGPD i altres normatives exigeixen la gestió adequada dels incidents i, en molts casos, la seva notificació en un termini concret.

- **Documentació i millora contínua:** La resposta a incidents genera informes i evidències útils per a auditories, assegurances cibernètiques i per millorar el pla de seguretat global de l'organització.

La solució haurà de permetre l'execució d'accions de resposta, tant **manuals com automatitzades**, en funció de l'índex de risc associat a usuaris, equips, aplicacions o serveis. Aquestes accions hauran d'implementar-se mitjançant playbooks dins d'un entorn amb capacitats **SOAR (Orquestració, Automatització i Resposta en Seguretat).**

Totes les accions de resposta **hauran d'estar integrades obligatòriament amb les eines actualment en ús a l'organització**, garantint-ne la compatibilitat, la continuïtat operativa i el respecte a les polítiques de seguretat vigents. En particular:

- **L'EDR corporatiu és Microsoft Defender**, i totes les accions sobre equips i dispositius (com l'aïllament, bloqueig, quarantena o recollida de proves) s'hauran de realitzar mitjançant la seva API o mitjans oficials.

- Servei de detecció i resposta gestionada (MDR), principalment sobre el EDR actual de l'Ajuntament de Sant Cugat, realitzant les següents tasques:

    - **Monitorització (Threat intelligence):** Validació de alertes, neteja de falsos positius, anàlisis, normalització i contextualització de tots el registres.
    - **Investigació (Threat hunting):** procés de cerca proactiva a través de les xarxes per a detectar i aïllar amenaces avançades capaces d'evadir les solucions de seguretat. La investigació de cerca de activitat sospitosa, més basada en el comportament i nebulosa, no basada en alertes o esdeveniment desencadenat, mirar a través de l'entorn i buscar proactivament patrons d'atac i crear regles.
    - **Resposta (24/7):** presa de mesures automàtiques de forma proactiva com remediació d'un atac, infecció, accés no autoritzat.

- **La gestió d'identitats es realitza mitjançant Microsoft Entra ID**, i per tant, qualsevol acció relacionada amb l'activació, desactivació, revocació d'accessos o aplicació de polítiques condicionals haurà d'integrar-se amb aquest sistema.

Igualment, les integracions amb **l'eina de ticketing** i altres sistemes corporatius han d'estar contemplades per permetre una automatització completa del flux de treball.

AJUNTAMENT DE SantCugat

Plaça de la Vila, 1
08172 Sant Cugat del Vallès
T. 935 657 000
santcugat.cat

El licitador haurà de:

- **Integrar i automatitzar els casos d'ús actuals de seguretat** dins la nova solució, i proposar l'automatització de tots aquells que tècnicament sigui viable.
- **Evolucionar i ampliar proactivament els playbooks** al llarg del servei, afegint noves automatitzacions segons els nous vectors de risc o canvis en l'entorn tecnològic.
- Establir un **procés col·laboratiu de validació amb el responsable de seguretat de l'organització**, per prioritzar i afinar les automatitzacions.

A tall d'exemple, com a mínim la solució proposada haurà de permetre:

- Aïllament automatitzat de dispositius mitjançant Microsoft Defender.
- Bloqueig o deshabilitació d'identitats en Entra ID.
- Notificació i registre automàtic d'incidents a l'eina de ticketing.
- Quarentena i anàlisi de fitxers maliciosos.
- Aplicació automatitzada de polítiques segons el nivell de risc.

Aquest enfocament garanteix una resposta coordinada, ràpida i basada en la infraestructura tecnològica real de l'Ajuntament, millorant la capacitat operativa del servei MSSP i reforçant la postura de seguretat global.

En aquells casos en què no sigui tècnicament possible automatitzar determinades accions de resposta davant incidents de seguretat, l'empresa adjudicatària haurà d'assumir la responsabilitat d'executar manualment les accions de mitigació corresponents directament sobre la plataforma o entorn afectat.

Amb l'objectiu de garantir la continuïtat del servei de ciberseguretat gestionada i una resposta ràpida i efectiva davant d'amenaces, l'organització proporcionarà a l'adjudicatari tots els accessos i permisos necessaris per realitzar aquestes tasques en condicions de seguretat i traçabilitat.

