

Plec de clàusules tècniques per a la contractació de la implantació i serveis gestionats d'una solució EDR (Endpoint Detection Response) per el Parc Sanitari Pere Virgili

Expedient 24/276

Índex

1	Antecedents	2
2	Objecte del contracte	3
3	Descripció de la situació actual	4
4	Descripció del servei	5
4.1	Implantació i desplegament de la plataforma, els agents i les polítiques.....	5
4.2	Servei Gestionat 24x7 MDR.....	6
4.3	Serveis de formació	8
5	Requeriments generals	10
5.1	Actitud proactiva	10
5.2	Model de relació	10
5.2.1	Perfils del Parc Sanitari Pere Virgili.....	10
5.2.2	Perfils de l'adjudicatari	11
5.3	Òrgans de gestió	14
5.3.1	Comitè de direcció	14
5.3.2	Comitè de seguiment	15
5.4	Adequació permanent a les necessitats.....	16
5.5	Condicions de la prestació del servei.....	16
5.5.1	Eina de gestió tiqueting (ITSM)	16
5.5.2	Canals de comunicació	17
5.5.3	Ubicació física del servei.....	17
6	Execució del projecte	18
7	Acords de Nivell de Servei (ANS)	19
7.1	Incompliments	19
7.2	Penalitzacions	20
8	Altres consideracions	21
8.1	Presentació de la documentació	21
8.2	Esquema Nacional de Seguretat	21

1 Antecedents

L'activitat principal del Parc Sanitari Pere Virgili, en endavant PSPV, és la prestació de serveis assistencials, d'investigació i docència. Addicionalment a aquesta activitat també es realitza la gestió de suport a d'altres serveis assistencials i a entitats de l'entorn sanitari ubicades al Parc, així com la gestió dels immobles i instal·lacions en el recinte. En l'any 2018 es va traspasar la gestió d'Atenció Primària del PAMEM que consta de 3 centres d'atenció primària i un CUAP.

Segons es reflecteix en la definició pròpia de l'empresa, els objectius a assolir son:

- Gestionar els edificis i les instal·lacions del recinte i, a aquest efecte, pactar els negocis jurídics que escaiguin a fi i efecte de possibilitat que tercers hi puguin realitzar les activitats que siguin d'interès del Servei català de la Salut, sense més limitacions que les establertes en les normes de patrimoni de la Generalitat de Catalunya i al Pla Especial d'Ordenació del recinte de l'antic Hospital Militar de Barcelona.
- Prestar serveis d'atenció sanitària i de salut mental, com també de promoció de la salut, prevenció de la malaltia i atenció sociosanitària a la població.
- L'execució de programes institucionals en matèria de protecció de la salut, prevenció de la malaltia, assistència sanitària i sociosanitària i rehabilitació.
- La prestació, en el seu cas, i la gestió de serveis de suport a d'altres serveis assistencials.
- Desenvolupar programes d'investigació en l'àmbit de la salut i col·laborar amb la universitat i la resta d'institucions competents en matèria de docència i recerca.
- Desenvolupar totes les actuacions necessàries per al compliment dels seus objectius, com també les actuacions en relació amb les funcions esmentades anteriorment que li siguin encomanades.

2 Objecte del contracte

L'objecte de la present licitació és la contractació de serveis per la implantació i gestió del (Managed Detection and Response) del EDR (Endpoint Detection and Response) del Parc Sanitari Pere Virgili. Els serveis gestionats inclouen:

- **Servei de implantació d'una solució EDR**
 - Desplegament de la plataforma.
 - Instal·lació dels agents.
 - Configuració polítiques EDR.
- **Servei de manteniment correctiu, normatiu i preventiu**
 - Servei de monitorització, detecció i resposta 24x7 de l'activitat registrada per la plataforma de CrowdStrike.
 - Informes periòdics.
- **Serveis de formació tècnica**
 - Traspàs de coneixements al equip IT de tot el desplegament i configuració de la plataforma i les polítiques.
 - Formació en els serveis de resposta a incidents de crowdstrike.

Amb aquests objectius, es pretén assegurar una solució, que suporti les necessitats operatives així com garantir la disponibilitat, la seguretat i el rendiment òptim del equips del PSPV, assegurant una operativa eficient i ininterrompuda.

- Garantir la homogeneïtat a nivell d'equipament de les solucions proposades.
- Garantir els màxims nivells d'homogeneïtat i integració en les solucions de xarxa resultants.
- Disposar dels serveis de suport del/s fabricant/s necessaris per tal d'integrar el manteniment del nou equipament dins del servei global de manteniment de xarxa actual, d'acord amb els nivells de servei establerts.
- Disposar d'una documentació acurada de les noves instal·lacions i garantir un correcte traspàs del coneixement al personal del PSPV mitjançant documentació i formacions.
- Realitzar una correcta gestió de residus amb l'equipament actual substituït.

3 Descripció de la situació actual

Actualment, el PSPV disposa de la solució Kaspersky Total Security for Business amb 800 punts finals llicenciats i una gestió centralitzada mitjançant la consola Kaspersky Security Center. Aquesta consola compta amb diferents usuaris amb permisos a nivell d'operador i d'administrador. La solució de Kaspersky inclou complements de control de dispositius, firewall, protecció web i xifrat d'unitats extraïbles. Cada punt final té instal·lat l'agent de xarxa i el Kaspersky Endpoint Security, disponible per a sistemes Windows, Linux i Mac. Aquesta solució està implementada tant a nivell client com servidor.

