Consorci Sanitari Integral

PLEC DE PRESCRIPCIONS TÈCNIQUES

SERVEI DE CIBERSEGURETAT I NOU TALLAFOCS AL CONSORCI SANITARI INTEGRAL

CSI2021026

(IMP-SC-006)

CatSalut Servei Català de la Salut

Generalitat de Catalunya Departament de Salut

Índex

1 Objecte de la licitació

SERVEI DE CIBERSEGURETAT

La solució tecnològica de seguretat actual del Consorci Sanitari Integral (en endavant CSI) està composta per diversos elements, físics i virtuals, del fabricants Fortinet i TrendMicro.

El CSI entén la ciberseguretat com una cadena d'elements que cal que estiguin perfectament alineats i lubricats per al seu òptim funcionament. És per això que desitja un servei global de ciberseguretat que a més de renovar tecnològicament aquells elements que ho necessitin, incorpori coneixement expert en el dia a dia de ciberseguretat i altres eines per tal de seguir avançant en l'infinit camí cap a la protecció de les seves dades.

El CSI desitja una solució global de ciberseguretat, per això la licitació es distribueix en un únic lot.
Dins d'aquest servei s'haurà d'incloure el subministrament dels equipaments físics i el software i llicències necessàries per al compliment del requeriments tècnics d'aquest plec. L'objecte comprèn tant el subministrament com instal·lació, posada en marxa i migració de serveis de tots els equipaments inclosos en aquesta licitació, així com treballs que s'hagin de realitzar per tal de poder realitzar la migració des d'equips ja existents al CSI. Quedaran fora d'aquest àmbit únicament el subministrament i instal·lació de noves línies elèctriques en cas necessari.

Aquest servei ha de disposar de les últimes tecnologies en el que respecta a la integració de serveis de nova generació com són l'antivirus / malware, serveis de reputació web i control d'aplicacions.

També s'inclourà dins del servei la implantació d'un sistema de gestió d'esdeveniments i informació de seguretat (SIEM), del qual no disposa actualment el CSI.

Tant els equips físics com el software inclosos en aquest servei hauran d'estar dins el manteniment oficial del fabricant durant tota la durada del servei. Aquesta durada serà de 5.

Dins la prestació del servei de ciberseguretat caldrà incloure la gestió d'incidències, peticions de servei i canvis als elements renovats durant tota la durada del contracte. I no només l'operació dels elements inclosos en el servei, sinó que també s'haurà d'incloure un perfil de consultor de seguretat que, alimentant-se de les dades recollides pels equips instal·lats al CSI i segons el seu coneixement de les bones pràctiques en ciberseguretat (ISO 27.001, Esquema nacional de seguretat, GDPR...), proposi mesures concretes a aplicar en els sistemes tecnològics del CSI, ja siguin inclosos en aquest servei o no. Per exemple, autenticació de doble factor per connexions externes o longitud i complexitat dels passwords dels usuaris del directori actiu.

2 Situació actual

2.1 Infraestructura de seguretat

Element	Quantitat
Fortinet FortiGate 1500D	2
Fortinet FortiMail 200E	1
Fortinet Fortisandbox en format virtual	1
Fortinet FortianAnalyzer en format virtual	1

El Consorci Sanitari Integral segueix des de fa anys un model de concentració dels seus serveis corporatius al CPD redundat ubicat a l'Hospital de Sant Joan Despí Moisés Broggi (en endavant HSJDMB). Tots els centres que composen el CSI tenen connexió de fibra òptica cap a aquest centre i redundada mitjançant FTTH de la mateixa capacitat. Les línies de comunicació externa, redundades i contractades a l'operador de comunicacions Orange, es concentren al mateix centre.
La infraestructura de seguretat del CSI es recolza majoritàriament en un ventall de solucions del fabricant Fortinet amb serveis de seguretat inclosos dintres del propi *security fabric* i instal·lats a l'HSJDMB.

2.2 Fortigate 1500D

El CSI disposa de dos equips NGFW Fortinet Fortigate 1500D en alta disponibilitat (HA – Actiu / Pasiu) instal·lats en dos *data-centers* ubicats en el centre HSJDMB. Aquests equips desenvolupen múltiples funcions, com són la de *Firewall* perimetral, *Firewall* de *data-center* i balancejador de línies WAN.

2.2.1 Firewall Perimetral

Com a Firewall perimetral gestionen la seguretat de les comunicacions amb l'exterior amb tres branques principals:

- Accés a Internet: Anàlisi i filtratge de la navegació mitjançant *security-profiles* de capa 7 com IPS, Anti-virus, Web-Filtering, Application control, DNS filtering, etc. Publicació de serveis interns a Internet amb NAT i gestió de les comunicacions a la DMZ.
- Nus sanitari: Accés i encaminament als rangs publicats a la xarxa de comunicacions hospitalària catalana i publicació de serveis interns amb NAT.
- Túnels VPN: Gestió del túnels "Lan to Lan" amb diverses organitzacions i proveïdors de servei.

2.2.2 Firewall de data-center

El CSI està actualment en procés de migració dels serveis corporatius cap a una xarxa segura gestionada pels Firewalls de *data-center*. L'objectiu és passar d'una xarxa sense restriccions, on les subxarxes corporatives estan completament obertes i accessibles des de les xarxes d'accés d'usuari cap a una sèrie de xarxes amb accés restringit exclusivament als serveis publicats.

2.2.3 Balancejador de línies WAN

El CSI disposa de línies redundades independents de comunicació entre els seus centres i, en cadascun d'aquests, hi ha al menys un equip Fortinet Fortigate que fa la funció de balancejador. Les dues línies proveïdes per Orange són actives i la tasca de balanceig (actiu / backup) recau en els balancejadors. Es dona prioritat a la línia de Fibra, i queda en mode backup les línies FTTH amb una qualitat de servei inferior.

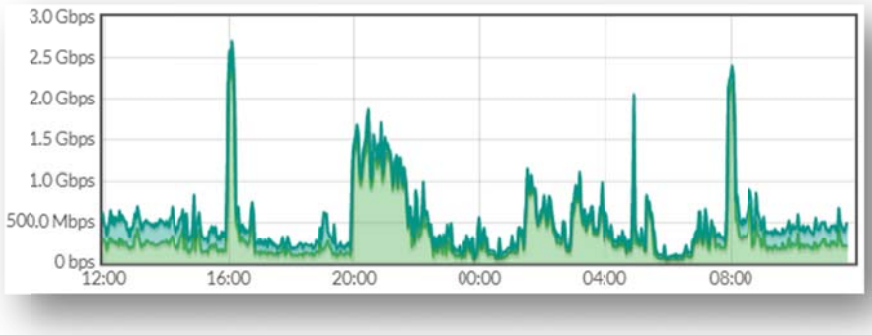
2.2.4 Dimensionament

Es presenta en format tabular un resum de les dimensions:

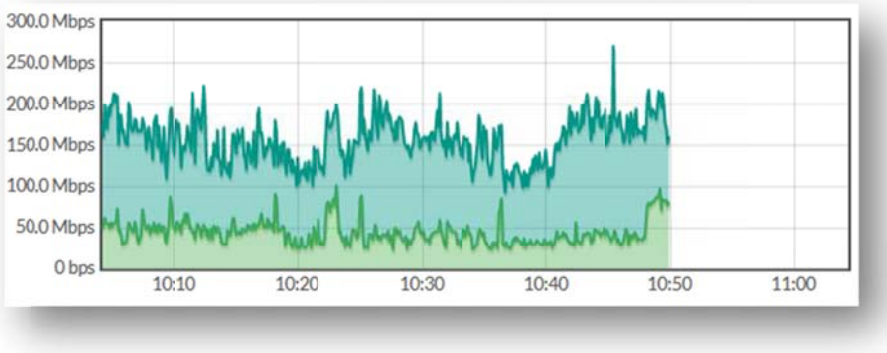
Regles actives	**556**	
Rutes estàtiques	120	
Tunels IKE VPN actius	8	
VDOMs	2	Root (perimetral + DC) i Balancejador
SSL VPN	0	Es fa servir solució de Citrix Access Gateway

Gràfiques d'ús:

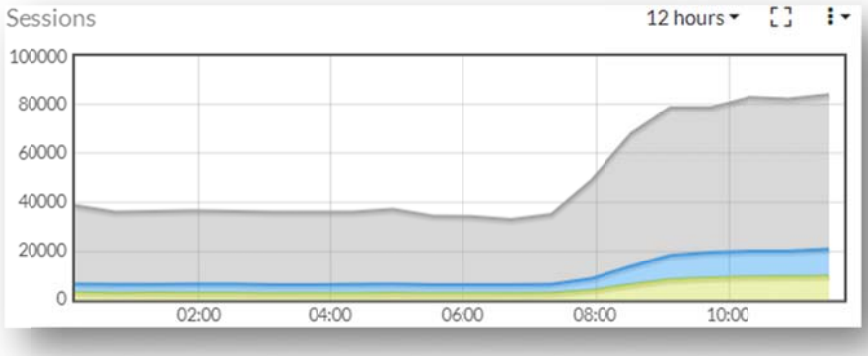
Ample de banda (perimetral + DC)



Ample de banda (balancejador)



Sessions



2.3 Fortimail 200E

Un *Appliance* físic que filtra *l'spam* als correus-e entrants.

2.4 FortiSandbox

Un *virtual-appliance* que analitza de manera aïllada determinats fitxers adjunts dels correus entrants, executant-los en màquines virtuals Windows XP y Windows 7.

2.5 FortiAnalyzer

Un *virtual-appliance* per anàlisi dels logs generats a la solució Fortinet

2.6 Punt de treball

Actualment el CSI fa servir la solució Apex One versió 2019 de TrendMicro per a la protecció dels seus punts de treball

2.7 Servidors

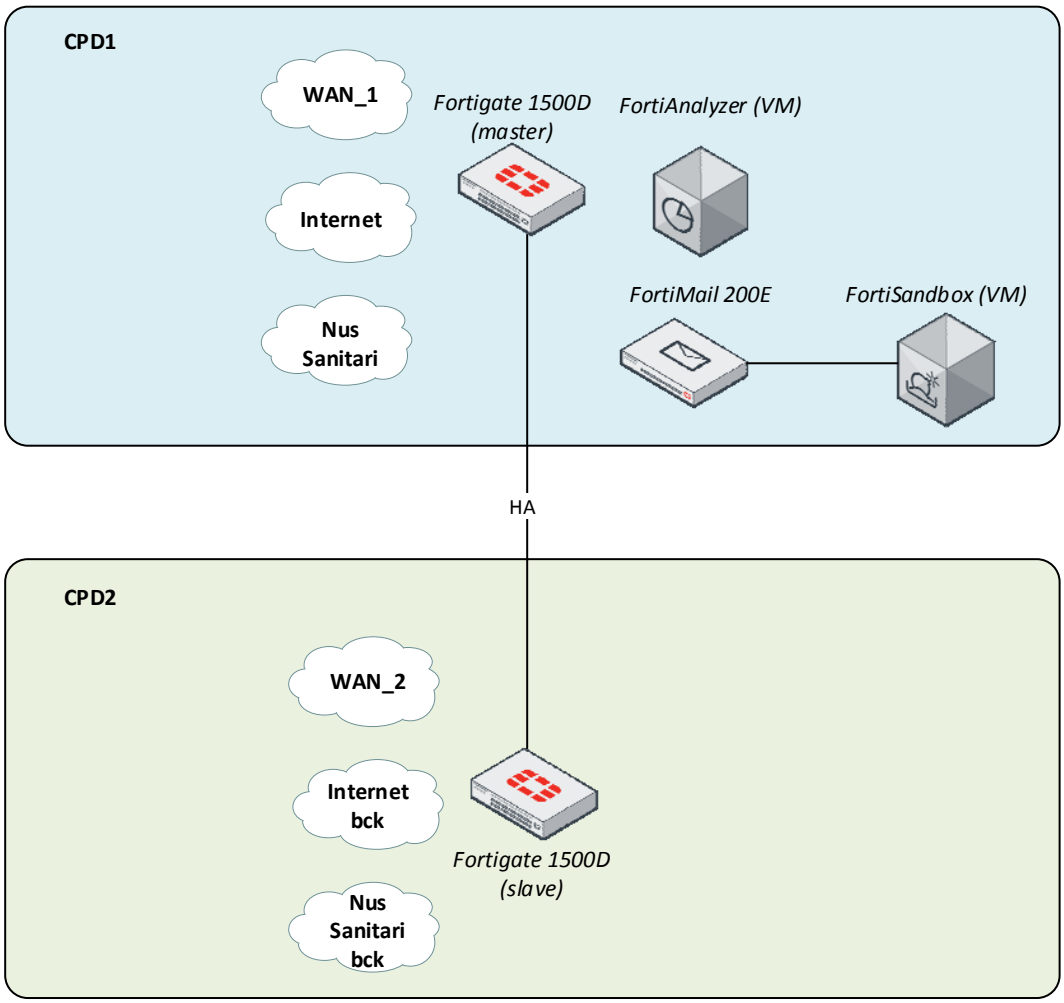
Els servidors actuals de CSI disposen de la solució Deep Security 11.0 de Trend Micro per a la seva protecció.