Aquesta obligació assegura que, fins i tot en absència d'orquestració automàtica mitjançant eines de resposta (SOAR), es pugui garantir la contenció i resolució de l'incident en els terminis establerts, mantenint els estàndards de qualitat i compromís del servei MSSP.

Fase 2.3.1 – Resposta especialitzada davant d'incidents greus de seguretat de la informació (CSIRT)

En cas de patir un incident greu de seguretat, l'Ajuntament de Sant Cugat del Vallès requereix d'un Equip de Resposta a Incidents de Seguretat de la Informació (CSIRT) especialitzat que proporcioni el suport i l'experiència necessària per a l'anàlisi, la contenció i la remediació d'atacs dirigits contra l'organització, amb l'objectiu de minimitzar el seu impacte operatiu i reputacional.

Aquest servei haurà de prestar-se en modalitat 24x7x365, garantint una resposta immediata davant situacions de crisi. L'equip tècnic haurà d'estar capacitat per actuar davant d'incidents com ara infeccions per ransomware, exfiltració de dades, intrusions, compromís d'identitats o altres ciberatacs avançats.

Plaça de la Vila, 1
08172 Sant Cugat del Vallès
T. 935 657 000
santcugat.cat

El servei s'ha d'integrar plenament dins l'estructura i fluxos de treball del servei MSSP (Proveïdor de Serveis de Seguretat Gestionada), aprofitant les dades i alertes recollides del servei unificat de seguretat, i activant els protocols de resposta segons el nivell de criticitat detectat.

El servei haurà de disposar, com a mínim, de les característiques següents:

- Investigació tècnica i anàlisi forense: validació de l'incident, extracció i conservació d'evidències, i anàlisi detallada de vectors d'entrada, tècniques d'ofuscació, propagació i exfiltració utilitzades per l'atacant.

- Obtenció d'indicadors de compromís (IOC – Indicadors de Compromís): recopilació i catalogació de dominis, IPs, fitxers, hashes, URLs i altres elements relacionats amb l'atac detectat.

- Identificació de l'abast de l'incident: detecció d'actius compromesos, moviments laterals, escalada de privilegis i persistències actives.

- Contextualització de l'amenaça: utilització de fonts d'intel·ligència del proveïdor per complementar la informació forense i entendre la motivació, objectiu i capacitat de l'atacant.

- Coordinació amb l'Ajuntament: comunicació directa i fluida amb els responsables tècnics municipals durant tot el cicle de resposta, des de la detecció fins al tancament formal de l'incident.

- Execució de mesures de contenció i remediació: suport actiu en la implantació de contramesures, recuperació d'actius, eliminació de persistències i restauració de serveis.

- Seguiment post-incident: monitoratge de l'entorn afectat per verificar que no es produeixin reinfeccions ni noves activitats anòmales.

- Resposta estructurada a incidents greus: guiatge en les decisions clau durant l'incident, documentació detallada de totes les accions i suport en comunicacions internes o externes si escau.

- Actuacions específiques davant l'incident: identificació del codi maliciós, objectiu de l'atac, tècniques utilitzades i recursos exposats, així com recomanacions específiques per bloquejar o aïllar les fonts d'amenaça.

La metodologia per la gestió i resposta als incidents de seguretat, haurà de ser en compliment del CCN-CERT, d'acord amb l'Esquema Nacional de Seguretat (ENS) i que esta referenciada en les guies CCN-STIC-403 i CCN-STIC-817.

Fase 2.3.2 - Classificació

Tots els incidents de seguretat detectats hauran de ser classificats de manera estructurada, segons el seu nivell de gravetat, abast i impacte sobre la infraestructura tecnològica, les dades i els serveis essencials de l'Ajuntament de Sant Cugat del Vallès.

Aquesta classificació permetrà establir la priorització en la resposta, l'activació de protocols específics i la notificació corresponent als responsables municipals.

Per tal d'establir la gravetat i la prioritat de resposta davant d'un incident de seguretat, s'estableix la següent matriu de classificació, que combina dues dimensions:

AJUNTAMENT DE SantCugat

Plaça de la Vila, 1
08172 Sant Cugat del Vallès
T. 935 657 000
santcugat.cat

- Impacte: grau de severitat de l'incident en termes de pèrdua de dades, afectació reputacional, compromís legal o tecnològic.

