HOSPITAL DE LA SANTA CREU I SANT PAU
FUNDACIÓ DE GESTIÓ SANITÀRIA
UNIVERSITAT AUTÒNOMA DE BARCELONA

Sant Antoni Maria Claret, 167
08025 Barcelona

Tel 935 53 76 21 – 76 23

EXP. OBE 23/936

PLEC DE PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE RELATIU AL SUBMINISTRAMENT D'UN FIREWALL PER ACCÉS PROVEÏDORS, AMB DESTÍ A LA FUNDACIÓ DE GESTIÓ SANITÀRIA DE L'HOSPITAL DE LA SANTA CREU I SANT PAU.

Índex

1 Presentació

1.1 Introducció

L'objectiu d'aquest document és definir el plec de requeriments tècnics per la compra d'un equipament Firewall dedicat exclusivament a l'accés de proveïdors.

1.2 Abast

Pel que fa a l'abast es considera:

- El subministrament de tot l'equipament, programari, subscripcions, i altre material necessari.
- Anàlisi i optimització de la configuració necessària.
- Instal·lació i configuració de l'equipament.
- Posada en marxa i validació de la instal·lació.
- Documentació de la instal·lació. Notificació de les incidències generades.
- Formació dels tècnics d'explotació designats per l'hospital, que podran ser o no ser membres de la plantilla de l'hospital.
- Garantia i manteniment, tant per a serveis reactius com evolutius. Es demana un mínim de 3 anys de garantia i un mínim de 3 anys de manteniment, incloses les llicències i subscripcions necessàries.
- Seguiment de projecte.

Tot el llicenciament requerit en tots els lots tindrà una vigència mínima de 3 anys.
Tots els productes i llicències adquirits tindran un termini de garantia i/o manteniment addicional fins a un període mínim de 3 anys.

L'àmbit funcional a migrar des del Firewall perimetral actual al nou equipament consisteix en:

- Integració a la xarxa i al domini actiu.
- Integració amb sistemes FortiAnalizer, FortiAuthenticator, i FortiSandbox ja existents.
- Totes les VPN site-to-site del checkpoint al nou tallafocs, fent interlocució amb tercers si cal.
- Totes les VPN client to site que corresponen a proveïdors del departament d'informàtica, fent interlocució amb tercers si cal.
- Migració de les polítiques i configuracions existents.
- Coordinació i notificació a proveïdors del canvi, incloent el lliurament d'un manual de connexió remota actualitzat.

1.3 Requeriments licitador

S'haurà de presentar la documentació que acrediti tots els punts següents.

El contractista haurà de complir els següents criteris:

- Certificacions ISO: ISO 9001:2015 o equivalent.
- Certificacions ISO: ISO 14001:2015 o equivalent.
- Relació de partnership amb el fabricant dels productes presentats o alternativament una carta de validació del fabricant conforme el contractista està adequadament preparat per implantar aquest servei amb els seus productes. Aquest requeriment no és necessari si el licitador és el propi fabricant.

Aquests requeriments es presentaran en el moment de formalitzar el contracte.

2 Especificacions tècniques

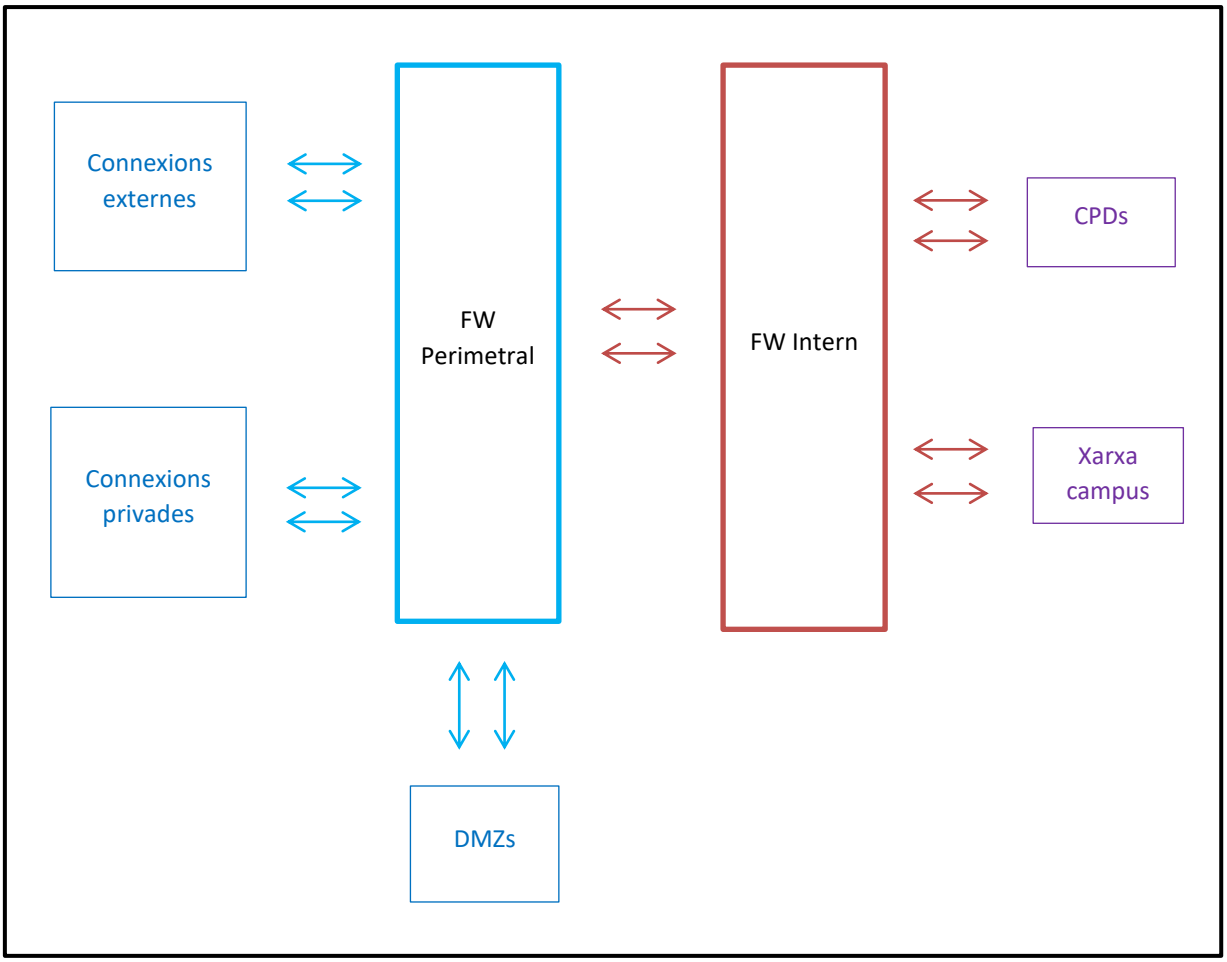
2.1 Objecte de l'adquisició

L'objecte del present lot és l'adquisició d'un sistema de seguretat de xarxa "tallafocs" per a l'Hospital de la Santa Creu i Sant Pau amb les característiques tècniques i condicions que es detallen més endavant.

2.2 Situació actual

En l'actualitat l'hospital disposa d'un sistema de seguretat perimetral format per 2 equips configurats en alta disponibilitat, i d'un sistema de protecció interna.

2.2.1 Esquema lògic de xarxa i funcionalitats



El Firewall intern, addicionalment als equips que fan les funcions de gateway, disposa de servidors auxiliars per a les funcions de WAF, anàlisi de fitxers sandbox; i registre i anàlisi de logs.

Internament hi ha prop de 4.000 usuaris actius, aproximadament 3000 PCs, més de 600 servidors virtuals, s'han configurat diverses zones DMZ, s'han establert diverses connexions VPN, i es disposa de diferents connexions a internet i amb l'exterior.

L'hospital disposa d'una connexió a l'anella científica de 1Gbps (compartida amb altres institucions), d'una connexió a Internet redundada de 100Mbps per aplicacions específiques, d'una connexió al "Nus sanitari" de 100 Mbps, d'un línia FTC per a proves...

