PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS DEL CONTRACTE DE SERVEI DE MANTENIMENT I GESTIÓ DE LA INFRAESTRUCTURA DE SEGURETAT PERIMETRAL I SERVEIS DE CIBERSEGURETAT DE LA CORPORACIÓ DE SALUT DEL MARESME I LA SELVA.

1 Introducció

El present document conté les especificacions tècniques per a la contractació dels serveis de manteniment i gestió de la infraestructura de serveis de seguretat perimetral de dades i de serveis de ciberseguretat de la Corporació de Salut del Maresme i la Selva, en endavant CSMS.

La CSMS disposa de serveis de comunicacions de dades a diferents edificis i ubicacions , a on hi treballen prop de 2000 treballadors. Està format per:

- 2 hospitals d'aguts
- 6 centres d'atenció primària
- 3 centres sociosanitaris
- 3 centres de rehabilitació
- 1 magatzem
- 2 nous centres encara no operatius

Per ampliar la informació relativa a la distribució de centres veure Annex I al present plec de prescripcions tècniques– Llistat de seus; per a qualsevol altre tipus d'informació, es pot consultar el web corporatiu www.salutms.cat.

En un entorn descentralitzat com aquest, els serveis de telecomunicacions i ciberseguretat són una eina d'importància estratègica, tant per la seva funcionalitat com pel seu cost.

L'objectiu del present procediment es la contractació de la seguretat perimetral de les dades que circulen dins totes les xarxes de comunicació de la CSMS, a part de les sortides/entrades d'internet, i la contractació de diversos serveis de ciberseguretat que ajudaran a la CSMS a protegir la integritat, confidencialitat i disponibilitat de la informació que administra.

Aquest Plec de prescripcions tècniques inclou els següents apartats:

- Objectius i abast de la licitació

- Descripció de la situació actual
- Descripció de la situació futura
- Requeriments tècnics i funcionals
- Pla d'implantació
- Servei d'operació i manteniment
- Pla de formació
- Garantia dels equips i instal·lacions
- Model de relació
- Pla de devolució del servei
- Millores sobre els requeriments bàsics
- Annexes
    - Annex I – Llistat de seus
    - Annex II – Inventari de dispositius
    - Annex III – Acords de Nivell de Servei

La presentació d'una oferta en resposta a aquest plec de prescripcions tècniques per part dels licitadors pressuposa l'acceptació de tots els requeriments inclosos, tant en aquest document com en el Plec de clàusules administratives particulars, d'ara endavant PCAP.

2 Objectius i abast

2.1 Objectiu

En línia amb el que s'exposa a l'apartat 1, els objectius principals que es plantegen en la present licitació es descriuen en els següents apartats:

2.1.1 Objectius generals

Els objectius generals de la present contractació són:

- Optimitzar els costos d'explotació dels serveis de seguretat perimetral de dades, millorant els serveis disponibles actualment, així com implantant nous serveis de valor afegit.
- Disposar de nous serveis avançats facilitats per les noves tecnologies de comunicacions.
- Simplificar la gestió, suport i manteniment dels diferents serveis rebuts pel nou adjudicatari.
- Establir acords de nivell de servei per assegurar el lliurament òptim dels serveis i disposar d'eines per a controlar el seu compliment.
- Establir els mecanismes per al seguiment del contracte per assegurar el manteniment de la qualitat i de la competitivitat econòmica de les telecomunicacions corporatives.
- Definir un model de gestió i relació on els operadors siguin veritables socis tecnològics de la CSMS.

2.1.2 Objectius funcionals

Des d'un punt de vista funcional, els objectius globals de la contractació són:

- Obtenir el millor escenari global de prestació de serveis de seguretat perimetral de dades, servidors i punt de treball (endpoint) i ciberseguretat per a tota la CSMS.

2.1.3 Objectius tecnològics

Des d'un punt de vista tecnològic, són objectius de la contractació:

- Adquisició de nous sistemes de tallafocs de capa 7 i regulació de les condicions del servei de manteniment i gestió de la infraestructura de serveis de seguretat perimetral de la CSMS, concretades en subministrament, instal·lació, auditoria, manteniment preventiu i suport proactiu d'aquesta infraestructura.
- Atendre les necessitats de formació dels tècnics de la CSMS, ajudant-los a gestionar eficientment la infraestructura i possibilitant el coneixement de noves tecnologies de seguretat que pugin resultar d'interès en la implantació de futures millores tècniques.
- Homogeneïtzar les solucions tecnològiques implantades i l'evolució tecnològica futura.
- Garantir l'escalabilitat de la solució proposada, així com, treure el màxim rendiment a les noves infraestructures.
- Garantir i millorar la connexió a Internet, entrades i sortides de serveis publicats, connexions VPN, etc.
- Assegurar l'ús d'una eina EDR/XDR com l'actual, per a endpoints i servidors corporatius, sent aquesta una solució cloud.
- Oferir serveis de ciberseguretat com a Oficina Tècnica de Seguretat, de manera que es treballin aspectes de compliment, alineació amb l'Esquema Nacional de Seguretat i d'altres normatives aplicables d'anàlisi de riscos i securització de la informació, plans de contingència i recuperació de desastres, etc.

2.2 Abast

- Interconnexió segura de seus. Aprovisionament, manteniment, gestió i monitorització dels enllaços de dades que interconnecten els edificis de la CSMS.
- Subministrament, gestió, administració i eines de monitorització de l'equipament necessari per mantenir l'adreçament implementat actualment per a la interconnexió de les ubicacions.
- Formació sobre tots els elements de servei per al personal tècnic de la CSMS.
- La solució haurà d'incloure la securització de l'accés de dades corporatiu (vpn), a Internet, a l'Anella Sanitària i a qualsevol nova connexió de xarxa que passi a través dels tallafocs.

3 Descripció de la situació actual

3.1 Infraestructura de seguretat perimetral

Actualment la CSMS basa la seva estratègia de seguretat perimetral amb solucions del fabricant Fortinet.

Dins d'aquest llistat de solucions, s'hi troben tallafocs de propera generació amb gestió centralitzada (NGFW), plataformes de gestió de correu electrònic (antispam) i analitzadors de tràfic, entre d'altres.

Els equips tallafocs, a més d'encarregar-se de la funció de seguretat perimetral i seguretat interna (segmentació), també s'encarreguen en l'actualitat de gestionar l'alta disponibilitat de comunicacions entre centres (SD-WAN), gestionant l'estat de les línies de dades i en cas de caiguda d'una línia activa son capaços d'encaminar el tràfic de dades automàticament per la línia de contingència que existeix a cada centre per tal propòsit i a l'hora notificar als administradors de xarxa de la Corporació de la incidència amb la línia primària.

Trobareu l'inventari de dispositius a *l'Annex II*

3.2 Servidors i punt de treball (endpoint)

La solució software actual respecte a la seguretat d'equips, tant a nivell de servidor com d'endpoint, està basada en el fabricant TrendMicro.

Trobareu l'inventari de llicències a *l'Annex II*

3.3 Ciberseguretat (CISO)

Actualment es disposa també amb la figura d'un responsable de seguretat de la informació (CISO) com a servei externalitzat, que ajuda a la CSMS a alinear les polítiques i procediments a les normatives vigents en matèria de ciberseguretat.

4 Descripció de la situació desitjada

4.1 Infraestructura de seguretat perimetral

Actualment tot l'equipament de seguretat perimetral que té la CSMS és una solució en modalitat servei, per la qual cosa, al finalitzar la licitació que està vigent, s'haurà de renovar tot el parc de dispositius que la composen.

Aquesta solució està basada íntegrament en solucions del fabricant Fortinet, és **d'OBLIGAT COMPLIMENT**, que la solució proposada pel adjudicatari sigui d'aquest fabricant.

Els motius d'aquesta decisió es fonamenten en:

1. Expertesa: tot el coneixement adquirit per part dels tècnics de TI de la CSMS els darrers 15 anys sobre dispositius Fortinet son un valor importantíssim per tal de poder seguir gestionant tots els dispositius relacionats amb la seguretat perimetral de forma autònoma i confiable.
2. Impacte: l'impacte de canviar de fabricant de tallafocs per un fabricant diferent a Fortinet pot ser importantíssim, no només a nivell de coneixements, sinó a nivell de transferència de configuracions (regles de tallafoc), implicant en el camí caigudes prolongades en tots els serveis de xarxa (dades, telefonia, accessos, vigilància, imatge digital, etc) i problemes puntuals d'aquests serveis de xarxa, derivats d'errors en el trasllat de configuracions d'un dispositiu a un altre.
3. Gestió centralitzada de commutadors Fortinet i controladora wifi de punts d'accés Fortinet: darrerament la CSMS ha adquirit molts dispositius commutadors del fabricant Fortinet que actualment es gestionen de forma centralitzada a través dels tallafocs Fortinet presents a cada seu. De la mateixa forma darrerament s'han adquirit moltes unitats de punts d'accés wifi que necessiten obligatòriament d'un tallafoc Fortinet a cada seu per tal de ser operatius i gestionables.
   Actualment tenim més de 200 punts d'accés wifi i 80 commutadors Fortinet, que al ser propietat de la CSMS, queden fora de l'abast d'aquesta licitació.

De forma resumida es demana:

- Solució FortiGate per a tots els centres
- Solució FortiMail per a la seu principal
- Solució FortiAnalyzer per a la seu principal
- Solució FortiSandbox en modalitat cloud
- Solució FortiSIEM en modalitat cloud
- Solució FortiManager (màquina virtual)

A l'apartat 16 trobareu el requeriments tècnics de tots els dispositius sol·licitats.

L'adjudicatari haurà de fer-se càrrec de la migració de la solució actual (Annex II) a la nova solució implementada, tant a nivell d'instal·lació com de configuració.

La totalitat d'aquesta feina l'haurà de realitzar l'adjudicatari i haurà d'estar inclosa dins la licitació, no podent generar càrrecs extraordinaris que la CSMS hagi d'assumir fora de licitació.

4.2 Protecció servidors i estacions de treball

Es demana una solució XDR similar a l'actual per a la totalitat d'endpoints i servidors, basat en una solució cloud.

L'adjudicatari haurà de fer-se càrrec de la migració de la solució actual (Annex II) a la nova solució implementada, tant a nivell d'instal·lació com de configuració.

4.3 Protecció correu online i eines col·laboratives

Serà necessari incorporar un nou element, que sigui del mateix fabricant de la solució XDR, que sigui capaç de treballar amb la plataforma Microsoft 365, realitzant tasques avançades d'anàlisi de correus i documents, i amb la possibilitat d'implementar una protecció DLP.

4.4 Oficina tècnica virtual de seguretat (OTS)

En quant a la antiga figura coneguda com a CISO virtual, es reconverteix a una solució d'Oficina tècnica virtual de seguretat (OTS).

Aquesta nova figura OTS, a part de fer les tasques de CISO, realitzarà tasques addicionals alineades a la seguretat definides als requeriments tècnics.

5 Requeriments tècnics i característiques del servei

En aquest apartat es detallen els requeriments mínims funcionals que ha de complir la solució proposada pels licitadors. En cas que el licitador no compleixi amb tots aquests requeriments serà exclòs.

