Consorci Sanitari Integral

# PLEC DE CARACTERÍSTIQUES TÉCNIQUES

# AMPLIACIÓ DE FUNCIONALITAT DE LA INFRAESTRUCTURA TREND MICRO AMB TECNOLOGIA D'EDR/XDR.

## EXPEDIENT CSI2023081

CatSalut Servei Català de la Salut

Generalitat de Catalunya
Departament de Salut

# Índex

# 1 Objecte de la licitació

L'objecte de la licitació és el subministrament de les llicències necessàries per l'ampliació de la funcionalitat EDR/XDR amb el pas al *cloud* de la solució d'antivirus i protecció del correu electrònic del fabricant Trend Micro instal·lada al Consorci Sanitari Integral, CSI en endavant, per 3 anys.

El llicenciament es subministrarà amb el suport del fabricant 24x7x365 al llarg dels 3 anys posteriors a l'inici del servei. Per altra banda, l'adjudicatari haurà d'incloure la migració de tots els agents i el suport i l'operació de la solució.

## 1.1 Lot únic

Adquisició del llicenciament i ampliació de la funcionalitat EDR/XDR del fabricant Trend Micro, amb la següent volumetria amb manteniment del fabricant i suport a l'operació de l'adjudicatari:

| Concepte | Quantitat | Anys |
|---|---|---|
| Trend Micro Cloud One Endpoint Security with XDR | 2.300 | 3 |
| Trend Micro Cloud One Workload Security with XDR | 300 | 3 |
| Trend Micro Email Security Standard | 5.300 | 3 |

## 1.2 Ubicació

El llicenciament subministrat així com el programari s'haurà d'instal·lar als centres del CSI:

| Ubicació | Direcció |
|---|---|
| Hospital General de l'Hospitalet i Hospital Sociosanitari | Av. de Josep Molins 29-41 08906 L'Hospitalet de Llobregat |
| Hospital Sant Joan Despí Moisès Broggi | C. Oriol Martorell, 12 08970 - Sant Joan Despí |
| Hospital Dos de Maig i ABS Sagrada Família i Gaudí | C/Dos de Maig, 301 08025 Barcelona |
| ABS Collblanc | c/ Creu Roja, 18 08904 L'Hospitalet de Llobregat |
| ABS La Torrassa i CAE La Torrassa | Ronda la Torrassa, 151-153 08903 L'Hospitalet de Llobregat |
| CAE Cornellà | C. de Bellaterra, 4108940 Cornellà de Llobregat |
| CAE Sant Feliu | Rambla Marquesa de Castellvell 98-100 08980 Sant Feliu de Llobregat |
| Residència Francisco Padilla | Av. de l'Electricitat, 35-43 08906 L'Hospitalet de Llobregat |
| Residència Collblanc | Riera Blanca, 18-20 08904 L'Hospitalet de Llobregat |

# 2 Situació actual

Actualment el CSI disposa de la *suite* del fabricant Trend Micro com a solució antivirus desplegada als equips d'usuari com als servidors, tant físics com virtuals. A més, disposa d'una solució al núvol del mateix fabricant pel filtratge i protecció del correu entrant i sortint.