3 Disseny general

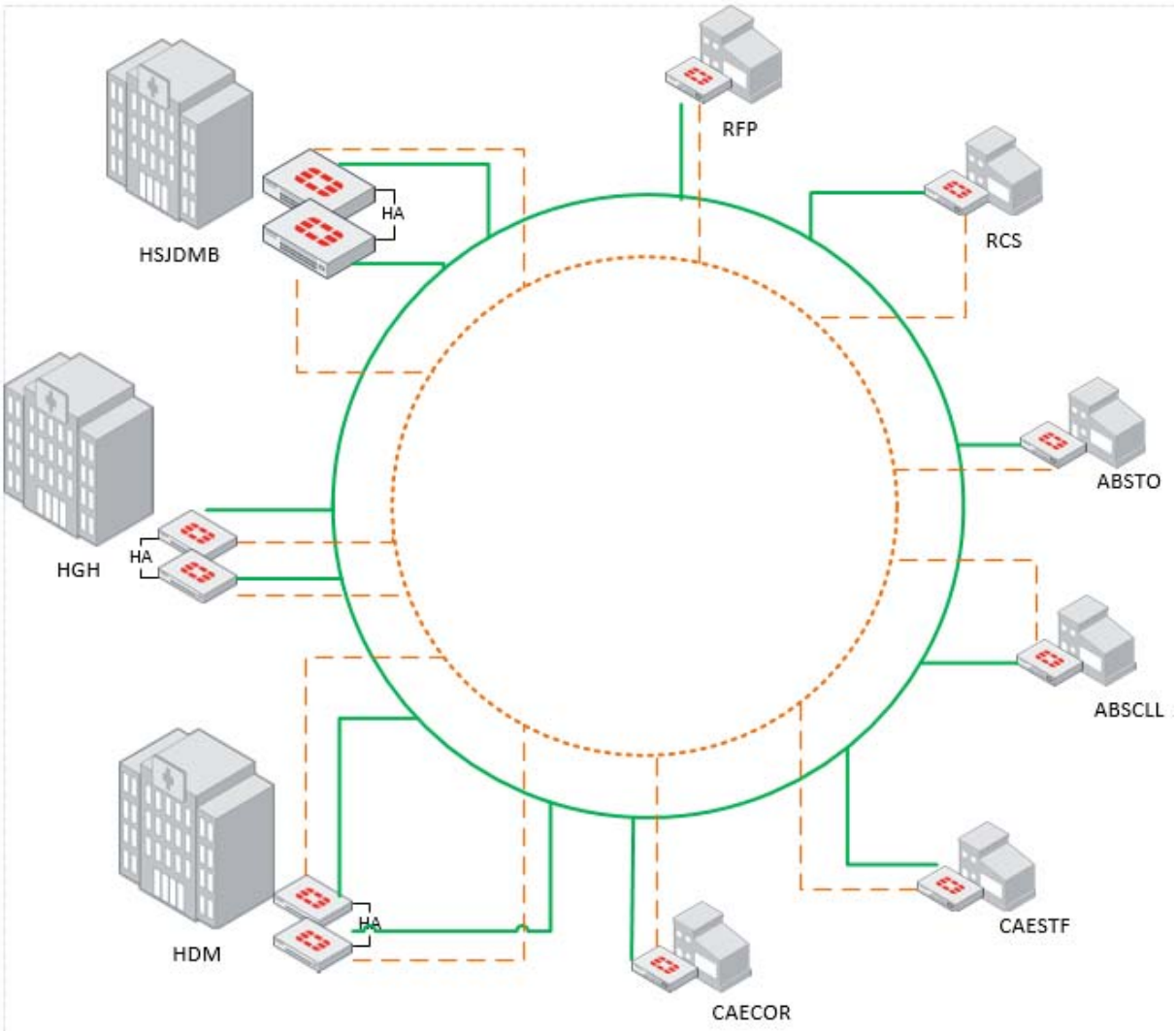
Totes les comunicacions, tant de veu com de dades, passen pel centre principal abans de sortir a l'exterior. També la majoria de tràfic de dades es produeix entre els diferents centres i el principal, havent-hi molt poc tràfic entre els diferents centres.

3.1 Arquitectura de comunicacions

3.1.1 Esquema físic



3.1.2 Esquema de comunicació WAN



El Consorci Sanitari Integral segueix des de fa anys un model de concentració dels seus serveis corporatius al CPD redundat ubicat a l'Hospital de Sant Joan Despí. Tots els centres que composen el CSI tenen connexió de fibra òptica cap a aquest centre i redundada mitjançant FTTH de la mateixa capacitat.

Totes les comunicacions, tant de veu com de dades, passen pel centre principal abans de sortir a l'exterior.

També la majoria de tràfic de dades es produeix entre els diferents centres i el principal, havent-hi molt poc tràfic entre els diferents centres.

4 Servei de ciberseguretat

El CSI desitja un servei claus en mà que abasti tant la seva seguretat perimetral com la d'accés als seus servidors. Aquest servei haurà de tenir com a mínim els mateixos elements identificats en el disseny actual més els demanats en aquest apartat de requeriments. Aquests elements es poden resumir en:

- **Protecció perimetral** -> Tallafocs que gestiona les comunicacions amb origen i/o destí xarxa interna de CSI (LAN/WAN) i xarxa externa (internet o Nus Sanitari)
- **Protecció de CPD** -> Tallafocs que gestiona les connexions entre els usuaris interns de CSI (LAN/WAN) i els servidors interns de CSI (CPD)
- **Protecció correu electrònic** -> Gestió del correu electrònic entrant i sortint dels servidors de CSI. S'haurà de tenir en compte tant els possibles virus, com l'spam i/o phishing
- **Anàlisi de logs** -> Eina de recopilació dels logs dels diferents equips
- **Anàlisi d'esdeveniments** -> Per a una sèrie d'equips especificats, tots els seus events seran recollits en un únic punt que faciliti la seva correlació en cas d'incidents de seguretat
- **Governança de la Ciberseguretat** -> Tots els elements que impacten en la seguretat no son eficients sinó hi ha un lideratge i un camí marcat a seguir de manera correcte. Aquest camí serà marcat per un especialista en ciberseguretat inclòs en aquest servei que acompanyi el CSI durant el trajecte.

El servei de ciberseguretat haurà de proporcionar els elements hardware i/o software necessaris per a garantir aquests aspectes de protecció, a més de la capacitat d'operar-los i evolucionar-los durant tota la durada del contracte.

Tant els equips hardware com el diferent software instal·lat haurà de ser actualitzat com a mínim un cop l'any de manera proactiva. Addicionalment, en cas que sigui necessari per a la resolució d'alguna incidència o amenaça, es faran tantes actualitzacions com siguin necessàries.

A més dels diferents tipus de protecció i anàlisi resumits anteriorment, el servei inclourà l'operació dels diferents elements que el composen per tal de donar resposta a les incidències, peticions de servei o canvis que es sol·licitin durant la durada del mateix.

