AJUNTAMENT DE VILADECANS

SERVEI D'INNOVACIÓ DIGITAL I GOVERNANÇA DE LES DADES
Departament de Sistemes de la Informació i Innovació Tecnològica
EXP.: 28/2025/CSERV

Plec de Prescripcions Tècniques

Serveis Gestionats d'Administració del Centre d'Operacions de Ciberseguretat de l'Ajuntament de Viladecans

Contingut

1 Resum executiu

L'Ajuntament de Viladecans, dins d'un procés de millora contínua en quan a Ciberseguretat, persegueix millorar la seguretat de les seves xarxes de dades i sistemes d'informació, amb l'objectiu de garantir la protecció permanent dels sistemes d'informació, la detecció primerenca d'incidents i la resposta efectiva davant les amenaces que puguin comprometre els serveis digitals que ofereix a la ciutadania, empreses i empleats públics.

El present projecte te com a objectiu subcontractar els serveis gestionats per continuar administrant i gestionant l'actual Centre d'Operacions de Ciberseguretat, d'ara endavant SOC, que s'implementa com a eix i motor principal, sobre una solució de SIEM amb Splunk i les eines LUCIA (Llistat Unificat de Coordinació d'Incidents i Amenaces) i microCLAUDIA, del CCN-Cert, el qual s'articula com a projecte de caràcter horitzontal i absolutament fonamental.

Per tant, aquests serveis s'han de realitzar en format 24x7 per a una gestió i control de la ciberseguretat de manera adequada i proporcionada als riscos actuals. És per això, que resulta essencial per a garantir el funcionament continuat, eficient i segur dels serveis que l'Ajuntament de Viladecans ofereix a la ciutadania.

2 Objectius

L'objectiu d'aquesta proposta és donar continuïtat al servei de ciberseguretat mitjançant la prestació de serveis gestionats del SOC en mode 24x7, sobre una infraestructura ja desplegada, que compta actualment amb una solució SIEM plenament operativa, basada en tecnologia líder del mercat (Splunk), amb 45 casos d'ús actius i funcionals, i una previsió d'ampliació de la capacitat d'ingesta de 25 a 35 GB/dia. El servei actual ja integra funcionalitats amb eines del CCN-CERT com LUCIA i microCLAUDIA, i forma part de la Xarxa Nacional de Centres d'Operacions de Ciberseguretat.

Dins aquest nou escenari, el servei proposat no contempla la implantació inicial del SIEM, sinó que es focalitza en garantir la gestió eficient, evolutiva i segura d'una plataforma ja establerta, assegurant la continuïtat operativa, la maximització del seu rendiment i el

desplegament de nous casos d'ús, integracions i funcionalitats avançades que permetin augmentar la capacitat de detecció, correlació i resposta davant de ciberamenaces complexes.

L'enfocament adoptat per aquest nou servei posa èmfasi en els següents pilars fonamentals:

- **Operació 24x7 del SOC**, amb equips tècnics altament qualificats i expertesa demostrada en la tecnologia desplegada.
- **Monitoratge i resposta davant incidents**, prioritzant nous vectors d'amenaça i l'evolució dels mecanismes de detecció mitjançant alertes, regles de correlació i intel·ligència d'amenaces. Per tant, el SOC liderarà i executarà la resposta immediata de mitigació, coordinada amb tercers i, amb autorització dels tècnics de l'Ajuntament de Viladecans, davant casos crítics, podrà executar accions de contenció o mitigació, seguint protocols establerts i documentant les intervencions.
- **Revisió, manteniment i optimització constant** dels casos d'ús, regles de correlació i integracions existents.
- **Compliment normatiu** amb ENS, NIS2, ISO/IEC 27001 i bones pràctiques de gestió ITIL/ISO 20000.
- **Ampliació i evolució de la capacitat tècnica**, garantint l'adaptació a l'augment previst del volum de logs a correlacionar (de 25 a 35 GB/dia), mantenint la disponibilitat i integritat de la informació.

La proposta ha de donar resposta a les necessitats específiques de l'Ajuntament de Viladecans, consolidant una operació SOC madura, amb una clara orientació a resultats, a la resiliència i a la millora contínua, tot integrant processos, persones i tecnologia d'alt nivell.

A més, els serveis de manteniment i monitorització de l'actual SOC de l'Ajuntament de Viladecans s'integren dins la Xarxa Nacional de Centres d'Operacions de Ciberseguretat. Això ha de permetre millorar les capacitats de protecció de la informació tractada i dels serveis digitals prestats així com de prevenció, detecció i resposta davant d'incidents de ciberseguretat mitjançant la integració de la solució SIEM (Security Information and Event Management) Splunk i les eines LUCIA (Llistat Unificat de Coordinació d'Incidents i Amenaces) i microCLAUDIA, del CCN-Cert.

D'aquesta manera s'aconseguiria l'alineament amb l'Estratègia Nacional de Ciberseguretat, millorant la seguretat i resiliència de les xarxes i els sistemes d'informació i comunicacions de l'Ajuntament i dels serveis prestats, fomentant la cultura i el compromís de l'Ajuntament amb la ciberseguretat i amb la potenciació de les capacitats humanes i tecnològiques. El projecte persegueix afavorir el desenvolupament i la prestació de serveis digitals eficients, segurs i fiables per a ciutadans, empreses i empleats públics.

Alhora, es persegueix afavorir l'alineament amb el compliment de l'ENS i NIS2, vetllant per la seguretat i fiabilitat de les infraestructures, comunicacions i serveis digitals prestats per l'Ajuntament, per així aconseguir les següents fites:

- Facilitar la interoperabilitat entre serveis. La solució a proposar ha d'estar basada en tecnologia certificada pel CCN-CERT en els actuals **S**erveis d'**A**lerta **P**rimerenca (SAP) i per altres Centres d'Operacions de Ciberseguretat integrats a la Xarxa Nacional de Centres d'Operacions de Ciberseguretat , com ara el CSIRT-CV, per la qual cosa ha de ser una solució plenament Inter operable amb els serveis desplegats a l'Administració General de l'Estat pel CCN-CERT.