## 2.1 Antivirus

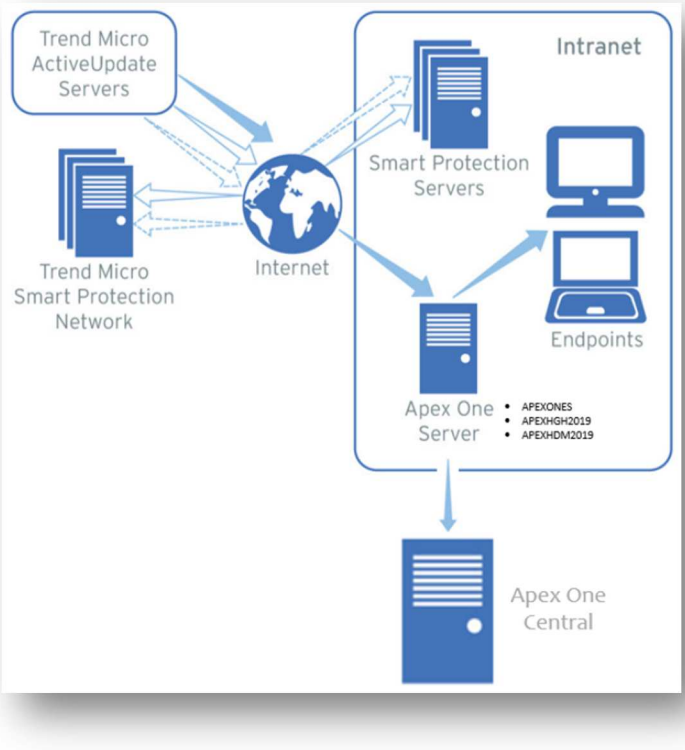
### 2.1.1 Endpoint

En el cas de la solució d'antivirus dels *endpoints*, el CSI te desplegat el producte Trend Micro Apex One en modalitat *on-premises* i instal·lat a la totalitat del parc d'equips d'usuari.

El parc actual d'equips client és compon de:

| Sistema operatiu | Quantitat |
|---|---|
| Windows 7 | 20 |
| Windows 10 | 2.270 |
| Windows 11 | 10 |

La infraestructura actual disposa d'un servidor local en cadascun dels 3 hospitals principals i un servidor central Apex One Central que gestiona tota la infraestructura:




Aquesta solució és la que actualment s'empra en alguns servidors físics i virtuals que no són compatibles amb el producte *Deep Security* del mateix fabricant.

### 2.1.2 Servidors

Als servidors virtuals allotjats a l'Hospital Sant Joan Despí Moisés Broggi, on es concentra la major part de les càrregues de computació del CSI, s'empra la solució del fabricant Trend Micro Deep Security versió 20.

El parc actual de servidors és el següent:

- 225 servidors Windows Server
- 75 servidors Linux

El client disposa de la funcionalitat de *Virtual Patching* (o IPS) per tal de poder donar resposta a vulnerabilitats presents sense aplicar els pegats de software i sistema operatiu al *host*.

## 2.2 EDR

Actualment el CSI disposa d'una solució EDR del fabricant Cisco anomenada Cisco Endpoint Security. Aquest software està distribuït a tots els *endpoints* i servidors de la organització. La gestió del *tenant* d'aquesta solució es porta a terme actualment des del SOC/CERT de l'Agència de Ciberseguretat de Catalunya.

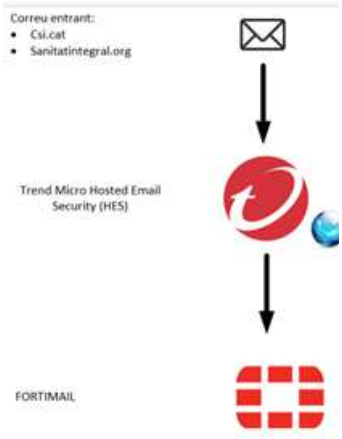
## 2.3 Protecció del correu-e

Per la protecció del correu, el CSI disposa de la solució al núvol Trend Micro Email Security, TMES en endavant, on filtra tant el correu entrant com el sortint dels dos dominis que gestiona:

- Sanitatintegral.org
- Csi.cat

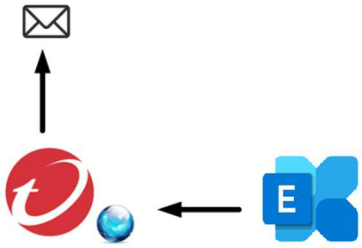
### 2.3.1 Fluxe del correu

El flux del **correu entrant** des de l'exterior es representa amb el següent esquema:




El correu te com a prioritat més alta els MTA de TMES per fer el primer filtrat de correu no desitjat i anàlisi del contingut. Un cop filtrats, els correus que es permeten continuar es reenvien a la solució de Fortinet Fortimail *on premisses* per un segon filtrat amb integració amb una *sandbox* del mateix fabricant. Aquest segon filtre fi del correu reenvia els correus cap a la solució de correu corporatiu Microsoft Exchange, en una arquitectura híbrida amb les bústies ja migrades a Microsoft 365.