Amb l'increment d'aparició d'actors del cibercrim, la millora en les seves tècniques i els atacs perpetrats, els antivirus tradicionals ja no són suficients per garantir unes mínimes mesures de seguretat. A causa de l'augment de les amenaces i la sofisticació dels atacs, el PSPV ha considerat necessari avançar cap a una solució més moderna, robusta i eficaç per protegir les dades i sistemes davant de les amenaces actuals.

Per abordar aquestes necessitats de seguretat avançada, el PSPV ha adquirit les següents llicències de la solució CrowdStrike Falcon:

- Falcon Endpoint Protection Enterprise Bundle
 - Falcon Prevent (NGAV)
 - Falcon Insight (EDR)
 - Threat Graph Standard
 - Device Control
 - Firewall Management
 - Support
 - CrowdStrike University

Aquesta nova solució de EDR (Endpoint Detection and Response) permetrà millorar significativament la capacitat de detecció, resposta i prevenció davant d'amenaces avançades. La implementació de CrowdStrike Falcon contribuirà a assolir els objectius de millora en la ciberseguretat que el PSPV s'ha proposat, proporcionant una protecció més integral i eficient contra les noves formes d'atacs cibernètics.

4 Descripció del servei

L'objecte de la present licitació és la contractació de serveis per la implantació i gestió del (Managed Detection and Response) del EDR (Endpoint Detection and Response). Aquest servei inclourà la configuració inicial, la migració dels punts finals des de la solució Kaspersky actual cap a CrowdStrike Falcon, i la formació necessària per al personal de TIC del Parc Sanitari Pere Virgili. A més, es proporcionarà un servei gestionat continu que garantirà la supervisió constant, la detecció proactiva d'amenaçes i la resposta ràpida a incidents de seguretat. La solució ha de ser capaç d'integrar-se amb les infraestructures actuals del PSPV, assegurant una transició suau i sense interrupcions en el servei. També s'espera que el proveïdor seleccionat ofereixi suport tècnic especialitzat i actualitzacions periòdiques per mantenir el sistema en òptimes condicions.

4.1 Implantació i desplegament de la plataforma, els agents i les polítiques

- a) Desplegament de la plataforma.
 - Alta del tenant CrowdStrike: Creació del tenant de CrowdStrike Falcon específic per al PSPV.
 - Creació d'usuaris: Configuració dels usuaris tant de l'empresa responsable de la gestió com dels usuaris del PSPV. En el cas del PSPV s'hauran de crear usuaris amb els permisos més elevats que permeti la plataforma.
- b) Instal·lació dels agents.
 - La instal·lació dels agents de CrowdStrike Falcon es realitzarà inicialment en un petit grup de endpoints on conviuran conjuntament amb la solució d'antivirus actual, aquest grup reduït d'endpoints estaran designats pel PSPV d'aquesta manera poder afrontar de manera controlada les incidències ocasionades per la implantació.
 - La implantació es durà a terme seguint les recomanacions i directrius establertes en les guies CCN-STIC del Centre Criptològic Nacional (CCN), per assegurar un nivell òptim de seguretat i compliment de les normatives vigents.
 - Un cop validat el bon funcionament de l'eina en els equips del primer grup designat per part del PSPV, es realitzarà la implantació de manera gradual, en petits grups tenint en compte les diferents tipologies i perfils dels endpoints, que poden incloure variacions en les aplicacions i els escenaris d'ús. Això assegurarà que cada grup d'endpoints sigui gestionat segons les seves necessitats específiques, garantint una transició efectiva i sense problemes.
 - L'empresa encarregada de la implantació proporcionarà suport tècnic per gestionar qualsevol incidència que pugui sorgir durant el desplegament dels agents en els endpoints.
- c) Configuració polítiques EDR.
 - El desplegament progressiu de les polítiques de CrowdStrike Falcon es realitzarà inicialment en mode de monitoratge per assegurar la compatibilitat i convivència amb l'actual solució de Kaspersky Endpoint Security. Aquesta estratègia permetrà observar el comportament dels endpoints sense interferir

amb les seves operacions normals. A mesura que es validi el correcte funcionament en els diferents grups designats, es procedirà a ajustar i aplicar les polítiques de seguretat de manera gradual, tenint en compte les peculiaritats i necessitats específiques de cada grup d'endpoints. Aquesta configuració de polítiques s'alinejarà amb el procés de desplegament dels agents descrits anteriorment, assegurant que cada grup d'equips sigui gestionat amb les polítiques adequades per garantir una transició suau i efectiva cap a la nova solució de seguretat.

- Configuració polítiques adaptades a les necessitats i circumstàncies de la empresa, calibració de les mateixes tenint en compte aspectes com aplicacions corporatives, falsos positius o altres que puguin sorgir.
- L'empresa encarregada de la implantació proporcionarà suport tècnic per gestionar qualsevol incidència que pugui sorgir durant el desplegament de les polítiques.

El licitador haurà de lliurar tota la documentació de suport, documentació de projecte, manuals d'implantació, documentació tècnica, documentació de processos, etc. que es generi durant el desenvolupament del projecte.

4.2 Servei Gestionat 24x7 MDR

a) Detecció

El servei gestionat 24x7 de Monitorització, Detecció i Resposta (MDR) de CrowdStrike Falcon proporcionarà una vigilància constant de les alertes generades per la plataforma. Això implica la monitorització contínua dels endpoints per identificar activitats sospitoses o malicioses. Utilitzant tècniques avançades de detecció d'amenaques basades en la metodologia MITRE ATT&CK, es garanteix la visibilitat completa sobre els comportaments anòmals i les amenaces avançades que podrien passar desapercibudes pels sistemes de seguretat tradicionals. L'objectiu és la detecció proactiva de possibles incidents abans que puguin afectar l'operativa diària de l'empresa.