- Facilitar la reutilització. Com que està basat en tecnologies que formen part del conjunt d'eines del CCN-CERT i que ja són emprades per altres organismes públics, la solució proposada és plenament reutilitzable per altres entitats públiques. D'altra banda, es tracta d'una solució de propietat compartida entre el CCN-CERT i les Administracions Públiques, amb la qual cosa no es requereix la compra de llicències particulars per part de cada organisme.

- Afavorir la millora de l'accessibilitat dels serveis públics digitals als ciutadans i empreses, garantint la privadesa i protecció de la informació, optimitzant la disponibilitat i fiabilitat i minimitzant l'impacte de les possibles ciberamenaces.

- Afavorir la millora de l'eficiència i l'eficàcia dels empleats públics mitjançant la protecció de l'accés i la disponibilitat dels serveis digitals que utilitzen.

- Utilització activa de tecnologies emergents per a l'automatització per a la detecció d'incidents de seguretat mitjançant tècniques de correlació automàtica i mineria de dades.

3 Pla d'implantació

Com a fase prèvia, es realitzarà una auditoria de la eines i elements de seguretat que integren l'actual SOC de l'AJUNTAMENT DE VILADECANS, en un termini màxim de 20 dies hàbils. El resultat d'aquests anàlisi, que s'haurà de lliurar en un document, permetrà definir un pla d'adequació i traspàs del servei, així com la correcta adopció del servei SOC.

A més durant aquest termini s'haurà de lliurar una memòria tècnica on es pugui evidenciar l'assumpció de la gestió del servei:

- L'activació de la monitorització i servei 24.
- Presentats els protocols d'actuació davant incidents greus.
- Configuració del servei 24x7 i sistema d'alertes.
- Configuració del sistema de seguiment i qualitat del servei.

No obstant això, a continuació es relaciona l'arquitectura actual del SIEM i els requeriments del servei SOC a prestar.

3.1. Arquitectura actual

L'Ajuntament de Viladecans disposa actualment d'un Centre d'Operacions de Ciberseguretat (SOC) plenament operatiu, amb una arquitectura tecnològica consolidada basada en una plataforma SIEM de referència en el mercat (Splunk), desplegada sota un model SaaS amb components d'ingesta i preprocesament ubicats al seu Centre de Processament de Dades.

L'actual eina de SIEM correla les següents fonts d'informació dels registres de successos de diferents serveis i servidors amb l'objectiu de disposar d'una visió comú de l'estat de la seguretat als nostres sistemes i per la detecció de ciberatacs:

Eines de seguretat perimetral

- Cluster de 2 Firewalls Fortigate 600E
- 1 VM Fortianalyzer on Premise.
- 1 Cisco Email Security (CES) al Núvol.

- 2 VM Citrix ADC (Netscalers), on Premise.
- 1 VM HP IMC (elements de xarxa HP).

Eines de Sistemes per servei d'accés usuaris

- 2 Windows Server Active Directory on Premise.
- 2 Windows File Servers en Cluster
- Infraestructura escriptoris virtuals XenDesktop on Premise.
- Microsoft 365

Eina d'Antivirus i EDR i monitorització

- Trendmicro APX One, Deep Security i EDR al Núvol.
- Monitorització dels sistemes i xarxa de dades amb Nagios.

Arquitectura actual del SIEM

La solució SIEM desplegada inclou:

- Components locals per a la recol·lecció, compressió i xifratge dels logs.
- Transmissió segura cap a una plataforma cloud amb alta disponibilitat i emmagatzematge redundant.
- Consola de gestió centralitzada amb quadres de comandament, motors de correlació, alertes en temps real i capacitats d'informe.

Casos d'ús desplegats

Actualment, es troben **45 casos d'ús operatius**, dissenyats i afinats per a cobrir:

- Monitoratge de seguretat perimetral i d'endpoints.
- Activitat sospitosa d'usuaris (UEBA bàsic).
- Integració amb Active Directory, tallafocs, antivirus i serveis de correu electrònic.
- Casos d'ús específics per a detecció de ransomware, accés no autoritzat, anomalies en la infraestructura i activitat maliciosa basada en signatures o comportament.

Capacitat d'ingesta i escalabilitat

La plataforma SIEM actualment suporta una capacitat d'**ingesta de 25 GB/dia de logs**, amb un increment ja planificat per aquest concurs de fins a **35 GB/dia**, sense limitació en el nombre

d'esdeveniments per segon (EPS). Aquesta ampliació haurà de tenir continuïtat operativa i no afectar la capacitat de correlació, disponibilitat ni rendiment de la solució.

Altres eines operatives: LUCIA i microCLAUDIA

Complementàriament, el SOC integra:

- **LUCIA**, eina oficial del CCN-CERT per a la coordinació i notificació d'incidents, operativa però pendent d'optimització i federació total amb la Plataforma Nacional.
- **microCLAUDIA**, ja desplegada parcialment en estacions de treball i servidors, per a la vacunació proactiva contra ransomware. El seu ús està consolidat i s'hi preveu la cobertura completa durant la prestació del servei.

Aquest entorn proporciona a l'Ajuntament de Viladecans una base sòlida per a la detecció i resposta a ciberincidents, i representa el punt de partida per a l'evolució i millora contínua del servei SOC.

3.2. Requeriments del Servei

L'objectiu principal del nou servei és garantir la **continuïtat operativa, l'evolució tecnològica i el compliment normatiu** del Centre d'Operacions de Ciberseguretat, a partir d'un entorn ja desplegat i en funcionament.