El flux del **correu sortint** fa un enviament directe des del servidor de correu Microsoft Exchange als servidors TMES per tal de detectar possibles intents d'enviaments fraudulents des de l'organització cap a l'exterior.



## 2.4 Infraestructura de computació

Actualment el CSI disposa d'una arquitectura de computació hiperconvergent basada en el hipervisor AHV de Nutanix. Les major part de les càrregues de computació s'allotgen als *datacenters* de l'Hospital Sant Joan Despí Moisés Broggi. Tot i això, hi ha seus que també disposen de servidors locals per poder instal·lar serveis que requereixen de comunicació directa amb el centre.

Centres amb infraestructura de computació:

- Hospital Sant Joan Despí: 18 nodes
- Hospital General de l'Hospitalet: 2 nodes
- Hospital Dos de Maig: 2 nodes
- ABS Torrassa: 1 node
- CAE Cornellà: 1 node
- CAE Sant Feliu: 1 node

Els servidors virtuals sobre els quals es pugui recolzar la solució proposada haurà d'integrar-se en aquesta infraestructura hiperconvergent.

# 3 Disseny general

La proposta ha de mantenir les funcionalitats actuals descrites a l'apartat 2 i, a més, incorporar com a mínim els nous requeriments especificats en aquest punt. Per altra banda, es requereix la migració al núvol dels serveis i agents que encara continuen operant en modalitat *on premisses*, com són els agents dels clients i servidors amb Apex One i Deep Security cap a la nova solució Cloud One.

## 3.1 Funció d'EDR/XDR

La solució proposta ha d'incloure la funcionalitat d'EDR/XDR del fabricant Trend Micro tant als agents *d'endpoint* com de servidor. La solució ha d'identificar el comportament maliciós dels fitxers executats, els processos en execució, les modificacions del registre o l'accés a la memòria i aturar-los en temps d'execució o generar una alerta.

La solució EDR ha d'oferir una protecció completa contra els vectors d'atac comuns i avançats. Ha d'oferir una combinació de protecció contra el malware basada en signatures, anàlisi de comportament i anàlisi estàtic amb aprenentatge automàtic per detectar amenaces desconegudes i comptes compromeses, anàlisi dinàmic d'amenaces mitjançant un entorn aïllat i supervisió de l'accés a la memòria, els processos en execució i el trànsit de xarxa.

La solució ha d'identificar i bloquejar els moviments laterals com SMB Relay i d'altres. Per altra banda, ha de poder identificar i bloquejar l'ús d'eines d'atac comuns com són Metasploit, Cobalt Strike, etc. També ha de disposar de mecanismes de control dels USB.

La solució ha de recopilar dades altament detallades sobre el que succeeix al punt final, al sistema d'arxius, al sistema operatiu, a l'autenticació i al nivell de xarxa, i també ha de permetre que el personal de seguretat gestioni aquestes dades, les cerqui, i pugui definir polítiques de seguretat basades en les dades i porti a terme investigacions forenses.

## 3.2 Desplegament d'actualitzacions

Les línies de comunicació del CSI, tot i estar dimensionades suficientment per les càrregues de treball habituals per al *software* corporatiu, no tenen la capacitat per suportar grans desplegaments d'actualitzacions o pegats centralitzats. És per això que es requereix que la solució disposi de múltiples servidors de desplegament de signatures i agents en com a mínim els 3 hospitals principals: Hospital Sant Joan Desí, Hospital General de l'Hospitalet i Hospital Dos de Maig.