Finalment, el servei inclourà les visites programades d'un especialista en ciberseguretat que analitzant la informació recollida per tots els elements d'aquest servei proposi accions de millora en la protecció de les dades del CSI. Aquest especialista també serà accessible sota demanda del CSI per a consultes puntuals sobre l'enfocament de nous projectes. Aquestes visites seran com a mínim amb una periodicitat mensual. Serà missió d'aquest especialista:

- Alinear l'estratègia de seguretat de la informació amb els objectius de l'empresa.
- Definir la normativa de seguretat (Polítiques, Normes i procediments) i vetllar pel seu compliment, adaptant-se a les diferents normatives específiques que cal complir (ENS, Directiva NIS, PCI, etc.).
- Gestionar els riscos de seguretat de la informació i establir el pla d'acció adient.
- Vetllar i impulsar la identificació de requeriments de seguretat.
- Identificar i impulsar la identificació i establiment dels controls de seguretat necessaris per controlar el risc (controls organitzatius, procedimentals, tècnics i humans).

- Supervisar el nivell de seguretat, compliment de controls i grau d'eficàcia de les mides aplicades.
- Supervisar el compliment de la legislació en els aspectes referits al seu abast d'actuació.
- Interlocutar amb l'alta direcció en matèria de seguretat de la informació (mètriques, reporting de riscos, plans d'actuació, amenaces i incidències).
- Supervisar el compliment de la legislació en els aspectes referits al seu abast d'actuació.
- Interlocutar amb d'altres empreses, institucions, etc. ,en matèria de seguretat de la Informació.
- Formar i conscienciar a la organització en matèria de seguretat de la informació.
- Gestionar la operació i els incidents de seguretat de la informació sigui directament, a través de serveis externs o d'altres àrees de la organització.
- Prevenir el frau, almenys el comés a través de mitjans electrònics.

El perfil de la persona que realitzarà la tasca disposarà d'alguna de les següents certificacions (CISA, CISM o CISSP), a més, demostrar experiència i coneixements en metodologies d'auditories de seguretat d'informació i hacking ètic acompanyades de les certificacions adients (CEH o OSCP).

4.1 Equips físics

Els equips hardware amb capacitat de tallafocs inclosos en aquest servei hauran de ser de nova generació (NGFW). Aquest concepte es correspon a una plataforma integrada de xarxa que combina un talla focs tradicional amb altres dispositius de funcionalitat de filtratge com són els tallafocs d'aplicacions amb inspecció de paquets profunda, IPS, i altres tècniques com SSL inspection, Webfiltering, DNS filter, Bandwidth management, Antivirus, etc.

La proposta haurà d'incloure durant la totalitat de la duració del contracte, així com les possibles pròrrogues, totes les llicències i subscripcions necessàries per activar, en el cas que sigui necessari, totes les funcionalitats associades als requeriments obligatoris que es llisten a continuació.

Els equips tallafocs han de ser en format appliance d'un únic fabricant, quedant exclosos màquines virtuals ni servidors de propòsit general. Han de poder ser instal·lats en un rack estàndard de 19'', no més de 2 RU.

Els equips hauran de permetre la monitorització via protocol SNMP per controlar la seva disponibilitat i capacitat i sFlow.

4.1.1 Alta disponibilitat i característiques

Per tal d'aportar una solució en alta disponibilitat, la redundància ha de ser completament física, en cap cas es donarà per vàlida una arquitectura en la que es faci mitjançant una solució de virtualització de *l'appliance*. Els dos equips físics han de ser de idèntiques característiques, redundats i en alta disponibilitat (HA, High availability).

Han de permetre treballar en mode HA actiu-actiu i actiu-passiu i mode mixta. El mode mixta implica poder tenir Firewalls virtuals actius i passius de forma barrejada, es a dir, el màster de certs Firewalls virtuals sigui la primera unitat de tallafocs, mentre que la segona unitat de tallafocs es màster de la resta de firewalls virtuals alhora.

La transferència de servei d'un equip a l'altre s'ha de poder fer sense talls, ni pèrdua de les connexions tcp, ni aturada de servei. Les configuracions s'han de traspassar de manera automàtica entre els dos equips.

En el cas de necessitat de llicenciament o subscripcions per activar l'alta disponibilitat, caldrà que aquestes estiguin incloses en la proposta durant la duració completa del contracte.

La instal·lació dels equips es farà en dos CPD's separats aproximadament per 200m amb disponibilitat de connexions de fibra òptica OM3 multimode per poder fer la interconnexió entre ells. Per aquesta funcionalitat de *heartbeat* es farà servir, com a mínim, una de les interfícies de 10G dels equips.

Cada equip ha de disposar com a mínim de:

- 6 interfícies 10Gbe SFP+ (amb els transceptors inclosos)
- 8 interfícies 10/100/1000Base-T
- 2 interfícies 25Gbe SFP28 (amb els transceptors inclosos)
- 2 slots 40Gbe QSFP
- Almenys una de les interfícies a 10Gbe es farà servir per a la connexió entre ells (*stack*)
- Els equips han de disposar de font d'alimentació redundada amb *Hot swap*.

En el cas que l'equipament permeti ampliacions modulars d'interfícies, caldrà que tots els mòduls d'ampliació estiguin equipats amb interfícies com a mínim de les mateixes velocitats que es sol·liciten pels ports mínims obligatoris.

En el cas que l'equip suporti ampliacions de memòria RAM i Disc Dur, caldrà que l'appliance estigui equipat amb el màxim de capacitats RAM i de Disc suportats pel fabricant.

Capacitat de gestió dels equips mitjançant accés via web (https) i terminal (ssh) per la total configuració de les polítiques de seguretat de la plataforma.

Quedaran excloses aquelles solucions que requereixin una plataforma de gestió externa per gestionar i administrar la solució.

Creació de diferents tipus d'usuari per l'administració podent aplicar diferents rols o perfils, així com definir xarxes d'origen confiables

4.1.2 Networking

Els equips han de suportar les següents tecnologies:

- Protocols RIP v1/v2, OSPF, ISIS, BGP, WCCP i Multicast per IPv4 e IPv6, Routing basat en política o PBR i funcionalitats avançades SD-WAN.
- Suport de VRFs (múltiples taules de Routing) i multiVRF Routing (per BGP i OSPF).
- Suport Dual Stack IPv4 e IPv6 simultàniament.
- Network address translation NAT IPv4, NAT64 i NAT66.
- DHCP server / DHCP Relay /DNS Server / DNS Proxy / NTP Server.

