PLEC DE PRESCRIPCIONS TÈCNIQUES QUE REGIRAN LA CONTRACTACIÓ DEL SERVEI DE SOC (SECURITY OPERATIONS CENTER) DE TECNOCAMPUS MATARÓ-MARESME

EXPEDIENT NÚMERO ES_LA0011122_2026_EXP_84

Contingut

1 Necessitat i idoneïtat de la contractació

La infraestructura tecnològica de TecnoCampus suporta els sistemes d'informació que utilitzen els diferents serveis corporatius en la seva gestió diària. És per això, que aquesta infraestructura de sistemes i comunicacions esdevé un element clau que ha d'assegurar el suport tècnic especialitzat al més alt nivell possible amb l'objecte de garantir un servei continu i d'excel·lència.

Sobre aquesta infraestructura s'implementen tots els serveis que TecnoCampus actualment està oferint i per tant, requereixen el més alt nivell possible de protecció envers amenaces externes com son virus informàtics, ciberatacs o qualsevol mal us, sigui intencionat o no, dels recursos informàtics existents a TecnoCampus per tal que el seu funcionament sigui adequat i de qualitat.

El TecnoCampus disposa en aquests moments d'una plataforma de seguretat Vision One de TrendMicro plenament implantada i amb un alt nivell de desplegament, adaptació a les solucions, serveis i operatives adaptades.

La plataforma Vision One de TrendMicro suposa la base tecnològica sobre la qual es sustenta la seguretat interna i perimetral de la infraestructura informàtica de l'organització. Aquesta plataforma està plenament integrada amb els sistemes i processos interns, i la seva substitució per una alternativa diferent implicaria:

- **Riscos tècnics**: Incompatibilitats amb les integracions existents, interrupció dels serveis i un període d'adaptació que podria comprometre la disponibilitat de serveis essencials.
- **Riscos operatius**: Necessitat de formació addicional del personal, redefinició de protocols i possibles incidències derivades del canvi.
- **Costos addicionals**: Inversió superior en migració, implantació i consultoria, molt per damunt del cost de la renovació de les llicències actuals.

Per tot això, la continuïtat de la solució instal·lada representa l'opció més eficient, segura i econòmica per garantir la protecció i estabilitat dels serveis, i per tant es considera com l'opció tècnicament més adequada i eficient per garantir la continuïtat i integració amb la infraestructura existent.

2 Objecte de la licitació

L'objecte de la licitació és la contractació del servei integral de seguretat SOC del TecnoCampus, dividit en 2 LOTS:

- LOT1: Llicenciament de la plataforma SOC
- LOT2: Servei gestionat SOC

LOT 1 – LLICENCIAMENT DE LA PLATAFORMA SOC

1.- Objecte

L'objecte del contracte dins del seu LOT 1 consisteix en la contractació, provisió i instal·lació del llicenciament dels mòduls actuals i de les millores considerades com a necessàries del Centre d'operacions de seguretat pels serveis i usuaris de Tecnocampus segons indicat a aquest contracte.

El TecnoCampus disposa d'una plataforma Vision One de TrendMicro amb els següents mòduls actualment en vigor i dimensionament, a renovar amb el volum de llicenciament segons definim a continuació:

VisionOne Endpoint Security Essentials (501 dispositius)

- Web and File Reputation
- Exploit & Variant Prevention
- Pre-execution + Runtime Machine Learning
- XDR Sensor

VisionOne Endpoint Security Pro (100 Endpoints)

- Network Security (Host IPS/IDS)
- Malware Protection + Web Reputation
- Integrity Monitoring + Log Inspection
- XDR Sensor

VisionOne Email & Collaboration Security Dual (300 comptes)

- Cloud App Security + Email Security
- Web & File Reputation
- File & URL Sandboxing
- AntiSpam Engine

XDR for Email (300 comptes)

- XDR Sensor

VisionOne Sandboxing (365 unitats)

- 1 Sample per day per 365 days

TrendMicro Internet Security (300 dispositius)

- AntiMalware
- Behavior Analysys

TrendMicro Managed XDR (601 dispositius)

- 24x7 Monitoring
- Incident Investigation & Automated Response

Per altra banda l'augment de l'activitat cibercriminal i la sofisticació de les amenaces actuals requereixen reforçar la solució existent amb un mòdul addicional també ofert dins de la mateixa plataforma i que per tant assegura el màxim nivell d'integració, valor afegit i sinèrgies amb la resta de serveis per assolir la màxima eficiència de la solució i inversió.