Aquests servidors tindran la capacitat de descàrrega d'actualitzacions, noves versions d'agents, signatures, etc. des del *cloud* de Trend Micro per després fer la distribució de paquets als *endpoints* de la xarxa local.

## 3.3 Consola unificada de gestió i telemetria

Es requereix que la solució es pugui gestionar des d'una única consola centralitzada que, a més, permeti realitzar la telemetria dels diferents productes desplegats. Degut a antigues vulneracions de la seguretat a l'organització, on s'ha perdut la capacitat de anàlisi forense per pèrdua d'informació, aquesta consola ha de ser en modalitat *SaaS* i accessible des de qualsevol ubicació.

## 3.4 Virtual patching

La solució requereix la funcionalitat bàsica de virtual patching al client *endpoint* amb regles de sistema operatiu, ofimàtica i navegadors.

És un requeriment que la solució dels servidors disposi de la funcionalitat avançada de virtual patching per tots els servidors descrits en aquest plec.

## 3.5 Integració amb altres solucions

La proposta ha de integrar-se amb altres eines que el CSI fa servir actualment. Aquesta integració, com a mínim, ha de comprendre els següents productes:

- Correu electrònic: Mitjançant la integració de la protecció al núvol amb la solució de correu del CSI: Microsoft Exchange 2019 en format híbrid amb M365.
- Active Directory: Per l'inventariat d'equips i usuaris així com la capacitat d'anàlisi de comportament erràtic o activitat sospitosa.
- SIEM: La solució actual SIEM del CSI és Fortinet FortiSIEM. S'ha d'integrar la solució per tal de poder enviar logs i incidents detectats.
- Firewalls: Els actuals equipaments *firewall* del CSI pertanyen a la família de productes Fortinet Fortigate. Es requereix la integració completa per tal de poder orquestrar mitigacions segons deteccions mitjançant les funcions de l'XDR.

# 4 Implantació

Dins d'aquesta licitació, a més del subministrament de les llicències, s'ha d'incloure els serveis necessaris per a la migració de la infraestructura d'antivirus actual cap a la nova solució. Caldrà incloure totes les tasques necessàries per a la configuració tant del *tenant* al cloud de Trend Micro com la migració dels agents dels *endpoints* i servidors segons les especificacions d'aquest plec.

El projecte d'instal·lació haurà de tenir en compte l'existència de l'actual solució de seguretat i preveure un procés de desplegament i migració dels amb el menor impacte possible per als usuaris.

A banda de la migració del servei actual d'antivirus, es requereix la migració de la solució actual d'EDR, Cisco Secure Endpoint, cap a la nova solució. Això implica, a banda de la desinstal·lació de l'antic agent i instal·lació del nou, l'anàlisi de les regles actuals i adaptació en la nova plataforma i desplegament als agents on apliqui.

## 4.1 Consideracions generals a les instal·lacions

Es considerarà instal·lat un component quan els serveis d'usuari destinats a córrer sobre aquell equipament estiguin en producció sobre ell. Això pot incloure:

- Instal·lació o desplegament físic, virtual o *SaaS* dels diferents components.
- Actualitzacions recomanades pel fabricant.
- Integració del nou component dins la infraestructura i/o serveis del CSI com poden ser: Active Directory, SIEM, Correu-e, Fortinet Fortigates, etc.
- Configuració de la monitorització del component.
- Actualitzacions d'altres components propietat del CSI per tal de que els equipaments i software s'hi puguin connectar.
- Suport post-migració per a les incidències que puguin sorgir.
- Documentació de la instal·lació i procediments bàsics d'operació del component.
- Traspàs de coneixements al personal del CSI.

## 4.2 Definició de l'abast del projecte d'implantació

En aquesta primera fase del desplegament, el Consorci Sanitari Integral i l'adjudicatari, basant-se en la proposta feta durant la fase de licitació, acordaran un pla d'implantació i desplegament dels elements de la proposta.