- 802.1Q VLANs i Point-to-Point Protocol over Ethernet (PPPoE).
- 802.3ad Capacitat de crear enllaços LACP per l'agregació de ports.
- Capacitat de balanceig de servidors a nivell 4 per tots els serveis, com també possibilitat de fer SSL off-loading pel tràfic HTTPS.
- Cal que la solució de seguretat tingui capacitats integrades de SD-WAN:
    - Balanceig intel·ligent de connexions físiques i lògiques, indiferentment del tipus de connexió WAN (MPLS, 3G/4G, FTTH, VPN, etc..).
    - Verificació de la disponibilitat d'Internet per cadascuna de les línies, per protocols http, ping, dns i TWANP.
    - Verificació de qualitat en temps real: jitter, packet loss i latència per línia.
    - Configuració de polítiques de SD-WAN intel·ligent basat en origen (usuaris AD i direcció IP), en el destí (direcció IP, aplicacions i/o serveis d'Internet/aplicacions) i en la línia amb millor qualitat d'aquell moment basat en valors de jitter, packet loss, latència, tràfic de pujada/baixada o ampla de banda, així com una combinació per pesos.
    - En el cas de necessitat de llicenciament o subscripcions per activar aquestes funcionalitats, caldrà que aquestes estiguin incloses en la proposta durant la duració completa del contracte.
- Suport d'VXLAN i VXLAN VTEP per extensió de nivell 2 sobre xarxes de nivell 3.
- El sistema proposat ha de tenir una funcionalitat integrada de Traffic Shaping tant de trànsit sortint com a entrant sent capaç de reservar ample de banda i marcar el trànsit amb DSCP. Aquest traffic shaping ha de basar-se en aplicacions i URLs a nivell global de perfil o per ip.

Dins del desplegament del servei caldrà migrar la funcionalitat de balanceig de línies WAN especificat a l'apartat de Situació Actual.

4.1.3 Identificació d'usuaris

La solució escollida pel licitador haurà d'integrar-se amb el directori d'usuaris (Active Directory) del Consorci Sanitari Integral tant per presentar els informes de manera discriminada per usuari així com per arribar a aquest grau de detall a l'hora de crear les regles. A més ha de complir les següents característiques:

- Control d'usuaris CITRIX
- Control d'usuaris Microsoft Terminal Server
- Autenticació en servidors remots mitjançant LDAP, RADIUS, i TACACS+
- Generació d'usuaris invitats amb caducitat configurable

4.1.4 Seguretat

A continuació es procedeix a enumerar les característiques que el model d'equip proposat ha de complir en quant a la gestió de la seguretat:

- Inspecció del tràfic SSL mitjançant tècniques de *SSL inspection* així com inspecció de certificat
- Arquitectura basada en interfícies per l'aplicació de polítiques de seguretat
- Capacitat de definir múltiples regles de seguretat en les interfícies origen / destí
- Ha de suportar diferents modes de funcionament: Transparent, *routed, sniffer*

- Ha de permetre la prevenció d'amenaces en temps real, detectant un ampli ventall de vulnerabilitats mitjançant malware, exploits (virus, *spyware, worms*, ...) sense afectar significativament a la latència
- Possiblitat d'integració amb funcionalitat "SandBox": Ja sigui amb equips físics o virtuals instal·lats al Consorci Sanitari Integral, o mitjançant serveis al núvol,
- Funcionament com IPS, mitjançant patrons pre-definits i també creats per l'usuari
- Possibilitat d'implementar funcionalitat "AntiFuga d'informació": Cercant patrons com poden ser DNI, Números d'història, etc.
- Descàrrega automàtica i desatesa de noves signatures IPS així com patrons d'AV i, Spyware, base de dades d'URLs i apliacions
- Suport de tràfic VoIP: H.323/SIP/SCCP/RTP
- Control de correu electrònic no desitjat

4.1.5 Capacitat (Throughput i sessions)

Actualment el CSI es troba en un procés de migració i securització de les xarxes de *Data center* pel que ha de garantir que els equips suportin l'increment a l'ample de banda que creixerà de manera exponencial.

Com a mínim els equipaments han de disposar de la següent capacitat:

- Throughput Raw: 100Gbps en 64 byte UDP
- Throughput IPS[1]: 9 Gbps
- Connexions concurrents: 11 Milions
- Noves sessions per segon: 500.000

[1]El valor de Throughput IPS ha de ser obtingut amb una estimació de tràfic real, no seran vàlids els valors obtinguts segons càlculs teòrics o suposant un determinat tipus o mida de paquet. En cas de formar un clúster actiu/passiu, cada equip ha de ser capaç unitàriament de suportar la totalitat de la càrrega de treball, tant en la banda perimetral com a nivell de Datacenter.
Els anteriors requeriments s'han de complir amb les següents funcionalitats (NGFW) activades per a cadascun dels entorns:

	A/V	IPS/IDS	DPI SSL	Malware	SPAM
Firewall Perimetral	✓	✓	✓	✓	✓
Firewall Datacenter	✓	✓			
Balancejador WAN					

4.2 Resta de la solució

Dins el servei s'ha d'incloure la renovació tecnològica de la resta de sistemes de seguretat complementaris esmentats anteriorment. Tot i que aquests es poden oferir en models físics, no és requisit indispensable en aquesta licitació.

En cas d'oferir la versió virtual d'alguna de les solucions, aquesta s'instal·larà i correrà a la infraestructura de virtualització corporativa del CSI basada en VMware ESXi, 6.7.0 en el moment de publicació.

4.2.1 Anàlisi de logs

La proposta inclourà un software de monitorització, gestió, emmagatzematge i anàlisi de logs dels equips oferts. Aquest software podrà córrer sobre el sistema propietari del fabricant o bé sobre una màquina virtual. En cas de tractar-se d'un equip físic, aquest ha de permetre la funcionalitat de backup per recuperació de la informació en cas de caiguda i substitució del mateix.

Com a mínim, aquest software ha de complir les següents funcionalitats:

- Possibilitat de crear informes personalitzats per l'usuari, amb enviament automàtic segons programació i/o consulta en temps real
- Utilització de plantilles per tal de crear informes així com consultes puntuals tant creades per l'usuari com pre-definides
- Quadre de comandament editable per veure en temps real les amenaces i alertes que s'estiguin produint
- Ús de tots els atributs gestionables pel NGFW per tal de poder crear consultes i informes per aplicacions, xarxes, amenaces, etc.
- Estat actual a nivell de sistema dels equips instal·lats: CPU, memòria, ús de disc, etc.
- Enviament d'alertes i alarmes configurables per diferents medis a multi-dispositius
- Integració, mitjançant traps SNMP, amb el sistema de gestió d'alertes del CSI: Nagios XI

La capacitat estimada de logs a emmagatzemar és d'un mínim aproximat de 6GB/dia per un total de 60 dies en caché ràpida així com un archiving dels últims 365 dies.

4.2.2 Seguretat i filtratge de correu-e

Es demana incorporar una plataforma de securització de correu electrònic, que vagi més enllà de una simple passarel·la de correu electrònic que descarti el correu no desitjat (SPAM). L'eina haurà d'incorporar diferents nivells de seguretat *d'antispam*, *antimalware* y prevenció de fuga de dades (DLP) xifrat basat en la identitat (IBE), arxivat del coreu electrònic, gestió de llistes negres i ajudar a mantenir el compliment de diferents regulacions normatives.