Aquest mòdul analitza de manera continuada el nivell d'exposició dels diferents elements i serveis de l'entorn tecnològics del TecnoCampus per prendre les mesures oportunes i optimitzar-los al seu nivell òptim.

Caldrà doncs incloure el següent paquet de llicenciament i volum indicat als descrits anteriorment.

Cyber Risk Exposure Management Essentials (601 dispositius)

- Attack Surface Discovery
- Threat and Exposure Management
- Risk Scoring
- Attack Path Prediction
- Security Awareness
- Compliance Management.

Codi CPV: 48760000-3*: Paquets de software de protecció antivirus*

2.- Abast

a) Estat actual

L'estructura actual securitza l'entorn Tecnocampus des de una Base XDR que gestiona de manera proactiva els serveis de correu, Office 365, entorns cloud, servidors i tots els endpoints corporatius.

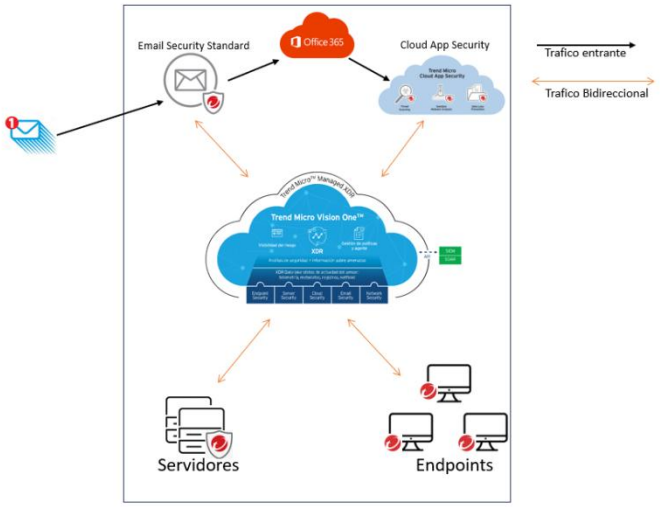

Figura 2 - Esquema serveis TrendMicro (Tecnocampus)

Les necessitats d'actualització i millora de la plataforma actual justifica l'abast de subministrament de llicències del LOT 1 conforme els següents punts específics.

Una vegada revisades les necessitats reals de provisionament i requeriments tècnics respecte el volum de llicenciament actual, es determinen els següents valors de llicenciament a provisionar, instal·lar i renovar anualment durant els 5 anys de subministrament a contractar:

Producte	**Volum**	**Tipologia**
VisionOne Endpoint Security Essentials	**501**	Dispositius
VisionOne Endpoint Security Pro	**100**	Servers
VisionOne Email & Collaboration Security Dual	**300**	Comptes
XDR for Email	**300**	Comptes
VisionOne Sandboxing	**365**	Unitats
TrendMicro Internet Security	**300**	Dispositius
TrendMicro Managed XDR	**601**	Dispositius
CyberRisk Exposure Management Essentials	**601**	Dispositius

b) Condicions de provisió i activació

- Les llicències hauran d'estar actives abans del 16/7/2026 sent que no pot haver-hi interrupció del servei.
- Les llicències hauran de ser oficials del fabricant.

3.- Seguretat i confidencialitat de la informació

L'adjudicatari estarà obligat a mantenir la més estricta confidencialitat respecte de qualsevol informació, dada, configuració, registre, arquitectura, credencial o documentació a la qual tingui accés amb motiu de l'execució del contracte, amb independència del seu format o suport. Aquesta obligació tindrà caràcter indefinit, fins i tot un cop finalitzat el contracte.

L'adjudicatari haurà de complir el Reglament (UE) 2016/679 (RGPD), la Llei Orgànica 3/2018, de protecció de dades personals i garantia dels drets digitals, així com la normativa aplicable en matèria de seguretat de la informació. Quan escaigui, tindrà la condició d'encarregat del tractament, formalitzant-se el corresponent contracte.