5.1 Requeriments funcionals generals

1. Els equips i serveis proposats han de suportar el creixement de la solució, així com garantir una evolució tecnològica coherent, és a dir, garantir escalabilitat per adaptar-se a les necessitats de creixement que pugin sorgir.
2. La solució proposada haurà de contemplar tots els equips i serveis necessaris per suportar la disponibilitat requerida per la CSMS per a cadascun dels serveis definits dins de l'abast del contracte, així com el material necessari per a la seva instal·lació i prestació del servei requerit.
3. L'adjudicatari haurà d'assegurar la totalitat del llicenciament necessari per a que tota la solució que es demana sigui funcional durant tota la licitació, incloent el cost de tot aquest llicenciament al preu de licitació, i per tant no podent aparèixer despeses extraordinàries que la CSMS hagi d'assumir.
4. Atenció personalitzada per part d'un Service Manager.
5. Servei de manteniment 24x7x365 per part de l'adjudicatari, amb un temps de resposta definit en el ANS corresponent.
6. Suport i manteniment de la plataforma. Compromís de tenir al dia tots els contractes de manteniment necessaris amb els fabricants, per garantir el canvi d'equips i continuïtat dels mateixos, així com els contractes d'ús o distribució de programari que apliqui en el servei contractat (Antivirus, IPS, Application Control, etc...) en cada cas, sense costos afegits per a la CSMS.
7. Suport telefònic i per correu electrònic il·limitat en format 24x7 per a la resolució d'incidències o problemes en la instal·lació, actualització o ús del programari.
8. No es fixarà cap límit en el nombre màxim d'incidències que puguin ser reportades ni en el nombre d'hores dedicades a una incidència.
9. Resolució de dubtes sobre infraestructura instal·lada per part de l'adjudicatari, si la CSMS ho sol·licita.
10. Suport de backend per part del fabricant, incloent la correcció de errors (bugs) mitjançant càrrega de paquets de correcció (hot-fix), descarrega de noves versions i d'altres paquets d'actualització.
11. Accés a tota la documentació dels productes adquirits i als fòrums dels fabricant.
12. Un pla de formació descrit al punt 8
13. Un pla de devolució descrit al punt 10
14. El suport per part de l'adjudicatari haurà de ser en català i castellà.
15. El licitador haurà de tenir la seva seu a un màxim de 100 km de distància de la seu principal de la CSMS.
16. Totes les solucions ubicades al cloud han d'acomplir la RGPD i estar ubicades en territori de la Unió Europea.

5.2 Requeriments tècnics seguretat perimetral

Es defineixen 3 perfils per als tallafocs necessaris, depenent de la ubicació que tindran:

1. Tallafocs del Hospital de Calella
2. Tallafocs del Hospital de Blanes
3. Tallafocs per a la resta de seus

Característiques Tècniques del Tallafocs del Hospital de Calella

Aquest tallafocs s'haurà d'instal·lar en configuració de alta disponibilitat Actiu / Passiu (HA), es a dir, que s'han d'instal·lar dues unitats idèntiques, i cadascun d'aquestes unitats han de complir amb les següents característiques tècniques:

- Haurà d'esser un dels models Fortigate del fabricant Fortinet, i no pot tenir anunciat el fi del seu cicle de vida.
- Aquest equip ha ser un equip en format appliance, no s'admetran equips en format màquina virtual (VM).
- Ha de comptar amb llicències que habilitin les seves funcionalitats de IPS, Antimalware i antispam, control d'aplicacions, filtratge de URLs i filtre de DNS. En aquest sentit, ha de suportar els següents amples de banda, que ha d'estar suportat amb la funcionalitat de logging activa:
    - Ha de suportar un tràfic al seu motor IPS d'almenys 14 Gbps.
    - Ha de poder fer un filtratge de com a mínim 10 Gbps amb el seu motor de protecció contra amenaces (antimalware).
    - Ha de suportar un tràfic d'almenys 30 Gbps de control d'aplicacions.
    - Treballant com NGFW, ha de suportar un tràfic d'almenys 11,5 Gbps.
- Ha de poder suportar un ample de banda de firewall d'almenys 135 Gbps, mesurat amb paquets UDP de 1518 bytes.
- Ha de suportar al menys 7,8 milions de sessions TCP simultànies, podent crear fins a 550.000 noves sessions per segon.
- Ha de ser capaç de fer inspecció de tràfic SSL, en aquest sentit, ha de suportar al menys un ample de banda de 9 Gbps.
- Aquest equip no hauria de generar un retard en el tràfic inspeccionat superior a 4,2 µS.
- Aquest equip ha de tenir doble font d'alimentació que a més ha de poder ser substituïda en calent, sense necessitat d'apagar l'equip.
- A nivell d'interfícies, cadascun dels 2 equips ha de tenir al menys els següents ports físics:
    - 16 interfícies tipus GE amb connector RJ-45
    - 8 slots SFP amb capacitat d'instal·lar mòduls GE
    - 4 slots SFP+ amb capacitat d'instal·lar mòduls 10GE
    - 4 slots SFP28 amb capacitat d'instal·lar mòduls 25GE
    - 1 Port de consola
    - Al menys 1 port per administració fora de banda i un port addicional per la connectivitat de la alta disponibilitat.

- Amb cadascun d'aquests tallafocs, l'adjudicatari lliurarà 4 unitats de mòduls òptics 10GE tipus SFP+ tipus LR, compatible amb la fibra òptica instal·lada, que es de tipus monomode.

Característiques Tècniques del Tallafocs del Hospital de Blanes

Aquest tallafocs s'haurà d'instal·lar en configuració de alta disponibilitat Actiu / Passiu (HA), es a dir, que s'han d'instal·lar dues unitats idèntiques, i cadascun d'aquestes unitats han de complir amb les següents característiques tècniques:

- Haurà d'esser un dels models Fortigate del fabricant Fortinet, i no pot tenir anunciat el fi del seu cicle de vida.
- Aquest equip ha ser un equip en format appliance, no s'admetran equips en format màquina virtual (VM).
- Ha de comptar amb llicències que habilitin les seves funcionalitats de IPS, Antimalware i antispam, control d'aplicacions, filtratge de URLs i filtre de DNS. En aquest sentit, ha de suportar els següents amples de banda, que ha d'estar suportat amb la funcionalitat de logging activa:
    - Ha de suportar un tràfic al seu motor IPS d'almenys 12 Gbps.
    - Ha de poder fer un filtratge de com a mínim 9 Gbps amb el seu motor de protecció contra amenaces (antimalware).
    - Ha de suportar un tràfic d'almenys 28 Gbps de control d'aplicacions.
    - Treballant com NGFW, ha de suportar un tràfic d'almenys 10 Gbps.
- Ha de poder suportar un ample de banda de firewall d'almenys 75 Gbps, mesurat amb paquets UDP de 1518 bytes.
- Ha de suportar al menys 7,8 milions de sessions TCP simultànies, podent crear fins a 500.000 noves sessions per segon.
- Ha de ser capaç de fer inspecció de tràfic SSL, en aquest sentit, ha de suportar al menys un ample de banda de 8 Gbps.
- Aquest equip no hauria de generar un retard en el tràfic inspeccionat superior a 4,2 µS.
- Cada equip ha de tenir doble font d'alimentació que a més ha de poder ser substituïda en calent, sense necessitat d'apagar l'equip.
- A nivell d'interfícies, cadascun dels 2 equips ha de tenir al menys els següents ports físics:
    - 16 interfícies tipus GE amb connector RJ-45.
    - 8 slots SFP amb capacitat d'instal·lar mòduls GE.
    - 8 slots SFP+ amb capacitat d'instal·lar mòduls 10GE.
    - 1 Port de consola.
    - Al menys 1 port per administració fora de banda i un port addicional per la connectivitat de la alta disponibilitat.

Característiques Tècniques del Tallafocs de la resta d'edificis

Per a la resta d'edificis, s'han de instal·lar tallafocs del mateix model per tenir una configuració homogènia. En total es volen adquirir 14 tallafocs (un d'ells de recanvi). Aquest tallafocs han de

instal·lar-se en modalitat standalone, no es necessària la configuració de HA, però cadascun d'aquests tallafocs han de complir amb les següents característiques tècniques:

- Haurà d'esser un dels models Fortigate del fabricant Fortinet, i no pot tenir anunciat el fi del seu cicle de vida.
- Aquest equip ha ser un equip en format appliance, no s'admetran equips en format màquina virtual (VM).
- Ha de comptar amb llicències que habilitin les seves funcionalitats de IPS, Antimalware i antispam, control d'aplicacions, filtratge de URLs i filtre de DNS. En aquest sentit, ha de suportar els següents amples de banda, que ha d'estar suportat amb la funcionalitat de logging activa:
    - Ha de suportar un tràfic al seu motor IPS d'almenys 1,4 Gbps.
    - Ha de poder fer un filtratge de com a mínim 700 Mbps amb el seu motor de protecció contra amenaces (antimalware).
    - Ha de suportar un tràfic d'almenys 1,8 Gbps de control d'aplicacions.
    - Treballant com NGFW, ha de suportar un tràfic d'almenys 1 Gbps.
- Ha de poder suportar un ample de banda de firewall d'almenys 10 Gbps, mesurat amb paquets UDP de 1518 bytes.
- Ha de suportar al menys 700.000 sessions TCP simultànies, podent crear fins a 35.000 noves sessions per segon.
- Ha de ser capaç de fer inspecció de tràfic SSL, en aquest sentit, ha de suportar al menys un ample de banda de 600 Mbps.
- Aquest equip no hauria de generar un retràs en el tràfic inspeccionat superior a 3,5 µS.
- A nivell d'interfícies, l'equip ha de tenir al menys els següents ports físics:
    - 10 interfícies tipus GE amb connector RJ-45.
    - 1 Port de consola.

El llistat d'edificis on s'instal·laran aquests tallafocs:

1. Hospital Sociosanitari Sant Jaume Blanes
2. Hospital Sociosanitari de Lloret de Mar
3. Magatzem Blanes
4. CAP Lloret de Mar
5. CAP Rieral
6. CAP Tossa de Mar
7. CAP Malgrat de Mar
8. CAP Palafolls
9. Centre Rehabilitació Tordera
10. Centre Rehabilitació Selva Marítima Lloret de Mar
11. Centre Rehabilitació Can Xaubet Pineda de Mar
12. Centre N-II Pineda de Mar
13. Centre N-II Calella
14. Recanvi (no cal instal·lació)

Consola d'Administració

La consola d'administració ha de ser totalment compatible amb els tallafocs descrits en les seccions anteriors de forma nativa, es a dir, ha de ser una consola Fortimanager, i ha de complir amb les següents característiques:

- Format VM, compatible amb VMWare i Hyper-V.
- La VM ha de tenir prou llicències per poder administrar tots els tallafocs descrits en les seccions anteriors. Ara mateix el Fortimanager existent compta amb 20 llicències.

Servidor de Processament Centralitzat de Logs

Es requereix d'un appliance que pugui recol·lectar la informació de logs de cadascun dels tallafocs anomenats a les seccions anteriors. Aquest appliance ha de ser un Fortianalyzer, i no es necessari el desplegament d'aquest producte en alta disponibilitat, però sí ha d'acomplir amb els següents requeriments tècnics:

- Format appliance, no podrà ser proporcionat en format VM.
- Capacitat de gestió de logs de 100 Gb/dia
- Capacitat de anàlisi de 2000 logs/seg
- Factor de forma enrackable, de màxim 1 RU.
- Capacitat d'emmagatzemament de 4TB, amb una configuració de RAID 1
- El sistema ha de comptar amb 4 interfícies GE tipus RJ-45.
- Aquest appliance ha de comptar amb una subscripció que pugui permetre el següent:
    - Visualitzar els indicadors de compromís dels diferents elements de la xarxa per valorar i prioritzar els problemes de seguretat detectats.
    - Ha de permetre detectar brots de virus i activitat maliciosa als logs.
    - Addicionalment, ha de permetre l'automatització en la resposta a esdeveniments trobats als logs, es a dir, sense intervenció humana, per exemple seria bloquejar una IP al tallafocs o tallar tots els accessos a una estació de treball.
    - Accedir a reports Premium de compliment.