Les alertes seran classificades segons la seva gravetat en les categories següents:

- Baixa: Alertes que indiquen activitats que poden representar un risc potencial menor per a la seguretat de la infraestructura.
- Mitja: Alertes que són més sospitoses o que poden indicar una activitat anòmla més significativa.
- Alta: Alertes que indiquen activitats que representen un risc considerable per a la seguretat.
- Crítica: Alertes que indiquen una amenaça immediata i altament perjudicial per a la seguretat de la infraestructura.

En el cas que es detectin alertes que necessitin d'un supervisió, es requeriment sigui realitzada per analistes de seguretat qualificats abans de ser categoritzada, assegurant així, una resposta adequada i proporcionant recomanacions per a la mitigació del risc. Aquest procés garantirà una resposta eficaç i oportuna davant de possibles amenaces, minimitzant l'impacte i protegint la integritat dels sistemes del PSPV.

b) Resposta

En aquesta fase un cop es rep una alerta generada per la detecció reportada per la plataforma CrowdStrike Falcon, es duu a terme una anàlisi inicial per confirmar o descartar el positiu. Aquest procés inclou la revisió detallada de la informació proporcionada per l'alerta i la correlació amb altres dades per determinar la veracitat de l'amenaça.

En cas que l'alerta sigui confirmada com a positiva, s'ha de procedir amb les següents fases:

- Identificació: Es determina la naturalesa i l'abast de l'amenaça, així com els sistemes afectats i els vectors d'atac emprats.
- Possibles Actuacions: l'ordre d'aplicació pot variar en funció de les necessitats
 1. Contenció: Es prenen mesures immediates per limitar la propagació de l'amenaça, com aïllar els sistemes compromesos o bloquejar comunicacions malicioses. Aquestes accions es prenen de manera controlada per assegurar la mínima interrupció dels serveis. Cap d'aquestes actuacions es pot fer sense el coneixement del Parc Sanitari Pere Virgili.
 2. Erradicació: Un cop continguda l'amenaça, es procedeix a la seva completa eliminació del sistema afectat. Això pot incloure la desinfecció de fitxers, l'eliminació de programari maliciós i sempre facilitar la informació perquè el Parc Sanitari Pere Virgili pugui fer les correccions de vulnerabilitats explotades adients.
 3. Accions de correcció: Es poden prendre o desfer accions de correcció segons sigui necessari per restablir la seguretat del sistema afectat i assegurar la seva operativitat. Això inclou la restauració de configuracions segures i l'aplicació de pegats o actualitzacions de seguretat.
- Adaptació de polítiques: En el cas que la política no reculli el procediment d'actuació davant una alerta, es requereix afegir i/o modificar les polítiques de seguretat i ajustar-les per prevenir futures incidències similars, millorant així la resposta davant d'amenaques i garantint la contínua evolució i actualització de les polítiques del Parc Sanitari Pere Virgili.

c) Informes periòdics.

El servei gestionat 24x7 de Monitorització, Detecció i Resposta (MDR) inclou la generació d'informes periòdics per proporcionar una visió completa i detallada de l'activitat rellevant i les amenaces detectades.

El Parc podrà demanar a l'adjudicatari la creació d'informes i documentació addicional o amb una altra periodicitat, sense que això suposi una despesa addicional. Totes les documentacions s'hauran de lliurar en format PDF. El idioma de la documentació serà el català.

Aquests informes seran elaborats amb els següents components:

- A. Informes d'activitat i amenaces: Basats en la matriu de MITRE ATT&CK, aquests informes documentaran l'activitat rellevant i les amenaces detectades i

bloquejades durant el període d'informe. Inclouran detalls sobre els vectors d'atac, el cicle de vida de les amenaces, i la classificació de les alertes en categories com Malware, Indicadors de Compromís (IoC), Exploits, comportaments sospitosos, robatori de credencials, persistència, moviment lateral, elevació de privilegis i exfiltració de dades. Quan sigui aplicable, s'inclouran els equips i usuaris afectats detectats durant els incidents.

La periodicitat de disponibilitat i presentació d'aquest informe ha de ser mensual.

- B. Informes de propostes d'optimització o evolució: Aquests informes proporcionaran recomanacions per millorar contínuament la seguretat de la infraestructura del PSPV. Inclouran suggeriments basats en les últimes tendències de seguretat, noves vulnerabilitats descobertes i millors pràctiques identificades durant el període d'informe.

Aquest informe s'entregarà a finals d'any i haurà d'incorporar com a mínim els següents apartats:

- Sobre les tendències tecnològiques: tendències de futur previstes per a la tecnologia analitzada, descripció de les possibles aplicacions de les tendències a futur identificades a les funcionalitats desenvolupades al Parc Sanitari Pere Virgili.
- Sobre les tendències estratègiques: anàlisi de tendència, propostes de millora, propostes de formació, gestió del canvi o documentals, propostes per reduir riscos identificats.

La periodicitat de disponibilitat i presentació d'aquest informe ha de ser semestral.

- C. Informes de noves necessitats: Identificaran i documentaran les noves necessitats de seguretat que puguin sorgir durant el transcurs del servei. Això pot incloure la necessitat de nous controls de seguretat, ajustos en les polítiques existents, o l'adopció de noves tecnologies o metodologies per enfrontar amenaces emergents.

La periodicitat de disponibilitat i presentació d'aquest informe ha de ser anual.