La configuració actual inclou diverses DMZ, cada una d'elles amb amples de banda puntuals que s'acosten al Gb.

La configuració actual filtra l'entrada i sortida des de la xarxa de l'hospital a l'exterior.

Les connexions externes inclouen:

- Enllaç anella científica
- Enllaç nus sanitari
- Connexió internet addicional

Les connexions privades inclouen:

- Connexions externes a llocs gestionats per l'hospital
    - Connexions via operadors a edificis externs gestionats per l'hospital.
- Connexions internes a "xarxes" no gestionades per l'hospital
    - Connexions a xarxes d'edificis del campus de l'hospital gestionades per altres empreses.
    - Vlans de la xarxa interna que connecten equips no gestionats per l'hospital.
    - Accessos WIFI de diferents tipus, com per exemple el servei a pacients o a empleats.
    - Sistemes de Servidors gestionats per empreses externes.
    - Túnels LAN to LAN.
    - Túnels PC to LAN.
    - Túnels https.

Les DMZs inclouen:

- DMZ externa per a la publicació de serveis a Internet
- DMZ interna per a l'accés a serveis interns

La xarxa d'usuaris interns inclou:

- Connexions LAN
- Connexions WIFI

La xarxa de servidors inclou:

- Servidors del CPD1 i servidors del CPD2

En els equips actuals estan disponibles i implementades les següents funcionalitats:

- Gestió via regles de les connexions autoritzades.
- Gestió de la configuració per aplicacions.
- Gestió de la configuració per usuaris.
- Filtratge de navegació web en funció de categories de classificació.
- Registre del tràfic de navegació, incorporant informació de classificació.
- Filtrar el tràfic de navegació i de correu per antivirus.
- Detecció d'intrusions: Detecció de comportaments no adequats d'equips de la xarxa.
- Prevenció d'intrusions: Detecció de tràfic propi d'atacs, de virus, ...
- Configuració de VPNs
- Configuració de Proxy invers
- Generació de reporting periòdic.

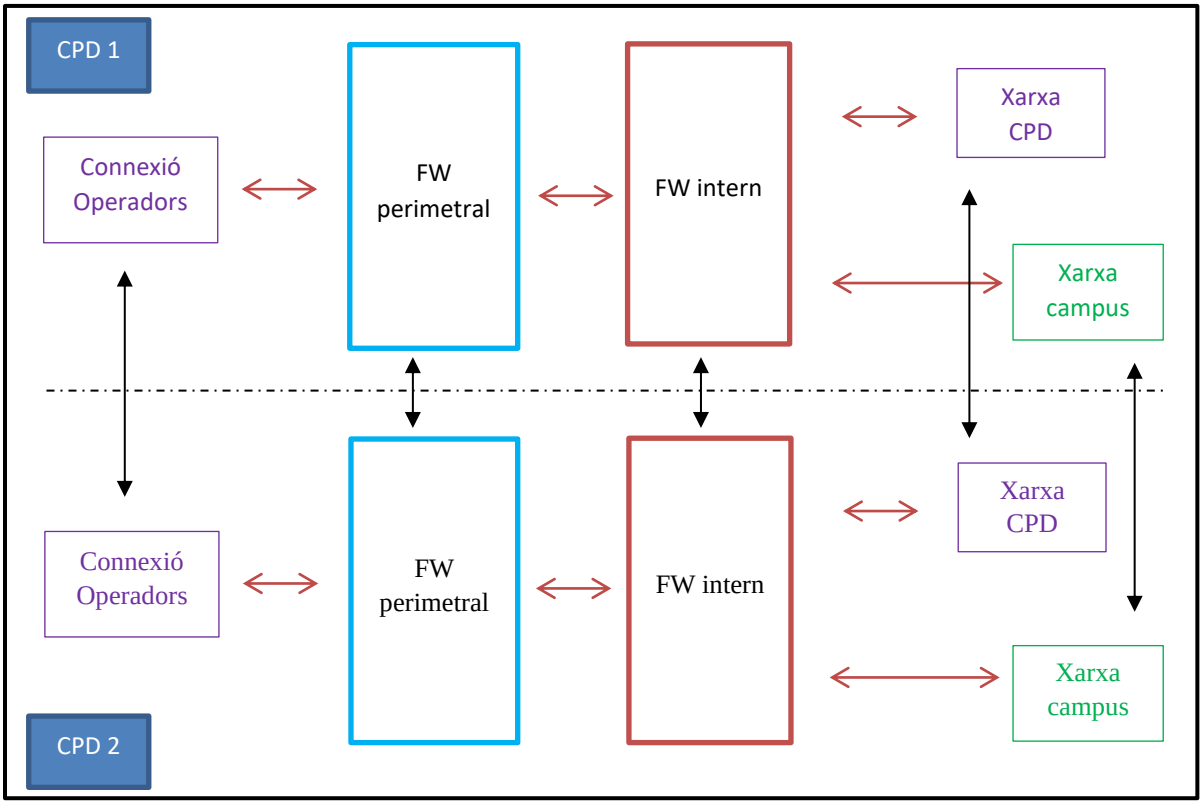
Actualment no es fan servir serveis anti-spam en l'anàlisi del correu entrant, atès que aquesta funció ve proporcionada pel proveïdor actual de la connexió a internet.

La configuració actual del firewall perimetral es composa de 2 instàncies virtuals, una amb aproximadament 200 regles de configuració i l'altra amb aproximadament 50 regles.

L'hospital disposa de 2 CPDs, ubicats en el mateix campus de l'hospital, on estan instal·lats els diferents servidors, cabines, equips de xarxa... en una configuració redundant actiu-actiu. Tant a nivell de xarxa com a nivell de gestió estan configurats com si fossin un únic CPD.

2.2.2 Esquema físic de xarxa

A cadascun dels CPDs:



Els Firewalls perimetrals són del fabricant Checkpoint i model 15400. Disposen de 10 interfícies 10/100/1000 BaseT i de 2 interfícies 10 Ge SFP+.

Els firewalls interns són Fortinet Fortigate 2601F. Disposen de 2 interfícies 10 Gb SFP+, 16 interfícies 10 Gb RJ45, 16 interfícies 25/10/1 SFP28, 4 interfícies 100/40 Gbps QSFP28.

El core dels CPDs són 2 equips Cisco Nexus 9372TX a cadascun dels CPDs, que disposen de 48 ports 10Gbps baseT i 6 ports QSFP+.

La xarxa de campus actualment s'està reconfigurant i els concentradors resultants seran 2 equips Cisco Catalyst C9500-48Y4C-A a cadascun dels CPDs. Els equips disposen de 48 boques 1/10/25 Gb SFP28 i 4 boques 40/100 Gb QSFP28.