Els pilars fonamentals sobre els quals es construeix aquesta nova fase del servei són:

Operació i manteniment 24x7 del SOC

Assegurar el funcionament ininterromput del SOC mitjançant un equip tècnic especialitzat, que vetlli pel **monitoratge continuat, la detecció primerenca i la resposta immediata** de mitigació davant incidents de seguretat, d'acord amb els Acords de Nivell de Servei (ANS) establerts.

Gestió de nous casos d'ús

Ampliar la cobertura de seguretat mitjançant la **definició, desplegament i optimització de nous casos d'ús**, d'acord amb l'evolució de l'entorn tecnològic, els nous riscos emergents i les necessitats operatives que es detectin.

Evolució i optimització del sistema

Revisió contínua de l'arquitectura, les regles de correlació, la qualitat de les dades ingesta i el rendiment global del sistema SIEM, incorporant millores funcionals, tecnològiques i de capacitat (com l'ampliació prevista fins als 35 GB/dia). Per tant, es contemplen accions de **manteniment preventiu, evolutiu i perfectiu**, així com la proposta proactiva de millores a nivell d'eficiència i detecció.

Compliment de les certificacions mínimes en Seguretat, sistemes i altres marcs normatius i estratègics

Amb l'objectiu d'assegurar un servei de qualitat, que tingui la seguretat dels sistemes i les dades, com a objectiu principal i estratègic, es requereix disposar de les següents certificacions, normatives i estàndards a nivell d'empresa:

- **ENS**: Nivell alt.
- **ISO/IEC 27001**, per al Sistema de Gestió de Seguretat de la Informació.
- **ISO/IEC 22301**, per a la Gestió de Continuïtat de Negoci.
- **ISO 20000**, pel model de prestació de serveis.
- **Xarxa nacional de SOC:** Nivell Gold.
- Acreditació en el CCN (Centro Criptografico Nacional).
- **SIEM Splunk:**
    - A nivell de Partner de Splunk, l'adjudicatari ha d'estar dins els següents nivells:
        - Sell
        - Buid
        - Manage

En conseqüència, la gestió de tota la plataforma SIEM es realitzarà atenent a l'Esquema Nacional de Seguretat, les instruccions tècniques de seguretat, les guies de seguretat de les tecnologies de la informació i les comunicacions elaborades pel Centre Criptològic Nacional, la tecnologia de les quals és la base del Centre d'Operacions de Ciberseguretat que es desplegarà.

Aquest nou servei ha de permetre a l'Ajuntament de Viladecans **reforçar la postura de ciberseguretat**, adaptant-se a un entorn de risc canviant, optimitzant recursos i garantint la prestació segura dels serveis públics digitals.

L'equip que constituirà el SOC haurà d'estar altament qualificat per donar resposta a les necessitats d'administració de les solucions, manteniment i accions proactives i correctives que esdevinguin necessàries per a garantir la qualitat en el servei.

A més, l'actuació ha d'incloure formació als equips tècnics de l'Ajuntament per a l'administració i l'operació de la plataforma desplegada.

Tot seguit es descriu un resum del servei a desenvolupar:

- Capacitats de recol·lecció d'esdeveniments de per part de l'eina de SIEM
  - Monitorització de disponibilitat de la pròpia plataforma.
  - Anàlisi de trànsit
  - Control d'integritat
  - Integració de fonts de logs
- Capacitats de correlació d'events aplicant intel·ligència mitjançant l'ús de regles.
- Consola de gestió d'esdeveniments.
- Quadre de comandament, amb informació d'evolució al volum d'alertes registrades segons criticitat o tipologia.
- Detecció d'Amenaces Persistents Avançades (ATP).
- Instància de LUCIA federada amb la Plataforma Nacional de Notificació i Seguiment de Ciberincidents. Actualment el servidor es troba instal·lat a una VM però manca la federació i algun ajust de configuració.
- Agents de microCLAUDIA per a la vacunació anti-ransomware dels llocs d'usuari i servidors. Actualment ja s'estan distribuint agents de microCLAUDIA als llocs d'usuari i servidors. En cas que durant l'execució del projecte no estiguin implementats en el 100% dels equips, l'adjudicatari es farà càrrec del seu desplegament i manteniment durant l'execució del contracte.
- Integració amb la Xarxa d'Intel·ligència Compartida del CCN-CERT.

3.2.1 Detall dels serveis desenvolupar

El servei a prestar es fonamentarà en un conjunt de **serveis gestionats integrals i proactius**, orientats a garantir un alt nivell de protecció, eficiència operativa i alineament normatiu. A continuació es detallen els serveis principals que conformen l'abast funcional del contracte:

Monitoratge 24x7 i resposta a incidents

Supervisió continuada 24x7 de la plataforma SIEM, gestió d'alertes i coordinació de la resposta a incidents de seguretat, amb especial atenció als casos d'alta criticitat. El SOC actuarà com a **centre coordinador** davant tercers proveïdors i, en cas d'autorització expressa per part dels Sistemes de l'Ajuntament de Viladecans, podrà executar **accions de resposta directa** seguint els protocols establerts, sempre garantint els ANS (Acords de Nivell de Servei), segons criticitat, definits en aquest a l'Annex 1 del present plec.

L'Ajuntament de Viladecans disposa amb una empresa subcontractada, de diferents Serveis Gestionats dels Sistemes Informàtics i Xarxa corporativa, amb servei de monitorització i resposta a incidents 24x7 amb un SLA determinat que ha de complir.

Es per aquest motiu, que un com assumit el serveis per part de l'adjudicatari d'aquest contracte, es determinarà quin model d'actuació esdevindrà com més idoni per donar resposta a incidents de seguretat greus fora de l'horari laboral: accions de resposta directa per part de l'adjudicatari o comunicació i seguiment a l'empresa de SSGG de Sistemes de que disposa l'Ajuntament.