Atesa la naturalesa del servei SOC, XDR i seguretat de correu electrònic, l'adjudicatari podrà tenir accés a telemetria d'endpoints, registres de seguretat, metadades i continguts en anàlisi de correu, informació d'usuaris i dispositius, dades d'incidents i vulnerabilitats. En conseqüència, haurà de garantir com a mínim:

- Accés restringit al personal estrictament autoritzat i aplicació del principi de mínim privilegi.
- Autenticació multifactor en els accessos a consoles i entorns del TecnoCampus.
- Registre auditable de totes les actuacions realitzades.
- Comunicacions xifrades mitjançant protocols segurs.
- Prohibició d'extracció o emmagatzematge no autoritzat d'informació.

- Notificació al TecnoCampus, en un termini màxim de 24 hores, de qualsevol incident de seguretat que pugui afectar la informació o els serveis objecte del contracte.

En cas de subcontractació, aquesta requerirà autorització prèvia del TecnoCampus i el subcontractista quedarà subjecte a les mateixes obligacions de confidencialitat i seguretat.

A la finalització del contracte, l'adjudicatari haurà de retornar o destruir tota la informació a la qual hagi tingut accés, certificant-ne per escrit la seva eliminació.

L'incompliment de les obligacions establertes en aquest apartat tindrà la consideració d'incompliment contractual greu.

LOT 2 – SERVEI GESTIONAT SOC

1.- Objecte

L'objecte del contracte dins del LOT 2 consisteix en la **prestació del servei gestionat de monitorització, operació i manteniment de la plataforma de seguretat SOC basada en Trend Micro Vision One**, incloent la gestió d'incidents de seguretat, manteniment preventiu i correctiu, així com l'optimització contínua dels seus mòduls de seguretatEl TecnoCampus disposa d'una plataforma Vision One de TrendMicro amb els següents mòduls en vigor i dimensionament:

- **VisionOne Endpoint Security Essentials (501 dispositius)**
- **VisionOne Endpoint Security Pro (100 Endpoints)**
- **VisionOne Email & Collaboration Security Dual (300 comptes)**
- **XDR for Email (300 comptes)**
- **VisionOne Sandboxing (365 unitats)**
- **TrendMicro Internet Security (300 dispositius)**
- **TrendMicro Managed XDR (601 dispositius)**
- **Cyber Risk Exposure Management Essentials (601 dispositius)**

Codi CPV: 72253200-5 Serveis de recolzament a sistemes

2.- Abast

La estructura actual securitza l'entorn Tecnocampus des de una Base XDR que gestiona de manera proactiva els serveis de correu, Office 365, entorns cloud, servidors i tots els endpoints corporatius.

Les necessitats d'actualització i millora de la plataforma actual justifica l'abast dels serveis gestionats del LOT 2 conforme els següents punts específics:

a) Servei Gestionat

El servei a prestar dins d'aquest contracte suposa la completa explotació i operació de la plataforma llicenciada conforme l'abast del LOT1, manteniment preventiu, manteniment proactiu cercant la millora contínua i màxima eficiència del servei i manteniment correctiu per resoldre i mitigar possibles problemes del servei, atacs, infeccions i afectacions al servei degudes a atacs externs o interns segons indicat als compromisos descrits a aquest contracte.

- VisionOne Endpoint Security Essentials
- VisionOne Endpoint Security Pro
- VisionOne Email & Collaboration Security Dual
- XDR for Email
- VisionOne Sandboxing
- TrendMicro Internet Security
- TrendMicro Managed XDR

S'incopora com a millora del llicenciament ja existent un nou mòdul per millorar els nivells de detecció, interació amb altres serveis tecnològics i minimitzar l'espai exposat a possibles riscos:

- Cyber Risk Exposure Management Essentials (601 dispositius)

Tal i com s'indica prèviament, aquest mòdul ha de ser afegit al servei gestionat conforme les condicions indicades a aquest plec, presentant un projecte d'implantació, operació i explotació per obtenir el màxim valor afegit al servei.

El servei de SOC ha de ser completament gestionat, alliberant de totes les tasques operatives, manteniment preventiu, proactiu i correctiu al personal del Tecnocampus, que restarà amb un paper de gestor i control de l'entorn i del servei.

El servei de CROC ha d'estar específicament dimensionat per poder fer seguiment de l'alt volum de notificacions, cercant sempre les millors solucions, gestió de les plataformes afectades i propostes de millora i optimització constants, assumint un mínim d'una reunió quinzenal i d'u inforrme específic mensual i trimestral.