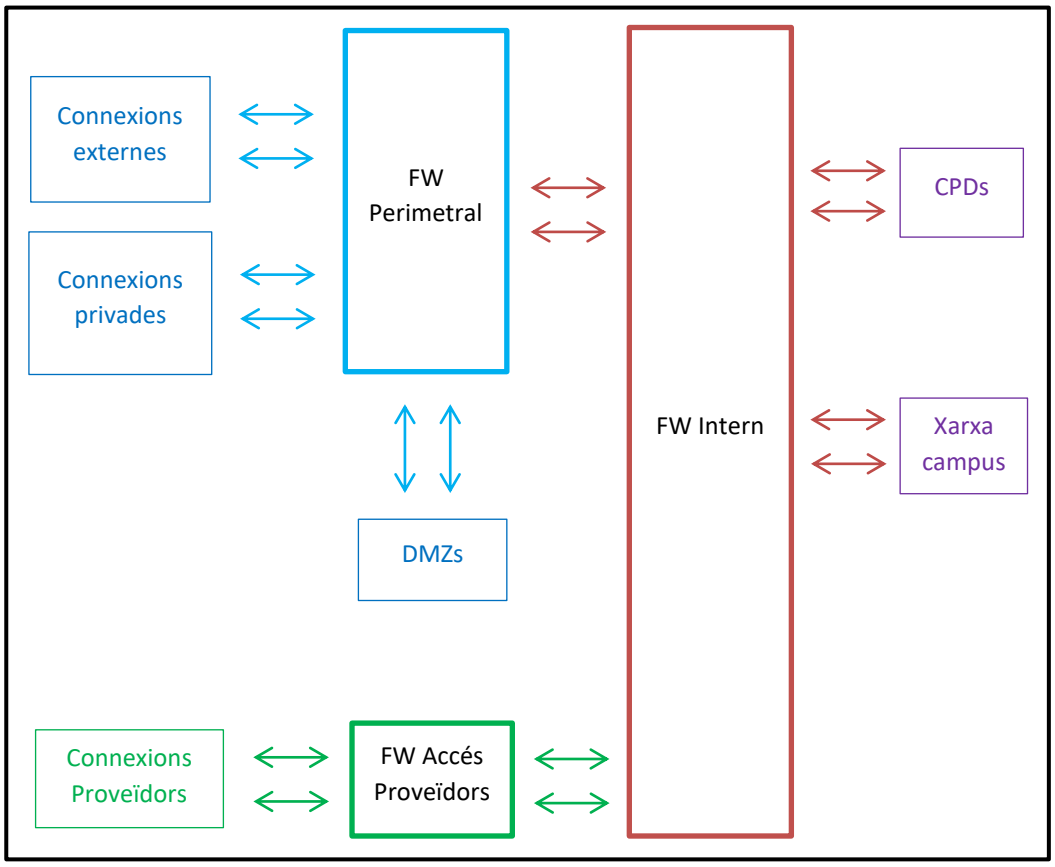
Per connectar els equips entre CPDs s'utilitza cablejat de FO Monomode. La distància d'aquestes fibres és inferior a 500 metres.

Aquesta no és una descripció detallada de la xarxa de l'hospital: és només una orientació per estimar les possibles necessitats de configuració.

2.3 Especificacions dels equips i programaris

2.3.1 Esquema lògic de la xarxa

Es demana implementar un nou FW d'accés per proveïdors seguint un esquema lògic com el següent:



Els equips a incorporar inicialment faran les funcions de connexió a la xarxa de l'hospital dels proveïdors que presten suport al departament d'informàtica, de manera que les dificultats en altres entorns no afectin a aquesta possibilitat de connexió.

2.3.2 Requeriments

2.3.2.1 Arquitectura

- Es requereixen equips físics per a la funció de gateway de dades, que incorporin totes les funcions necessàries, o que utilitzin els equips ja existents a l'hospital per a les funcions administratives i de registre.
  - Configuració d'alta disponibilitat amb un mínim de 2 equips.
  - Es requereixen equips appliance dissenyats específicament per a la funció.
  - No s'admeten servidors de propòsit general
  - No es permeten equips virtuals.
  - Els equips redundants també seran físics.

- Seran equips per muntar en rack estàndard.
- Alçada màxima de 2 unitats de Rack.

- Utilització de hardware específic amb ús de components tipus ASIC que assegurin el rendiment.
  - Processament per hardware de tot el tràfic LAN.
  - Processament per hardware de la protecció AntiDos.
  - Processament per hardware del tràfic encriptat.
  - Hardware específic per anàlisi de capa 4, diferenciat del hardware específic d'anàlisi de capa 7.
  - Processament per hardware de la recerca de signatures d'atacs.

- Configuració en alta disponibilitat.
  - Utilització de 2 equips que permetin configuració actiu-actiu o bé actiu-passiu.
  - Redundància de tots els components físics que intervinguin en la prestació del servei als usuaris.
  - Cadascun dels equips s'instal·larà en un CPD diferent dels 2 que disposa l'hospital. Els CPDs estan ubicats tots dos a l'edifici de l'hospital nou. Es disposa de fibres òptiques d'interconnexió de tipus monomode.
  - Els 2 equips seran iguals.
  - Els equips físics han d'incorporar font d'alimentació redundada, amb funcionalitat hot-swap.
  - Commutació automàtica entre els diferents equips en cas de fallida d'un dels equips.
  - Sincronització automatitzada de la configuració entre els dos equips.
  - Sincronització de la informació entre els equips redundants, de manera que una commutació entre equips ocasioni el mínim d'incidència possible als usuaris. Es demana que, al menys, el sistema disposi de la funcionalitat d'actiu / passiu amb sincronització d'estats, connexions i sessions per evitar la pèrdua de connexions entre ambdós equips en cas de balanceig per fallida d'un d'ells.
  - Tant en cas de configuració actiu-passiu com actiu-actiu cada un dels equips ha de suportar el total dels requeriments de capacitat especificats més avall.
  - Modificació de la configuració de polítiques sense aturada de servei apreciable.

- Capacitat per configurar firewalls virtuals:
  - Capacitat d'execució dels firewalls virtuals en qualsevol dels 2 equips subministrats.
  - Capacitat de configurar firewalls virtuals actiu-passiu distribuint la càrrega entre els 2 equips.

- Suport de diferents modes de comportament: router, transparent i snifer:
  - Diferents firewalls virtuals han de poder treballar en diferents modes

- Capacitat d'integració amb altres sistemes gestors d'identitats i gestors d'infraestructures per recollir informació, identificacions i inventaris.
  - Cloud Google, Azure, AWS, Oracle

- Vmware ESX, Vmware NSX, Openstack, Kubernetes, Cisco ACI
- Directori Actiu i Radius
- BBDD d'amenaces: llistats d'IPs, dominis DNS, URLs, Hashs

- Totes les funcions de xarxa apropiades:
  - Routing OSPF, RIPv2, ISIS, BGP, WCCP;
  - NAT;
  - IEEE 802.1Q;
  - PPPoE.
  - 802.3ad
  - Multicast.
  - DHCP Relay. DHCP server.
  - DNS server, DNS Proxy.
  - NTP server.
  - QoS suportat per hardware.
  - VXLAN.
  - Traffic Shaping (regularització) in & out. Configuració per aplicacions, URLs, IPs.
  - Suport de IPv6 amb les mateixes funcionalitats que IPv4.
  - Altres prestacions habituals.

- Accés via SNMP per control de disponibilitat i capacitat.

- Port USB que permeti la càrrega de firmware.

- Capacitat de SSL Off-loading.

- Administració via els equips Fortianalyzer ja existents:
  - Equips Fortinet FAZ-800G
  - Integració de les funcions de configuració, reporting, i anàlisi dels equips subministrats

- Execució de test Sandbox via els equips FortiSandbox ja existents:
  - Equip Fortinet FSA-500F
  - Integració de les funcions d'anàlisi de malware via test en sandbox

- Integració amb sistemes FortiAuthenticator de validació d'usuaris ja existent:
  - Servidor FortiAuthenticator
  - Integració de les funcionalitats 2FA

- Un cop finalitzada la subscripció el sistema continuarà funcionant, (excepte serveis de filtratge URL), tot i que no s'actualitzi la informació dinàmica com són les signatures.

2.3.2.2 Funcionalitats

- Polítiques i regles de gestió per origen i destí.
  - El concepte zona de seguretat permet agrupar diferents xarxes. Les regles han de considerar la zona origen i la zona destí, i permetre també l'ús d'interfícies.
  - IPs, xarxes, països.
  - Dinàmicament: adreces de xarxes TOR o de proxis anònims.
  - Objectes definits via eines d'integració (veure més avall).

- Polítiques i regles de gestió per capes 3 i 4 de xarxa.
  - Servei de xarxa.
  - Capacitat de configuració via regles del NAT sortint.
  - Base de dades de serveis Internet, agrupats i actualitzats de forma dinàmica pel propi fabricant del producte, que permeti configurar ports i adreces pel nom o funció, sense necessitat d'establir-ho manualment.