Anàlisi de vulnerabilitats mensual

Execució d'anàlisis regulars sobre els sistemes crítics per detectar vulnerabilitats conegudes i avaluar-ne l'impacte potencial. Els resultats d'aquestes exploracions es recolliran en informes tècnics amb recomanacions d'actuació prioritzades per criticitat.

Auditoria anual externa

Realització d'una **auditoria tècnica anual externa basada en el marc NIST SP 800-53 o NIST Cybersecurity Framework (CSF)**, que permeti verificar el nivell de compliment dels controls i requisits de seguretat establerts. Aquesta auditoria contribuirà a reforçar la postura de seguretat de l'Ajuntament de Viladecans davant requeriments reguladors o certificacions.

Test d'intrusió anual (intern i extern)

Execució d'un **test d'intrusió de forma anual**, amb enfocament doble:

- **Extern (caixa negra)**: simulant l'actuació d'un atacant desconegut des d'Internet.

- **Intern (caixa grisa/blanca)**: emulant un escenari d'amenaça interna o accés privilegiat (ex. empleat descontent).

Les proves seguiran metodologies reconegudes (OSSTMM, PTES) i inclouran un informe complet amb resultats, evidències i pla d'acció associat.

Ingesta de noves fonts de dades

El servei inclourà la **integració progressiva de noves fonts de dades** (equipament, aplicacions, serveis en núvol o sistemes OT), assegurant-ne la normalització, correlació i enriquiment dins el SIEM. Aquesta ingesta es farà d'acord amb el creixement natural de l'entorn de l'Ajuntament de Viladecans, sense limitació rígida, i seguint bones pràctiques de seguretat i rendiment.

Inclusió de nous casos d'ús

Amb l'objectiu de mantenir l'eficàcia del SOC davant l'evolució de l'amenaça, el servei inclourà la **definició i desplegament de 10 a 15 nous casos d'ús anuals**, en funció de les necessitats detectades. Aquests es definiran conjuntament amb l'equip tècnic del client i es prioritzaran segons riscos emergents, noves integracions o obligacions normatives.

Propostes de millora contínua i manteniment evolutiu

S'establirà un cicle actiu de **revisió, optimització i evolució** de la plataforma, els casos d'ús i les integracions. El servei incorporarà propostes de millora continua i plans de manteniment evolutiu alineats amb les recomanacions del fabricant, l'evolució del context de riscos i les necessitats operatives que es vagin detectant durant el transcurs del servei.

Es per això, que es requereix, a més, la revisió i confecció d'un informe trimestral dels elements de Seguretat que conformen el perímetre i l'endpoint, com regles del Firewall i necessitat d'actualitzacions de firmware o versions, revisió dels pegats de Microsoft en els serveis crítics com Fileserves, DCs, etc..., auditoria del CES (Cisco Email Security), estat del l'antivirus i EDR en servidors i endpoints.

Davant de detecció d'amenaces, atacs que es puguin produir, a banda de fer una comunicació formal a les empreses col·laboradores amb els Sistemes d'Informació de

l'Ajuntament, es col·laborarà estretament amb elles en els casos d'altra criticitat per així pal·liar els danys als sistemes informàtics i a les dades corporatives, concretament amb l'empresa que ens gestiona els Sistemes Informàtics i la que administra l'eina d'antivirus i EDR de TrendMicro.

Per tant, es realitzarà una reunió conjunta amb els Service Manager dels diferents serveis per coordinar-se en cas d'un atac greu i establir procediments.

En cas que sigui necessari, d'avant d'un incident greu de seguretat, s'haurà de personar el perfil tècnic necessari a les dependències de l'Ajuntament, per ajudar a l'equip tècnic de Viladecans a mitigar l'atac i ajudar en les tasques de coordinació amb tercers.

No es preveu un màxim de dedicació d'hores anuals dels serveis SOC objecte d'aquest contracte.

3.2.2 Ampliació de la Capacitat i Optimització de la ingesta de logs

Amb l'objectiu d'assegurar l'escalabilitat i la continuïtat operativa del sistema SIEM davant l'augment previst del volum d'informació a monitorar, el nou servei inclou un pla específic d'ampliació i optimització tècnica que abasta els àmbits següents:

Adaptació a 35 GB/dia

S'adaptarà la configuració actual del sistema per absorbir l'increment previst de capacitat d'ingesta, passant dels **25 GB/dia actuals als 35 GB/dia**, garantint la disponibilitat, estabilitat i eficiència en la ingestió i correlació d'esdeveniments. Aquesta adaptació tindrà en compte el **manteniment dels SLA existents** i l'absorció de pics puntuals.

Revisió de la infraestructura de recol·lecció i normalització

Es realitzarà una **anàlisi tècnica de la infraestructura de recol·lecció de logs**, incloent agents, connectors, pipelines i mètodes de compressió/encriptació. També s'avaluarà el procés de **normalització de dades**, assegurant que compleix criteris d'estandardització, integritat i rendiment, i que permet una correlació efectiva amb la resta de sistemes integrats.

Avaluació de rendiment del SIEM

S'implementarà un procés periòdic d'**avaluació del rendiment del sistema SIEM**, tant a nivell de plataforma (temps de resposta, latència, disponibilitat), com funcional (eficàcia de detecció, índex de falsos positius, càrrega de treball associada als casos d'ús). Aquesta anàlisi servirà com a base per a les accions de **manteniment evolutiu** i per garantir un ús òptim dels recursos disponibles.

Aquest conjunt d'actuacions garantirà que la infraestructura SIEM de l'Ajuntament de Viladecans **evoluciona al ritme de les seves necessitats**, mantenint l'eficiència, la qualitat del servei i la capacitat d'adaptació a futurs increments de dades o complexitat en la monitorització.

3.2.3 Pla de formació

Un dels eixos fonamentals del servei proposat és garantir la **capacitat operativa interna de l'equip tècnic de l'Ajuntament de Viladecans**, mitjançant accions concretes de formació, documentació tècnica i suport directe als equips TIC municipals. Aquest component assegura la **transferència efectiva de coneixement** i l'empoderament dels equips interns en matèria de ciberseguretat.