L'adjudicatari haurà de designar un Responsable de Compte (Account Manager) que actuarà com a interlocutor únic amb TecnoCampus per als aspectes estratègics, institucionals, de gestió i control del servei.

Aquest perfil haurà d'acreditar una experiència mínima de 8 anys en la direcció o coordinació de projectes o serveis similars en l'àmbit de la ciberseguretat o serveis gestionats TIC.

El Responsable de Compte garantirà que el servei ofert estigui d'acord amb els objectius establerts i marcats pel TecnoCampus a aquest contracte.

Un cop posat en marxa el servei el licitador designarà un responsable de servei (Technical Account Manager), qui actuarà com a interlocutor únic i supervisarà en tot moment la qualitat de servei i serà responsable de la gestió i del seguiment del servei objecte d'aquest plec de base.

Aquest perfil haurà d'acreditar una experiència mínima de 8 anys en la implantació i gestió operativa d'entorns de similars caracteristiques en volum de llicències igual o superior a les tractades a aquest plec.

La proposta presentada haurà d'incloure l'equip de treball assignat al projecte tant a la fase d'implantació com a la de prestació del servei. L'equip de treball del projecte haurà d'estar format i certificat en tots els productes i solucions de TrendMicro definit en l'objecte i abast d'aquest contracte, i així s'haurà d'acreditar.

b) Sinèrgies servei seguretat LAN / Perimetral

El servei gestionat del SOC tindrà evidents sinèrgies amb el servei de seguretat Perimetral (Firewall) i de LAN del TecnoCampus actual (Checkpoint/Sophos), així com en qualsevol canvi de plataforma que esdevingui durant la vigènca del contracte, adaptant, modificant o incorporant noves funcionalitats disponibles sempre cercant la excel·lència del serevei envers les sinèrgies establertes entre els entorns de securització del TecnoCampus.

Es requerirà una col·laboració habitual entre els dos serveis a fi d'aconseguir una solució de seguretat òptima aprofitant les fortaleses de les dues solucions i evitant processos o polítiques de seguretat repetitives o innecessàries. A les reunions de seguiment d'ambdós serveis hi haurà sempre un punt del dia per tractar aquestes situacions i seran avaluades com a events de qualitat de servei amb SLA específiques.

Les adaptacions, desenvolupaments dins de les capacitats de la plataforma SOC i el seu seguiment quedarà en tot cas dins de les obligacions contractuals de l'adjudicatari.

c) Manteniment Correctiu

En el moment de que de manera proactiva per part dels serveis del SOC o bé per una notificació del TecnoCampus es consideri que un comportament compatible amb una infecció o incident de seguretat dins de l'àmbit d'actuació de la plataforma gestionada per aquest contracte caldrà iniciar els procediments de avaluació, resolució i informe de les actuacions efectuades, afectacions mitigades i procediments de millora a executar dins del servei de SOC per evitar la seva reproducció.

El servei ha d'incloure específicament la assistència en casos urgents (24x7) no urgents (9x5) segons indicat a continuació:

Serveis davant d'incidents 24x7 (urgents)

- Situacions incloses:
    - **Infecció de virus**: Quan es detecti una amenaça dins de la xarxa i aquesta es trobi afectant servidors crítics del TecnoCampus o un parc d' estacions de treball major al 10%, comptabilitzant en tots els casos només equips protegits per la plataforma Vision One.
    - **Comportament víric a la xarxa**: Quan es presentin símptomes anòmals dins de la xarxa, els quals puguin ser directament relacionats amb noves amenaces i aquests símptomes afectin la continuïtat del negoci, denegant el servei d' enllaços, estacions de treball i serveis crítics per al normal funcionament del TecnoCampus.
    - **Inconvenients de producte** que ocasionin riscos a la continuïtat operativa dedel TecnoCampus. En totes aquelles situacions on es provoqui talls en els serveis crítics protegits per les nostres solucions i on per alguna causa pugui provocar-se denegació de servei o caiguda dràstica del rendiment de la solució.

      Reportat l'incident, el tècnic de guàrdia realitzarà una anàlisi de la situació de manera remota (logs, configuracions i/o mostres de virus recol·lectades). En cas de no poder brindar una solució adequada, es procedirà al tractament on site de l' incident. En tot moment es prioritzarà el temps de resolució de l' incident.