- Afectació: extensió o abast de l'incident dins l'organització (nombre d'usuaris, serveis, sistemes o dades afectades).

Matriu de classificació d'incidents:

		IMPACTE		
		Baixa	Mitja	Alta
AFECTACIÓ	Baixa	Molt baixa	Baixa	Mitja
	Mitja	Baixa	Mitja	Alta
	Alta	Mitja	Alta	Molt Alta

- **MOLT ALTA / ALTA:** Incidents amb un impacte elevat i una afectació significativa o generalitzada, que poden provocar degradació greu o pèrdua de serveis crítics, compromís de dades personals, infeccions greus, exfiltració de dades o incompliment normatiu greu. Requereixen actuació immediata i coordinació prioritària.

- **MITJANA:** Incidents rellevants amb impacte potencialment significatiu, però sense afectació directa a serveis essencials o dades sensibles. Requereixen gestió en un termini breu, amb anàlisi completa i accions correctives planificades.

- **BAIXA:** Incidents menors, com anomalies puntuals, intents d'intrusió sense èxit, errors de configuració sense explotació aparent o deteccions automatitzades sense impacte real. Es gestionen segons disponibilitat, i poden servir per millorar controls o alertes preventives.

		Temps de resposta		
		Criticitat alta	Criticitat mitja	Criticitat baixa
Descripció	Resposta d'incident	1h	4h	16h
	Anàlisis incidents criticitat alta	4h	8h	48h
	Informe incident criticitat alta	8h des de el tancament incident	48h des de el tancament incident	72h des de el tancament incident

Descripció	Temps de resposta
Intervenció in-situ	< 4h
Informe bretxa de seguretat	40h després de donar resposta

AJUNTAMENT DE SantCugat

Plaça de la Vila, 1
08172 Sant Cugat del Vallès
T. 935 657 000
santcugat.cat

L'adjudicatari haurà d'establir un sistema de control i seguiment basat en Indicadors Clau de Rendiment (KPI) que permetin a l'Ajuntament de Sant Cugat del Vallès avaluar de manera objectiva la qualitat i l'eficàcia dels serveis prestats.

Aquests KPI han de cobrir, com a mínim, els següents àmbits:

- Temps mitjà de detecció d'incidents (MTTD)
- Temps mitjà de resposta a incidents (MTTR)
- Nombre d'incidents resolts dins dels SLA acordats
- Nombre de falsos positius descartats
- Nombre de vulnerabilitats detectades i resoltes
- Compliment dels terminis de lliurament dels informes
- Grau d'automatització de processos de resposta i millores implantades

Els valors d'aquests indicadors s'hauran d'incloure a la memòria anual, a l'informe mensual i a les reunions de seguiment *(Fase 3 – Supervisió, Coordinació i Lliurament de Documentació)*, on es revisarà conjuntament el seu compliment, evolució i possibles accions correctores. Aquest seguiment permetrà una avaluació contínua del servei i facilitarà la presa de decisions informades sobre l'evolució i adaptació del servei MSSP.

Fase 2.4.- Interlocutor únic del proveïdor responsable de servei

L'Ajuntament de Sant Cugat del Vallès requereix que l'empresa adjudicatària designi un coordinador tècnic altament qualificat, en serveis gestionats de ciberseguretat (MSSP), que actuarà com a interlocutor únic i responsable global del servei objecte d'aquesta licitació.

Aquest perfil haurà de comptar amb coneixements tècnics avançats en àmbits com SIEM, EDR, SOAR, detecció i resposta davant incidents, gestió de vulnerabilitats, compliment normatiu i governança de la seguretat. Haurà de tenir capacitat per liderar equips multidisciplinaris, facilitar la presa de decisions estratègiques i garantir el correcte desplegament, operació i evolució dels serveis contractats.