El responsable del servei designat per l'empresa adjudicatària haurà de presentar informes periòdics, i tots aquells altres que a petició del Responsable/s del Projecte del Parc Sanitari Pere Virgili poguessin servir per a la òptima consecució dels objectius previstos.

4.3 Serveis de formació

L'objecte de les sessions de formació es facilitar i assegurar que el personal del **Parc Sanitari Pere Virgili** estigui plenament preparat per gestionar la nova solució de seguretat, maximitzant així l'eficàcia del servei gestionat i garantint una protecció contínua i robusta contra les amenaces cibernètiques

L'adjudicatari serà responsable de proporcionar una formació completa i detallada als tècnics del PSPV. Aquesta formació inclourà els següents aspectes:

- a) **Traspàs de coneixements:** Traspàs de coneixements al equip IT: Es realitzarà una formació exhaustiva per assegurar que l'equip IT del PSPV compregui completament el desplegament i la configuració de la plataforma CrowdStrike Falcon, així com les polítiques aplicades.
- b) **Formació en serveis de resposta a incidents:** Es proporcionaran sessions de formació específiques sobre els serveis de resposta a incidents de CrowdStrike. Això inclourà la identificació, contenció, erradicació i recuperació davant de diverses amenaces, així com l'ús eficient de les eines i funcionalitats de la plataforma per a la gestió d'incidents. Es requeriment que aquesta formació garanteixi que els tècnics estiguin capacitats per gestionar i mantenir la solució de manera autònoma.
- c) **Formació contínua en canvis i actualitzacions:** L'adjudicatari haurà de proporcionar formació contínua per assegurar que els tècnics estiguin al corrent de qualsevol canvi o actualització en la plataforma CrowdStrike Falcon. Això inclourà noves funcionalitats, millores en les polítiques de seguretat i adaptacions a les noves amenaces emergents.

5 Requeriments generals

Adicionalment als requeriments de cada servei, hi ha un conjunt de requeriments, vinculats no tant a les tecnologies sinó als serveis associats, que són comuns a tots els serveis, i que l'empresa contractista haurà de satisfer segons la següent relació de requeriments:

5.1 Actitud proactiva

En tots els àmbits dels serveis a contractar es demana una permanent actitud proactiva per part del proveïdor seleccionat, és a dir, es desitja que el proveïdor seleccionat sigui un veritable soci tecnològic del PSPV. Això implica, entre d'altres, a més de la gestió reactiva de les alertes, la **cerca proactiva** d'amenaques emergents i l'anàlisi de sospites d'amenaça. Això permet identificar potencials riscos abans que es materialitzin en incidents de seguretat, garantint una protecció contínua i robusta del PSPV.

5.2 Model de relació

L'empresa contractista i el PSPV constituïran, com a mínim, un Comitè de Direcció i un Comitè de Seguiment. Totes les decisions adoptades per ambdós comitès seran d'obligat compliment per part de l'empresa contractista i del PSPV, vetllant pel correcte compliment del contracte i facilitant la presa de decisions d'alt nivell.

S'ha de considerar que és molt possible que s'hagin de realitzar desplaçaments a PSPV per part de l'equip de projecte del licitador, per a temes relacionats amb les diferents fases del projecte.

El licitador aportarà els mitjans tècnics que requereixi el seu equip de projecte per a poder realitzar les tasques necessàries durant el projecte (portàtil, telèfon mòbil, etc.).

Les despeses de desplaçament o dietes seran a càrrec del proveïdor, i s'hauran d'incloure dins del preu final de la licitació.

5.2.1 Perfils del Parc Sanitari Pere Virgili

En general per part del **PSPV** els membres i les seves funcions seran:

Cap de projecte ocupat per Direcció d'Organització i Comunicació (responsable del contracte).

- Gestionar el contracte amb l'empresa contractista.
- Coordinar-se amb la direcció funcional, el coordinador del projecte i l'equip de treball del PSPV.
- Acordar amb el responsable del projecte de l'empresa contractista les mesures de qualitat i resultats, i controlar la prestació del servei d'acord amb elles.
- Acordar amb el director del servei de l'empresa contractista mesures per solucionar qualsevol deficiència en la qualitat del servei.
- Acordar els procediments d'escalat de problemes i assegurar la resolució de problemes no resolts mitjançant els canals normals.
- Assegurar que el contractista compleixi amb els requeriments de protecció, confidencialitat i seguretat necessaris, realitzant quan sigui necessari les oportunes auditories.

- Revisió del compliment dels compromisos acordats en sessions anteriors

Responsable del projecte, ocupat per Sots Direcció TIC

- Realitzar el seguiment i control regular de la consecució d'objectius.
- Realitzar un seguiment detallat de l'execució de les tasques planificades i el calendari previst.
- Proporcionar canals de comunicació adequats que permetin dur a terme les tasques necessàries per al projecte, tant amb els usuaris com amb les altres àrees del PSPV.

Coordinador del projecte, ocupat per Cap de Sistemes, Comunicacions i Ciberseguretat.

- Oferir atenció especialitzada i coneixement sobre assumptes relacionats amb el funcionament i la utilització concreta dels serveis a migrar al PSPV.
- Acordar procediments per a la gestió eficient dels canvis i controlar l'efectivitat dels mateixos, minimitzant l'impacte als usuaris.