Fortimail + FortiSandbox

El correu electrònic es una eina imprescindible per al desenvolupament de les diferents tasques que es porten a terme cada dia a la CSMS, per aquest motiu, ha d'estar protegit, com ha sigut fins ara, amb una eina capaç d-integrar-se de manera nativa amb la resta de components de ciberseguretat que formen la solució integral demanada en aquesta licitació. En aquest sentit, es demana un Fortimail amb les següents característiques tècniques:

- Aquest component s'ha de subministrar en format appliance
- La instal·lació es farà en alta disponibilitat (HA)
- Ha de ser capaç de fer reports de l'activitat detectada
- Ha de comptar amb una subscripció que pugui permetre el següent:
    - La captura de més del 99,9% de spam

  - Que pugui detectar virus i malware amb una base de dades actualitzada, incloent brots de virus detectats al mon.
  - Protecció als usuaris al fer clic a distintes URLs incloses als correus.
  - Tenir afegida una solució de sandboxing integrada.
- Ha de suportar funcionar com relay o en mode API.
- Ha de ser capaç de fer tracking del correu electrònic entrant, de manera que es pugui detectar el recorregut d'un correu maliciós que ja estigui en les bústies.
- Quan està reballant en mode relay, aquest appliance ha de ser capaç d'enrutar un volum de 50.000 correus per hora sense anàlisi, i un volum de al menys 30.000 correus per hora fent un anàlisi sencer d'amenaces.
- En mode API, ha de ser capaç d'enrutar un volum de 18.000 correus per hora sense anàlisi, i un volum de al menys 12.000 correus per hora fent un anàlisi sencer d'amenaces.
- Ha de tenir una interfície web per alliberar o esborrar correu detectat com a spam abans de que arribi a una bústia de correu electrònic, i que sigui accessible per al propietari de la bústia.

Aquesta solució ha d'estar preparada per analitzar fitxers adjunts al correu electrònic i valorar si es tracta de qualsevol amenaça, fins i tot que sigui desconeguda. Com això no es pot assegurar en tots els casos, es demana una solució de sandboxing addicional a la que ja porta el Fortimail, que permetrà l'anàlisi del correu d'una manera més ràpida i eficient. Per assegurar la integració, es demana un FortiSandbox amb les següents característiques tècniques:

- El servei de sandboxing ha d'estar a la cloud del fabricant (Forticloud), perfectament integrat amb el Fortimail.
- La solució ha de comptar amb 5 VMs on es fa la execució del fitxer adjunt sospitós.

FortiSIEM

Actualment, la CSMS compta amb un FortiSIEM integrat amb totes les solucions de Fortinet i d'altres sistemes corporatius existents. Aquest FortiSIEM és l'encarregat de fer la recepció i correlació d'esdeveniments de tots aquests sistemes.

L'adjudicatari haurà de proporcionar un FortiSIEM en format cloud, amb una quantitat de llicències igual o superior a la solució actual. Tot i que es demana una solució basada en cloud, els col·lectors del FortiSIEM podran ser en format màquina virtual.

Actualment, la solució de FortiSIEM existent té un llicenciament per 50 dispositius.

Certificacions

Per assegurar la qualitat en la instal·lació de la solució de Fortinet, es demana que les empreses licitadores estiguin certificades amb els més alts estàndards de qualitat del fabricant, així, es demana que comptin amb una certificació de Partner de Fortinet i una certificació ISO 27001 i a més que estigui certificat en les següents especialitzacions:

- SD-WAN: Per assegurar la correcta configuració de SD-WAN dels firewalls.

- Secure connectivity: Per assegurar la qualitat de la configuració i funcionament amb els components LAN propietat de la CSMS com son els punts d'accés i els commutadors.

A part, es demana que durant el procés d'instal·lació i configuració dels dispositius, almenys un dels tècnics involucrats estiguin en possessió d'una certificació Fortinet NSE7 vàlida, i la resta de tècnics una certificació Fortinet NSE4 vàlida.
També és requerit que almenys un dels tècnics involucrats en la instal·lació de FortiSIEM estigui en possessió d'una certificació Fortinet NSE5 FortiSIEM vàlida.

5.3 Requeriments tècnics protecció de servidors i endpoint

5.3.1 Requeriments Generals

La solució proposada haurà de complir amb els requeriments generals següents:

- La solució proposada ha de cobrir la mateixa quantitat de dispositius coberts amb les llicències actuals, mantenint o millorant les característiques existents.
- La gestió de la solució s'haurà de realitzar mitjançant una consola única desplegada al núvol del fabricant. Així mateix, el fabricant de la solució serà el responsable de mantenir aquesta consola actualitzada.
- En el cas que els agents de protecció requereixin de comunicació amb serveis al núvol per cobrir alguna de les seves funcionalitats (p.ex. serveis de reputació de fitxers o reputació web), aquesta haurà de poder realitzar-se a través d'un proxy o passarel·la dissenyat a tal efecte, proporcionat pel propi fabricant de la solució i que haurà de desplegar-se en la infraestructura virtual de la CSMS.
- La solució de protecció d'estació de treball i servidors haurà d'estar basada en tecnologia XDR, que pugui permetre a la pròpia solució prendre mesures correctives quan es detecta una amenaça, basades en playbooks. A més, la solució XDR permetrà fer un estudi forense amb les causes, abast i control de danys posterior a la detecció.
- S' haurà de poder designar un o diversos equips dins de la xarxa de la CSMS perquè actuïn com a repositoris per a l'actualització de signatures i programari d' agent.
- Totes les funcionalitats descrites en els apartats de seguretat corresponents s'han d'integrar en un únic agent de protecció, no sent vàlides aquelles solucions que requereixin de més d'un agent per cobrir-les en la seva totalitat.
- L'agent de protecció haurà de suportar, com a mínim, les següents versions de sistema operatiu:
    - Windows Server: 2003, 2008, 2008 R2, 2012, 2012 R2, 2016, 2019 i 2022
    - Windows: XP, 7, 8, 8.1, i 10
    - Red Hat Enterprise Linux: 5, 6, 7 i 8
    - Oracle Linux: 5, 6, 7 i 8
    - SUSE Linux Enterprise Server: 10, 11, 12 i 15
    - Debian: 6, 7, 8, 9 i 10

5.3.2 Requeriments de la Consola de Gestió

La consola de gestió de la solució haurà de complir amb els requeriments següents:

- Per a l'autenticació dels usuaris administradors de la plataforma, haurà de permetre l'autenticació mitjançant SAML suportant com a mínim els proveïdors d'identitat ADFS i Azure AD.
- Haurà de permetre l'accés basat en rols.
- Haurà de permetre l'ús de doble factor d'autenticació.
- S'haurà d'integrar nativament amb vCenter i Azure per a l'inventari automàtic d'equips.
- Haurà de permetre l'agrupació automàtica d'equips mitjançant filtres basats en les característiques o atributs d'aquests, així com l'ús d'etiquetes personalitzades.
- Haurà de proporcionar la capacitat d'aplicar una política de seguretat a equips individuals o grups d'equips.
- Una política de seguretat haurà d'incloure la configuració de tots els mòduls detallats en els apartats *"Requeriments de Seguretat" per a cada cas.*
- Haurà d'incloure informació detallada sobre els equips protegits: nom, IP, sistema operatiu, mòduls instal·lats, política aplicada, informació d' actualització, etc.

- Haurà de permetre que els administradors personalitzin els seus quadres de comandaments amb informació que considerin rellevant, utilitzant widgets proporcionats per la pròpia eina.
- Haurà d'incloure reports automatitzats basats en plantilles.
- Haurà de permetre el reenviament dels esdeveniments de seguretat a un SIEM utilitzant el protocol Syslog en format CEF.
- Haurà de proporcionar una API que permeti gestionar el producte, totalment o parcialment, de manera programàtica. La documentació d'aquesta API haurà de ser de domini públic.

5.3.3 Requeriments de Seguretat per a la Protecció de Servidors

La solució proposada haurà de complir amb els requeriments de seguretat següents:

5.3.3.1 Antimalware Avançat

El mòdul de protecció antimalware haurà d'incorporar, com a mínim, les següents funcionalitats de detecció:

- Detecció basada en signatures i reputació de fitxers per a malware conegut.
- Machine Learning predictiu per a la detecció d'amenaces desconegudes i Zero-Day.
- Detecció de Spyware i Grayware.
- Anàlisi de comportament per a la detecció i bloqueig d'activitats sospitoses i canvis no autoritzats, inclòs el ransomware.
- Anti-ransomware avançat que permeti la detecció de variants de ransomware conegut i que incorpori un motor de recuperació de dades que creï còpies dels arxius xifrats, permetent la recuperació d' aquests en el cas que hagin estat xifrats per un procés de ransomware.
- Protecció Anti-Exploit que permeti l'anàlisi de fitxers i processos a la recerca de codi d'explotació incrustat.
- Detecció en temps real d'execució de codi maliciós en memòria.

5.3.3.2 Anàlisi de Reputació Web

- Aquest mòdul haurà de proporcionar un filtratge de continguts mitjançant el bloqueig de l' accés a URLs, IPs i dominis maliciosos coneguts, així com el bloqueig de comunicacions C&C.

- Aquesta protecció no s' haurà de limitar únicament a les comunicacions realitzades des del navegador, sinó que haurà de ser funcional a nivell de kernel, permetent l'anàlisi de les comunicacions de processos, serveis i altres aplicacions.

5.3.3.3 Firewall de Host

- Haurà de permetre regles de firewall per al trànsit entrant i/o sortint a nivell de host.
- Haurà de permetre definir IPs o xarxes d'IPs com a confiables per tal de no analitzar-ne el trànsit provinent.
- Haurà de proporcionar un conjunt de regles predefinides per als casos d'ús més comuns, per tal de facilitar la configuració per part dels administradors.
- Haurà de poder detectar i bloquejar, com a mínim, els següents atacs de reconeixement:
    - Escaneig de ports TCP i UDP.
    - Escaneig TCP Null.
    - Proves de detecció d'empremta del sistema operatiu (OS Fingerprint).