Obligacions i tasques mínimes del coordinador tècnic:

- Ser l'interlocutor principal del servei davant el responsable designat per l'Ajuntament de Sant Cugat, exercint la gestió, coordinació i comunicació contínua de qualsevol aspecte relacionat amb la prestació del servei.
- Establir, amb l'aprovació de l'Ajuntament, reunions de seguiment periòdiques setmanals, amb una cadència pactada amb el responsable del contracte.
- En cas d'incidents greus de seguretat, es convocaran reunions extraordinàries d'urgència amb periodicitat acordada fins a la seva resolució.
- En un termini màxim de 48 hores després del tancament d'un incident, s'haurà de dur a terme una reunió de revisió i anàlisi dels informes proporcionats, amb l'objectiu d'extraure conclusions i propostes de millora.

- Les reunions de seguiment es podran realitzar en format telemàtic, a excepció dels següents casos, en què es requerirà la seva realització de forma presencial:
    - Entrega de la memòria anual del servei
    - Seguiment trimestral del servei
    - Quan així ho sol·liciti explícitament l'Ajuntament de Sant Cugat
- Ser el responsable de revisar els informes generats pels serveis prestats i, si escau, proposar millores o mesures correctives.
- Exercir la centralització de les peticions i comunicacions de forma bidireccional entre l'Ajuntament i l'empresa adjudicatària, canalitzant i prioritzant adequadament totes les sol·licituds.
- Conèixer i aplicar els principis, metodologies i pràctiques de la seguretat informàtica, i integrar-los dins d'un enfocament estratègic alineat amb els objectius i la visió del consistori.
- Ser el responsable directe de la provisió, operació i qualitat dels serveis contractats, així com de la seva evolució i adaptació a les necessitats de l'organització.
- Gestionar, planificar i coordinar tots els serveis de ciberseguretat per optimitzar-ne el funcionament i garantir el compliment dels nivells de servei acordats (SLA), vetllant especialment per la correcta gestió dels incidents i la seva resolució eficient.
- Dirigir la gestió dels canvis i vetllar perquè la prestació del servei sigui òptima, fent seguiment del control de qualitat, el compliment d'acords i el reporting continuat cap a l'Ajuntament.
- Proporcionar assessorament en millors pràctiques i recomanacions relacionades amb la seguretat de la informació, la seva confidencialitat, integritat i disponibilitat, així com en aspectes relacionats amb la continuïtat dels serveis.
- Coordinar i fer seguiment de totes les fases del servei descrites en aquest plec tècnic, assegurant la seva correcta execució i evolució.

El coordinador tècnic designat per l'empresa adjudicatària haurà de tenir una actitud clarament proactiva en la gestió del servei. Aquesta figura no només haurà de vetllar pel correcte funcionament del servei contractat, sinó que també haurà d'impulsar de manera contínua propostes de millora, optimització i evolució dels serveis de seguretat.

A tal efecte, serà responsabilitat del coordinador:

- Detectar oportunitats de millora tècnica o operativa, a partir de l'anàlisi de resultats, incidents o evolució tecnològica.
- Proposar noves funcionalitats, automatitzacions o mòduls complementaris que puguin reforçar la postura de ciberseguretat de l'Ajuntament de Sant Cugat.
- Presentar iniciatives de valor afegit basades en les necessitats específiques del consistori, tendències del sector o detecció de noves amenaces.
- Garantir l'actualització contínua del servei, tant a nivell funcional com d'adequació normativa o tecnològica.

AJUNTAMENT DE SantCugat

Plaça de la Vila, 1
08172 Sant Cugat del Vallès
T. 935 657 000
santcugat.cat

Aquestes propostes hauran de ser avaluades conjuntament amb els responsables de l'Ajuntament, i s'incorporaran al servei mitjançant un pla de millora o roadmap acordat entre les parts.

En els casos en què una incidència o situació derivada del servei requereixi la intervenció d'un altre grup resolutor o proveïdor extern, serà obligatori que el interlocutor únic designat per l'adjudicatari realitzi un seguiment actiu i continuat de la resolució de la incidència.

Aquest seguiment haurà de realitzar-se de manera coordinada i en col·laboració directa amb el responsable designat per l'Ajuntament de Sant Cugat del Vallès, amb l'objectiu de garantir que la incidència es resol de forma adequada, dins dels terminis establerts i amb la traçabilitat i documentació necessàries.