Tècnics àrea TIC:

- Realitzar un seguiment detallat de l'execució de les tasques planificades.
- Realitzar el seguiment i control regular de la consecució d'objectius.
- Oferir atenció especialitzada i coneixement sobre assumptes relacionats amb el funcionament i la utilització concreta dels serveis a migrar al PSPV.
- Proporcionar canals de comunicació adequats que permetin dur a terme les tasques necessàries per al projecte, tant amb els usuaris com amb les altres àrees del PSPV.
- Acordar procediments per a la gestió eficient dels canvis i controlar l'efectivitat dels mateixos, minimitzant l'impacte als usuaris.

5.2.2 Perfils de l'adjudicatari

Per part de l'**empresa contractista** els perfils que es requereixen son:

Responsable del projecte

- Es requereix:
 - o FHT LP-S Security and IT Operation
 - o Enginyeria superior.
 - o Gestió de projectes.
 - o Experiència mínima demostrable de 5 anys en tasques similars.
- Les seves funcions són:
 - o Assegurar que l'empresa contractista compleixi les seves obligacions contractuals.
 - o Assegurar el compliment d'objectius i ANS.
 - o Assegurar la disponibilitat i el seguiment dels procediments de seguiment de resultats i la gestió del contracte.
 - o Escalar assumptes a la direcció de l'empresa contractista quan sigui necessari.
 - o Donar suport a l'especificació de qualsevol requeriment de servei addicionals i canvis d'abast davant del PSPV.

- Mantenir una preocupació proactiva pels objectius, millores tècniques i estratègiques de contracte.
- Resoldre de forma satisfactòria qualsevol assumpte de facturació o compatibilitat que pogués sorgir.
- Realitzar la coordinació efectiva amb el responsable de l'equip de treball de l'empresa contractista.

Cap de projecte i responsable de l'equip de treball, per part de l'adjudicatari.

Serà el màxim responsable del procés d'implantació per una banda i de garantir la correcta prestació del servei de suport i manteniment per l'altra, i realitzarà com a mínim les següents tasques:

- Es requereix:
 - Enginyeria tècnica.
 - FHT LP-S Security and IT Operation
 - Gestió i implantació de projectes similars.
 - Experiència mínima demostrable de 3 anys en tasques similars.
- Les seves funcions són:
 - Liderar el projecte.
 - Interlocució i coordinació amb la direcció de projecte del PSPV.
 - Planificació i seguiment de la implantació.
 - Elaboració i entrega d'actes de les reunions de seguiment d'implantació.
 - Garantir que la prestació del servei es realitza complint amb els paràmetres establerts en el present concurs.
 - Gestió dels equips de treball.
 - Gestió dels riscos detectats així com la presentació del pla de mitigació dels mateixos.
 - Detecció d'oportunitats de millora.
 - Entrega de documentació final d'implantació.
 - Entrega d'informes de prestació del servei.
 - Aquest recurs haurà de disposar de titulació universitària en enginyeria.
 - Aquest recurs haurà de disposar de la certificació ITIL Foundation, valorable certificacions superiors.

Responsable de l'equip de treball

- Es requereix:
 - FHT LP-S Security and IT Operation
 - Gestió i implantació de projectes similars.
 - Experiència mínima demostrable de 3 anys en tasques similars.

- Les seves funcions són:
 - o Assegurar la gestió eficient de la provisió dia a dia del servei contractat pel client.
 - o Gestionar la provisió del servei per complir els objectius i nivells de servei acordats.
 - o Actuar com a referent de l'empresa contractista per a facilitar la comunicació amb les diferents àrees involucrades en la provisió del servei.
 - o Assegurar la gestió eficient dels problemes, assegurant que es segueixen els procediments d'escalat acordats.
 - o Informar del servei proporcionat en base a estadístiques exactes i actualitzades.
 - o Realitzar la coordinació amb el Coordinador del projecte del PSPV.
 - o Establir i assegurar el compliment dels nivells de qualitat acordats i mantenir una actitud proactiva per tal de suggerir iniciatives que incideixin en la millora continuada del servei.
 - o Establir un procediment de revisió regular del servei que assegurï que tots els assumptes del servei es tracten de forma eficient i dins del temps requerit.
 - o Assegurar la provisió del servei per complir els objectius i nivells de servei acordats.
 - o Promoure sessions de treball per facilitar la comunicació amb l'equip de control del servei del PSPV.

Equip de treball

- Es requereix:
 - o Gestió i implantació de projectes similars.
 - o Experiència mínima demostrable d'1 any en tasques similars.
- Les seves funcions són:
 - o Situació escalat de peticions i incidències
 - o Escalat de peticions i incidències
 - o Detalls derivats de la resolució dels tiquets
 - o Documentació afegida o modificada a la Base de Dades de Coneixement de la solució aplicada - Dades de volum del servei

Es requereix dos perfils:

- o Esdevindran els responsables dels serveis professionals d'implantació sol·licitats.
- o Esdevindran els referents tècnics des del punt de vista del suport i gestió.
- o Entrega d'informes de prestació relatius a implantació i incidències.
- o Esdevindran l'escalat de les incidències i peticions a nivell més especialitzat o suport de fabricants.

5.3 Òrgans de gestió

S'estableixen els següent òrgans de gestió i es detalla el funcionament

5.3.1 Comitè de direcció

Seràn objecte del Comitè de Direcció les següents funcions:

- Seguiment de nivells de qualitat.
- Modificació d'acords de nivell de servei (ANS).

Els membres d'aquest comitè són: Per part del PSPV:

- Cap de projecte ocupat per Direcció d'Organització i Comunicació (responsable del contracte).
- Responsable del projecte, ocupat per Sots direcció TIC
- Coordinador del projecte, ocupat per Cap de Sistemes, Comunicacions i Ciberseguretat.