- Polítiques i regles de gestió per usuaris.
  - Creació de grups d'usuaris.
  - Utilització d'usuaris i grups de Directori Actiu en les regles d'autorització de tràfic.
  - Integració amb Directori Actiu per identificar als usuaris de les connexions internes de manera transparent.
  - Integració amb Directori Actiu per validació de connexions externes, túnels ipsec i https.
  - Publicació de portal captiu sol·licitant usuari autoritzat pels intents de navegació que realitzin usuaris no autoritzats.
  - Sol·licitud de segon mecanisme de validació via token únic als usuaris externs de l'hospital: es requereix com a mínim la possibilitat de fer-ho via email, SMS i token mòbil.

- Polítiques i regles de gestió segons horari o calendari.

- Control d'aplicacions. Polítiques i regles de gestió per aplicacions.
  - S'ha de poder indicar quin tràfic s'analitzarà a nivell 4 i quin a nivell 7.
  - Es demana que la solució sigui capaç d'identificar i controlar les aplicacions actives actuals, incloent aplicacions Web 2.0, amb la corresponent categorització i agrupació de les mateixes segons el seu propòsit.
  - Identificació de totes les aplicacions habituals. BBDD mínima de 1900 aplicacions.
  - Identificació independent del port que facin servir.
  - Aquestes aplicacions han de ser identificades també quan fan servir el protocol HTTPS.
  - El sistema ha de permetre la creació de regles específiques de seguretat per categories, sub-categories així com aplicacions.
  - Control granular de les diferents funcionalitats dins de les aplicacions.
  - Identificació de l'intercanvi de fitxers efectuat dins de les aplicacions.
  - Creació de signatures específiques per aplicacions personalitzades.
  - Identificació i suport de tràfic VoIP.

- Protecció Dos i DDos.
    - Protecció davant atacs Dos i DDoS implementada per hardware.
    - Creació de regles per aplicar llindars de protecció a nivell 3 i 4.

- Antivirus
    - En l'anàlisi de fitxers transmesos per les diferents aplicacions.
        - En especial, anàlisi dels fitxers adjunts a correus.
        - En el tràfic de navegació web.
        - Fitxes transmesos utilitzant altres aplicacions, com per exemple les socials.
    - Identificació intel·ligent dels fitxers, no basada només en el tipus d'extensió.
    - Suport de sandbox. Veure més avall.
    - Capacitat per eliminar contingut, com codi java, macros o URLs de documents i de correus.
    - Suport d'anàlisi de contingut via ICAP.

- Anàlisi de comportament de les mostres sospitoses via emulació en entorn aïllat, (servei de sandbox) i reporting dels resultats.
    - La solució ha de poder prevenir l'entrada de malware de dia zero de forma dinàmica abans de que es generi una signatura que ho pugui reconèixer.
    - S'ha d'incloure la funcionalitat de Sandbox per tal que tots els arxius entrants a l'hospital puguin ser analitzats simulant el comportament d'aquests arxius abans de lliurar-los a l'usuari final.
    - L'anàlisi ha de considerar no només ".exe", sinó també fitxers java, flash, pdf, documents office, fitxers d'agrupació tipus ".zip", ".rar", i similars.
    - Utilització de base de dades global per al registre i consulta de valoració de fitxers coneguts.
        - El control de reputació per hash és obligatori.
        - Aquest mecanisme ha d'evitar emular fitxers sense càrrega potencial o que ja hagin estat emulats recentment.
        - Es valorarà el temps que tarda el sistema en assabentar-se dels hash de fitxers maliciosos descoberts a altres instal·lacions.
    - Capacitat de bloquejar o no els fitxers amb valoració desconeguda.
    - Es requereix implantar la solució d'anàlisi a l'hospital, i també la possibilitat d'utilitzar serveis de núvol en cas d'incidència en la solució local.
        - Es valorarà el compromís de termini màxim en el temps de resposta.
        - L'anàlisi en el núvol complirà amb els requeriments legals derivats de la LOPD i del RGPD.
    - Anàlisi de fitxers
        - Anàlisi d'executables (bat, cmd, dll, eml, exe, jar, jse, msi, ps1, upx, wsf, vbs)
        - Capacitat de descompressió (7z, arb, bzip, bzip2, cab, iso, eml, gzip, lzw, rar, tar, xz, zip)

        - Anàlisi de fitxers word, excel, powerpoint, Outlook, pdf, swf,
        - Anàlisi de fitxers web: html, js, url, lnk
        - Anàlisi d'aplicacions android, linux i MAC
    - Anàlisi de URLs.
    - Anàlisi de carpetes compartides.
    - Sistema utilitzable també per altres solucions de seguretat
        - Connexió sniffer PCAP.
        - Connexió com a MTA.
        - Connexió ICAP.
        - Integració via JSON API.
    - Compartir els hash dels fitxers analitzats per evitar validar fitxers ja coneguts.
    - Compartir els hash a nivell mundial en temps real.
    - Informe detallat dels resultats positius.
        - Classificació per categories.
        - Generació de PDF de l'informe.
    - Dashboard de situació
        - Us dels recursos hw i sw
        - Volums d'activitat per equip emissor
        - Amenaces detectades
        - Amenaces detectades per canal d'entrada
        - Equips infectats
        - Usuaris afectats
    - La solució local s'implementarà amb appliance específics per a la funció
        - Equips específics diferents del HW utilitzat en el tallafocs.
        - Hardware mínim:
            - 4 Ge rj45, 1Tb de disc, suport de 6VM simultànies.
            - Muntatge en rack estàndard. Mida màxima 1U.
        - Implementarà servidors virtuals en el hardware físic proporcionat
        - Sanboxing en sistemes Windows i en sistemes Linux.
        - Mateix fabricant que la solució de Firewall.
        - Ús obert a altres sistemes de seguretat.
        - Imatges customitzades.
            - Possibilitat d'utilitzar imatges personalitzades que implementin el mateix entorn de treball utilitzat a l'hospital.
        - Rendiment mínim:
            - Prefiltratge de 4500 fitxers per hora
            - Sanboxing de 120 fitxers per hora
            - Anàlisi de 5000 emails per hora
            - Sniffer de 500 Mbps
        - Possibilitat de configuració en mode Sniffer, identificant el fitxers transmesos via els protocols HTTP, FTP, POP3, IMAP, SMTP, SMB, DNS i raw TCP.

- Funcionalitats intel·ligència WAN
  - Balanceig intel·ligent de connexions físiques i lògiques.
  - Identificar disponibilitat de les línies, inclosa també la detecció de l'accés a Internet.
  - Detecció de la qualitat de la línia: latència, pèrdua de paquets, jitter.
  - Regles de configuració que considerin usuaris, destí, qualitat de la línia, tràfic i ample de banda.

- Configuració de VPNs
  - Site to Site. Túnels IPSEC per a la interconnexió de xarxes.
  - PC to LAN. Túnels IPSEC per a l'accés remot d'equips concrets.
  - Túnels Https. Túnels https per a l'accés remot d'equips puntuals.
    - Suport del mode accés web sense agent i mode túnel complet amb agent.
  - Suport dels protocols IPSEC, PPTP, L2TP i GRP sobre IPSEC.
  - Suport d'agregació de túnels amb balanceig per paquet.

- Suport d'aplicacions que inclouen fluxos diversos, de manera que aquests resultin transparents a l'aplicació de polítiques:
  - Suport FTP i similars.
  - Suport de tràfic VoIP: H.323/SIP/SCCP/RTP.
  - Altres aplicacions amb dificultats similars.

- Funcions d'auto-diagnòstic, que com a mínim auditi polítiques de seguretat sense ús, contrasenyes dèbils, i disponibilitat de llicències i manteniments actius.

- Actualització automatitzada de les funcionalitats requerides: identificació d'aplicacions, signatures antivirus, "checksums de fitxers malware".

2.3.2.3 Gestió i reporting

- Utilització dels equips actualment existents per realitzar questa funció:
  - Equips Fortinet FAZ-800G

- Gestió i reporting via consola gràfica, que resulti intuïtiva, amigable, i poc propensa a errors.