En aquest abast es veuran les tasques a realitzar, com possibles actualitzacions, finestres d'aturada de servei així com un Planning de totes les tasques que servirà per al seguiment de la implantació.

## 4.3 Instal·lació física i lògica

La instal·lació inclourà totes les tasques necessàries per tal que els nous components quedin operatius i disponibles per al seu ús. Algunes de les tasques incloses en aquesta fase son:

- Instal·lació física i lògica i configuració dels nous elements.
- Migració de la totalitat d'agents, tant de servidor com *d'endpoint*.

- Tasques de xarxa i seguretat per accessos interns o a l'exterior.
- Actualització de tots els components a la versió recomanada pel fabricant en aquell moment.

És a dir, quan un component es munti ha d'estar ja en disposició de donar servei als usuaris.

El CSI disposa de l'eina PDQ per la distribució de paquets. Es requereix la col·laboració conjunta i directa de l'adjudicatari amb l'equip de suport del CSI encarregat de la distribució de paquets pel desplegament dels nous agents a la totalitat *d'endpoints*.

# 5 Suport i serveis post-implantació

## 5.1 Suport i garantia de fabricant

Tots els elements objecte de la licitació inclouran una garantia de fabricant mínima de 3 anys a partir de l'acta de recepció de la licitació. Aquest manteniment haurà d'incloure tot el software, llicències o subscripcions incloses en la oferta del lot únic d'aquest plec.

La modalitat de suport i assistència davant incidències serà en horari 24x7x365. Per les incidències que pugui patir la solució, l'esforç en la seva resolució ha de ser continuat fins donar per finalitzat l'incident.

Es defineixen els següents acords de nivell de servei (SLA):

| Severitat | Descripció | Temps de resposta |
|---|---|---|
| Nivell 1 – Crítica | Els components principals de Trend Micro són inoperables. Impacte crític en les operacions. Ni hi ha solució alternativa. | 30 minuts en 24x7x365 |
| Nivell 2 – Alta | Els principals components estan degradats. Impacte significatiu. | 2 hores laborables |
| Nivell 3 – Mitjana | Els components estan danyats però són operatius. Impacte mitjà/baix a les operacions. Solució alternativa disponible. | 4 hores laborables |
| Nivell 4 – Baixa | Incident sense impacte a les operacions. No requereix solució immediata. Gestió de dubtes. | 1 dia laborable |

### 5.1.1 Service Manager

Es requereix la disponibilitat d'un gestor de servei amb les següents característiques:

- Interlocució en castellà.
- Actua com a assessor de confiança.
- Proporciona assessorament en temps real sobre riscos o amenaces de seguretat actuals.
- Coordina migracions i actualitzacions de programari sense esquerdes.
- Proporciona informes regulars d'estat i compromís.
- Actua com a punt únic de contacte per a casos crítics.

## 5.2 Suport de l'adjudicatari

Es demana suport de la solució per part de l'adjudicatari al llarg de tota la durada del manteniment. Aquest suport tindrà aquestes característiques,

Revisió setmanal de consoles:

- Revisió de l'estat dels agents, versions i registres de seguretat.
- Consola de gestió unificada:
  - Estat del risc
  - Activitat rellevant setmanal
  - Estat dels serveis contractats i riscos per servei
  - Estat dels agents sense contacte o desactualitzats per prendre les mesures pertinents sobre els agents
  - Alertes rebudes

- Proposta d'accions si n'hi hagués
-

Suport a la solució:

- Escalat d'incidència de nivell 3 al fabricant i gestió i seguiment de les mateixes fins a la seva resolució.
- Canvis de la configuració i polítiques, seguint les millors pràctiques del Fabricant.
- Recepció d'alarmes en horari ininterromput de 8:00 a 18:00.
- Informació en temps real d'alertes crítiques, risc i accions a realitzar per a la seva mitigació.
- Informes mensuals de seguiment del servei.
- Suport al desplegament dels agents.
- Security Assessments publicats per Trend Micro.