5.3.3.4 Pegat Virtual (protecció contra explotació de vulnerabilitats)

- Haurà de detectar i bloquejar atacs basats en xarxa a vulnerabilitats conegudes, tant en aplicacions com en sistemes operatius, mitjançant l'ús de regles de prevenció d'intrusions (HIPS).
- L' aplicació d' aquests pegats virtuals s'haurà de realitzar sense que es requereixi el reinici dels equips i sense que es produeixi cap pèrdua de servei.
- Els pegats virtuals s'hauran de poder configurar indistintament en mode detecció i notificació o en mode bloqueig, tant a nivell de política com a nivell individual de cada pegat virtual.
- L'agent de protecció haurà de realitzar una anàlisi de les vulnerabilitats de xarxa del sistema operatiu i les aplicacions que afecten l'equip per, seguidament, aplicar únicament aquells pegats virtuals als quals aquest és vulnerable. Tant l'anàlisi de vulnerabilitats com l' aplicació dels pegats virtuals, s'haurà de realitzar de manera automatitzada i periòdica sense que es requereixi intervenció per part dels administradors de la solució.
- Haurà de proporcionar pegats virtuals per a tots els sistemes operatius detallats en l'apartat *"Requeriments Generals"*, inclosos aquells que són obsolets i per als quals els diferents fabricants ja no desenvolupen els pegats oficials.
- Haurà de proporcionar, com a mínim, pegats virtuals per a les següents aplicacions crítiques:
    - Servidors de Base de Dades: Oracle, MySQL i Microsoft SQL Server
    - Servidors Web: Microsoft Internet Information Server, Apache i Nginx
    - Servidors d' Aplicació: Apache Tomcat, Oracle Weblogic i servidors d'aplicació basats en PHP

5.3.3.5 Control d' aplicacions

La solució ha de tenir aquest mòdul, que permetrà limitar l'execució d'aplicacions en el servidor basant-se en el checksum de l'arxiu (hash SHA-1 o altra). Aquest mòdul ha de permetre aplicar la protecció en 2 modes:

- Mode restrictiu: En aquesta manera no es permet l' execució de cap executable excepte aquells que hagin estat expressament autoritzats.
- Mode permissiu: En aquesta manera es permet l' execució de qualsevol executable amb excepció d'aquells que hagin estat denegats expressament.

El mòdul haurà de permetre l'activació d'un mode de manteniment, durant el qual es permeti l'execució de programari (ex.: instal·lació de nou programari, actualitzacions, etc...).

5.3.3.6 Correlació d'esdeveniments

La solució ha de comptar amb un mòdul per a la correlació d'esdeveniments de seguretat detectats en els logs de sistema operatiu i aplicacions. Aquesta correlació es basarà en regles assignades automàticament pel producte en base al sistema operatiu i aplicacions instal·lats.

Les regles definides permetran identificar comportaments sospitosos (ex.: Creació de comptes, intents d'autenticació per força bruta, etc) associant les deteccions efectuades a tàctiques i tècniques d'atac identificades pel framework de MITRE ATT&CK.

5.3.3.7 Monitoratge d' integritat

La solució ha de tenir un mòdul que permeti monitoritzar arxius, serveis, processos, programari instal·lat i claus de registre comparant el contingut i permisos d'aquests en qualsevol moment davant una línia de base inicial.

Aquest monitoratge es basarà en regles definides aplicades de manera automàtica pel producte en base al sistema operatiu i programari instal·lat. Aquestes regles facilitaran el compliment normatiu: ex.: PCI-DSS, GDPR, etc., mapejant tècniques i tàctiques d' atac del framework ATT&CK de MITRE. El sistema generarà una alerta en el cas de detectar qualsevol modificació sobre els mateixos.

5.3.4 Requeriments de Seguretat per a la Protecció d'Estacions de Treball

La solució proposada haurà de complir amb els requeriments de seguretat següents:

5.3.4.1 Antimalware Avançat

El mòdul de protecció antimalware haurà d'incorporar, com a mínim, les següents funcionalitats de detecció:

- Detecció basada en signatures i reputació de fitxers per a malware conegut.
- Machine Learning predictiu per a la detecció d'amenaces desconegudes i Zero-Day.
- Detecció de Spyware i Grayware.
- Anàlisi de comportament per a la detecció i bloqueig d' activitats sospitoses i canvis no autoritzats, inclòs el ransomware.
- Anti-ransomware avançat que permeti la detecció de variants de ransomware conegut i que incorpori un motor de recuperació de dades que creï còpies dels arxius xifrats, permetent la recuperació d' aquests en el cas que hagin estat xifrats per un procés de ransomware.
- Protecció Anti-Exploit que permeti l' anàlisi de fitxers i processos a la recerca de codi d' explotació incrustat.
- Detecció en temps real d' execució de codi maliciós en memòria.

5.3.4.2 Anàlisi de Reputació Web

- Aquest mòdul haurà de proporcionar un filtratge de continguts mitjançant el bloqueig de l' accés a URLs, IPs i dominis maliciosos coneguts, així com el bloqueig de comunicacions C&C.
- Aquesta protecció no s'haurà de limitar únicament a les comunicacions realitzades des del navegador, sinó que haurà de ser funcional a nivell de kernel, permetent l' anàlisi de les comunicacions de processos, serveis i altres aplicacions.

5.3.4.3 Firewall de Host

- Haurà de permetre regles de firewall per al trànsit entrant i/o sortint a nivell de host.
- Haurà de permetre definir IPs o xarxes d' IPs com a confiables per tal de no analitzar-ne el trànsit provinent.
- Haurà de proporcionar un conjunt de regles predefinides per als casos d' ús més comuns, per tal de facilitar la configuració per part dels administradors.
- Haurà de poder detectar i bloquejar, com a mínim, els següents atacs de reconeixement:
    - Escaneig de ports TCP i UDP.
    - Escaneig TCP Null.
    - Proves de detecció d'empremta del sistema operatiu (OS Fingerprint).

5.3.4.4 Pegat Virtual (protecció contra explotació de vulnerabilitats)

- Haurà de detectar i bloquejar atacs basats en xarxa a vulnerabilitats conegudes, tant en aplicacions com en sistemes operatius, mitjançant l'ús de regles de prevenció d'intrusions (HIPS).
- L' aplicació d' aquests pegats virtuals s' haurà de realitzar sense que es requereixi el reinici dels equips i sense que es produeixi pèrdua de servei.
- Els pegats virtuals s'hauran de poder configurar indistintament en mode detecció i notificació o en mode bloqueig, tant a nivell de política com a nivell individual de cada parxís virtual.
- Haurà de proporcionar, com a mínim, un set de pegats predefinits per a sistemes operatius Microsoft d' escriptori.

5.3.4.5 Control d' aplicacions

La solució ha de tenir aquest mòdul, que permetrà limitar l'execució d'aplicacions en el servidor basant-se en el checksum de l'arxiu (hash SHA-1 o altra). Aquest mòdul ha de permetre aplicar la protecció en 2 modes:

- Mode restrictiu: En aquesta manera no es permet l' execució de cap executable llevat d' aquells que hagin estat expressament autoritzats.
- Mode permissiu: En aquesta manera es permet l' execució de qualsevol executable llevat d' aquells que hagin estat denegats expressament.

El mòdul haurà de permetre l'activació d'una manera manteniment, durant el qual es permeti l'execució de programari (ex.: instal·lació de nou programari, actualitzacions, etc...).

5.3.4.6 Control de dispositius

La solució ha d'incloure un mòdul que permeti el control d'accés a dispositius d'emmagatzematge extern. Haurà de cobrir, com a mínim, els casos següents:

- Accés a dispositius d'emmagatzematge extern USB amb els següents permisos: Accés complet, Només Lectura, Bloqueig.
- Accés a dispositius mòbils com emmagatzematge extern amb els següents permisos: Accés complet, Només Lectura, Bloqueig.
- Prevenir l'autoejecció (autorun) de dispositius USB.

A més, es requereix poder fer excepcions dispositius USB a nivell global o per política, indicant el fabricant, model i número de sèrie d'aquests.

5.4 Requeriments tècnics protecció de correu electrònic online i eines col·laboratives.

5.4.1 Requeriments generals

La solució ha d'oferir protecció per a les solucions següents:

- Exchange Online
- One Drive
- Sharepoint Online
- Microsoft Teams
- Teams Chat

A més, ha de fer una protecció multicapa a través de l'**API del fabricant**, en real-time i sense necessitat de modificar els registres MX ni el flux de correu, ha de donar protecció en Real-time de les solucions requerides i comptar amb la possibilitat de llançar anàlisis sota demanda sobre les diferents plataformes.

La solució haurà de proporcionar les llicències necessàries per tal de cobrir la totalitat dels elements protegibles de 2000 usuaris.

5.4.2 Requeriments de la Consola de Gestió

- La consola ha de permetre la integració i gestió de múltiples organitzacions / comptes / tenants de les solucions a protegir.
- Ha de permetre la gestió de rols i usuaris de manera granular, per poder realitzar delegació de permisos sobre una mateixa organització, o sobre funcions específiques dins d' aquesta.
- Ha de disposar d'un dashboard on es podran veure els punts més importants de les diferents solucions protegides.
- Ha de tenir un sistema de logs separats per organitzacions i solucions protegides, basada en objectes amb recerques dinàmiques, de manera que pugui permetre anar acotant la recerca de forma ràpida i orientada.
- Ha de tenir un sistema de reports que permeti generar reports personalitzats i granulars, per organitzacions i solucions protegides.

- Ha de permetre quarantena per organitzacions i solucions protegides amb diferents possibilitats d'acció per a l'administrador com podrien ser descarrega, restauració o esborrat. Aquesta quarantena esborrarà els elements de forma automàtica, als 30, 60 o 90 dies.
- Ha de permetre SSO mitjançant Azure AD, Active Directory i Okta.
- Ha de tenir una API disponible i documentada per a la seva explotació.

5.4.3 Requeriments de seguretat

La solució ha de tenir diferents mòduls, que seran com a mínim els detallats a les següents sub-apartats

5.4.3.1 Prevenció de Spam (Exchange Online)

- Ha de tenir diferents nivells de sensibilitat de detecció SPAM (Alt, Mig i Baix).
- Ha de comptar amb un motor de detecció de Spoofing així com de dominis de nova creació o sospitosos.
- Ha de comptar amb un motor capaç de detectar una cosa que ja va ser analitzada en el seu moment i marcat com a net, i ara es determina que no ho és, de manera automàtica pren l'acció definida per l'administrador per a la protecció de l'usuari.
- Ha de detectar el anomenat "graymail", diferenciant per categoria: Màrqueting, xarxes socials, fòrums o massiu.
- Ha de tenir motors de detecció de BEC (Business Email Compromise) basats en regles, machine learning i patrons d'escriptura dels usuaris, (al menys els de perfil alt). Aquest motor ha de tenir:
    - Blacklist i Whitelist per a exclusions o bloquejos.
    - Ha de permetre executar múltiples accions davant les deteccions. (Marcatge, Esborrat, Posar en Quarantena, reemplaçar fitxers, deixar passar o enviar a carpeta de correu massiu (Junk))
    - Ha de ser capaç de enviar notificacions granulars a l'Administrador, als usuaris o ambdós.
    - Ha de tenir granularitat per tipus d'amenaça en les deteccions. (Spam, Graymail, Scam, Ransomware, Phishing, Malware, etc...)

5.4.3.2 Antimalware Multicapa (per a totes les solucions requerides en el punt Requeriments Generals)

Aquest mòduls ha de tenir les següents funcionalitats:

- Diferents capacitats d'anàlisi (Tots els fitxers, o fitxers específics, o categoritzats amb Fitxer de tipus real)
- Ha de detectar patrons o signatures.
- Ha de tenir una detecció bassada en IA/Machine Learning en pre-execució sense suport d'una Sandbox. Ajudant a la detecció d'amenaces de tipus Zeroday.
- Neteja de contingut actiu, per la neteja de macros.
- Anàlisi i protecció davant arxius comprimits amb al menys 5 capes de compressió.
- Ha de Tractar de buscar la contrasenya al cos d'un missatge que porta un adjunt protegit amb contrasenya i d'aquesta manera poder analitzar el contingut d'aquesta informació protegida.
- Múltiples accions davant les deteccions. (Etiquetat, esborrat, posar en quarantena, Reemplaçar fitxers, deixar-los passar, o enviar a carpetad e correu massiu (Junk))

- Ha de deixar enviar notificacions granulars a l'administrador, als usuaris o ambdós.
- Ha de tenir granularitat per tipus d' amenaça en les deteccions. (Virus, Worm, Ransomware, Troià, etc.)