En finalitzar l'etapa d'implantació s'organitzaran sessions de formació als usuaris del sistema per tal de reforçar els coneixements adquirits a través de la vostra experiència en el procés d'implantació. Les sessions de capacitació anual previstes són les següents:

Formació	Durada	Sessions
Resum implantació (un cop s'hagi assumit el servei)	1 hora	1
Administració eina SIEM bàsica	2 hores	2
Administració eina SIEM avançada	2 hores	2

Anàlisi de vulnerabilitats i interpretació d'informes	2 hores	1
Bones pràctiques per a l'ús de microCLAUDIA i altres eines CCN-CERT	2 hores	1

Es lliurarà un **manual tècnic actualitzat anualment** amb les millors pràctiques aplicables a la gestió d'un SOC local, recollint:

- Procediments operatius estàndard (SOPs).
- Recomanacions de configuració i resposta.
- Alertes típiques i pautes de tractament.
- Bones pràctiques d'enduriment i segmentació.

Aquest document estarà adaptat al context de l'Ajuntament de Viladecans i servirà com a referència per als tècnics i responsables de seguretat de la institució.

A més, l'equip del servei de SOC realitzarà un **acompanyament continuat** als tècnics interns de Viladecans durant les activitats clau:

- Revisió conjunta de regles i casos d'ús.
- Participació en comitès operatius i tècnics.
- Suport en la gestió de proves d'intrusió, auditories i inspeccions externes.

Aquest enfocament permet consolidar un **model col·laboratiu**, on el coneixement adquirit durant el servei es transfereix progressivament al CLIENT_X, incrementant l'autonomia i maduresa del seu model de ciberseguretat.

4 Descripció de l'equip tècnic

La proposta ha de contemplar la configuració d'un **equip tècnic multidisciplinari**, amb experiència acreditada i coneixement expert en operació de SOC, detecció d'amenaces, auditoria tècnica i gestió de riscos. Aquest equip actuarà com a extensió de l'equip de ciberseguretat de l'Ajuntament de Viladecans, garantint una prestació de servei proactiva, flexible i alineada amb els requisits normatius i operatius del contracte.

Cal esmentar que sempre que es pugui, la gestió i administració del servei es realitzarà en remot.

AFEGIR EL QUE LAIA HA POSAT DE SOLVENCIA TÈCNICA I PROFESSIONAL

Coordinador de servei

Perfil amb experiència contrastada en gestió de serveis de ciberseguretat i actuant com a punt únic de contacte amb l'Ajuntament de Viladecans. Tindrà la responsabilitat de coordinar l'operativa diària, liderar els comitès de seguiment, vetllar pel compliment dels ANS i facilitar la comunicació transversal entre àrees tècniques i organitzatives.

Enginyers i analistes SOC Juniors

Perfils tècnics encarregats de la gestió i monitoratge 24x7 del sistema SIEM i les eines complementàries (LUCIA, microCLAUDIA), així com de l'anàlisi i correlació d'esdeveniments, detecció d'incidents i generació d'informes tècnics. També participaran activament en la definició de nous casos d'ús i en la millora contínua de les regles i processos de detecció.

Especialistes Sèniors en auditoria i detecció de vulnerabilitats

Professionals amb experiència en **auditories tècniques, anàlisi de vulnerabilitats, pentesting i avaluació de controls**, formats en marcs de referència com NIST SP 800-53, OSSTMM o PTES. Seran responsables d'executar l'auditoria externa anual, el test d'intrusió intern i extern, i els escanejos mensuals de vulnerabilitats. També elaboraran els informes de risc i els plans d'acció associats.

Aquest equip es dimensionarà i assignarà en funció del volum de servei i les necessitats evolutives de l'Ajuntament de Viladecans,

garantint la **continuïtat operativa, la qualitat tècnica i la resposta davant qualsevol escenari de ciberamenaça.**

5 Sistema de seguiment i control

El model de seguiment i control del projecte es basarà en un model a tres nivells per tal de garantir la comunicació i la interlocució amb les diferents parts i assegurar un seguiment adequat del projecte.

Es crearà un comitè per a cada nivell, establint-se un Comitè de Direcció, un Comitè de Seguiment i un Comitè Operatiu. Aquests comitès es reuniran amb la periodicitat que es determini durant l'establiment del contracte i en la fase inicial del projecte d'implantació del servei. A més, es duran a terme tantes reunions addicionals com es consideri oportú per garantir la gestió adequada del servei.

- **Comitè de direcció.** L'objecte del Comitè de Direcció serà la definició d'aspectes estratègics del servei (ampliacions, tractament de riscos, redefinició del projecte,...). La freqüència de les reunions es proposarà inicialment de manera semestral. Els seus documents de treball principals seran els informes executius de progrés del projecte, així com les agendes i actes de reunió.

- **Comitè de Seguiment.** Aquest comitè estarà conformat pels Coordinadors del Projecte. Per a aquest comitè es proposa una reunió mensual per revisar els informes de control, revisar incompliments, riscos i accions correctores, així com verificar el progrés i la millora continua dels nivells de seguretat. En aquest marc s'elaboraran els informes de compliment d'ANS (Acords de Nivell de Servei), el registre de risc i els informes de control i seguiment. El Comitè de Seguiment serà el principal responsable del control del projecte, utilitzant per a això:

  - La definició d'Acords de Nivell de Servei (ANS) amb els proveïdors.
  - La definició del calendari i fites del projecte
  - Informes mensuals de l'estat del projecte en què:
    - Es mesuren els indicadors associats als ANS per verificar la correcta execució
    - Es mostri el progrés i el grau de compliment de les fites programades
  - Les eines que es posin a disposició per part de la IGAE per al seguiment dels projectes associats al PRTR

- **Comitè Operatiu.** Amb una funció eminentment tècnica i pràctica, assumirà la coordinació i la gestió diària del projecte. Estarà constituït pels diferents responsables i tècnics involucrats al projecte. Es reuniran de forma setmanal, o sempre que el servei ho requereixi, per assegurar la resolució de conflictes, revisar les solucions implantades i avaluar riscos i propostes de millora.