El interlocutor únic serà responsable de:

- Mantenir la comunicació fluïda amb el grup resolutor extern.
- Coordinar les accions de resposta o aportació d'informació per part del servei MSSP.
- Assegurar que l'Ajuntament rep informació actualitzada sobre l'estat de la incidència.
- Vetllar perquè l'impacte als serveis municipals sigui el mínim possible.

La capacitat d'aportar millores innovadores i útils serà un element clau per a la consolidació d'un servei de ciberseguretat eficient, resilient i alineat amb l'evolució de les necessitats de l'organització.

Per la seva importància estratègica dins del servei, el coordinador tècnic haurà de disposar de disponibilitat alta (24/7) i estar accessible en tot moment sempre que sigui necessari per atendre qualsevol situació objecte de la licitació, inclosa la gestió d'incidents, seguiment de tasques o coordinació operativa.

Cap perfil tècnic assignat al servei podrà ser substituït sense un preavís:

- En el cas del coordinador tècnic, el període de preavís haurà de ser mínim de 3 mesos, i el canvi haurà de ser aprovat explícitament pel responsable del contracte.
- En el cas dels altres perfils assignats al servei, el preavís serà mínim d'un mes, i qualsevol canvi també haurà de ser aprovat expressament per part del responsable de l'Ajuntament de Sant Cugat, el qual podrà rebutjar la proposta de substitució si així ho considera justificat.

Els terminis d'acord de servei (SLA) per part del interlocutor únic, hauran de ser acordats i validats per el cap de projecte assignat per l'Ajuntament de Sant Cugat i mai podran superar els temps establerts en la següent taula.

	Resposta	Resolució	Consultes
CRITIC	30 min	4h	2d
ALT	30 min	8h	3d
MIG-BAIX	30 min	48h	3d

L'Ajuntament podrà requerir que es justifiqui l'experiència i qualificacions d'aquest perfil, i en cas necessari, demanar-ne la substitució si no compleix els estàndards esperats.

Fase 3 – Supervisió, Coordinació i Lliurament de Documentació

Tots els informes detallats a continuació hauran de ser presentats i explicats durant les reunions de seguiment periòdiques o, si escau, en reunions extraordinàries convocades per incidents o situacions crítiques. Aquestes reunions seran liderades per la figura de l'interlocutor únic designat per l'adjudicatari, amb capacitat tècnica per supervisar, justificar i proposar accions derivades del contingut dels informes, garantint així la transparència i l'alineament amb els objectius de seguretat de l'Ajuntament de Sant Cugat del Vallès.

Els documents a lliurar inclouen:

- **Protocols d'actuació davant alertes de seguretat**: Derivats del funcionament habitual del sistema de gestió centralitzada de la seguretat i l'experiència de l'adjudicatari, es definiran els nivells de gravetat de les alertes i els protocols d'actuació corresponents, incloent accions de resposta automatitzades o manuals.

- **Informe d'incident:** Davant d'un incident greu, s'haurà de lliurar en un termini màxim de 48 hores un informe inicial amb la descripció, afectació (objecte o servei afectat, temps d'afectació, etc.), antecedents, causa arrel, accions realitzades i mesures de contenció. Posteriorment, en un termini màxim de 7 dies naturals, s'haurà de lliurar l'informe complet detallat.

- **Informe de vulnerabilitats**: Lliurament setmanal d'un informe amb totes les vulnerabilitats detectades i corregides, incloent evidències tècniques, valoració d'impacte (confidencialitat, integritat i disponibilitat) i, en cas de no correcció, recomanacions concretes per a la seva resolució.

- **Informe d'estat dels sistemes i equipaments:** Document periòdic que reflecteixi l'estat actual de seguretat dels actius administrats, nombre i detall d'incidents, peticions obertes, alertes registrades, així com el grau de disponibilitat dels equips.

- **Informe mensual d'incidents**: Resum mensual dels incidents gestionats, amb classificació per criticitat, origen, temps de resposta, accions de remediació i evolució de tendències.