I per part de l'empresa contractista:

- Responsable del projecte.
- Responsable de l'equip de treball.

L'empresa contractista haurà de presentar previ a cada sessió de treball:

- Ordre del dia.
- Resum de l'estat de les instal·lacions indicant l'avançament i fites aconseguides, així com els problemes trobats relacionats amb la instal·lació i seguiment dels ANS.
- Informe descriptiu de l'execució del servei durant el període. L'informe de seguiment haurà de presentar-se en el Comitè de Direcció. Aquest document haurà d'incorporar com a mínim els següents punts:
 - Revisió acords i temes pendents comitè anterior i Visió global
 - Quadre de comandament global del servei
 - Acords de Nivell de Servei i tiquets en garantia - Seguiment operatiu.
 - Quadre d'indicadors tècnics per presentar la situació dels serveis per tecnologia i les propostes de millora de parametrització

Aquests informes seran revisats per PSPV que podrà modificar l'estructura d'aquests informes en funció de nous paràmetres del servei que vulgui avaluar.

- Informes de propostes d'optimització o evolució i Informes de noves necessitats (descrits a l'apartat 4.2 Servei Gestionat 24x7 MDR)
- De la mateixa forma es requeriment elaborar acta de seguiment posterior on constin els acords presos per poder fer-ne el seguiment.

La periodicitat de les reunions serà mensual durant la implantació i semestral pel servei de suport i planificació d'actuacions derivades d'actualitzacions del programari per part del fabricant.

Tots els documents, informació de recolzament i qualsevol tipus d'element obtingut en el desenvolupament dels treballs, seran propietat del PSPV.

Durant el procés de implantació, la periodicitat de les reunions dels comitès podrà veure's afectada per les necessitats concretes de la provisió i implantació dels serveis i s'hi haurà d'adaptar.

Durant el període d'exploració, la composició dels comitès de direcció i de seguiment pot ser diferent que la del període d'implantació

5.3.2 Comitè de seguiment

Seràn objecte del Comitè de Seguiment les següents funcions:

- Seguiment dels acords de nivell de servei (ANS).
- Generació d'informes.
- Coordinació d'accions.

La Comissió de seguiment té com objectius:

- La inspecció i control de la prestació del servei, anàlisi de l'activitat i seguiment detallat del projecte, de l'estat de situació i d'aquells aspectes del projecte que requereixen decisió operativa
- Informe de l'estat de situació de les activitats i les fites planificades.
- Revisió d'aspectes rellevants de la vessant tecnològica.
- Plantejament dels aspectes del projecte que requereixen decisions estratègiques.
- Propostes d'evolució funcional del sistema (línies de treball en curs i compromisos en calendari).
- Anàlisi i elaboració de propostes sobre altres aspectes que puguin influir el desenvolupament del projecte.

Els membres d'aquest comitè són: Per part del PSPV:

- Responsable del projecte, ocupat per Sots direcció TIC
- Coordinador del projecte, ocupat per Cap de Sistemes, Comunicacions i Ciberseguretat.
- Tècnic àrea TIC.

I per part de l'empresa contractista:

- Responsable de l'equip de treball.
- Tècnics assignats.

L'empresa contractista haurà de presentar previ a cada sessió de treball:

- Ordre del dia
- Informe descriptiu de temes tècnics i de coordinació tècnica del servei durant el període. Aquest document haurà d'incorporar com a mínim els següents punts:
 - Revisió acords i temes pendents comitè anterior.
 - Anàlisi situació:
 - Relació de temes tècnics:
 - Descripció
 - Estat
 - Planificació
 - Realització
 - Responsable
 - Impactes
 - Dependències
 - Riscos identificats i proposta de solucions

- Informe d'activitat i amenaces (descriu a l'apartat 4.2 Servei Gestionat 24x7 MDR)

Aquests informes seran revisats per PSPV que podrà modificar l'estructura d'aquests informes en funció de nous paràmetres del servei que vulgui avaluar.

- Relació de fets rellevants i el seu impacte en el nivell de servei. De la mateixa forma es requeriment elaborar acta de seguiment posterior on constin els acords presos per poder fer-ne el seguiment.

La periodicitat de les reunions serà setmanal durant la implantació i a posteriori mensual pel seguiment del servei de suport i planificació d'actuacions.

Tots els documents, informació de recolzament i qualsevol tipus d'element obtingut en el desenvolupament dels treballs, seran propietat del PSPV.

Durant el procés de migració, la periodicitat de les reunions dels comitès podrà veure's afectada per les necessitats concretes de la provisió i implantació dels serveis i s'hi haurà d'adaptar.

Durant tota la vigència del contracte, qualsevol canvi que es produeixi per part de l'empresa contractista a nivell d'interlocució o composició dels comitès serà correctament informada al PSPV amb una antelació mínima d'1 mes previ al canvi previst.

5.4 Adequació permanent a les necessitats

El PSPV és un organisme dinàmic i això comporta, entre d'altres adaptar-se a la necessitat del Parc Sanitari Pere Virgili, pel que l'empresa contractista haurà adequar els sistemes a la realitat del Parc.

El PSPV no assumirà cap cost associat a la implantació dels serveis contractats, a banda dels especificats pels licitadors en les seves propostes. A més, els licitadors no han de preveure cap tipus de dedicació tècnica per part del personal del PSPV en tasques associades a la posada en marxa, a excepció de tasques de seguiment i de les necessàries col·laboracions en el coneixement de la configuració interna dels serveis i sistemes del PSPV.