L'eina ha de bloquejar el correu brossa i el *malware* abans que pugui saturar la xarxa i propagar-se, evitant la sortida del mateix i que altres gateways antispam posicionin les bústies en llistes negres. La plataforma ha de estar recolzada per algun servei extern d' anàlisis (laboratori) que mantingui actualitzades les B.D. de *spam, malware, phising* coneguts. Per altre banda també cal que la eina pugui sincronitzar amb una plataforma SANDBOX per tal d'aïllar arxius adjunts / enllaços sospitosos i comprovar el comportament del mateix abans de lliurar-lo al destinatari.

La plataforma haurà de tenir les següents característiques:

- Una configuració d'interfície flexible, amb suport de VLAN i d'interfície redundant
- Inspecció de correu tant entrant com sortint
- Múltiples dominis de correu electrònic amb personalització a nivell de domini
- Suport d'adreces IPv6 i IPv4

- Hosting virtual utilitzant la font i/o pools d'adreces IP de destí
- Arxiu de correu basat en polítiques amb opcions de emmagatzematge remot
- Suport d'autenticació SMTP via LDAP, RADIUS, POP3 i IMAP
- Encaminament de correu electrònic basat en LDAP
- Inspecció per usuari utilitzant atributs LDAP sobre una base per política (Domini)
- Interfície integral Webmail per implementació en Mode Servidor i administració de quarantena
- Administració de correus en cua
- Suport de múltiples idiomes per interfície de Webmail i de administració
- Validació de correu electrònic
- Manteniment de la llista de Reputació del remitent Local basat en:
    - Marc de Política del remitent (SPF)
    - Correu Identificat per Claus de Domini (DKIM)
- Quarantena centralitzada per implementacions a gran escala
- Suport SNMP utilitzant MIB Estàndard i Privada amb llindars basats en traps
- Suport de Servidor d'Emmagatzematge Extern o local, incloent dispositius ISCSI
- Suport extern Syslog

A nivell d'administració la plataforma haurà de tenir un assistent de configuració ràpida, tindrà dos modes d'administració una bàsica i un altre avançada i les contes d'administració estaran basades en rols per Domini. La plataforma ha d'esser capaç de registrar l'activitat integral de la plataforma, mantenir un registre d'incidències i de tasques de reporting , registres de canvi de configuració i registre d'esdeveniments d' administració.

La plataforma de securització de correu estarà disponible en appliance per cloud privat amb les característiques especificades a l'inici del punt 4.2.

4.2.2.1 Característiques de la solució

La plataforma de securització de correu-e ha de tenir les següents característiques:

AntiSpam:

- Reputació Global del Remitent
- URI's de spam i phishing i adreces de correu electrònic
- Combinació de diferents opcions de verificació d'objectes de spam
- Regles heurístiques dinàmiques
- Llistes grises per adreces IPv4 i IPv6 i contes de correu electrònic
- Reputació del remitent Local (IPv4, IPv6 i End Point basat en I + D)
- Inspecció minuciosa d'encapçalament de correu electrònic
- Acció flexible i perfils de notificació
- URI de spam de tercers i llistes negres en temps real (SURBL / RBL)
- Quarantena, etiquetatge i reporting del usuari final
- Escaneig de PDF i anàlisi d'imatges
- Llistes negres i blanques a nivells globals, de domini i de usuari
- Filtrat de llistes bayesianes

Antivirus:

- Quarantena, re-empaquetat, reemplaçament i accions de monitorització

- Escaneig d'arxiu niat
- Detecció de Malware

Protecció del contingut:

- Diccionari basat en el filtrat en direcció entrant i sortint
- Filtre per tipus d'arxiu adjunt
- Filtre de paraules prohibides

Protecció denegació de servei:

- Límit de velocitat de missatges entrants i sortints
- Atac d'adreces de recipients
- Revisió de DNS revers (anti-spoofing)
- Direcció de Remitent Fals

Encriptació:

- Encriptació basada en identitat de lliurament push/pull de missatges encriptats.
- Suport S / MIME per encriptació gateway-a-gateway
- Suport de protocols criptogràfics forts incloent: HTTPS, SMTPS, SSH, IMAPS i POP3S.

4.2.2.2 Requeriments tècnics

El mètode de llicenciament NO ha d'esser per usuari o per bústia de correu, la plataforma ha d' oferir una protecció complerta multi-capa d'antivirus, *antispyware i antiphishing* per un numero il·limitat d'usuaris.

Els requeriments tècnics son els següents:

- Plataforma Cloud compatible amb VMWare ESXi
- Volum enrutament de correu electrònic fins 67.000 per hora
- Volum d' anàlisis Antispam fins 54.000 per hora
- Anti-spam / Antivirus de 52.000 per hora
- Gestió fins a 100 dominis de correu
- Polítiques basades en domini/sistema (entrant o sortint) 400/ 1.500
- Gestió fins a 400 bústies de correu en mode Servidor
- Antispam, antivirus, autenticació i perfils de contingut
- 50 per domini / 200 per sistema
- Prevenció pèrdua dades inclosa
- Gestió de quarantena centralitzada
- Llicencies d' usuari il·limitades

4.2.3 Sandbox

Es requereix la incorporació d' una eina de Sandbox a la infraestructura de seguretat, la qual ens permet complementar les defenses establertes amb capacitat de tecnologia avançada. Protegint-nos especialment de *ransomware, crypto malware i malware* avançat de dia zero. L'eina de *Sandbox* haurà de realitzar filtrats previs multicapa exclusius per una detecció d' amenaces mes efectiva i ràpida. Haurà d'esser una eina de defensa eficaç contra atacs dirigits avançats mitjançant una arquitectura cohesionada i extensible treballant per protegir xarxes, correus electrònics i aplicacions web.

4.2.3.1 Característiques de la solució

Gestió de la plataforma

- Configuracions per WebUI i CLI
- Possibilitat de creació de múltiples comptes d'administrador
- Còpia de seguretat i restauració d'arxius de configuració
- Generar correu electrònic de notificació quan es detecten arxius malintencionats
- Informe setmanal per a una llista de correu electrònic
- Disposar d'una pàgina de recerca centralitzada que permeti als administradors crear condicions de recerca personalitzades
- Rebrà actualitzacions automàtiques de signatures freqüents
- Comprovació i descàrrega automàtiques de noves imatges de VM
- Supervisió del estat de VM

Xarxa e implementació

- Suport d'encaminament estàtic
- Gestionarà entrada d'arxius a analitzar en quatre modalitats:
  - Mode fora de línia
  - Analitzador de protocols
  - Càrrega d'arxius a demanda
  - Enviament d'arxius des de dispositius integrats
- Disposarà d'una API basada en web on els usuaris podran carregar mostres per explorar de forma indirecta
- Disposarà d'una opció per crear una xarxa simulada d'arxius explorats als que accedir en un entorn de xarxa tancat
- Permetrà la integració amb altres dispositius
- Entrada d'enviament d'arxius: firewalls, plataformes correu
- Allotjament de bases de dades d'actualització
- Registre remot: servidor de Syslog i altres