- **Memòria trimestral:** Essencial per garantir un seguiment sistemàtic i documentat del servei MSSP, permetent a l'organització avaluar l'estat de la seguretat, l'evolució de les amenaces i el compliment dels compromisos establerts. A més, facilita la detecció precoç de possibles desviacions en la prestació del servei i possibilita l'adopció de mesures correctores de manera proactiva per assegurar-ne l'eficiència i la qualitat continuada.

- **Memòria anual del servei**: Document que resumeixi l'activitat realitzada durant l'any natural anterior, amb indicadors clau de rendiment (KPI), estat dels serveis, evolució dels incidents, grau de compliment dels objectius de seguretat, recomanacions de millora i propostes de valor afegit.

- **Pla de seguretat**: Document estratègic que estableixi la planificació de millores i accions correctores, reforços de mesures de seguretat, avaluació de riscos i línies d'evolució a curt i mitjà termini en base a les necessitats detectades durant la prestació del servei.

- **Informes sota demanda:** L'Ajuntament podrà sol·licitar en qualsevol moment informes addicionals que es considerin necessaris per al control, auditoria o suport en la presa de decisions en matèria de ciberseguretat. L'adjudicatari haurà de lliurar-los en un termini raonable, pactat prèviament segons l'abast i urgència.

AJUNTAMENT DE SantCugat

Plaça de la Vila, 1
08172 Sant Cugat del Vallès
T. 935 657 000
santcugat.cat

Tots aquests informes hauran de ser lliurats en llengua catalana i hauran d'estar disponibles per a la seva consulta en qualsevol moment mitjançant el sistema de gestió establert.

Fase 4 - Serveis a demanda

L'Ajuntament de Sant Cugat del Vallès estima la necessitat de disposar d'una bossa flexible de jornades tècniques, amb l'objectiu de donar resposta a serveis o actuacions no previstes inicialment en la licitació, però que puguin sorgir al llarg de l'execució del contracte com a part de l'evolució natural de les necessitats en matèria de seguretat de la informació.

A aquest efecte, es disposarà de 100 hores/any, que podran ser utilitzades per a la provisió de tasques generals relacionades amb la seguretat, com per exemple:

- Suport puntual en anàlisis tècnics específics o revisions de seguretat.
- Implementació de mesures de millora no previstes inicialment.
- Suport en activitats d'auditoria, proves de penetració o simulacres.
- Formació o assessorament especialitzat a demanda.
- Acompanyament tècnic en projectes o processos d'adequació normativa.
- Desenvolupament de nous casos d'ús o automatitzacions dins el servei MSSP.
- Qualsevol necessitat sobrevinguda en el servei no contemplada com objecte de la licitació

Aquestes jornades no tenen una destinació preassignada i s'activaran sota demanda, sempre amb validació prèvia del responsable tècnic de l'Ajuntament de Sant Cugat.

S'haurà de complir els següents acords de terminis de servei:

	Criticitat alta	Criticitat mitja	Criticitat baixa
Temps de resposta	24h	3d	5d
Temps de execució	48h	5d	10d

Les jornades no consumides durant l'any natural seran acumulables i podran ser utilitzades durant el següent període contractual, incloent-hi tant l'anualitat inicial com les futures pròrrogues del contracte, garantint així la màxima flexibilitat i adaptabilitat del servei a l'evolució de les necessitats de seguretat.

Tercer. Acta d'inici de prestació del servei

Una vegada formalitzat el contracte en document administratiu, s'haurà d'estendre l'acta d'inici de prestació del servei, per triplicat exemplar, que serà signada pel legal representant de l'empresa i el responsable del contracte. Aquest haurà de remetre un dels exemplars a la Secció de Contractació i Compres per a la seva incorporació a l'expedient.

AJUNTAMENT DE SantCugat

Plaça de la Vila, 1
08172 Sant Cugat del Vallès
T. 935 657 000
santcugat.cat

Quart. Entrega dels treballs i/o realització dels serveis

El contractista haurà d'entregar els treballs realitzats dins del termini estipulat en el contracte; el responsable del contracte efectuarà l'examen de la documentació presentada i, si estimés complides les prescripcions tècniques i restants condicions contractuals, proposarà que es porti a terme la seva recepció.