5.5 Condicions de la prestació del servei

5.5.1 Eina de gestió tiqueting (ITSM)

L'adjudicatari ha d'integrar-se amb l'eina de gestió de tiquets que té actualment PSPV per crear, generar i atendre els tiquets i fer el seguiment individualitzat de les demandes fetes i avaluar de forma global el servei.

L'eina de tiqueting del PSPV permet la generació de tiquets mitjançant els canals de comunicació establerts pel PSPV (correu, telèfon, etc.) a través del servei del CAU.

Les dades a recollir en cada cas estaran tabulades a la Base de Dades de Coneixement (CMDB), que serà propietat del PSPV i compartida amb el CAU, que s'anirà actualitzant amb la informació que es vagi recollint, per part de l'adjudicatari i el propi PSPV en les actuacions presencials. Caldrà definir durant la implantació les dades mínimes que cal recollir.

5.5.2 Canals de comunicació

Els canals de comunicació disponibles pels serveis d'atenció són:

- Telèfon.
- Correu electrònic.
- Eina tiqueting PSPV.
- Altres mitjans que l'adjudicatari o el PSPV puguin posar a l'abast dels usuaris.

5.5.3 Ubicació física del servei

El servei s'oferirà a les instal·lacions de l'adjudicatari a menys que requereixi actuació presencial.

6 Execució del projecte

L'adjudicatari designarà un equip de treball responsable de la prestació del servei de forma que faciliti les interlocucions i la gestió de forma eficaç.

Els licitats han de detallar els aspectes relatius a l'organització proposada per a la realització dels treballs requerits, sota la direcció del responsable del servei al Parc i que hauran les següents fases metodològiques per a la posada en marxa del servei:

- El Desplegament de la solució Crowdstrike Falcon EDR per 800 endpoints, es considera en **termini mínim de tres mesos**.
- La pla de posada en marxa del Servei gestionat 24x7 MDR solució Crowdstrike Falcon EDR per 800 endpoints es considera en **termini màxim d'una setmana**.
- Pla de formació

La formació vinculada al traspàs de coneixement a l'equip IT ha de ser realitzada i lliurada la documentació **1 mes com a màxim** un cop finalitzat el desplegament.

La formació continua a l'equip IT (Formació en serveis de resposta a incidents i Formació contínua en canvis i actualitzacions) ha de ser realitzar-se en **4 sessions formatives anuals** de cadascuna de les indicades durant tot l'any com a mínim, que responguin s les necessitats d'actualització de coneixements que es requereixin- Aquestes sessions caldrà cordar-les al comitè de direcció.

7 Acords de Nivell de Servei (ANS)

Aquesta planificació s'explicitarà en uns objectius a aconseguir en un termini determinat. Per mesurar el grau d'assoliment dels objectius s'establiran indicadors numèrics.

Per mesurar la qualitat del nivell rebut pel Parc Sanitari Pere Virgili també s'establiran indicadors que tindran un valor mínim a assolir (ANS).

Semestralment com a mínim, el licitador subministrerà informes d'indicadors, tan els descrits en aquest plec, com aquells que el propi licitador o el Parc Sanitari Pere Virgili proposi de forma addicional.

El personal del Departament d'Organització i Comunicació tindrà accés directe a les dades generades pels mecanismes de control.

El servei es realitzarà en base al següents acords de nivell de servei i penalitzacions associades al seu incompliment, per assegurar la qualitat en la seva prestació. Els licitadors poden proposar altres ANS i penalitzacions addicionals o millores en els mateixos.

Quan s'incompleixi un ANS, l'adjudicatari haurà d'explicar les causes per les que s'ha produït l'incompliment i fer propostes de resolució i millora per aconseguir que no es repeteixi.

7.1 Incompliments

L'objectiu d'aquest apartat és descriure el model d'Incompliments o ANS que defineix els indicadors i establir una base objectiva i mesurable que reflecteixi el compromís de l'adjudicatari per a prestar els serveis requerits de forma satisfactòria.

Es pretén obtenir un nivell de servei d'alta qualitat. Per aquest motiu s'han definit els ANS amb l'establiment d'un model de penalitzacions que relacioni el nivell de prestació del servei amb la seva facturació o altres mecanismes de compensació.

Per tal de disposar de la informació necessària per a una gestió i governança homogènia dels sistemes, el licitador haurà d'implantar el Model de Mesura del Nivell de Servei de forma progressiva al llarg de l'execució del contracte.

S'analitzarà:

- Nivell gravetat alertes:
Les alertes seran classificades segons la seva gravetat en les categories següents:
 - o Baixa: Alertes que indiquen activitats que poden representar un risc potencial menor per a la seguretat de la infraestructura.
 - o Mitja: Alertes que són més sospitoses o que poden indicar una activitat anòmla més significativa.
 - o Alta: Alertes que indiquen activitats que representen un risc considerable per a la seguretat.
 - o Crítica: Alertes que indiquen una amenaça immediata i altament perjudicial per a la seguretat de la infraestructura.
- Temps de resolució

Àmbit	Paràmetre	Criticitat	ANS	Penalització mínima
Resposta alerta	Temps de resposta	Baixa	24 hores naturals	0,25% de la facturació mensual per cada hora de demora en la detecció del tiquet de nivell no crític
		Mitja	12 hores naturals	0,5% de la facturació mensual per cada hora de demora en la detecció del tiquet de nivell no crític
		Alta	4 hores naturals	0,75% de la facturació mensual per cada hora de demora en la detecció del tiquet de nivell no crític
		Crítica	1 hora natural	1% de la facturació mensual per cada hora de demora en la detecció del tiquet de nivell no crític
Resolució alerta	Temps de resolució	Baixa	48 hores naturals	0,25% de la facturació mensual per cada hora de demora en la detecció del tiquet de nivell no crític
		Mitja	24 hores naturals	0,5% de la facturació mensual per cada hora de demora en la detecció del tiquet de nivell no crític
		Alta	8 hores naturals	0,75% de la facturació mensual per cada hora de demora en la detecció del tiquet de nivell no crític
		Crítica	4 hores natural	1% de la facturació mensual per cada hora de demora en la detecció del tiquet de nivell no crític