  Davant qualsevol d'aquestes situacions s'haurà de donar un servei de suport 24x7 amb una anàlisi remota o on site si es determinés la necessitat per analitzar i solventar l'incident de seguretat aplicant la solució de workarround que es determini. No hi ha d'haver cap límit en les intervencions d'aquesta tipologia a aquest contracte, incloent actuacions dins o fora d'hores d'oficina, remotes o on-site a petició directa del TecnoCampus.

Serveis Resolutius (no urgents)

En assistències que no siguin considerades urgents caldrà oferir un servei en horari d'oficina per la atenció a possibles incidències menors, resolució de dubtes i qualsevol interacció del SOC sobre la que el responsable del contracte per part del Tecnocampus requereixi. Tots aquests serveis restaran inclosos al contracte sense representar cap sobrecost dins l'àmbit del servei contractat i de les eines que formin part de la plataforma SOC.

Modalitats de prestació:

- Atenció immediata telefònica i via mail pel nostre equip de suport tècnic.

- Sessions remotes compartides amb el client.
- Visites in situ.

En tot moment es prioritzarà la millor opció per arribar a la resolució de l'incident. Les visites presencials hauran de coordinar amb una antelació de dos dies hàbils si és possible.

El TecnoCampus podrà fer ús del servei en qualsevol de les següents situacions:

- Anàlisi i/o resolució de casos oberts.
- Recol·lecció d'informació necessària per a l'obertura/anàlisi de cas.
- Aplicació de configuracions demanades per qualsevol de les parts.
- Neteja d' equips infectats

d) Manteniment Preventiu

L'adjudicatari haurà de presentar un pla de manteniment preventiu que asseguri un correcte funcionament i operació de tota la plataforma del SOC. Aquest pla s'implementarà el primer dia de contracte amb els serveis existents i incorporarà els nous serveis una vegada productius.

Aquest pla de manteniment preventiu haurà d'assegurar que tot el potencial de la plataforma estigui activa conforme les necessitats de l'entorn del Tecnocampus, assegurant tot l'entorn tecnològic i serveis relacionats.

Aquest pla ha d'incorporar:

- Auditoria dels serveis actuals, elaborant un informe específic on s'analitzi la seva definició i funcionament, detectant punts de millora i proposant els plans necessaris per assolir el màxim nivell d'eficiència. (4 setmanes des de inici de contracte)
- Incorporació del nou servei, incrementant la capacitat de control i el nivell de securització de la plataforma del SOC del TCM.
- Llistat de tasques pròpies de manteniment de la plataforma per optimitzar el seu servei de securització, incloent els següents àmbits:
  - Plataforma Trend Micro i serveis
  - Servidors de la plataforma, si aplica.
- Informes de seguiment de projecte

Dins d'aquets manteniment també quedaran incorporades totes les configuracions i canvis dels serveis de la plataforma que siguin necessaris per disposar en tot moment de la millor solució de SOC possible.

e) Formació personal TCM

El licitador inclourà en la seva proposta un Pla de Formació proposat per a la transferència de coneixement sobre el servei desplegat que inclourà:

- Administració i configuració de la plataforma.
- Resolució de problemes.
- Gestió del servei.
- Formació sobre el servei desplegat adreçada a personal del TecnoCampus amb perfils no tècnics en cas necessari

Aquesta proposta ha de ser d'una duració de 8 h per personal tècnic i de 2 hores per usuari no tècnic, ha de ser impartida en versió online o webinar en cas de la formació no técnica, i ha de ser disposada en cas de petició justificada per part de TecnoCampus durant tot el període contractual.

Reunions de seguiment

L'adjudicatari es compromet a generar informes que inclouran com a mínim les següents dades:

- Estat i evolució dels diferents serveis del SOC
- Incidències de seguretat i procediments aplicats.
- Tasques programades (executades i planificades)
- Interaccions amb altres serveis
- Propostes de millora
- Altres

Aquests informes hauran de ser entregats i posats a la disposició de TecnoCampus, per ser revisats i analitzats quan sigui necessari.