# 6 Condicions d'execució del subministrament

## 6.1 Consideracions generals

L'àrea de sistemes del Consorci Sanitari Integral basa el seu funcionament en les bones pràctiques marcades per estàndards del món de la gestió de les tecnologies de la informació, com el Project Management Institute o ITIL. En aquest sentit, durant la fase d'implantació del subministrament es seguiran les bones pràctiques del PMI en la realització de projectes. En aquells punts en què no es detalli amb prou claredat detalls de gestió del projecte s'emprarà el PMBOK 5 Ed. com a document de guia de projecte. Durant la fase de producció, les bones pràctiques basades en ITIL seran la referència.

## 6.2 Gestió del projecte d'implantació

### 6.2.1 Direcció del projecte

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

La direcció de projecte estarà liderada pel CSI, que definirà el calendari i fites. Durant la fase d'anàlisi es definirà el comitè de seguiment de projecte en que s'avaluarà el projecte i es detectaran mancances.

### 6.2.2 Comitè de seguiment

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

El comitè serà l'òrgan màxim de direcció del projecte i es tindran que complir les seves directrius.

### 6.2.3 WBS

Durant la fase d'anàlisi es realitzarà un nou WBS en base al WBS entregat pel licitador amb l'objectiu de coordinar les diferents tasques en funció de l'especificitat del CSI o per la seva relació amb altres projectes. Aquest WBS s'aprovarà en un comitè de seguiment.

### 6.2.4 Calendari de projecte i fase de projecte

A partir del WBS aprovat de projecte es realitzarà un calendari de projecte. En aquest punt també s'avaluaran les fases de projecte i les fites i dates clau.

L'adjudicatari es tindrà que adaptar al calendari de projectes i disponibilitat de recursos interns del CSI, pel que el calendari final reflectirà, no només la disponibilitat de recursos del licitador, sinó també del CSI i les dependències amb altres projectes del Consorci.

Durant el projecte, i per causes alienes a l'àmbit de sistemes, el CSI podrà replanificar les tasques de projecte i calendari en funció de les necessitats de negoci del CSI. Aquesta replanificació es presentaria 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 requisits de calendari del CSI com a la disponibilitat de recursos del licitador.

### 6.2.5 Recursos

El licitador es compromet a proporcionar els recursos humans i tècnics oferts en la seva proposta. En cas de que el licitador tingui que reemplaçar un dels recursos, tindrà que informar amb una setmana d'antelació d'aquest fet.

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

### 6.2.6 Faltes

Es defineixen 2 tipus de faltes durant la consecució del projecte, faltes lleus o faltes greus:

#### 6.2.6.1 Faltes lleus

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

#### 6.2.6.2 Faltes greus

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

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

### 6.2.7 Penalitzacions

L'acompliment de terminis de projecte es clau en la estratègia de l'àrea de sistemes del CSI, és per això que s'estableixen penalitzacions amb l'objectiu de mantenir els projectes dins d'un llindar de compliment de terminis acceptable.

Per cada falta greu es planteja una penalització d'un 2% de l'adjudicació.

Aquestes penalitzacions s'aplicaran en tot cas respectant els límits establerts en l'article 192 de la Llei de contractes del Sector Públic.

### 6.2.8 Seguiment del projecte

El CSI proporcionarà unes plantilles a l'adjudicatari on reportar la dedicació d'hores i estat de les diferents tasques del projecte. Aquests documents serviran per mesurar el grau d'avenç del projecte, així com detectar desviacions respecte la planificació original i poder prendre les mesures apropiades per reconduir el projecte.

Es realitzaran reunions de seguiment, de manera general cada dues setmanes, tot i que es poden acordar altres periodicitats segons el moment del projecte i el seu grau d'avenç. En aquestes reunions es repassaran els reports d'hores per veure l'estat general del projecte.