5.4.3.3 Bloqueig de Fitxers (per a totes les solucions requerides en el punt Requeriments Generals)

Aquest mòdul ha de tenir les següents capacitats:

- Bloquejar qualsevol tipus de fitxer o un tipus específic.
- El bloqueig pot realitzar-se per tipus de fitxer (Existint preconfigurat diferents categories), extensió o nom.
- Ha de permetre múltiples accions davant les deteccions. (Esborrat, Posar en Quarantena, reemplaçar el fitxer o deixar passar)
- Ha de permetre l'enviament de notificacions granulars a l'administrador, usuaris o ambdós.

5.4.3.4 Reputació Web (per a totes les solucions requerides en el punt Requeriments Generals)

Aquest mòdul ha de tenir les següents funcionalitats:

- Ha de comptar amb diferents nivells de sensibilitat de detecció de reputació d'IPs, dominis i URLs.
- Ha de tenir la possibilitat d' analitzar URLs incrustades en fitxers adjunts.
- Ha de poder fer un escaneig dinàmic d'URLs, arribant a analitzar tots els possibles salts d'aquesta URL fins a arribar al seu destí. No només es basa en la reputació de la URL inicial.
- Ha de tenir un motor capaç de detectar un objecte (URL, IP, etc.) que ja va ser analitzada en el seu moment i marcat com a net, i ara es determina que no ho és, de manera automàtica pren l'acció definida per l'administrador per a la protecció de l'usuari.
- Protegeix l'usuari al moment del click, comprovant en temps real la reputació d'aquest destí. Aquesta tecnologia es pot aplicar a totes les URLs, a les no testades per al fabricant, o aquelles URLs marcades com a sospitoses.
- Ha de comptar amb una tecnologia basada en tècniques OCR per a la detecció de llocs de Phishing mitjançant la comparació amb els sites originals a baix nivell.
- Escaneig de codis QR per a extracció d' URLs.
- Blacklist i Whitelist per a exclusions o bloquejos.
- Múltiples accions davant les deteccions. (Etiquetat, Esborrat, Posar en quarantena o deixar passar)
- Ha de permetre enviar notificacions granulars a Administrador, usuaris o ambdós.
- Ha de tenir granularitat per tipus d' amenaça en les deteccions. Podent així concretar més en el tipus d' amenaça. (C&C, Malware, Ransomware, Phishing, Scam, etc.)

5.4.3.5 Sandbox (per a totes les solucions requerides en el punt Requeriments Generals)

Es requereix un mòdul de sandox integrat amb la resta de components d'aquesta solució, amb les següents característiques:

- Que pugui treballar en mode "Monitor", només notificant les troballes sense realitzar cap acció.
- Que permeti Blacklists i Whitelists per a exclusions o bloquejos.
- Després de fer l'anàlisi, haurà de classificar la mostra segons diferents nivells de risc: Alt, Mig, Baix o No Classificat.
- Ha de permetre múltiples accions davant les deteccions i granularitat en base al resultat de l' anàlisi. (etiquetat, esborrat, posar en quarantena o deixar passar)
- Ha de permetre enviar notificacions granulars a l'administrador, els usuaris o ambdós.

5.4.3.6 Prevenció de pèrdua de dades (per a totes les solucions requerides en el punt Requeriments Generals)

Es demana un mòdul DLP sobre els canals protegits en temps real i sota demanda per a recerca puntual d'una dada sobre tots els canals que tingui les següents característiques:

- Ha de tenir més de 240 plantilles preconfigurades.
- Ha de comptar amb la possibilitat de generar identificadors de dades i plantilles personalitzades.
- Els identificadors de dades es podran crear mitjançant expressions regulars, paraules clau o llistes que combinin ambdós mètodes.
- Les accions per realitzar són, al menys, deixar passar, esborrar o posar en quarantenta.

5.5 Requeriments tècnics Oficina tècnica virtual de seguretat (OTS)

1. La persona o equip de persones designades per desenvolupar la part d'auditoria normativa hauran de disposar d'alguna de les següents certificacions amb vigència que els acrediti per fer-la (CISA, CISM o CISSP).
2. La persona o equip de persones designades per desenvolupar la part d'auditoria tècnica hauran de disposar d'alguna de les següents certificacions amb vigència que els acrediti per fer-la (CEH o OSCP).
3. La persona o equip de persones designades per desenvolupar la part de gestió de la ciberseguretat i monitorització dels sistemes descrits als punts 5.2 hauran de disposar de les següents certificacions amb vigència que els acrediti per fer-la (Fortinet NSE5 FortiSIEM).
4. La persona o equip de persones designades per desenvolupar la part de gestió de la ciberseguretat i monitorització dels sistemes descrits als punts 5.3 i 5.4 hauran de disposar de les certificacions amb vigència que proporcioni el fabricant de la solució guanyadora que els acrediti per fer-la.
5. Auditoria normativa:
    a. Definir la normativa de seguretat (Polítiques, normes i procediments) i vetllar pel seu compliment, adaptant-se als diferents reglaments o normatives que calgui complir (LPIC, NIS, ENS, RGPD)
    b. Gestionar els riscos de seguretat de la informació i establir el pla d'acció adient
    c. Vetllar i impulsar la identificació de requeriments de seguretat
    d. Identificar i impulsar la identificació i establiment dels controls de seguretat necessaris per controlar el risc (controls organitzatius, procedimentals, tècnics i humans)

e. Supervisar el nivell de seguretat, compliment de controls i grau d'eficàcia de les mides aplicades
f. Supervisar el compliment de la legislació en els aspectes referents al seu abast d'actuació
g. Fer d'interlocutor amb la direcció en matèria de seguretat de la informació (mètriques, reporting de riscos, plans d'actuació, amenaces i incidències)
h. Fer d'interlocutor amb d'altres empreses, institucions, etc., en matèria de seguretat de la informació
i. Formar i conscienciar a la organització en matèria de seguretat de la informació
j. Gestionar la operació i els incidents de seguretat de la informació sigui directament, a través de serveis externalitzats o d'altres àrees de la organització
k. Prevenir el frau, al menys el que prové de mitjans electrònics.

6. Administració i revisió de la solució FortiSIEM
7. Administració i revisió de la solució FortiAnalyzer
8. Administració i revisió de la solució de protecció de servidors i endpoint
9. Administració i revisió de la solució de protecció de correu electrònic online i eines col·laboratives
10. Caldrà demostrar expertesa i coneixements de metodologies d'auditories de seguretat de la informació i hacking ètic, cursos, certificacions, etc.
11. A efectes de compliment normatiu, caldrà demostrar expertesa en gestió de sistemes d'informació en l'àmbit Sanitari.
12. La persona que desenvolupi aquesta tasca haurà d'estar disponible en horari d'oficina (8x5), a tal efecte haurà de proporcionar-se un número de telèfon mòbil on localitzar-la.
13. Haurà de dedicar-se una jornada presencial setmanal a les instal·lacions CSMS.
14. En el cas de que la persona designada hagi d'abandonar el projecte de manera definitiva, l'adjudicatari haurà de substituir-la per un altra del mateix perfil.

6 Implantació del subministrament

Aquest capítol té com a objectiu definir les bases i etapes en què s'organitza la implantació dels nous serveis i les regles per estructurar el treball que ha de servir de referència al licitador per a l'elaboració de la seva oferta.

Aquesta visió en fases i etapes no és prescriptiva, sinó que només serveix a nivell de referència per estructurar els treballs a realitzar en la implementació.

El que sí és preceptiu és la realització per part de l'adjudicatari del pla d'implantació que ha de dur a terme, minimitzant els possibles impactes en el servei durant aquesta fase. Per aquesta raó, durant el desplegament del servei s'ha de garantir la qualitat d'execució del projecte, l'eficiència en el traspàs i la qualitat del servei final, així com la mínima afectació possible al servei de comunicacions, per la qual cosa s'ha de considerar que qualsevol tasca que suposi tall de servei a usuaris s'haurà de realitzar fora de l'horari laboral del personal afectat.

El pla d'implantació del servei ha de tenir en compte com a mínim:

- La planificació de la implantació i gestió del projecte: elaboració del projecte executiu que inclourà tots els aspectes tècnics de la solució (disseny final, arquitectura, tecnologia, dimensionament i pla de proves) i de l'explotació (procediments i eines per a la provisió dels serveis associats).
- Pla de proves: l'adjudicatari haurà de realitzar el test dels serveis d'acord amb el pla de proves presentat al projecte i d'acord amb la normativa vigent per cada tipus de sistema i/o servei.
- Acceptació dels serveis: un cop finalitzades les proves amb èxit i lliurada la documentació de les instal·lacions, el responsable del servei per part de la CSMS procedirà a l'acceptació del mateix i podrà iniciar-se la facturació, segons model d'acceptació descrit en els següents apartats.

En cap cas la implantació podrà comportar una pèrdua de nivell de servei o una interrupció del mateix.

Els licitadors hauran d'indicar en les seves propostes els mecanismes existents per garantir l'aplicació de les condicions pactades de forma coordinada amb el pla d'implantació.

6.1 Consideracions generals.

La Corporació de Salut del Maresme i la Selva disposa de tallafocs a totes les seves seus que s'encarreguen d'assegurar la connectivitat amb internet, Nus Sanitari i proveïdors de servei.

El subministrament del nou equipament haurà d'incloure el compliment de tots els requeriments tècnics sol·licitats.

En el cas de que el servei sigui afectat per la implantació del subministrament caldrà pactar l'horari de les tasques, podent ser necessari efectuar-les en horari nocturn o de cap de setmana.

Durant tota la implementació del projecte es seguiran les condicions que es detallen a continuació.

6.2 Gestió de projecte d'implantació

6.2.1 Direcció de projecte

L'adjudicatari es compromet a complir els requeriments que marqui la oficina de projectes de la CSMS, tant pel que fa a requeriments de procés com tècnics.

La direcció de projecte estarà liderada per la CSMS, que redefinirà el calendari i fites presencials per l'adjudicatari. Durant la fase d'anàlisi . Durant la fase d'anàlisi es definirà el comitè de seguiment de projecte en que s'avaluarà el projecte i es detectaran les mancances.

6.2.2 Comitè de seguiment

Es definirà un comitè de seguiment en que hi participarà tant les direccions de sistemes de la CSMS com la direcció de l'adjudicatari, així com aquelles persones, tant de la CSMS com de l'adjudicatari rellevants per les reunions específiques.

6.2.3 Calendari i fases del projecte

Es realitzarà un calendari del projecte on s'avaluaran les seves fases, fites i dates clau.

L'adjudicatari haurà d'adaptar-se al calendari de projectes i disponibilitat de recursos interns de la CSMS.

Durant el projecte la CSMS podrà replanificar les tasques de projecte i calendari en funció de les necessitats de negoci de la CSMS. Aquesta re planificació es presentarà en el següent comitè de projecte o en un comitè de projecte d'urgència. L'adjudicatari podrà ajustar la planificació en base als seus propis recursos per tal de tancar una nova planificació que s'ajusti, tant als nous requeriments de calendari de la CSMS com de la disponibilitat de recursos de l'adjudicatari.