Protecció avançada contra amenaces

- Inspecció de noves amenaces, inclosa la mitigació de malware protegit amb contrasenya i ransomware.
- Anàlisi de codi estàtic basat en IA que identifica possibles amenaces dins del codi que no s'executa
- Anàlisi heurística / patró / reputació
- Sandbox de SO virtual:
  - Anàlisis del comportament basat en IA
  - Compatible amb SO: Windows 7, Windows 8.1, Windows 10, macOS i Linux
  - Tècniques anti-evasió: petició en repòs, consultes de registre i processos
  - Detecció de devolució de petició: visites a URL malintencionades, comunicació de C & C de botnet i tràfic d'atacants procedent de malware activat
  - Descàrrega de paquets capturats, arxius originals, registres de seguiment i captures de pantalla,
- Suport per a mides d'arxius il·limitats, opció de configurar mida de arxiu màxim
- Suport de tipus d'arxius:

  - Arxius comprimits: .tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj
  - Arxius executables: (.exe, .dll), PDF, docs Ms Office, Javascript, AdobeFlash i arxius JavaArchive (JAR)
  - Arxius multimèdia: .avi, .mpeg, .mp3, .mp4
- Protocols / aplicacions admeses:
  - Mode d'analitzador de protocols: HTTP, FTP, POP3, IMAP, SMTP, SMB
  - Mode integrat de forma nativa: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM i les seves versions equivalents xifrades en SSL
- Detecció d'amenaces de xarxa en mode de analitzador de protocols:
  - Identificació d'activitats de Botnet i atacs de xarxa, visites a URL malintencionades
- Exploració dels recursos compartits de xarxa SMB / NSF i posi en quarantena els arxius sospitosos, en aquest cas l'exploració s'hauria de poder programar
- Exploració fitxers amb vincles URL de llocs web
- Opció per integrar-se amb les regles de Yara de tercers
- Opció per enviar arxius sospitosos automàticament a un servei al núvol per a l'anàlisi manual i la creació de signatures
- Opció per reenviar arxius a un recurs compartit de xarxa per a la seva exploració posterior per part d'un tercer
- Opció de llista blanca i llista negra per arxius Checksum
- Enviament d' URL des de correus electrònics i fitxers per ésser escanejat

4.2.3.2 Requeriments tècnics

El mètode de llicenciament ha d'esser en appliance per VM , que permeti gestionar fins a 8VM's.

Llicencia de 4VM concurrents per tant capaç d'aixecar VM: Win7, Win8, Win10, Linux i 1 llicencia Ms Office que permet utilitzar llicencia office en una de les VM aixecades per comprovar arxius de tipus office (Word, Excel, etc..).

4.2.4 SIEM

Incorporació d'un SIEM, sistema de gestió d'informació i events de seguretat, que centralitzi l'emmagatzemen i la interpretació de les dades rellevants de seguretat permetent un anàlisi de la situació en múltiples ubicacions des de un punt de vista unificat que faciliti la detecció de tendències o patrons no habituals. L'eina serà capaç de realitzar anàlisis en temps real mitjançant el processament avançat de logs i la correlació d'events en temps real que ajudin tant en la operació de sistemes i serveis com en la gestió de les obligacions legals de custodia d'evidències i comunicació d'incidents en el terminis establerts.

El SIEM haurà de disposar i mantenir una base de dades de configuracions (CMDB) nativa mitjançant tècniques de auto-descobriment i aprenentatge de actius i mapejos inter-relacionals en entorns tant físics com virtuals i de cloud, d'aplicacions, usuaris i dispositius.

L'arquitectura ha de ser escalable amb capacitat d'operació tant en entorns Datacenter com cloud, amb emmagatzemen d'events NoSQL i correlació distribuïda d'events en temps real. Es podran desplegar en tants nodes per processar la informació com nodes recol·lectors sense que això suposi un cost extra en el llicenciament.

El SIEM haurà d' esser capaç de monitoritzar rendiment i disponibilitat per SNMP y WMI. Ha de suportar integracions ràpides de tecnologia amb múltiples integracions i casos d'us pre-establerts per dispositius tant físics com virtuals. Ha de disposar de la capacitat d'incorporar indicadors de compromís (IOC) per incrementar el nivell de seguretat en correlació a events. L'Eina ha de permetre la integració nativa amb Fortinet Fortigate i els escàners de vulnerabilitats del sistema de la organització essent capaç d'alertar si un atac podria afectar a una vulnerabilitat CVE detectada prèviament.

Correlació d'events SOC/NOC per disposar en un únic punt de gestió no sols d'events de seguretat sinó també de:

- Rendiment i disponibilitat
- CPU, memòria i emmagatzemen.
- Detecció de canvis de configuració.
- Monitorització de transaccions sintètiques.
- Quadres de comandament dinàmics.

4.2.4.1 Desplegament

L'eina haurà de desplegar-se com a virtual appliance. Haurà de permetre créixer afegint recursos addicionals de CPU, memòria i emmagatzemen sense necessitat de processos de migració de dades. Haurà d'incloure capacitats natives d'alta disponibilitat i multi-tenant, permetent escalar ràpidament mitjançant la inclusió de components virtualitzats addicionals: workers o col·lectors.

El SIEM permetrà el desplegament d'agents Windows o Linux que permetran realitzar una monitorització més granular especialment sobre servidors crítics, així com el desplegament de Collectors que actuïn com a Proxy per arribar als dispositius que cal monitoritzar i queden darrera el Firewall.

4.2.4.2 Operativa

L'eina haurà d'oferir una interfície molt intuïtiva per dur a terme recerques en temps real tant amb text lliure com buscant valors específics en atributs parsejats. Tant mateix les recerques s'hauran de fer tant sobre esdeveniments parsejats com en format RAW. Haurà de permetre fer "drill down" en cada esdeveniment per obtenir informació detallada, i en qualsevol moment fent doble clic a les barres individuals dels gràfics s'hauria de poder analitzar els esdeveniments en un interval de temps determinat en la vista sobre històric.

En quan a la resolució d'incidències, l'eina ha de tenir la seva pròpia eina de ticketing interna que permeti crear i assignar casos de suport. D'aquesta manera, un tiquet pot ser creat automàticament cada vegada que es produeix un incident i esser assignat a un usuari / grup específic per a la seva resolució. Incloent mecanismes automatitzats per incrementar les capacitats no només de detecció, sinó també de resposta davant un eventual atac i / o bretxa de seguretat, el SIEM s'hauria de poder integrar amb eines de ticketing externes, eines d'anàlisi de vulnerabilitats y dispositius de seguretat per dur a terme una remediació automàtica que permeti mitigar qualsevol amenaça en temps i forma.

En referència als sistemes de ticketing externs s'hauria d'integrar bi-direccionalment amb JIRA.