Elaboració d'auditories de sistemes i realització de test d'intrusió i solucions de programari (hacking ètic)

Els serveis de Hacking Ètic han de ser objectius i seguir els mateixos passos que un atacant seguiria si estigués intentant vulnerar els sistemes de l'Ajuntament.

La millor manera de fer aquesta avaluació de la seguretat és fer atacs controlats sobre els sistemes. Es poden dur a terme tant de forma remota com des de les instal·lacions de l'Ajuntament, depenent dels objectius cercats i l'àmbit de l'auditoria.

Un Test d'Intrusió es compon de les fases següents:

- **Planificació:** Definició i identificació dels sistemes a auditar.
- **Auditoria:** Realització de les proves que es duen a terme de forma progressiva fins aconseguir la intrusió i, una vegada aconseguida, escalat als sistemes.
- **Documentació**: Redacció de tots els resultats obtinguts.

Per realitzar aquests atacs s'utilitzaran tant tècniques com eines de hacking. Les eines seran les mateixes que les utilitzades al món underground pels propis hackers per realitzar els atacs, així com eines creades per l'equip tècnic d'Internet Security Auditors per realitzar els Test d'Intrusió i que han estat elaborades a partir de les pautes definides als estàndards OSSTMM, ISSAF PTES.

S'haurà de realitzar un test cada 6 mesos i executar les tres fases definides. Davant les millores detectades, es realitzarà un pla d'implantació i seguiment per tal que en el proper test ja estiguin resoltes.

6 Indicadors clau KPI de seguiment i Gestió de Riscos

El servei inclourà un sistema de reporting estructurat, amb generació d'informes mensuals i trimestrals, adaptats als perfils executiu i tècnic. Els indicadors clau inclouran, entre d'altres:

- **KPI** (Key Performance Indicators): volum i temps de resposta a incidents, percentatge de cobertura d'ingesta, eficiència de casos d'ús, reducció de falsos positius, etc.
- **KRI** (Key Risk Indicators): vulnerabilitats crítiques pendents, superfície d'atac, exposició a tercers, desviacions respecte controls de seguretat, etc.

A més, els informes que es presentaran a les reunions inclouran:

- Número de casos d'us implementats i els previstos per al següent període de revisió
- Percentatge d'alertes més comuns i correlació amb períodes anteriors.
- Relació i percentatge de tiquets oberts per període classificat per casos d'us.
- Percentatge de centralització dels registres dactivitat.
- Nombre i relació d'alertes i incidents de seguretat més crítiques a nivell d'usuari, xarxa i equips, per a la seva posterior gestió, anàlisi, prevenció.
- Altres que s'identifiquin conjuntament i siguin rellevants pel seguiment i millora del servei.

Gestió de riscos i compliance

El servei incorporarà un **model actiu de gestió de riscos de ciberseguretat**, alineat amb els requeriments del marc NIS2, ENS i ISO 27001. Es mantindrà un **registre de riscos actualitzat**, amb control d'estat, avaluació de severitat i pla d'accions associat. A més, es donarà suport en l'adaptació a canvis normatius, auditories i requeriments de compliance, amb l'objectiu de garantir una postura robusta i resilient davant auditories internes i externes.

7 Calendari i Full de Ruta

El desplegament i l'operació del servei es realitzarà segons un **full de ruta planificat i estructurat en fases**, amb fites clares i tasques recurrents que assegurin la continuïtat, qualitat i millora progressiva del servei.

Fases d'inici, transició i estabilització

El servei s'estructura en tres grans fases inicials:

- **Fase d'inici**: Reunió de kickoff, revisió d'objectius i establiment dels comitès de governança. Actualització de la documentació de serveis, calendaris i procediments compartits.
- **Fase de transició**: Transferència de coneixement de l'operador anterior (si aplica), validació de les fonts d'ingesta i casos d'ús existents, revisió de regles actives i adaptació del sistema al nou volum d'ingesta (35 GB/dia).
- **Fase d'estabilització**: Verificació del funcionament del servei segons ANS, desplegament de les primeres accions de millora (afinament de regles, integració de fonts addicionals, etc.) i inici del cicle regular de reunions i informes.

Tasques recurrents i milestones anuals

Un cop estabilitzat, el servei seguirà un calendari anual amb **activitats planificades** que asseguren la seva evolució i el compliment dels requisits normatius i operatius:

- **Mensualment**:
  - Emissió d'informes d'activitat del SOC.
  - Comitè operatiu (o setmanal, segons necessitat).
- **Trimestralment**:
  - Execució de l'anàlisi de vulnerabilitats.
  - Revisió de regles, quadres de comandament i rendiment del SIEM.
  - Comitè de seguiment i informes de servei.
  - Revisió dels KPIs i KRI.
- **Semestralment**:
  - Revisió d'arquitectura d'ingesta i normalització.

- Informe tècnic de riscos.
- Reunió de coordinació de millores evolutives.

- **Anualment**:
  - Execució de test d'intrusió (intern i extern).
  - Auditoria externa de seguretat basada en NIST SP 800-53 o NIST CSF.
  - Sessió de formació i entrega de manual tècnic.
  - Inclusió de 10-15 nous casos d'ús.
  - Comitè de Direcció i avaluació estratègica.

Aquest enfocament ha de permetre garantir una **visió de cicle de vida del servei**, on es conjuguen la continuïtat operativa i la millora contínua amb un model de treball predictible i orientat a resultats.