## 6.3 Formació

L'adjudicatari farà una proposta de formació per al traspàs de coneixements de la solució. El CSI vol fer un refresc formatiu al personal tècnic de la solució un cop implantada. Aquesta formació inicial serà com a mínim de 8 hores, dividida en 2 sessions de 4 hores per a facilitar l'assistència de tot el personal necessari.

El contingut mínim d'aquesta formació serà:

- Descripció general de les tecnologies emprades en la solució.
- Descripció dels diferents elements que composen la solució.
- Funcionament habitual de la solució.
- Funcionalitats que es poden implementar en la solució, tot i que no hagin estat implementades en primera instància.
- Passos habituals per a la diagnosi d'incidències.
- Aprofundir a les eines de monitorització i gestió.
- Registre d'errors.

Les sessions formatives les realitzarà un tècnic especialitzat i qualificat, coneixedor de la estructura de forma global que pot donar solucions a dubtes i explicació de les funcionalitats de la solució.

# 7 Documentació a lliurar per l'adjudicatari

L'adjudicatari, a l'etapa de tancament de projecte, haurà d'entregar la següent documentació.

## 7.1 Arquitectura general

L'adjudicatari haurà d'entregar una document d'arquitectura final instal·lada. En aquest document s'hi ha de poder veure clarament:

- Nom i/o IP dels diferents equips i/o servidors instal·lats.
- Adreces, tant de gestió com de producció, dels diferents components.
- Mètode d'accés a la gestió de cada component (ssh, web...).
- Usuaris i *password* de gestió de cada component.
- Esquemes tècnics, que inclouran esquemes de xarxa.
- Telèfons, webs i credencials d'accés al suport de fabricant i/o adjudicatari de cada component post-implantació.

## 7.2 Documentació tècnica

Durant la etapa d'anàlisi l'adjudicatari i el CSI acordaran la definició dels protocols tècnics més habituals per a cadascun dels entorns. L'adjudicatari serà l'encarregat de redactar aquests protocols operatius per tal que els tècnics del CSI, o altres persones no habituades a treballar amb aquesta infraestructura siguin capaços de realitzar operacions habituals.

S'acordaran un màxim de 10 protocols. A continuació es mostren alguns exemples de protocols per a que els licitadors es puguin fer una idea de l'esforç que suposarà la tasca:

- Instal·lació d'un nou agent (Windows, Windows Server, Linux).
- Desinstal·lació o reinstal·lació d'agents.
- Ús de les eines d'anàlisi.
- *Troubleshooting* incidència de *l'endpoint*.
- Actualització dels elements.
- Obertura cas a fabricant.

# 8 Oferta tècnica del licitador

L'oferta del licitador haurà d'incloure la següent documentació tècnica per a la licitació:

1. Document de disseny general i resum executiu
2. Document de proposta, tal i com es detalla en els següents punts

Tota ella s'ha d'entregar en format electrònic no escanejat (ha de permetre cerques de text) en format DIN A4 i lletra no inferior a 12 punts). Es podran entregar altres documents annexes.

## 8.1 Document de disseny general

El document de disseny no pot superar les 6 pàgines i ha d'incloure (només) els següents punts:

1. Resum executiu (1 pàgina max).
2. Detall de punts d'oferta tècnica amb els seus valors nominals (sense puntuació final que realitzarà el CSI (1 pàgina max).
3. Esquema general de connectivitat (1 pagina max)
4. Resum de la solució i punts més rellevants (3 pàgines max).

## 8.2 Document de disseny específic

El document de disseny específic no pot superar les 25 pàgines i ha de contenir (només) els següents punts:

1. Resum del document
2. Disseny específic de la solució, incloent:
    a. Esquema de la solució tant de xarxa física, lògica o *cloud* i connectivitat com de solució global
3. WBS del projecte d'implantació, en un format detallat basat en hores/home i incloent el perfil professional de cada tasca i empresa que ha de realitzar les taques (CSI o Licitador).
4. Calendari de projecte en format Gantt incloent les dependències
5. Camí crític del projecte proposat