- Accés:
  - Accés via https.
  - Identificació de l'usuari via doble factor.

- Gestió de la configuració:
  - Plataforma de gestió inclosa en els propis equips firewall, sense necessitat d'equips auxiliars.
  - Eina interactiva que faciliti la configuració.

- Aplicació dels canvis sense necessitat de compilar o similars.
- Creació d'usuaris i permisos organitzats per rols.
- Visualització gràfica de l'arquitectura de connexió dels diferents firewalls del fabricant.
- Visualització de l'ús que tenen les regles existents, en nombre i en data de darrer ús.

- Registre del tràfic:
  - Es registraran les connexions autoritzades i les no autoritzades:
  - Registre per ips, ports, usuari, aplicació, orígens i destinació, classificacions, i per tots els criteris que el FW gestiona.
  - Registre de nivell 4 i de nivell 7.
  - Emmagatzematge intern que permeti com a mínim els logs de 40 dies d'activitat i 200 GB per dia.
    - Disc intern dels gateways SSD.
  - Exportació de logs via Syslog, FTP, SCP i TFTP.
  - Registre, monitoratge i anàlisi de logs incorporat en equip extern virtual addicional.
    - Emmagatzematge extern que permeti analitzar un mínim de 6 mesos d'activitat i 200 GB per dia.
    - Hardware mínim requerit:
      - Hardware físic dedicat, no virtualitzat, independent d'altres sistemes.
      - Mínim 2 equips, en configuració d'alta disponibilitat.
      - Cadascun dels equips disposarà de
        - 2 Boques GE SFP
        - 4 boques GE RJ45
        - 16 TB de disc

- Monitoratge del tràfic a temps real:
  - Panell de control amb informació destacada.
  - Quadre de comandament editable per veure en temps real les amenaces i alertes que s'estiguin produint.
  - Filtratge per a la visualització de logs que inclogui origen, destí, aplicació, amenaça, website i política.
  - Visualització de logs consolidats amb diferents nivells d'agrupació que inclogui origen, destí, aplicació, amenaça, website i política. Estructura d'arbre que permeti navegar per la consolidació fins arribar al detall complet.
  - Gestió d'events i generació automàtica d'alertes.
  - Notificació d'alertes per email, snmp i syslog
  - Enviament de logs històrics a altres sistemes i rotació automàtica de logs.

- Anàlisi de logs, incorporant, com a mínim, les següents funcionalitats:
  - Ús de tots els atributs gestionats pel NGFW en la creació de consultes i informes, com aplicacions, xarxes, amenaces, usuaris, grups d'usuaris, etc.
  - Centralitzar i correlacionar informació dels diferents equips.
  - Visió per dispositiu o agregada.

- Filtratge per a la visualització de logs que inclogui origen, destí, aplicació, amenaça, website i política.
- 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.
- Generació automàtica de reports periòdics. Generació i enviament automàtics.
- Generació d'alertes sobre informació històrica.

- Monitoratge del sistema tallafocs, incorporant, com a mínim, les següents funcionalitats:
  - 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 múltiples dispositius.
  - Integració, mitjançant traps SNMP, amb el sistema de gestió d'alertes Nagios de l'hospital.

2.3.2.4 Configuració mínima

Configuració	**Requeriments**
Regles de Firewall suportades	100.000
Nombre màxim de **sessions** concurrents: (valor mínim)	24 milions
Connectivitat (mínim per equip)	2 x 10 Gbps SFP+ 8 x 1 Gps SFP 16 x 10/1 Gbps RJ45 2 x 1 Gbps RJ45 gestió
Instàncies multidomini (firewalls virtuals) (mínim llicenciat)	10
Instàncies multidomini (firewalls virtuals) (mínim ampliable)	500

2.3.2.5 Rendiment mínim

Rendiment (Valors nominals mínims en condicions de laboratori)	**Valor mínim**
Rendiment **capa 4** amb paquets de 1518 bytes	27 Gbps
Rendiment **control d'aplicacions + motor antimalware**	3 Gbps
Sessions concurrents	3 milions
Nombre màxim de **noves sessions per segon**: (valor mínim)	280.000
Túnels IPSEC site to site	2.000
Túnels IPSEC client to site	16.000
Connexions VPN-SSL simultànies	500
Throughput de VPN SSL: (valor mínim)	2 Gbps

Throughput de VPN IPSEC (512 bytes): (valor mínim)	13 Gbps

Els requeriments de rendiment han de ser vàlids amb logging actiu.

La configuració a implantar activarà totes les funcionalitats indicades.

El conjunt de totes les actuacions sobre les aplicacions interactives i sobre el tràfic web no ha de penalitzar ni el temps de resposta ni la satisfacció de l'usuari.

Es valoraran positivament els valors superiors a aquests requeriments mínims.

2.4 Requeriments generals

Són requeriments imprescindibles:

- Equipament nou, sense utilització prèvia.
- Llicenciament de totes les funcionalitats esmentades en aquest Plec per a tot el període contractat.
- Manteniment de hardware, actualització de programari, activació de subscripcions per tot el període contractat.
- Incloure totes les subscripcions necessàries per implementar els requeriments indicats.
- El llicenciament ha d'incloure marges suficients que permetin un creixement raonable a l'hospital en usuaris, equips protegits, polítiques, amples de banda... Com a mínim s'ha de suportar sense cost addicional un increment del 20% sobre els valors actuals.
- Tots els equips i funcions s'instal·laran on-premise a l'hospital. Només s'accepten configuracions de núvol per:
    - Funcions d'emmagatzematge de backups.
    - Funcionament alternatiu en cas d'error en els sistemes principals.
    - Consultes de bases de dades dinàmiques i anàlisi de fitxers (sandbox) pel lot 2.
- Cal incloure les òptiques, connectors, cables de connexió, i tot el que sigui necessari per a la implantació.

- Contractació directa al fabricant de les garanties: reparacions, substitucions, noves versions i escalat d'incidències.
- Dret d'actualització del programari amb les noves versions que el fabricant publiqui, sempre que estiguin suportades pel hardware adquirit, tant pel que fa a la correcció d'incidents i errors de seguretat com per a millores evolutives.
- Servei in-situ.

2.5 Especificacions dels serveis

2.5.1 Abast dels serveis

2.5.1.1 Abast

Es demanen serveis d'instal·lació i configuració tipus "claus en mà", amb lliurament de la instal·lació un cop estigui en funcionament:

- Preparació d'un pla detallat de projecte que l'hospital haurà de validar
- Instal·lació i configuració
  - Anàlisi de la configuració necessària
  - Configuració de les polítiques actualment necessàries
  - Adaptació de les polítiques per a la seva optimització
- Posada en funcionament
- Traspàs de coneixement
- Manteniment integral
  - Resolució d'incidències
  - Resolució de crisis
  - Atenció a dubtes i consultes
- Seguiment de projecte

El servei s'ha de proveir en horari 24x7 en tot allò que s'esdevingui necessari pel funcionament normal de l'hospital.

Segueixen especificacions més detallades dels punts enumerats.

2.5.1.2 Pla de projecte

- Preparació d'un pla detallat de projecte en base al pla presentat en la proposta.
- L'hospital haurà de validar el pla.
- Si les necessitats de l'hospital així ho recomanen, aquest tindrà dret a modificar la planificació del projecte.

2.5.1.3 Instal·lació i configuració dels equips

- Instal·lació dels equips:
  - El licitador haurà d'instal·lar els equips amb els seus propis recursos.
  - El projecte inclou aportar sense cost addicional les connexions de cablejat necessàries en els racks.
  - En el cas del lot 1, generació d'un procediment que permeti, en cas de crisi, evitar l'ús dels nous equips per tornar a la situació actual, de la manera més ràpida i immediata possible.
- En la fase d'instal·lació de l'equipament, es demana l'execució de les actualitzacions de programari disponible i compatible amb el hardware actual:
  - Planificació conjunta amb l'hospital segons necessitats i avaluació de riscos.
  - Es considera inclòs en el preu d'aquest contracte l'actualització inicial, i tantes actualitzacions com siguin necessàries per motius de seguretat, estabilitat o garanties de funcionament de la instal·lació.