4.2.4.3 Llicenciament

El mètode de llicenciament ha de ser escalable tant per nombre de dispositius com per Events Per Segon (EPS) associades, podent triar al menys entre llicències perpètues o subscripció. Així mateix, es disposa de paquets de llicència d'agents avançats per monitorització de servidors crítics Windows i Linux, tant en manera perpètua com a manera subscripció, i paquets de llicència d'agents de UEBA per equips Windows, tant en manera perpètua com a mode subscripció.

En el cas que la solució de SIEM presentada es llicenciï tant per dispositius monitoritzats com per events per segon caldrà llicenciar almenys 10 EPS per a cada dispositiu.
Els requeriments especificats son per 150 dispositius, amb un volum de 1500 EPS i 25 agents avançats per Windows en la modalitat de llicencies perpetues.

5 Implantació

Dins d'aquesta licitació, a més del subministrament s'ha d'incloure els serveis necessaris per a la migració dels serveis actuals. Caldrà incloure totes les tasques necessàries per a la configuració dels nous equipaments segons les especificacions de l'apartat 4 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 d'instal·lació dels dispositius i migració dels serveis amb el menor impacte possible per als usuaris.

5.1 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 física dels diferents components
- Actualitzacions de firmware recomanades pel fabricant
- Integració del nou component dins la infraestructura del CSI
- Configuració de la monitorització del component
- Actualitzacions de firmware d'altres components propietat del CSI per tal de que els nous equipaments 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

5.2 Definició de l'abast del projecte d'implantació

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

5.3 Instal·lació física i lògica

La instal·lació física inclourà totes les tasques necessàries per tal que els nous equipaments quedin operatius i disponibles per a la seva configuració lògica. Algunes de les tasques incloses en aquesta fase son:

- Instal·lació física dels nous equipaments
- Connexió dels cables elèctrics i de xarxa
- Assignació d'adreces ip per a la seva gestió si fos necessari
- Actualització del firmware de tots els components a la versió recomanada pel fabricant en aquell moment

Molt relacionada amb la instal·lació física hi ha la configuració lògica a la infraestructura actual de tots els components. És a dir, quan un component es munti ha d'estar ja en disposició de donar servei als usuaris.

5.4 Faltes i penalitzacions

Per tal d'assegurar els nivells de servei establerts entre l'àrea de sistemes d'informació de Consorci Sanitari Integral i la resta de l'organització és crític seguir la planificació del projecte d'implantació i evitar els errors de configuració i migració dels serveis cap a la nova infraestructura. És per això que es defineixen les següents faltes i conseqüents penalitzacions:

5.4.1 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.

5.4.2 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.
L' acumulació d'un 10% de faltes lleus sobre el total de tasques realitzades també serà considerada una falta greu.

5.4.3 Acords de nivell de servei (SLA)

A continuació es mostren els nivells de servei acordats entre el Consorci Sanitari Integral i la seva àrea de sistemes d'informació per als serveis més crítics de l'organització:

Servei	SLA	Disponibilitat
SRVSAP	99.8%	24x7 – tots els dies de l'any
SRVACC	99.8%	24x7 – tots els dies de l'any
SRVTEL	99.8%	24x7 – tots els dies de l'any
SRVDOC	99.8%	24x7 – tots els dies de l'any
SRVSIS	99.8%	24x7 – tots els dies de l'any

El comptatge dels SLA es realitza a partir del temps reportat al sistema d'incidències del Consorci.
En cas que alguna incidència causada per la instal·lació i/o migració de serveis cap a la nova infraestructura provoqui que algun dels serveis no assoleixi el seu SLA s'imputarà aquesta desviació directament a l'adjudicatari.

5.4.4 Penalitzacions

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

Es penalitzarà en un factor multiplicador de 10 per cada punt percentual que l'adjudicatari no compleixi de SLA per aquell servei (un servei que tingui un SLA real de 99,7%, tenint per contracte un SLA del 99,8%, tindrà una penalització d'un 1,0% sobre l'import del subministrament).

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

6 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.

6.1 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).

6.2 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 i connectivitat com de solució global
    b. Inventari de ports ocupats pels diferents equipaments, tant del licitador com del CSI (SAN i/o LAN).
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

7 Condicions d'execució del subministrament

7.1 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.

7.2 Gestió del projecte d'implantació

7.2.1 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.

7.2.2 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.

7.2.3 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.

7.2.4 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.

7.2.5 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.

7.2.6 Faltes

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

7.2.6.1 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.

7.2.6.2 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.

7.2.7 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.

7.2.8 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.

7.3 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 el servei de ciberseguretat
- Descripció dels diferents elements que composen la solució, tant hardware com software.
- 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
- Còpies de seguretat

Al llarg de la durada del contracte es requereix una sessió de formació anual, típicament repartida en 2 jornades de 4 hores, per resoldre dubtes operatius i aprofundir en la gestió i administració de la solució.

Les sessions formatives les realitzarà un tècnic especialitzat i qualificat, coneixedor de la estructura de forma global que pot donar solucions a dubtes, explicació de noves funcionalitats per upgrade de versió o resposta a futures necessitats que es puguin plantejar.

8 Suport i serveis de la infraestructura

Per a tots els serveis i suport descrits a continuació caldrà tenir en compte la distribució que s'ha comentat anteriorment en aquest document.

8.1 Suport i Garantia de fabricant

Tots els equipaments inclouran una garantia de maquinari mínima de 5 anys 24x7 a partir de la data de l'acta de recepció. Aquesta garantia haurà de tenir un temps de resposta per canvi de peces hardware de màxim 4 hores in-situ. Aquest manteniment haurà d'incloure tant el manteniment hardware dels equipaments com tot el software, llicències o subscripcions incloses en la oferta del lot 1 d'aquest plec.

Si el fabricant no disposa de suport proactiu l'adjudicatari haurà de cobrir el suport de tots els elements, monitoratge, proves de contingència i upgrade mitjançant una bossa d'hores suficientment dimensionada per cobrir el suport durant la vigència del contracte, i amb personal certificat en la màxima qualificació disponible per cadascun dels diferents elements de la infraestructura oferta.

Tant en les incidències de la plataforma com en la reposició de peces, l'esforç en la seva resolució ha de ser continuat fins a la seva resolució.

8.2 Monitoratge

El Consorci disposa d'una plataforma de monitorització basada en Nagios XI. Durant el desplegament del servei l'adjudicatari haurà de donar suport a CSI en les tasques necessàries per monitoritzar tot el hardware i software instal·lat.

9 Documentació a lliurar per l'adjudicatari

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

9.1 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's dels diferents equips i/o servidors instal·lats
- Adreces ip, tant de gestió com de producció, dels diferents equipaments
- Mètode d'accés a la gestió de cada equipament (ssh, web...)
- Usuaris i password de gestió de cada equipament
- Esquemes tècnics, que inclouran cablejat i connexionat físic i lògic, esquemes de xarxa de diferents capes (2, 3).
- Telèfons, webs i credencials d'accés al suport de fabricant de cada equipament