Resum de la prestació de serveis

Es consideren com a elements de compliment obligatori per assegurar la màxima eficiència del servei els següents punts:

Serveis professionals	Característiques del servei
Suport resolutiu 9x5	Sense límit d'incidents. Contacte via correu electrònic, telefònic, suport remot o in situ, depenent de la incidència i la seva gravetat.
Servei d'emergència 24x7 remot i on-site davant incidents que puguin posar en perill la continuïtat dels serveis del TecnoCampus i que requereixin unes accions d'urgència fora de l'horari habitual.	El servei serà aplicable davant d'incidències (infecció de virus, ransomware, o fallides de producte) classificades amb impacte ALT o CRÍTIC i que afectin com a mínim a: • Servidors crítics. • 10% estacions de treball o servidors. • 10% usuaris de la Fundació Tecnocampus També en cas de comportament víric de la xarxa corporativa. I finalment, davant d'inconvenients de producte que ocasionin riscos a la continuïtat operativa de l'organització; és a dir, en totes aquelles situacions on es provoqui talls en els serveis crítics protegits per les solucions TrendMicro i on per alguna raó pugui provocar-se denegació de servei o caiguda dràstica del rendiment de la solució. Sense límit tant de número d'incidents com d'hores a dedicar a la seva resolució.
Centre d'operacions de ciber risc (CROC)	Servei que dóna gestió integral del ciber risc. Es requereix que el servei cobreixi les fites següents: descobriment constant de la superfície d'atac, identificació de potencials amenaces i recomanacions accionables per disminuir els riscos de la companyia.

Revisió de la infraestructura.	Totes les solucions esmentades a l'objecte i abast d'aquest contracte
Responsable tècnic del servei (technical account manager).	Destinat a revisions de la infraestructura, presentació de l'estat i resultats, planificació anual de manteniments i gestió i execució del pla d'accions consensuat. Pla anual de treball amb visites programades.
Responsible del compte (Account manager)	Destinat a sser l'interlocutor únic amb TecnoCampus per als aspectes estratègics, institucionals, de gestió i control del servei.
Capacitacions d'administració de la plataforma. Una formació de 8 hores en dos dies no consecutius.	Assistents il·limitats.
Capacitacions pe personal no tècnic (formació de 2 hores)	Assistents il·limitats.
Monitoratge i seguiment de VisionOne (XDR).	Sense límit d'Incidents.

3.- Adscripció de mitjans al contracte

El licitador designarà en l'àmbit estratègic un responsable del compte (Account Manager) qualificat , que actuarà com a interlocutor únic i estarà a disposició de tots els aspectes estratègics, institucionals, de gestió i control i garantirà que el servei ofert estigui d'acord amb els objectius establerts i marcats pel TecnoCampus a aquest contracte.

Un cop posat en marxa el servei el licitador designarà un responsable de servei (Technical Account Manager), qui actuarà com a interlocutor únic i supervisarà en tot moment la qualitat de servei i serà responsable de la gestió i del seguiment del servei objecte d'aquest plec de base.

Ambdós recursos hauran d'acomplir els requisits indicats a l'abast del LOT 2.

La proposta presentada haurà d'incloure l'equip de treball assignat al projecte tant a la fase d'implantació com a la de prestació del servei.

L'equip de treball del projecte haurà d'estar format i certificat en tots els productes i solucions de TrendMicro definit en l'objecte i abast d'aquest contracte.

4.- Paràmetres de gestió de la qualitat del servei

Els següents aspectes i indicadors seran un referent per avaluar la correcta gestió de la qualitat del servei i seran revisats de forma mensual pel TecnocCmpus.

Es consideraran per la correcta gestió: els indicadors d'incidències, seguiment del servei i interaccions amb el servei gestionat de seguretat Perimetral i LAN/WAN del TecnoCampus i el seu temps de resposta i resolució.

a) Incidències

Es classificaran els diferents tipus d'incidències segons la seva criticitat, urgent o normal segons indicat a punt 2 b) d'aquest document lot "Manteniment correctiu"

b) Interaccions amb servei de seguretat Perimetral i LAN/WAN

Els servei gestionat del SOC i el de Seguretat Perimetral requeriran d'una interlocució i seguiment comú evident i serà responsabilitat del TecnoCampus establir les vies de comunicació adient per assolir aquesta sinèrgia del tot necessària. En qualsevol moment i sota petició de qualsevol de les parts es pot iniciar una comunicació per solucionar una incidència, gestionar una petició d'informació o qualsevol consideració necessària pel bon funcionament dels dos serveis. Es considera crítica aquesta col·laboració i per això es defineixen els indicadors de seguiment següents:

- **Urgents**: Requeriments per solucionar incidències de servei que tinguin afectació greu (serveis indisponibles)
- **Normals**: Requeriments d'informació, configuracions, tasques programades o reunions de seguiment

c) Temps de resposta i temps de resolució

Es defineix com a **Temps de Resposta** el període entre la recepció per part de l'adjudicatari als seus sistemes de monitorització (incidències) o bé per les vies de comunicació habituals (trucada telefònica i/o email) per peticions de seguiment de servei o interaccions amb el Servei de seguretat Perimetral.

Es defineix com a **Temps de Resolució** el període entre la seva recepció i la recuperació del servei afectat una vegada aplicats els procediments adients en el cas de les incidències i del període entre la recepció de la notificació i la seva resposta fonamentada i/o resolutòria.

SLA incidències		
Tipus	**Temps resposta**	**Temps resolució**
Urgent	< 5'	< 30'
Normal	< 15'	< 240'

Figura 3 - SLA Incidències

SLA Interaccions SSP		
Tipus	**Temps resposta**	**Temps resolució**
Urgent	< 5'	< 30'
Normal	< 15'	< 240'

Figura 4 - SLA Interaccions amb el Servei seguretat Perimetral

Els acords de servei aquí indicats hauran de ser d'obligat compliment per l'adjudicatari i seran auditats i penalitzats en cas d'incompliment segons referit a la documentació d'aquest contracte

5.- Règim de penalitzacions

Les penalitzacions derivades de l'incompliment dels nivells de servei (SLA) establerts al present Plec seran aplicables en aquells supòsits en què l'adjudicatari no compleixi els Temps de Resposta i/o els Temps de Resolució definits per a les incidències i per a les interaccions amb el Servei de Seguretat Perimetral. L'aplicació d'aquestes penalitzacions es fonamenta en el que disposa l'article 192 i concordants de la Llei 9/2017, de 8 de novembre, de Contractes del Sector Públic, relatiu a la imposició de penalitats per compliment defectuós o incompliment de les obligacions contractuals, així com en la facultat de l'òrgan de contractació de vetllar pel correcte desenvolupament del contracte.

L'aplicació de les penalitats tindrà caràcter automàtic un cop verificada objectivament la desviació respecte dels valors compromesos, sense que en cap cas l'existència de penalització eximeixi l'adjudicatari de l'obligació de restablir el servei afectat amb la màxima diligència i conforme als procediments tècnics adequats.

El càlcul de les penalitzacions es realitzarà amb periodicitat mensual, prenent com a base la facturació mensual del servei, i en cap cas l'import total acumulat de les mateixes podrà superar el vint per cent de la facturació corresponent al període mensual afectat, d'acord amb els límits establerts per la normativa aplicable. La reiteració sistemàtica d'incompliments podrà ser considerada incompliment contractual greu als efectes previstos en la LCSP, podent donar lloc, si escau, a l'adopció de mesures addicionals, inclosa la resolució del contracte en els termes legalment establerts.

a. Penalitzacions

Incidències Urgents (*SLA: Temps de Resposta < 5 minuts | Temps de Resolució < 30 minuts)*

Tipus incompliment	Franja de desviació	Penalització sobre facturació mensual
Temps de Resposta	> 5' i ≤ 10'	2 %
Temps de Resposta	> 10' i ≤ 20'	4 %
Temps de Resposta	> 20'	6 %
Temps de Resolució	> 30' i ≤ 60'	8 %
Temps de Resolució	> 60' i ≤ 120'	10 %
Temps de Resolució	> 120'	15 %

Incidències Normals (*SLA: Temps de Resposta < 15 minuts | Temps de Resolució < 240 minuts)*

Tipus incompliment	Franja de desviació	Penalització sobre facturació mensual
Temps de Resposta	> 15' i ≤ 30'	1 %
Temps de Resposta	> 30' i ≤ 60'	2 %
Temps de Resposta	> 60'	4 %
Temps de Resolució	> 240' i ≤ 360'	6 %
Temps de Resolució	> 360' i ≤ 600'	8 %
Temps de Resolució	> 600'	10 %