- Les actualitzacions del programari planificades s'hauran de realitzar en horari de mínima afectació als usuaris, que en la majoria dels casos haurà de ser fora de l'horari estàndard d'oficina.
- El procés d'actualització inclourà un anàlisi, que com a mínim:
  - Justificarà la proposta de versió a instal·lar.
  - Indicarà els errors coneguts de la versió a instal·lar.
  - Validació de requeriments hardware.
  - Alternatives possibles a la proposta.

- Integració a la xarxa i amb el directori actiu.
- Identificació de les polítiques actualment necessàries.
  - Identificació i creació de les regles necessàries.
- Configuració inicial de tots els serveis requerits i tot el que figuri en la proposta del licitador.
- La implementació del projecte podrà ser progressiva en el temps, però no es donarà el projecte per acabat fins que aquesta no finalitzi.
- La implementació del projecte requerirà comptar amb la col·laboració del personal que gestiona els equips interrelacionats amb els adquirits i amb qui gestionarà els nous equips en el dia a dia de l'hospital. En tot cas, el licitador assumirà la direcció i la responsabilitat de la implantació i la gestió dels equips proporcionats fins a la signatura de l'acta de "lliurament i posada en funcionament".
- El licitador aportarà suport i solucions en totes les dificultats que puguin sorgir.

2.5.1.4 Posada en funcionament

- Posada en funcionament amb el mínim tall de servei possible.
- Posada en funcionament en horari adequat per generar els mínims inconvenients possibles.
  - Els horaris concrets per efectuar les actuacions amb afectació als usuaris s'hauran de pactar amb l'hospital, i probablement implicaran actuacions en horaris no habituals de treball.
- Validació de les funcionalitats i rendiment especificats en la proposta del licitador.
  - En el supòsit de que la instal·lació incompleixi amb les especificacions de la proposta presentada pel licitador l'hospital podrà retornar els equips, declarar guanyador de la licitació a una altra proposta, i tindrà dret a reclamar danys i perjudicis.
- Suport presencial i resposta "immediata" durant el període d'estabilització de la instal·lació.

2.5.1.5 Traspàs de coneixement

- Traspàs als tècnics de l'hospital, i/o als tècnics que l'hospital contracti per a la gestió d'aquest equipament.
- Formació suficient per poder assumir la gestió del dia a dia de la instal·lació.
- Documentació de la instal·lació.
- Documentació de les incidències generades en el procés d'instal·lació, configuració i posada en funcionament.
- L'adjudicatari haurà de proporcionar procediments apropiats per a l'explotació en el dia a dia de l'hospital.
- Veure més avall detalls de l'abast i format de la documentació a presentar.

2.5.1.6 Manteniment integral

2.5.1.6.1 Condicions generals de manteniment

- Garantia (o contractació de millores, si cal), de reparació i suport via el fabricant.
  - El manteniment del hardware estarà garantit pel fabricant.
  - Es disposarà de capacitat d'escalar suport als fabricants sempre que sigui necessari.
  - Dret d'actualització de drivers i firmware, tant per la necessitat de resoldre incidències com per evolució.
  - Les noves versions del firmware estaran a disposició de l'hospital conforme el fabricant les publiqui.
- El manteniment serà in-situ.
- En principi el contractista actuarà com a punt únic de contacte per a l'hospital per a tota la solució. Tot i això, si l'hospital ho considera convenient tindrà dret a accedir directament als serveis de garantia del fabricant (o a exigir al fabricant un canvi d'interlocució).
- La proposta i el preu han d'incloure el manteniment proposat per al termini proposat**,** a comptar des de la posada en producció de la instal·lació. El preu del manteniment està inclòs en el pressupost de licitació.
- El monitoratge continu de la instal·lació i el primer nivell d'actuació davant d'incidències no està inclòs en aquesta licitació.
- Els serveis de manteniment i suport preventius, reactius i conductius no estan inclosos en aquesta licitació.

2.5.1.6.2 Resolució d'incidències

- Esforç continuat fins a la solució de la incidència.
- Resolució d'incidències 24x7. Es requereix "Resolució incidències 24x7" per a les incidències que tinguin implicacions per als usuaris en la disponibilitat de la funcionalitat, i "Resolució incidències NBD" en cas d'incidents que no afectin al servei als usuaris.
- Resolució de reparacions NBD.
- Veure més avall paràmetres de servei.
- Enviament anticipat dels equips de reposició.
- Termini mínim de 10 dies per retornar els equipaments avariats.
- Capacitat de diagnòstic remot.
- Capacitat de presència in-situ en cas necessari.
- Gestions amb els fabricants per escalar i solucionar les incidències que requereixin de la seva participació.
- El servei de suport general del departament d'informàtica s'encarregarà del primer nivell d'atenció. El servei contractat via aquesta licitació es refereix a suport expert per situacions no habituals en el dia a dia de l'hospital.
- L'adjudicatari subcontractarà obligatòriament la resolució d'avaries al fabricant de l'equipament. L'adjudicatari contractarà al fabricant els mateixos SLAs sol·licitats en aquest contracte.
- El contractista haurà de presentar proves de la contractació als fabricants dels requeriments esmentats. L'hospital tindrà dret a no pagar cap factura del contracte fins que no s'hagin presentat aquestes proves.
- Es requereix informació constant de l'estat de les incidències en curs.

2.5.1.6.3 Crisi

- Es demana col·laboració amb l'hospital en cas de crisi deguda a la no disponibilitat de la instal·lació, en cas d'afectació greu deguda a intents d'atacs o a atacs exitosos, o en cas d'altres situacions greus no previstes a priori.
- La situació de crisi es refereix al context d'aquest contracte: situacions on els equips subministrats no funcionen i això ocasiona un gran impacte a l'hospital. No es refereix a treballs en profunditat per analitzar la base o l'impacte d'un atac o tasques similars. En aquest cas, si fos el cas de sol·licitar-se, es faria a banda d'aquest contracte.
- En cas de situació excepcional l'adjudicatari es compromet a l'aportació de recursos extraordinaris per resoldre la situació tan aviat com sigui possible.
- A priori, la gestió de crisis no serà motiu per facturació addicional.

2.5.1.6.4 Atenció de dubtes i consultes

- Es demana l'atenció als dubtes o consultes que el departament d'informàtica pugui tenir sobre els sistemes de l'àmbit del contracte:
  - Veure SLAs indicats en l'apartat "Paràmetres de nivells de servei sol·licitats".
- Accés via Web a consultes sobre el servei.
- Assessorament en la millora dels sistemes i dels serveis:
  - Actitud proactiva per tal de suggerir millores en els serveis i sistemes adients al contracte.

2.5.1.7 Paràmetres d'Acord de Nivell de Servei Sol·licitats

Àmbit	Paràmetre	Valor mínim demanat
Resolució incidències 24x7		
	Horari de cobertura	24x7
	Temps d'atenció màxim	1 hora
	Temps de resposta màxim	4 hora
	Temps de resolució màxim	6 hores
	Penalització per cada hora de retard en el temps de resolució d'una incidència.	10€
	Penalització per excessiu nombre d'avaries. Penalització per cada avaria (sense comptar les 2 primeres avaries), computat anualment.	100€
Resolució incidències i Reparacions NBD		
	Horari de cobertura	10x5
	Temps d'atenció màxim	4 hores
	Temps de resposta màxim	Dia següent
	Temps de reposició màxim	Dia següent
	Temps de resolució màxim	Dia següent

	Penalització per cada dia de retard en el temps de resolució o reposició d'una incidència.	20€
Atenció de dubtes i consultes		
	Horari de cobertura	10x5
	Temps d'atenció màxim	4 hores
	Temps de resposta màxim	Dia següent
	Penalització per cada dia de retard en el temps de resposta d'una consulta	20€
Administració de sistemes		
	Horari de cobertura	10x5
	Temps d'atenció màxim	4 hores
	Temps de resolució màxim	Dia següent
	Penalització per cada dia de retard en el temps de resolució d'una petició	20€
Petites projectes		
	Horari de cobertura	10x5
	Temps d'atenció màxim	Dia següent
Límit màxim de penalitzacions		
	L'import màxim de possibles penalitzacions	10% de l'import d'adjudicació contracte

2.5.2 Condicions dels serveis

2.5.2.1 Documentació del projecte

La documentació generada, com a mínim inclourà:

DESCRIPCIÓ

1. Descripció del maquinari/programari adquirits:
    a. Presentació
    b. Funcionalitats
    c. Memòria d'implantació
    d. Procediments d'instal·lació utilitzats
2. Esquema de components i llicències.
3. Màquines que donen el servei.
4. Programari utilitzat, versions i configuració.
5. Relació amb altres serveis.
6. Memòria de les proves de la instal·lació efectuades.
7. Relació d'incidències generades en el procés d'instal·lació, configuració i posada en funcionament.
8. Detall de la configuració realitzada.
9. Mètode d'accés a cada element.
10. Usuaris i passwords de gestió de cada element.