En qualsevol cas els terminis màxims d'execució del projecte hauran de ser:

- 3 mesos des de la la formalització del contracte per a la part de seguretat perimetral.
- 3 mesos des de la formalització del contracte per a protecció de servidors i punt de treball

Aquests terminis màxims només podran ser superats a petició expressa de la CSMS i degut a necessitats organitzatives de la pròpia CSMS.

6.2.4 Recursos

L'adjudicatari es compromet a proporcionar els recursos humans i tècnics oferts en la seva proposta. En cas de que l'adjudicatari hagi de reemplaçar un dels recursos, haurà d'informar amb una setmana d'antelació d'aquest fet.

La CSMS es reserva el dret de demanar un canvi de recurs si aquest no compleix amb els requeriments de qualitat, coneixements tècnics o d'entrega de tasques a temps.

6.2.5 Faltes

6.2.5.1 Faltes lleus

Es defineix com a falta lleu la no entrega d'una tasca o entrega en el temps especificat per part de l'adjudicatari. La comunicació de faltes es realitzarà en la següent reunió de seguiment de projecte.

6.2.5.2 Faltes greus

Es defineix com a falta greu el no compliment d'una fita clau o entrega. Aquesta falta greu serà deguda a l'adjudicatari si en el camí crític per l'assoliment de la fita no hi ha tasques fora de termini associades a la CSMS.

També es defineix coma falta greu la acumulació d'un 10% de faltes lleus sobre el total de tasques realitzades.

6.2.5.3 *Penalitzacions*

Amb l'objectiu d'assolir els projectes dins d'un llindar de compliment raonable s'establiran Per cada falta greu es planteja una penalització del 5% de l'adquisició.

En tot cas, la quantia de cada una de les penalitats no podrà excedir del 10% del preu del contracte, IVA exclòs, ni el seu total podrà superar en cap cas el 50% del preu del contracte.

6.2.6 Etapes de projecte

Es divideix la implementació del projecte en diferents etapes per facilitar-ne la seva gestió.

6.2.6.1 *Etapa 1. Anàlisi i entrega d'equipament*

S'estableix un projecte basat en etapes d'implantació. En una primera etapa es realitzarà un anàlisi específic de la proposta de l'adjudicatari, de les hores/home informe presentades i de les entregues de material. A partir d'aquí es tancarà un calendari de projecte en base als projectes en curs i disponibilitat de persones per part de totes les bandes. Sobre aquest calendari es marcaran les fites parcials i total del projecte i servirà com a base per a controlar l'evolució del projecte.

En aquesta fase es farà l'entrega de tots els materials que comprèn l'adjudicació inicial.

6.2.6.2 *Etapa 2. Execució*

Durant aquesta etapa es farà la implantació de l'equipament en ordre de prioritat segons el calendari consensuat amb la CSMS.

6.2.6.3 *Etapa 3. Tancament*

En aquesta etapa s'entregarà tota la documentació de projecte, es farà el traspàs d'informació i es farà la signatura de fi de projecte.

7 Servei d'operació i manteniment

7.1 Horari del servei

El servei s'oferirà en format 24x7

7.2 Temps de resposta

El tècnic de la Corporació que obri una incidència fixarà el nivell de prioritat de la mateixa. L'adjudicatari haurà de complir els següents temps de resposta màxims per a l'atenció de les incidències en funció del seu nivell de prioritat:

- Incidències de prioritat alta: 15 minuts.
- Incidències de prioritat normal: 4 hores.
- Incidències de prioritat baixa: dia següent laborable.

El temps de resposta es considera dins de l'horari indicat amb anterioritat.

7.3 Actualització de versions

Trimestralment es farà una revisió de les versions de tots els components que formen part de la solució sol·licitada en aquesta licitació, i si s'escau es procedirà – prèvia planificació amb la CSMS – a fer l'actualització del que es pacti.
No obstant, si es detecta una vulnerabilitat crítica, com a part del suport proactiu, l'adjudicatari avisarà el més aviat possible a la CSMS per tal de posar-hi remei.

S'instal·larà la darrera versió i "hot-fix" disponibles del programari o be la que es pacti amb el personal de la Corporació.

Previ a l'actualització, es farà un procés d'estudi de les diferències entre les versions i els possibles problemes o punts a tenir en compte en la migració o que afectin al desplegament de la nova versió en la infraestructura. Abans de cometre-la es presentarà un informe a la Corporació amb les conclusions d'aquest procés d'estudi.

Tant les revisions com les actualitzacions de versió no podran repercutir econòmicament a la CSMS, ja que formen part del servei de manteniment de la solució.

7.4 Equip de suport tècnic

L'adjudicatari, assignarà un o més gestors de servei que coneixeran de primera mà la infraestructura i realitat de la CSMS.

Tot i això, les incidències es registraran sempre seguint el procediment habitual, per correu electrònic o de manera telefònica amb el servei de suport tècnic en horari laboral i trucant al telèfon guàrdies fora d'horari laboral.

S'emprarà un equip tècnic de suport composat mínim per 5 tècnics certificats pel fabricant, que respondrà a les incidències. L'adjudicatari es compromet a que, a excepció de situacions extraordinàries i excepcionals, seran aquests tècnics i no d'altres els que atendran les incidències de seguretat.
Com a mínim un d'aquests tècnics haurà d'estar localitzable 24x7 per si es produeix una incidència crítica.
És obligatori que com a mínim un d'aquests tècnics tingui la certificació Fortinet NSE7 o equivalent, i la resta de tècnics tinguin com a mínim la certificació Fortinet NSE4 o equivalent. Ambdues certificacions vigents durant la durada de tota la licitació.
Si durant l'execució del contracte l'adjudicatari necessités reemplaçar a algun dels tècnics, haurà de fer-ho per un altre amb la mateixa capacitat tècnica, havent de comunicar-ho i acreditar-ho a la Corporació per a la seva acceptació.

7.5 Característiques del servei

Es requereix un servei de suport integral, que pugui anar més enllà del típic servei de suport reactiu, per això es demana que els licitadors incloguin en les seves propostes els següents serveis de suport:

7.5.1 Suport Preventiu/Proactiu:

Aquest servei de suport s'encarregarà de lo següent:

- Fer una revisió de tota la solució al menys 1 cop a l'any, per detectar problemes de rendiment de CPUs, memòria, regles de tallafocs que estiguin en desús, i altres similars que puguin

detectar problemes abans de que apareguin i d'aquesta manera es mantingui la solució optimitzada.

- Es demana una actualització de firmware dels equips si el fabricant las ha publicat com estables al menys un cop a l'any. Si es detecta una vulnerabilitat a la versió aplicada a algun component de la solució que pugui comprometre la seguretat de la CSMS, aquesta actualització s'ha de notificar de manera immediata. En tot cas, la actualització s'aplicarà en una franja horària consensuada entre l'adjudicatari i la CSMS.
- Monitorització i notificació de tots els dispositius Fortinet desplegats a la solució.

7.5.2 Suport Reactiu

El servei de suport reactiu s'ha d'encarregar de resoldre totes aquelles incidències de hardware o software que poguessin produir-se, per restablir el correcte funcionament del equipament afectat. Dins d'aquest tipus de suport s'inclouen els següents serveis:

- Assistència tècnica remota il·limitada, contactant per correu, web de suport o via telefònica
- Assistència in-situ: Quan es determini remotament la necessitat, es farà el desplaçament d'un tècnic (o més si es necessari) a les dependències de la CSMS.
- Reposició d'equipament: Tramitació de RMA amb Fortinet, que inclou l'enviament del hardware necessari a la localitat del client.
- Escalat d'incidències amb fabricant: En el cas poc probable de que una incidència no pugui ser resoldre per Dagram, s'efectuarà l'escalat amb Fortinet i es gestionarà la comunicació entre fabricant i client fins a la resolució d'aquesta incidència.

Atenció a dubtes i consultes: Es respondran les dubtes i consultes relatives a la solució instal·lada, amb el SLA mostrat a l'apartat corresponent. Les consultes podran ser relatives a noves funcionalitats ofertes pel fabricant i funcionament en general de la solució, i similars.

7.6 Durada del servei

El servei haurà de contemplar tots els requeriments anteriors per a una durada inicial de contracte de 3 anys, més la possibilitat de pròrroga per a 2 anualitats més.

8 Pla de formació

L'adjudicatari haurà d'incloure un pla de formació enfocat al personal tècnic que la CSMS consideri oportú, amb la finalitat de donar-los a conèixer les característiques, funcionament i explotació dels serveis, així com els processos de gestió del mateix.
Aquesta formació serà presencial a un dels centres de la CSMS.
L'adjudicatari haurà de preveure aquest pla de formació en la seva oferta sense posteriorment repercutir cap cost addicional a la CSMS.

Com a base, els objectius bàsics del Pla de Formació són:

- Transferència de coneixements sobre tots els components que formen part de la solució sol·licitada en aquesta licitació.
- Resolució de dubtes sobre la operativa en referència als diferents tots els components que formen part de la solució sol·licitada en aquesta licitació.

Per a la consecució d'aquests objectius, el pla de formació dissenyat per l'adjudicatari haurà de tenir en compte les següents consideracions:

- La formació s'orientarà a les peculiaritats i característiques de tots els components que formen part de la solució presentada.
- Tota la documentació de suport i les sessions de formació s'han d'impartir en català i l'adjudicatari haurà de proveir tot el material necessari (en línia o a través d'altres mitjans) per a tots els usuaris. Tot el material utilitzat en les sessions de formació es lliurarà a la CSMS, a la finalització de les mateixes.
- Cadascuna de les sessions formatives s'hauran de dimensionar de manera que la durada establerta permeti assegurar el compliment dels objectius marcats i la logística s'organitzarà perquè puguin assistir un mínim de 4 persones.

Addicionalment a aquest pla formatiu:

- A la finalització del contracte, i amb la plena transferència del servei, l'adjudicatari garantirà la disponibilitat de recursos amb prou nivell de coneixement durant els tres (3) mesos següents per donar suport puntual al nou adjudicatari, si escau.

9 Model de relació

9.1 Informació general

En aquest apartat es vol marcar quin és el model de seguiment del projecte d'implantació.

9.1.1 Direcció del projecte

La direcció del projecte per part de la CSMS serà designada per la Direcció de Sistemes de la CSMS, que actuarà com a impulsor principal del projecte. La persona designada per aquesta Direcció s'encarregarà de la supervisió i coordinació del projecte. Per part de l'adjudicatari hi haurà un cap de projecte encarregat d'organitzar i portar a la pràctica l'execució dels treballs del projecte.

9.1.2 Equip de treball

L'adjudicatari determinarà la composició de l'equip de treball de tal manera que s'ajusti als entorns tant funcionals com operatius establerts, amb la capacitat de portar a terme tots els objectius i serveis que es descriuen en el present document. Aquest equip de treball estarà liderat per un cap de projecte el qual serà l'interlocutor amb la direcció de projecte designada per part de la CSMS. L'equip de treball proposat haurà de tenir els nivells adients de qualificació i certificació:

- En l'àmbit tècnic, experiència en la instal·lació i/o configuració dels serveis de comunicacions d' interconnexions de seus, per als equips que s'encarregaran d'aquestes tasques.

- Cadascun dels diferents components considerats crítics, ha de tenir associat mínim un tècnic de "nivell 3" de l'equip de treball. Aquests components crítics (disruptius) son:

    - Tallafocs
    - Protecció del correu electrònic

Aquest tècnic de nivell 3 no haurà de ser qui gestioni totes les incidències relacionades amb equipament crític, però si que en cas d'incidències urgents/greus amb aquest equipament crític se n'hauria de fer càrrec per tal de no passar per nivells de tècnics intermedis (nivell 1 i nivell 2).