7.2 Penalitzacions

El licitador haurà de garantir que l'oferta que presenti està acord amb el que s'exposa en el plec. Les desviacions de caràcter greu que puguin condicionar el desenvolupament del projecte quedaran penalitzades segons es detalla a continuació:

- Si el contractista ha incorregut en demora per una causa imputable a ell mateix, l'òrgan de contractació pot rescindir el contracte o imposar les penalitats que procedeixin, d'acord a les previsions de la Llei de Contractes del Sector Públic.
- Les sancions es fan efectives no tan sols sobre la garantia sinó també, si escau, en la quantia necessària sobre els pagaments que s'han de satisfer a l'adjudicatari. Quan es fan efectives sobre la garantia, el contractista està obligat a completar-la dintre dels quinze dies naturals següents a la notificació de la sanció.

8 Altres consideracions

Tots els treballs hauran de desenvolupar-se en el marc de la legislació vigent aplicable en matèria de Tecnologies de la Informació i Comunicacions per a l'entorn d'un Campus o Parc.

El Parc facilitarà a l'adjudicatari tota la informació requerida corresponent a la situació actual en infraestructures, sistemes actuals, organització, responsables i interlocutors, etc., per tal de garantir l'optimització en la planificació del servei requerit.

L'adjudicatari facilitarà la visita i examen de qualsevol procés o fase del servei, estant obligat a subministrar quanta informació tècnica li sigui requerida i jurídicament resulti possible.

8.1 Presentació de la documentació

Les empreses licitant hauran d'incloure en llurs ofertes els següents documents:

1. Explicació detallada, clara, concreta i suficient del pla de treball per dur a terme el Desplegament de la solució CrowdStrike Falcon EDR per 800 endpoints, segons els subcriteris següents:
 - a. Organització i posada en marxa del servei.
 - b. Gestió i operació del servei..
 - c. Documentació, Tancament i traspàs del servei.
2. Elaboració del pla de posada en marxa del Servei gestionat 24x7 MDR solució CrowdStrike Falcon EDR per 800 endpoints que inclourà tots els aspectes organitzatius, procedimentals, de planificació i tècnics necessaris per al inici del servei segons els subcriteris següents:
 - a. - Organització i posada en marxa del servei.
 - b. - Monitorització del servei.
 - c. - Gestió i operació del servei.
 - d. - Pla de seguiment de la prestació del servei.
 - e. - Documentació, Tancament i traspàs del servei.
3. Pla de formació

L'empresa contractista es responsabilitzarà de la realització dels cursos de formació per al personal de gestió i explotació del PSPV. La proposta de formació haurà de detallar el nivell de la formació, el contingut i hores, així com el dimensionat, cursos inclosos, facilitats per la seva assistència, documentació aportada en cadascun d'ells de cadascuna de les formació requerides a l'apartat 4.3 Serveis de formació.

8.2 Esquema Nacional de Seguretat

L'article 2 del vigent Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat, disposa que els plecs de prescripcions administratives o tècniques dels contractes que celebrin les entitats del sector públic incloses en l'àmbit d'aplicació del reial decret de l'ENS contemplaran tots aquells requisits necessaris per assegurar la conformitat amb el mateix dels sistemes d'informació en els quals es recolzen els serveis prestats pels contractistes, tals com la presentació de les corresponents Declaracions o Certificacions de Conformitat amb l'ENS. Aquesta

precaució s'estendrà també a la cadena de subministrament d'aquests contractistes, en la mesura que sigui necessari i d'acord amb els resultats de l'anàlisi de riscos corresponent.

En conseqüència, el PSPV considera necessari que els proveïdors que vagin a concórrer a la licitació hauran d'estar en condicions de mostrar la corresponent Certificació de Conformitat amb l'Esquema Nacional de Seguretat, acceptant-se en el seu lloc, no obstant això, una Declaració de Conformitat amb l'ENS.

Així doncs, en base a l'anterior, i a l'anàlisi dels riscos als quals estan exposats els subministraments i serveis objecte de la licitació, el PSPV estableix com a necessari que l'entitat licitadora hagi d'estar en condicions de mostrar la corresponent Declaració o Certificació de Conformitat amb l'Esquema Nacional de Seguretat, per a la categoria de seguretat ALTA, dels sistemes que intervinguin en la prestació dels serveis indicats, així com mantenir la conformitat en vigor durant la vigència del contracte. Aquesta declaració, o certificat, de conformitat amb l'ENS s'entén que ha d'englobar en el seu abast, com a mínim, l'àmbit objecte de la contractació.

En el cas que l'adjudicatari no pogués mantenir la conformitat amb l'ENS durant la vigència del contracte -per pèrdua, retirada o suspensió de la Certificació de Conformitat o impossibilitat de mantenir la Declaració de Conformitat-, haurà de comunicar aquesta circumstància, de forma immediata i sense dilació indeguda, a l'ENTITAT CONTRACTANT, qui considerarà l'impacte d'aquesta circumstància en la prestació objecte del contracte.