EXPLOTACIÓ (pels casos on apliqui)

1. Processos de parada i arrancada

a. Procés de parada (i checklist de verificació)
b. Procés d'arrancada (i checklist de verificació)

2. Monitoratge
    a. Aplicació (o servei)
    b. Processos associats
    c. Llindars i espais
3. Revisió de logs, dumps, jobs, ... i altres alertes
    a. Tasques necessàries
    b. Procediments
4. Treballs planificats / jobs
    a. Treballs configurats
    b. Monitorització específica
    c. Procediment d'actuació en cas d'incident
    d. Procediment de configuració
5. Arxivat
    a. Tasques necessàries
    b. Procediments
6. Housekeeping (gestió de manteniment del sistema)
    a. Tasques necessàries
    b. Procediments
7. Tunning periòdic
    a. Tasques necessàries
    b. Procediments
8. Canvis
    a. Opcions i procediments de configuració i administració.
    b. Actualitzacions periòdiques de programari. Requeriments, recomanacions.
    c. Redacció dels protocols i procediments més habituals de treball.
9. Gestió de seguretat del propi equipament
    a. Comprovacions de seguretat
    b. Recomanacions de mesures preventives
    c. Gestió d'incidents de seguretat
    d. Instal·lació d'actualitzacions crítiques. Publicació, validació, instal·lació, ...
10. Troubleshooting
    a. Opcions i procediments. Requeriments, recomanacions.
11. Mecanismes d'alta disponibilitat implantats
    a. Descripció
    b. Monitorització específica dels components i mecanismes de redundància
    c. Procediment de prova periòdica
    d. Procediment d'activació (si és manual)
    e. Procediment de recuperació de la situació habitual

SERVEI, CONTACTES I SUPORT

1. Suport / Garantia / Manteniment
    a. Descripció de serveis inclosos
    b. Terminis dels serveis inclosos
    c. Horari
    d. Contracte / ANS / Penalitzacions
    e. Contactes. Mètode d'accés als serveis.
    f. Procediment d'escalatge

2.5.2.2 Cobertura horària i presència in-situ

- Els serveis es contracten in-situ, tot i que es permet la utilització d'accés remot per ajudar-se en la seva realització.
- Segons l'equipament i l'impacte de les sol·licituds aquestes s'han d'atendre en horari 24x7x365.

- Anomenem horari habitual de treball o horari d'oficina a l'horari de 8 a 18 dels dies laborables, i anomenem horari estès a l'horari de 18 del vespre a 8 del matí dels dies laborables, i a les 24 hores dels caps de setmana i festius.
- Normalment les activitats planificades que impliquin aturada o reducció del servei als usuaris s'hauran d'efectuar en horari estès, sempre en horari pactat amb l'Hospital. Totes les accions que afectin al servei percebut pels usuaris i que es puguin planificar s'hauran de pactar prèviament amb el personal de l'Hospital.
- Per necessitats del servei, algunes tasques de les descrites al present plec s'hauran de realitzar en horari estès, amb l'objectiu de minimitzar l'impacte als serveis. Aquestes tasques estan contemplades dins de l'àmbit del servei i no generaran cap cost associat.

2.5.2.3 Provisió dels serveis tipus claus en mà

Els preus proposats per a la provisió i posterior gestió dels sistemes i serveis sol·licitats han d'incloure tots els possibles elements de cost associats a la implantació i gestió d'aquests (planificació, enginyeria, permisos, cablejats d'interconnexions, ... així com els costos associats a la implantació de la llengua catalana, (si és el cas)).

És a dir, l'hospital no assumirà cap altre cost associat a la implantació dels serveis contractats, a banda dels especificats pels licitadors en les seves propostes.

Així mateix, el licitant no podrà comptar amb la dedicació de personal de l'hospital, ni en disposar d'espai per a emmagatzematge d'equipaments pendent d'instal·lació sense comptar abans amb una autorització explícita per part de l'hospital.

Per tal que els licitadors puguin contemplar totes les possibles despeses, aquests si ho estimen convenient podran visitar les instal·lacions.

2.5.2.4 Dimensionament de l'equip de treball

- El dimensionament ha de ser el necessari per complir amb les tasques, horaris i SLAs demanats en aquest plec.
- L'equip de treball ha d'estar configurat per persones amb coneixements i experiència suficient per garantir l'execució i la qualitat de les tasques contractades.
- Tots els perfils tindran la formació i el bagatge necessari per executar la seva funció.
- Per cada un dels membres de l'equip de treball ha de poder acreditar-se el nivell de coneixements i bagatge adequat a les funcions que realitza.

2.5.2.5 Coneixement especialitzat

- El contractista haurà de proporcionar pel seu compte el coneixement "molt especialitzat" necessari per realitzar les tasques contractades.

2.5.2.6 Escalat de casos

- El contractista haurà de gestionar autònomament l'escalat dels casos a tercers sempre que les circumstàncies ho requereixin.
- És obligació del contractista aportar el coneixement i l'experiència suficients per escalar només allò que de manera justificada requereixi la intervenció de tercers, ja siguin els fabricants, els operadors, o altres.

2.5.2.7 Normatives legals

- Les empreses licitadores hauran d'assegurar el compliment dels estàndards i normatives aplicables, incloent els codis de bones pràctiques en la prestació de serveis d'informàtica i de telecomunicacions.
- El contractista haurà de complir amb la tota la reglamentació vigent que apliqui als serveis prestats, tant la normativa europea, com la de l'Estat espanyol, com la de la Generalitat de Catalunya.
- El contractista s'adequarà a tota la normativa interna que desenvolupi l'Hospital.

2.5.2.8 Calendari

- El calendari laboral utilitzat serà el de Barcelona.

2.5.2.9 Accés remot

- El contractista podrà utilitzar mecanismes d'accés remot per accedir al monitoratge, diagnòstic, i a l'administració dels equips i sistemes.
- Els equips de l'Hospital destinats a la gestió de la seguretat perifèrica podran utilitzar-se per configurar l'accés a aquesta funció.
- Les possibles necessitats que generi la configuració de l'accés remot (llicències, línies, maquinari, programari, ...) no suposaran cap cost addicional per a l'Hospital.

2.5.2.10 Idioma

- La comunicació oral i escrita amb el departament d'informàtica de l'Hospital es farà en català, tret que s'acordi el contrari.
- El servei serà capaç de comunicar-se en anglès amb els proveïdors sempre que això sigui necessari per la prestació dels serveis.

2.5.2.11 Substitució de persones

- L'Hospital es reserva el dret d'entrevistar o examinar a qualsevol persona de l'adjudicatari que participi habitualment en el servei a l'Hospital.
- L'Hospital es reserva el dret de demanar la substitució de persones adjudicades al servei, que el contractista haurà de fer efectiva en el termini màxim de 15 dies naturals.
- Els canvis en els perfils de les persones assignades al servei requeriran d'aprovació prèvia per l'Hospital.