Dins de la presentació de la oferta s'aportarà informació sobre els professionals que conformaran aquest equip de treball amb detall dels coneixements professionals, dedicació prèvia, certificacions de gestió i tecnològiques que aporta i rol assignat.

La substitució posterior d'algun membre dels inicialment adscrits al servei només es podrà fer si els coneixements i currículum són equivalents i la CSMS dona el vist i plau a la mateixa.

9.1.3 Seguiment i control

La direcció del projecte serà l'encarregada de controlar i supervisar tant la productivitat com la qualitat dels treballs realitzats per l'adjudicatari.

La quantitat, periodicitat i assistents a les reunions de seguiment s'establirà de mutu acord entre ambdues parts, tot i que es demana, com a mínim, una reunió de seguiment cada tres mesos a les instal·lacions de la CSMS.

9.1.4 Documentació de seguiment durant la instal·lació

Durant l'execució de les diferents tasques d'instal·lació el director de projecte per part de l'adjudicatari facilitarà documentació al director del projecte designat per la CSMS amb informació relativa al desenvolupament del projecte. Aquesta documentació constituirà el quadre de comandament i contindrà tota la informació necessària per tal de poder realitzar el correcte seguiment i control sobre l'estat d'execució del projecte. El quadre de comandament es lliurarà com a màxim al final de cada mes i contindrà al menys els següents elements:

- Dades de disponibilitat de l'equipament associat al servei.
- Dates d'inici i final previstes per a cadascun dels sistemes a implantar
- Percentatges d'execució
- Llista d'incidències i accions correctores que es porten a terme
- Llista de riscos que afectin a l'execució del projecte i pla d'acció per cadascun d'ells

A més del quadre de comandament, també s'anirà facilitant aquella documentació relativa als equipaments definitivament instal·lats, com per exemple manuals, configuracions, diagrames, etc. Tota aquesta documentació s'haurà de consensuar entre l'adjudicatari i la CSMS a l'inici del projecte.

9.2 Fase d'explotació

S'espera de l'adjudicatari una actitud proactiva durant la durada del contracte que faciliti la relació fluïda entre les dues parts, assumint un gran nivell de compromís i responsabilitat.

Els licitadors hauran d'incloure en les seves ofertes una proposta del model de relació plantejat. En aquest apartat s'exposen els requeriments mínims a complir i que hauran de ser desenvolupats i / o ampliats en les propostes.

El model de relació defineix les funcions i responsabilitats de l'adjudicatari i de la CSMS en un marc d'actuació comú per assegurar el compliment de les obligacions de cadascuna de les parts. És un marc de relació que permet acordar el contingut i nivell de la prestació dels serveis, així com el seguiment de la prestació real en els aspectes estratègics, contractuals, tàctics i operatius.

L'adjudicatari pot ampliar, millorar i detallar, en base a les directrius aquí marcades, l'organització proposada i l'esquema específic de la relació amb la CSMS, així com els mecanismes de control propis de cada servei i funció transversal.

El model de relació es sustenta en una estructura de competències i funcions que recauen sobre un esquelet de responsables de l'adjudicatari, que es relacionaran amb la CSMS en base a dos àmbits de gestió: gestió del Contracte i gestió Operativa.

9.2.1 Àmbits i òrgans de gestió

A continuació es presenten els òrgans de gestió en què es vol desglossar el model de relació. El model de relació entre la CSMS i l'adjudicatari es pretén articular entorn a dos nivells de comunicació i coordinació, també anomenats comitès.

Tot i que la composició i periodicitat d'aquests comitès es definirà a l'inici de la prestació del servei, la CSMS planteja una sèrie de tasques mínimes sobre les quals s'haurà de realitzar un seguiment periòdic.

Comitè Direcció

Responsable de la presa de decisions estratègiques a mig-llarg termini:

• Seguiment econòmic global del contracte, evolució de la facturació i del consum (pressupost).

• Seguiment global d'expectatives i feedback de la CSMS a l'adjudicatari amb el servei prestat.

• Seguiment del grau d'avanç de les iniciatives de transformació que s'hagin abordat durant el període i plantejament de noves iniciatives.

• Seguiment i control global de l'operació i provisió del servei. Compliment de nivells de servei i penalitzacions aplicables dins del període.

• Nivell d'alineació dels processos de gestió de l'adjudicatari amb els processos de la CSMS.

• Seguiment de situacions especials no recollides en els processos de gestió.

• Anàlisi i aprovació del pla de millora contínua de l'adjudicatari.

• Gestió de riscos: Riscos identificats i plans de mitigació.

La CSMS sol·licita que en la seva proposta els licitadors defineixin els integrants que participarien en aquest comitè per la seva part. En el cas del comitè direcció la CSMS estima que la seva freqüència hauria de ser com a mínim cada tres mesos, sense perjudici que es puguin convocar ad hoc en cas necessari.

Comitè operatiu

• Revisió i aprovació d'ANS.

• Anàlisi de KPIs de processos de gestió de forma global i per servei.

• Compliment de l'adjudicatari dels models de qualitat i seguretat dels serveis de la CSMS.

• Seguiment d'indicadors de qualitat de servei.

• Desenvolupar i mantenir els procediments operatius necessaris per al correcte funcionament del servei.

• Seguiment d'incidències i de la resolució d'incidències de casos específics o crítics.

• Seguiment d'accions correctives i preventives.

• Anàlisi de peticions i situacions de canvi en els serveis, així com el seu escalat a l'àmbit directiu si fos necessari.

• Escalat de possibles millores detectades en el servei.

• Planificació gestió d'auditories, anàlisi de resultats, gestió de no conformitats i punts de millora.

• Seguiment d'accions correctives i preventives derivades de les auditories.

• Tractament de les problemàtiques específiques detectades.

La CSMS sol·licita que en la seva proposta els licitadors defineixin els integrants que participarien en aquest comitè per la seva part.

9.2.2 Model de Reporting

Per al control i seguiment s'utilitzaran mètriques i informes periòdics que serviran de suport als òrgans de gestió establerts i que són, en conjunt, el mecanisme de seguiment i avaluació del servei.

L'adjudicatari és el responsable de generar i lliurar els informes i mètriques de reporting que es determinen en els diferents àmbits. Aquests han de permetre a la CSMS governar, controlar i gestionar els serveis prestats per l'adjudicatari, tant des d'una òptica individual, com transversal i global.

S'ha de tenir en consideració que:

- El format exacte i el contingut detallat de la informació a elaborar serà acordat entre l'adjudicatari i la CSMS. La CSMS podrà sol·licitar, durant la vigència del contracte canvis en l'estructura i contingut de la informació per ajustar-se a les necessitats de seguiment dels serveis.
- En cas que la CSMS sol·liciti informació, l'adjudicatari realitzarà el lliurament d'aquesta, complint, si escau, amb els ANS definits pel servei.
- La CSMS podrà sol·licitar alguna informació de forma immediata. L'adjudicatari automatitzarà l'elaboració d'aquesta, per poder donar una resposta ràpida fora de la planificació inicial establerta.
- La CSMS podrà sol·licitar informació diària dels indicadors que consideri necessaris per al seguiment dels serveis. L'adjudicatari automatitzarà l'elaboració d'aquesta informació, per poder donar una resposta ràpida.
- L'adjudicatari es compromet a lliurar la informació en format electrònic i tractable com a màxim el dia 10 de cada mes. Aquesta informació s'emmagatzemarà de forma centralitzada on la CSMS estimi oportú.
- L'adjudicatari haurà de disposar dels mecanismes necessaris per garantir que les mètriques i indicadors de mesura són correctes, i que la CSMS podrà dur a terme les auditories que consideri necessàries per a la seva verificació.
- La CSMS és la propietària de tota la documentació elaborada per l'adjudicatari referent al servei prestat.
- La CSMS serà la responsable de la validació i aprovació dels documents elaborats per l'adjudicatari.
- L'adjudicatari haurà de mantenir la documentació actualitzada segons política de gestió documental de la CSMS.
- Així mateix l'adjudicatari haurà de mantenir un registre de la documentació enviada a la CSMS amb el detall de les versions, dates i destinataris. Aquest registre estarà a disposició de la CSMS en el repositori d'informació que la CSMS hagi designat a aquest efecte.
- També es demana que es faci un registre de tots els arxius que lliuri a la CSMS o que siguin generats per qualsevol petició concreta.

9.2.3 Informes de servei

L'adjudicatari haurà de presentar un informe dels serveis oferts. Aquest informe ha d'incloure, almenys:

- **Equipament**. Caldrà incorporar en l'informe totes les dades identificatives d'aquells equipaments aprovisionats al mes. Addicionalment, aquestes dades s'hauran de recollir a l'inventari corporatiu per tal de mantenir-lo actualitzat. Aquest inventari corporatiu contindrà tot l'equipament existent a totes les seus i s'haurà de presentar actualitzat de forma mensual i a la finalització del contracte.
- **Disponibilitat**. L'informe haurà de presentar la disponibilitat de forma individualitzada de cada enllaç. Aquest llistat haurà d'estar ordenat per tipus de centre i per disponibilitat, de menor a major.
- **Ús i Ocupació**. L'informe d'incorporar informació gràfica i numèrica de l'ocupació dels enllaços d'accés, tant en valor absolut com en percentatge de l'ample de banda disponible.
- **Incidències**. Es detallaran totes les incidències produïdes durant el mes tant a la xarxa, en l'equipament com en el servei. Per a això s'indicarà la data i hora d'inici, la data i hora de resolució de la incidència i la solució a la incidència.
- **Actuacions i modificacions**. L'informe ha de recollir els canvis que s'hagin produït a la xarxa, en l'equipament (incloent activitats de manteniment) o a les prestacions del servei a causa d'actuacions o modificacions.

Addicionalment, la CSMS podrà sol·licitar informes especials de xarxa, equipament o servei a l'adjudicatari si així ho considera convenient (per exemple per incidències reiterades, en la posada en marxa d'un nou servei, etc.).

9.2.4 Benchmark

A partir de la finalització del segon any de contracte, i amb periodicitat anual, la CSMS es reserva el dret d'avaluar l'evolució tecnològica i del mercat que afecta de forma directa als serveis inclosos al contracte. D'aquest estudi es podrà derivar una revisió de l'equipament subministrat, adequant-lo si s'escau a les necessitats tecnològiques del moment actual.

L'estudi de mercat serà realitzat per una empresa externa independent acordada per ambdues parts. Les tasques de contractació també aniran a càrrec de l'adjudicatari. No és objectiu de la CSMS la reducció de la factura global de l'adjudicatari mitjançant aquest procés d'avaluació. L'objectiu és destinar els possibles estalvis a l'ampliació de capacitats o la millora dels serveis relacionats amb l'objecte del contracte que poguessin ser de l'interès de la CSMS.

9.2.5 Proves periòdiques

Cal establir un calendari periòdic de proves sobre aquells entorns que han de donar una continuïtat de servei.

Aquestes proves poden ser:

- Comprovar l'alta disponibilitat (HA) en cas de caiguda d'un dels nodes d'un clúster
- Correcte balanceig entre línia principal de dades i línia de backup en els centres on hi ha més d'una línia de dades física cap a la seu central.