6. Finalització i transferència del servei

En cas de finalització del contracte l'adjudicatari restarà obligat a efectuar un traspàs de coneixement al nou prestatari de manera adequada per assegurar que el SOC no es veu afectat ni pel canvi de prestatari ni per el possible canvi de plataforma. Aquest període de traspàs de coneixement serà de 4 setmanes (iniciant 2 setmanes abans de la finalització del contracte actiu), o es proporcionarà al nou adjudicatari tota la informació que requereixi per assegurar la continuïtat del servei sota control del personal responsable del TecnoCampus. Aquesta informació inclourà, com a mínim els informes de seguiment mensuals i anual del del servei, operatives habituals, recursos assignats, incidents de seguretat reportats i tractament aplicat en informe específic, així com tota la informació que es consideri necessària validada pel responsable del contracte.

7. Proposta tècnica

Els licitadors hauran de presentar una memòria tècnica de compliment dels requeriments indicats a la documentació d'aquest contracte conforme indicat a aquest punt, amb un màxim de 35 fulls, coberta inclosa, sense considerar annexos. Més enllà de 35, no es tindrà en compte la informació inclosa.

- Documentació que justifiqui i evidencii de manera clara el la implemetació i/o compliment dels punts requerits dins d'aquest document, específicament:
  - Proposta justificada de continuïtat dels serveis existents i millores segons indicades a punts 2 d'aquest document "Servei Gestionat"
  - Compliment específic documentat de tots els requeriments indicats a la taula d'aquest document, "Resum de Prestació de serveis"
  - Tots els punts especificats dins de l'apartat de Solvència Tècnica i professional d'aquest contracte
- Proposta d'implementació detallada i justificada del nou servei "CREM"
- Proposta de Pla de Servei gestionat
- Proposta del Pla de gestió del servei "CROC"

- Proposta de sinèrgies amb l'entorn de seguretat perimetral del TecnoCampus
- Proposta de Manteniment Correctiu
- Proposta de Manteniment Preventiu
- Proposta de Formació
- Proposta de finalització de servei
- Qualsevol altra documentació que justifiqui els requeriments a acomplir pel servei.

8.- Seguretat i confidencialitat de la informació

L'adjudicatari estarà obligat a mantenir la més estricta confidencialitat respecte de qualsevol informació, dada, configuració, registre, arquitectura, credencial o documentació a la qual tingui accés amb motiu de l'execució del contracte, amb independència del seu format o suport. Aquesta obligació tindrà caràcter indefinit, fins i tot un cop finalitzat el contracte.

L'adjudicatari haurà de complir el Reglament (UE) 2016/679 (RGPD), la Llei Orgànica 3/2018, de protecció de dades personals i garantia dels drets digitals, així com la normativa aplicable en matèria de seguretat de la informació. Quan escaigui, tindrà la condició d'encarregat del tractament, formalitzant-se el corresponent contracte.

Atesa la naturalesa del servei SOC, XDR i seguretat de correu electrònic, l'adjudicatari podrà tenir accés a telemetria d'endpoints, registres de seguretat, metadades i continguts en anàlisi de correu, informació d'usuaris i dispositius, dades d'incidents i vulnerabilitats. En conseqüència, haurà de garantir com a mínim:

- Accés restringit al personal estrictament autoritzat i aplicació del principi de mínim privilegi.
- Autenticació multifactor en els accessos a consoles i entorns del TecnoCampus.
- Registre auditable de totes les actuacions realitzades.
- Comunicacions xifrades mitjançant protocols segurs.
- Prohibició d'extracció o emmagatzematge no autoritzat d'informació.
- Notificació al TecnoCampus, en un termini màxim de 24 hores, de qualsevol incident de seguretat que pugui afectar la informació o els serveis objecte del contracte.

En cas de subcontractació, aquesta requerirà autorització prèvia del TecnoCampus i el subcontractista quedarà subjecte a les mateixes obligacions de confidencialitat i seguretat.

A la finalització del contracte, l'adjudicatari haurà de retornar o destruir tota la informació a la qual hagi tingut accés, certificant-ne per escrit la seva eliminació.

L'incompliment de les obligacions establertes en aquest apartat tindrà la consideració d'incompliment contractual greu.