8 Facturació

El servei de subscripció SIEM Cloud Anual Pla 35 GB/dia es facturarà durant el primer mes de cada any del servei. Els serveis gestionats SOC es facturaran mensualment.

ANNEX 1: Marc Metodològic i Acord de Nivell de Servei (ANS)

El desenvolupament de les activitats de serveis gestionats que es preveu en aquesta contractació s'haurà de cenyir a l'ús de les millors pràctiques generalment acceptades en el sector, i que en el cas de l'Ajuntament s'identifiquen amb el marc metodològic d'ITIL en la seva

versió 3. Pel que fa a la documentació, l'adjudicatari s'haurà d'adaptar a les eines i programari que l'Ajuntament posarà a disposició per gestionar la mateixa.

També s'haurà de realitzar una provisió eficaç dels serveis gestionats mitjançant la millora contínua definida a la ISO 20.000, i d'altra banda, executar les millors pràctiques recomanades en Seguretat de la Informació i Sistemes de Gestió de la Seguretat de la Informació (SGSI), definides a la ISO 27.000. D'aquesta manera, s'assegurarà que l'empresa te experiència i aplica una gestió de qualitat, tenint en compta la seguretat dels sistemes en tot moment.

Conceptes i definicions

En aquest apartat es defineixen una sèrie de conceptes que seran utilitzats a l'hora de realitzar els serveis objecte d'aquesta contractació.

• Incidències

Les incidències són qualsevol anomalia en la infraestructura tecnològica que causa una interrupció al servei o una reducció (degradació) en la qualitat del mateix. La resolució d'incidències es centra en retornar a l'operativa normal el més ràpid possible, amb el menor impacte pel negoci i l'usuari, i amb el menor cost possible. Les incidències són el resultat de fallides en la infraestructura TIC.

Es pot tenir coneixement de l'existència d'incidències en la infraestructura TIC a partir de la identificació directa en les infraestructures, a través de la informació proporcionada pels sistemes de monitoratge NAGIOS o a través de la plataforma de gestió d'esdeveniments SIEM.

Pel correcte tractament de les incidències s'utilitzarà un esquema de prioritats que s'indica més endavant en aquest document.

En els càlculs pel dimensionament del servei, s'ha considerat un volum de 8 hores mensuals destinades a la resolució d'incidències de prioritat 1, fora de la franja horària del servei gestionat o en dissabtes i festius. Aquesta xifra és orientativa i no suposarà cost econòmic addicional en la prestació del servei, ni reducció econòmica en cas de no realització.

• Peticions de servei

Les peticions de servei són aquelles sol·licituds dels usuaris orientades a:

- Sol·licitud d'informació o consell
- Peticions de canvis estàndard
- Peticions d'accés a la plataforma SIEM.

- Nous quadres de comandament i informes.
- Altres...

La gestió de les peticions de servei s'atendrà segons els criteris de l'Ajuntament.

• Temps de detecció

És el temps que passa des que hi ha una fallida en la infraestructura TIC fins que la organització TIC té constància de la mateixa (ja sigui directament o a través de tercers).

• Temps de resposta

És el temps que passa des de la detecció d'un problema fins que es realitza el registre s'inicia el diagnòstic del problema.

• Temps de resolució

És el temps emprat en resoldre la incidència o problema, o aplicar una solució temporal per a retornar el sistema a l'estat anterior previ a la interrupció del servei. Aquest temps inclou els desplaçaments del personal tècnic si fos precís.

• Assistència remota

L'assistència remota és aquella que es duu a terme a través de connexions a distància amb l'equip o sobre la infraestructura sobre la que es vol intervenir.

• Manteniment preventiu

El manteniment preventiu s'orienta a prevenir i detectar, amb antelació suficient, situacions futures que poden afectar a la disponibilitat d'ús de la infraestructura tecnològica, tant de maquinari com de programari. L'adjudicatari haurà d'incloure un pla de tasques periòdiques orientades a aquesta finalitat per als diferent entorns de serveis gestionats que opera.

- ## Manteniment correctiu

El manteniment correctiu s'orienta a resoldre les incidències de la infraestructura tecnològica donant compliments als SLA establerts, imputant les actuacions a la bossa d'hores establerta en cada Lot. Aquest manteniment té aplicació tant a nivell de maquinari com de programari. En aquest darrer supòsit, no serà falta imputable a l'adjudicatari els errors de programari de sistema provocats pel fabricant dels equips, si fos el cas.

Com a criteri general, el manteniment correctiu (maquinari i programari) podrà ser requerit a petició del personal autoritzat del DSI enfront una situació de no disponibilitat de la infraestructura TIC que no hagi estat detectada pel propi adjudicatari.

- ## Manteniment evolutiu

Les activitats associades al manteniment evolutiu s'orienten a mantenir actualitzada, en tot moment, la plataforma tecnològica segons les recomanacions i actualitzacions de programari que proporciona el fabricant dels equips.

L'adjudicatari informarà puntualment a l'Ajuntament sobre les recomanacions d'actualització que el fabricant proposa en les seves plataformes de maquinari o programari. Les reunions semestrals programades poden ser l'espai idoni per plantejar les millores detectades.

- ## Manteniment perfectiu

Les activitats associades al manteniment perfectiu s'orienten a la configuració i parametrització de la plataforma tecnològica per tal de millorar-ne el seu rendiment i manteniment.

En aquest sentit, el licitador pot incloure en la reunió semestral de coordinació la seva proposta i la realització d'auditories i/o revisions de les configuracions dels sistemes (maquinari o programari), a l'objecte de detectar possibles aspectes de millora o també com a seguiment de recomanacions del fabricant.