10 Pla de devolució del servei

Per garantir la correcta transferència d'actius i coneixements s'articula una fase de devolució dels serveis a la CSMS, o a qui aquest determini; durant el qual es transferiran les possibles infraestructures i serveis d'operació / manteniment dels serveis objecte del present plec o del contracte. Totes les tasques relacionades amb la devolució del servei s'executaran durant els últims mesos de vigència de contracte. Aquesta fase es regirà per un pla de devolució del servei, d'acord amb els requeriments del apartat 11 d'aquest document.

10.1 Descripció del pla de devolució

L'adjudicatari inclourà un pla de devolució del servei detallat que descrigui les obligacions i tasques que hauran de ser desenvolupades per cadascuna de les parts en relació amb la devolució, i que inclogui els termes i condicions en què aquesta es realitzarà.

Un cop finalitzat el contracte resultat de la present licitació, i realitzada la nova licitació, amb la finalitat d'evitar que l'operador que resulti adjudicatari i estigui prestant el servei pugui realitzar un mal ús de la seva posició, durant el procés d'implantació estarà obligat a retornar el control dels serveis i la infraestructura objecte del contracte, havent de realitzar en paral·lel els treballs de devolució amb els de prestació del servei, sense cost addicional per la CSMS

Durant el període de devolució del servei, l'adjudicatari ha de complir els acords de nivell de servei. El pla de devolució no ha de causar cap discontinuïtat en el servei.

Les fases del període de devolució són les següents:

- **Prestació actual**: període en què el proveïdor actual presta servei.
- **Transferència del coneixement**: període en què el proveïdor entrant es coordina amb el sortint i es porta a terme el pla de traspàs del coneixement. Per a aquesta fase s'estableix un període màxim de dos (2) mesos.
- **Prestació en transició**: El nou adjudicatari comença a prestar servei i compta amb l'assistència i el suport funcional del proveïdor sortint; durant aquest període s'aniran migrant seus i serveis i el proveïdor sortint donarà suport i resoldrà qualsevol qüestió o problema que pugui plantejar el proveïdor entrant, dedicant els recursos que fossin necessaris. Es mantenen durant aquest període els ANS vigents durant el contracte anterior, en cas d'haver d'aplicar penalitzacions es realitzarien sobre aquest supòsit.

- **Nova prestació**: el nou proveïdor assumeix totalment el servei. Comencen a operar amb els nous ANS i condicions del servei definits en el present plec.

El pla de devolució ha de complir, com a mínim, els següents principis i continguts:

- El termini d'execució serà com a màxim de sis (6) mesos.
- El proveïdor sortint ha de mantenir, durant la devolució del servei, el mateix equip de treball que durant la resta de la prestació.
- La CSMS no assumirà una dedicació significativa de recursos propis o del nou adjudicatari en les activitats de devolució.
- Serà la CSMS, o qui la CSMS designi, el responsable de coordinar la devolució del contracte íntegre, gestionant aquesta activitat extrem a extrem amb els prestadors entrant i sortint del servei.
- L'adjudicatari haurà d'oferir tota l'ajuda en la transferència a la CSMS, o a terceres parts indicades per aquest, de serveis subcontractats, garanties o contractes de manteniment existents fins al moment de la terminació en els mateixos termes pactats amb els adjudicataris d'aquests.
- L'adjudicatari haurà d'oferir un pla per definir les responsabilitats i gestionar la resolució de problemes entre el nou adjudicatari, la CSMS i / o altres adjudicataris.
- Inclourà la metodologia de transferència del coneixement dels aspectes fonamentals d'operació i, com a mínim, ha de descriure:
    - L'assistència, la formació i la documentació sobre els procediments de negoci o sistemes de la CSMS al nou adjudicatari.
    - L'accés al hardware, el software, la informació, la documentació i altre material utilitzat per l'adjudicatari o la CSMS a la provisió del servei.
    - La formació pràctica tutelada, en què el personal designat per la CSMS o el nou adjudicatari realitzi les tasques pròpies de cada procés o funcionalitat tutelats pel personal de l'adjudicatari.
    - L'adjudicatari haurà de revertir tot l'equipament i llicenciament, adscrit de forma exclusiva als serveis objecte del contracte, a la CSMS o a terceres parts acordades per facilitar la continuïtat del servei sense cap cost. També s'han d'incloure els sistemes i llicències necessàries per a la gestió, administració, monitorització de tots els equips, igual que els sistemes i llicències.
    - Es garantirà la completa actualització de l'eina d'inventari de la xarxa per tot el material subministrat, incloent:
        - Documentació operativa per tot l'equipament vinculat als serveis:
            - Marca, model i números de sèrie.
            - Manual tècnic.
            - Manual d'usuari.
            - Manual d'instal·lació.
            - Manual de manteniment.
            - Usuaris i Contrasenyes d'accés.
        - Paràmetres de configuració de tots els elements dels equips.
        - Plànols de la planta instal·lada, i esquemes o fotografies dels equipaments.

        - Esquema de connexions físics i lògics entre els diferents equips i el repartidors elèctrics i òptics dels espais tècnics.
        - Serveis professionals o de manteniment associats a l'equipament, i estat d'aquests serveis.
        - Registre de l'estat dels recanvis i dels moviments realitzats amb aquest estoc des del començament del contracte.
        - Informe d'incidències tractades des del començament del contracte de manteniment. Si hi ha incidències obertes en el moment del traspàs, es farà una descripció exhaustiva de totes les tasques realitzades per solucionar-les.
        - Quan finalitzi el servei, l'adjudicatari lliurarà a la CSMS el control de l'inventari del maquinari, programari i / o llicències associades a la prestació del servei.
    - La CSMS pot subscriure un contracte de llicència d'ús sobre els sistemes de l'adjudicatari que fossin necessaris per assegurar la continuïtat del servei.
    - L'adjudicatari posarà a disposició de la CSMS qualsevol eina desenvolupada durant l'execució del contracte, tant per l'adjudicatari com pels tercers que hagi contractat, per a millorar la prestació del servei, sense cost addicional. El codi font i la documentació d'aquestes eines seran lliurats a la CSMS, a la finalització del contracte.
    - El proveïdor haurà de prestar a la CSMS serveis d'assistència addicionals sense cost durant almenys els tres (3) mesos posteriors a la devolució del servei, en cas de ser sol·licitats.
    - La devolució del servei no es considerarà finalitzada fins a la signatura per part de la CSMS de l'acta d'acceptació de la devolució del servei, condició necessària per al pagament de l'última factura.

En cas d'incompliment, la CSMS podrà aplicar les següents penalitzacions:

- 5% de la facturació mensual corresponent a la totalitat dels serveis contractats per la CSMS, per cada setmana de retard en facilitar la informació al "proveïdor entrant".
- D'altra banda, i amb l'objectiu de des incentivar la reducció de recursos assignats pel proveïdor sortint, la CSMS duplicarà el valor de les penalitzacions en cas d'incompliment dels ANS establerts en el present plec, sempre respectant els límits establerts a la Llei de Contractes del Sector Públic.

10.2 Execució del pla de devolució

El pla de devolució s'executarà, com a mínim, sis (6) mesos abans de la finalització del servei en vigor, segons es defineixi en el PCAP. A aquest efecte, la CSMS **comunicarà per escrit, com a mínim amb un mes d'antelació, la seva voluntat d'executar el pla de devolució.**

L'adjudicatari haurà de tenir en compte, per tant, que en els últims 6 mesos de prestació del servei, la CSMS podrà anar donant de baixa i migrant al nou proveïdor tant seus com serveis, amb la conseqüent reducció en la facturació.

11 Annexes

11.1 Annex I – Llistat de seus

11.2 Annex II – Inventari de dispositius i llicències

11.3 Annex III – ANS (Acords de nivell de Servei)

Per a la gestió i seguiment dels serveis prestats per l'adjudicatari, la CSMS defineix uns Acords de Nivell de Servei (ANS), que els licitadors poden complementar i millorar, que permeten monitoritzar i avaluar la qualitat i la gestió d'aquests serveis a través d'uns indicadors que parametritzin el grau de consecució acordat per a cada servei. Aquests acords es divideixen en dos grups:

- ANS per a la gestió del contracte de serveis prestats, que permeten a través de mètriques objectives l'avaluació de cada indicador.
- ANS de la gestió del desplegament i qualitat operativa dels serveis prestats, que permeten, a través de mètriques objectives, valorar la qualitat operativa del servei prestat i la seva evolució.

Per a aquesta gestió l'adjudicatari haurà de proporcionar a la CSMS:

- Informes periòdics: Detallant els paràmetres de mesura i l'evolució d'aquests

Dins de cada grup de gestió es defineixen un conjunt d'indicadors que permetran, a partir de mètriques de dades operatives, mesurar els nivells de rendiment i consecució de cada servei segons el nivell acordat.

En relació a les incidències, es defineixen les següents prioritats (en funció del grau d'afectació dels serveis, la seva criticitat, impacte i importància):

- Molt greu: incidències que suposen la pèrdua del servei en qüestió o que tenen una afectació generalitzada a la majoria dels usuaris del servei.
- Greu: incidències que suposen una degradació del servei en qüestió o que tenen una afectació acotada a alguns dels usuaris del servei.

A la plantilla Excel adjunta es descriuen els diferents ANS que s'utilitzaran per mesurar el nivell de prestació del servei. Els indicadors tindran la següent estructura:

- Codi: Identificador únic de l'indicador.
- Descripció: Definició de l'indicador i de l'objectiu de mesura.
- Mètrica: Descripció per al càlcul de l'indicador o parametrització del nivell segons una escala de valorització.
- Periodicitat: Interval de temps de mesurament i presentació del resultat de l'indicador.

- Valor requerit: Valor mínim/màxim a partir del com l'indicador compleix amb l'acord de nivell de servei acordat. L'indicat en les taules defineix el valor requerit per plec, que podrà ser millorat pels licitadors.
- Valor màxim: Valor mínim/màxim a partir del com la penalització és la màxima establerta. L'indicat en les taules defineix el valor requerit per plec, que podrà ser millorat pels licitadors.
- ΔX i ΔY: Valors que determinen l'increment de la penalització (ΔY) en funció de l'empitjorament del valor de l'indicador (ΔX) fins a arribar a la penalització màxima determinada. L'indicat en les taules defineix el valor requerit per plec, que podrà ser millorat pels licitadors.
- Penalització màxima: Valor màxim que pot assolir la penalització associada a l'incompliment de nivell de servei de l'indicador. L'indicat en les taules defineix el valor requerit per plec, que podrà ser millorat pels licitadors.
- En les seves propostes els licitadors hauran d'incloure:
- La plantilla Excel annexa amb la seva proposta d'ANS.
- Metodologia de l'operador per garantir el compliment dels compromisos (especificar matriu d'escalat).
- Procediment del càlcul dels ANS per part dels licitadors.
- Procediments de contrastació de dades dels ANS amb els de la CSMS.
- Termini màxim de lliurament dels indicadors ANS a la CSMS.
- Procediments i calendari per fer efectives les penalitzacions.
- Procediments per afegir nous ANS.
- La CSMS es reserva el dret a afegir nous paràmetres i afegir/modificar els proposats a fi de garantir la màxima qualitat dels serveis prestats per al compliment de les necessitats pròpies de la CSMS. La CSMS podrà realitzar auditories periòdiques dels paràmetres oferts amb personal propi o amb recursos externs. Per aquest motiu l'adjudicatari estarà obligat a facilitar la realització de les labors associades i col·laborar amb els mitjans necessaris.

Domingo Barrabés
Director de Sistemes de la Informació i Comunicacions
Corporació de Salut del Maresme i la Selva

Calella, a la data de la signatura digital.