En el cas que estimés incomplides les prescripcions tècniques del contracte, donarà per escrit al contractista les instruccions precises i detallades amb la finalitat d'esmenar les faltes o defectes observats, fent constar en l'esmentat escrit el termini per efectuar les esmenes i les observacions que estimi oportunes.

En cas de reclamació per part del contractista respecte de les observacions formulades, el responsable del contracte l'elevarà, amb el seu informe, a l'òrgan de contractació per a la seva resolució.
Si el contractista no reclamés per escrit respecte a les observacions del responsable del contracte, s'entendrà la seva conformitat quedant obligat a corregir o esmenar els defectes detectats.

En serveis de prestació continuada, el plec de clàusules administratives podrà establir altres formes de constatar la correcta execució dels serveis prestats.

Cinquè. Recepció dels treballs i serveis

Quan la prestació s'ajusti a les condicions del contracte procedirà la seva recepció i s'estendrà l'acta corresponent que serà signada pel responsable del contracte i el representant legal del contractista.

Si la prestació no fos ajustada a les condicions necessàries per procedir a la seva recepció es donaran per escrit les instruccions oportunes al contractista a fi que esmeni els defectes observats i acompleixi les seves obligacions en el termini que per això es fixi; no procedirà la recepció fins que les instruccions hagin estat complimentades, estenent-se llavors l'acta corresponent.

En serveis de prestació continuada, el plec de clàusules administratives podrà preveure altres formes de recepció.

L'acta de recepció serà estesa per triplicat exemplar, un dels quals serà incorporat a l'expedient de contractació.

Sisè. Obligacions en matèria de prevenció de riscos laborals

1. El contractista està obligat al compliment de la Llei 31/1995, de 8 de novembre, de Prevenció de Riscos Laborals i restant legislació general i sectorial aplicable en aquesta matèria respecte dels treballadors adscrits a la contracta.

2. En el supòsit de concurrència de treballadors del contractista amb altres treballadors en un centre de treball municipal, l'Ajuntament vetllarà pel compliment de la normativa de prevenció de riscos laborals per part de les empreses que presten serveis corresponents a la pròpia activitat en els termes establerts pel RD 171/2004, de 30 de gener, pel qual es desenvolupa l'art. 24 de Llei 31/1995, de 8 de novembre, de Prevenció de Riscos Laborals, en matèria de coordinació d'activitats empresarials.
   L'Ajuntament facilitarà a l'empresa que resulti adjudicatària del contracte els documents i informació a que es refereix l'art. 7 del Reial Decret 171/2004, de 30 de gener, relatius a:

AJUNTAMENT DE SantCugat

Plaça de la Vila, 1
08172 Sant Cugat del Vallès
T. 935 657 000
santcugat.cat

Avaluació de riscos del centre de treball, mesures de prevenció, pla d'emergència i qualsevol altre que correspongui.

El contractista resta obligat a presentar, abans de formalitzar-se l'acta d'inici de prestació del servei, els documents que seguidament s'indiquen en compliment del que disposa l'art. 10.2 del Reial Decret 171/2004:

a) Avaluació de riscos i planificació de l'activitat preventiva.
b) Compliment de les obligacions en matèria d'informació i formació respecte dels treballadors que vagin a prestar serveis al centre de treball.
c) Qualsevol altre que l'Ajuntament consideri convenient o necessari.

3. El contractista tindrà accés a la documentació municipal a través de la plataforma informàtica autoritzada per l'Ajuntament en la forma que li serà indicada pel responsable del contracte i haurà de presentar el documents a través de la mateixa plataforma.

Setè. Documentació que facilita l'Ajuntament

Amb l'objectiu de garantir una correcta continuïtat del servei i facilitar el procés d'implantació del nou contracte, l'Ajuntament de Sant Cugat del Vallès proporcionarà a l'empresa adjudicatària tota la documentació generada en el marc del contracte relleu o anterior, anomenat CUGAT-SOC (Centre d'Operacions de Seguretat de l'Ajuntament de Sant Cugat del Vallès), amb referència Expedient: 50249/2021.

L'adjudicatari haurà d'utilitzar aquesta informació com a base per garantir la transició fluida i eficient del servei, aprofitant les lliçons apreses i optimitzant les funcionalitats implementades anteriorment.