Categorització d'Incidències

A l'objecte que el tractament de les incidències sigui unificat en els diferents àmbits d'acció d'aquest contractació, en aquest apartat s'indiquen els criteris objectius que determinaran la prioritat de les incidències que es produeixin. En aquest sentit, la prioritat és el resultat de la combinació de dues variables que fan referència a:

a) IMPACTE: Mesura la importància de la incidència en l'afectació al volum d'activitat que se'n deriva. Es valorarà, fonamentalment, a partir del nombre d'usuaris que es veuen afectats per la mateixa així com per el tipus de sistemes corporatius o serveis transversals afectats.

b) URGÈNCIA: Amb caràcter general s'associa a la rellevància del servei IT que es veu afectat (per exemple: correu electrònic, web, altres...) i la demora que el client accepta per a la seva resolució, d'acord amb el SLA establert.

Tenint en compte l'anterior, s'estableix la següent classificació de prioritats en la resolució d'incidències segons es mostra en la taula adjunta:

Figura2: Matriu de classificació de les prioritats de les incidències

PRIORITAT INCIDÈNCIES		IMPACTE			
		Organització	*Edifici Departament*	*Usuaris múltiples*	*Usuari*
URGÈNCIA	*CRÍTICA*	Prioritat 1	Prioritat 1	Prioritat 2	Prioritat 2
	ALTA	Prioritat 1	Prioritat 2	Prioritat 2	Prioritat 3
	MITJA	Prioritat 2	Prioritat 2	Prioritat 3	Prioritat 3
	BAIXA	Prioritat 2	Prioritat 3	Prioritat 3	Prioritat 4

Com a criteri general es consideraran dos grans grups d'incidències:

- **CRÍTIQUES** les que tenen associades prioritats 1 (Crítica) i 2 (Alta).
- **NO CRÍTIQUES** les que tenen associades prioritats 3 (Mitja) i 4 (Baixa)

La classificació que es presenta podrà ser modificada pel DSI en funció de les necessitats dels serveis o altres criteris de necessitats puntuals. També s'haurà de definir la prioritat en TIC que l'Ajuntament precisi incorporar.

Descripció de les prioritats i Acords de Nivell de Servei (ANS)

A continuació es fa una descripció orientativa de les situacions associades a cada tipus de prioritat i el temps de resposta en el que l'adjudicatari ha

d'atendre-les. En funció de la prioritat de la incidència s'assignaran els recursos per a la seva resolució, en nombre i expertesa. Es tindrà en compte que per a incidències de prioritat equivalent, es prioritzaran les que tinguin un impacte més gran. En cas d'igualtat en el nivell de prioritat i impacte, s'aplicarà el criteri d'atendre la més urgent i, per últim, en cas d'igualtat en impacte i urgència es prioritzarà la resolució de la primera que es va detectar. Aquest criteris podran ser variats en funció de les necessitats del servei a l'objecte de la millora continua del mateix. Les prioritats que s'han fixat són:

Prioritat 1 (CRÍTICA)

Associada a les aplicacions més crítiques, atenció al ciutadà (OAC's), amb impacte a tota la organització, departaments, edificis sencers amb alta urgència per a la seva resolució. Té impacte en els serveis que l'Ajuntament presta al ciutadà. No hi ha "workarounds" (solucions temporals provisionals).

Afectació que representa no donar compliment a terminis de lliurament oficials amb conseqüències legals, impacte en tercers (p.e. processos de transferència per a pagament de la nòmina) o altres processos que no poden demorar els terminis establerts.

- Temps màxim d'atenció d'incidències: 15'

- Temps màxim per a que es comenci a resoldre: 30'

Prioritat 2 (ALTA)

Associada amb problemes de VIP's, aplicatius departamentals o que afecten a col·lectius d'usuaris, situacions en que existeix un "workaround" i altres situacions amb degradació del servei.

La rellevància de l'afectació suposa que es disposa de marge en el temps, però que cal no demorar l'actuació i portar-la a terme amb caràcter prioritari, i no més tard del següent dia laborable.

- Temps màxim d'atenció d'incidències: 15'

- Temps màxim per a que es comenci a resoldre: 4 hores.

Prioritat 3 (MITJA)

Incidències de VIP amb baixa urgència, afectació a múltiples usuaris amb urgència mitja o baixa. Afectació que causa poc impacte en els serveis al ciutadà però interromp la productivitat dels usuaris.

L'afectació permet continuar amb l'activitat de l'usuari però caldrà disposar del servei amb un termini inferior als TRES (3) dies.

- Temps màxim d'atenció d'incidències: 30'

- Temps màxim per a que es comenci a resoldre: 1 dia laborable

Prioritat 4 (BAIXA)

Processos d'atenció al ciutadà no afectats, afectacions a usuaris individuals amb baixa urgència.

La prioritat d'una incidència pot variar durant el seu cicle de vida. Per exemple, es poden trobar solucions temporals que restaurin acceptablement els nivells de servei i que permetin retardar el tancament de la incidència sense repercussions greus.

La prioritat d'una incidència serà calculada a partir de la taula que s'han indicat anteriorment i, en cap cas, serà arbitràriament assignada per l'operador d'atenció al CAU.

La rellevància de l'afectació és molt reduïda i permet un termini de resolució dins una mateixa setmana laboral.

- Temps màxim d'atenció d'incidències: 30'

- Temps màxim per a que es comenci a resoldre: 2 dies laborables

Classificació de l'impacte

Per a la determinació de l'impacte es tindrà en compte l'àmbit de repercussió que provoca la incidència d'acord als grups d'afectats següents:

Organització: afectació general o a la pràctica totalitat d'usuaris del consistori i/o ciutadà (p.e. accés a Internet, Directori Actiu no disponible, etc).

Edifici/Departament: afectació a nivell d'ubicació determinada a un grup d'usuaris departamentals (aplicacions específiques, etc).

Usuaris múltiples: afectació amb impacte a col·lectius d'usuaris diversos i no necessàriament vinculats a la mateixa àrea o departament.

Usuari: afectació individual en el lloc de treball o associada a privilegis d'accés,

errors en la plataforma local, etc.

Viladecans, en la data de signatura electrònica