2.5.2.12 Preu hora per tasques addicionals

En els criteris de valoració automàtica es valora un preu hora de tècnic especialista que ha de permetre, si fos el cas, contractar tasques addicionals a les previstes en aquest contracte. Aquesta situació requeriria tramitar una modificació de contracte.

Són exemples de tasques que podria fer falta contractar una reconfiguració en profunditat de la implantació, un canvi de polítiques, un anàlisi de viabilitat d'alguna iniciativa...

El licitador es compromet a disposar, en cas necessari, de recursos apropiats, i conforme al preu presentat.

En aquest cas considerem un recurs apropiat un tècnic especialista en temes de firewall, amb formació d'enginyer, amb formació especialitzada en els productes oferts, i amb una experiència en l'àrea mínima de 2 anys.

2.6 *Seguiment del contracte*

- El contractista definirà interlocutors comercials i tècnics per a la prestació dels serveis
    - Nomenament d'un "***Responsable Comercial del Contracte***", encarregat de:
        - Assegurar que el Contractista compleix les seves obligacions contractuals.
        - Assegurar el compliment dels nivells de servei pactats.
        - Donar suport davant l'hospital a l'especificació de qualsevol requeriment de servei addicional i possibles canvis d'abast.
        - Mantenir una preocupació proactiva pels objectius, millores tècniques i estratègiques del contracte.
        - Negociar possibles renovacions o pròrrogues del contracte (si és el cas).
        - Resoldre de forma satisfactòria qualsevol assumpte de facturació o comptabilitat que pogués sorgir.
        - Participar en les reunions de coordinació.
        - Proposar i participar en les reunions que es vegin necessàries per qualsevol de les parts per atendre assumptes de coordinació, reporting, dificultats, millores, queixes, incompliments de SLA, ...
    - Nomenament d'un "***Responsable Tècnic del Servei***", encarregat de:
        - Assegurar la disponibilitat i el seguiment dels procediments de seguiment de resultats i gestió del contracte.
        - Gestionar la prestació del servei per complir els objectius i nivells de servei acordats i establerts en els SLAs.
        - Mantenir una preocupació proactiva pels objectius, millores tècniques i estratègiques del contracte.
        - Realitzar la coordinació dels serveis associats en aquest contracte amb l'interlocutor tàctic i amb els tècnics de l'àrea de sistemes de l'hospital.
        - Actuar com a referent del Contractista per facilitar la comunicació amb les diferents àrees involucrades en la prestació del servei.
        - Assegurar la gestió eficient dels problemes, assegurant que es segueixen els procediments d'escalat acordats.
        - Informar del servei proporcionat en base a estadístiques exactes i actualitzades.
        - Establir i assegurar el compliment dels nivells de qualitat acordats i mantenir una actitud proactiva per tal de suggerir iniciatives que incideixin en la millora continuada del servei.
        - Establir un procediment de revisió regular del servei que asseguri que tots els assumptes del servei es tracten de forma eficient i dins del temps requerit.
        - Gestionar els assumptes propis del servei.
        - Coordinar als departaments interns del contractista afectats.
        - Coordinar als diferents fabricants afectats.
        - Assegurar la gestió eficient de la provisió dia a dia del servei contractat per l'hospital.

- Participar en les reunions de coordinació.
- Proposar i participar en les reunions que es vegin necessàries per qualsevol de les parts per atendre assumptes de coordinació, reporting, dificultats, millores, queixes, incompliments de SLA, ...

- L'Hospital definirà ***interlocutors operatius***, i un ***interlocutor tàctic*** per a la coordinació del servei:
  - Inicialment els ***interlocutors operatius*** seran diferents tècnics de l'àrea de sistemes de l'Hospital, en funció dels diferents àmbits i processos implicats. Les seves principals responsabilitats seran:
    - La coordinació constant amb el contractista.
    - El seguiment i valoració constants de resultats i objectius.
  - Inicialment ***l'interlocutor tàctic*** serà el Cap de Sistemes del Departament d'Informàtica de l'Hospital. Les seves responsabilitats principals són:
    - Coordinar-se amb el responsable comercial i el responsable tècnic del contractista.
    - Acordar amb el responsable comercial i el responsable tècnic del contractista mesures per solucionar qualsevol deficiència en la qualitat del servei.
    - Definir i acordar els nivells de servei i assegurar el compliment dels SLAs.
    - Fer el seguiment i control regular dels nivells de servei pactats.
    - Oferir atenció especialitzada i coneixement sobre assumptes relacionats amb àrees concretes de l'Hospital i la seva activitat.
    - Gestionar el contracte en curs amb el contractista.
    - Negociar possibles renovacions o pròrrogues del contracte.

- Pel que fa als processos de compra i instal·lació del nou equipament el servei inclourà els següents nivells de coordinació:
  - Validació amb l'hospital del pla d'implantació, (que inclourà pla de proves, instal·lació, configuració, validació, documentació i formació), corregint el licitador els aspectes que l'hospital demani modificar.
  - Reunions de seguiment de l'execució dels plans d'implantació.
    - Aquestes reunions es faran amb periodicitat quinzenal mentre hi hagi processos d'implantació actius.
    - En aquestes reunions hi participaran, com a mínim, el responsable comercial i el responsable tècnic del licitador i el responsable tàctic de l'hospital.
    - Qualsevol de les parts podrà convocar reunions addicionals "ad hoc" sempre que les consideri necessàries.
  - Es farà acta de lliurament de la instal·lació i d'acord en la data d'inici del període de manteniment.

- Pel que fa als processos de manteniment el model de seguiment del servei inclourà 2 nivells diferents de coordinació:
  - ***Reunions anuals***, amb enfoc tàctic i estratègic:

- Participació, com a mínim, de:
    - Responsable comercial del contracte
    - Responsable tècnic del contracte
    - Interlocutor tàctic de l'hospital
- Revisió dels resultats en relació als nivells de servei acordats i dels objectius de qualitat establerts.
    - Es presentaran els resultats del servei.
    - (Si fos el cas), el contractista haurà d'explicar les causes per les que s'han produït incompliments de SLA i fer propostes per aconseguir que no es repeteixi.
    - Valoració continuada d'objectius del servei i millores de qualitat.
    - Valoració continuada de funcions i responsabilitats, àrees de responsabilitat, punts d'interfície, objectius del servei i millores de qualitat i abast de la relació contractual.
    - Es presentarà avaluació de l'estat del servei, punts a destacar, problemàtiques específiques, i propostes de modificació que es considerin adequades
- Revisió de l'estat dels projectes acordats i acords de requeriments.
- Escriptura de l'acta de les reunions, i seguiment del compliment dels acords.

- ***Coordinació operativa*** continuada entre els responsables operatius amb els objectius:
    - Revisió de:
        - Sol·licituds acumulades
        - Sol·licituds demorades
        - Sol·licituds amb més intervencions
        - Sol·licituds fora del termini SLA
        - Problemes puntuals
        - Queixes pendents de resoldre

- El contractista presentarà anualment un report amb la informació:
    - Nombre d'incidències, temps mig de resolució, compliments d'SLA.
    - Tasques preventives, d'administració, de suport, i assessorament efectuades i pendents d'efectuar.
    - Resultats de les actuacions preventives i informes de recomanacions.

3 Signatura

Barcelona, a 12 de desembre de 2023.

Vist-i-plau

Nacho Nieto

Director de sistemes d'informació

DG

***NOTA 1**: El present document es troba incorporat a l'expedient de contractació amb la signatura electrònica emesa per les persones competents.*

***NOTA 2:** A tots els efectes, es considera que la data d'aquest document és la que figura al final del mateix.*

***NOTA 3:** Amb la signatura del present document, el/s/la sotasignat/s declara/en que no existeix conflicte d'interès en la pròpia actuació professional. Així mateix, declara que coneix les seves obligacions, segons el que consta al Protocol en relació als Conflictes d'interès aprovat per la Fundació de Gestió Sanitària de l'Hospital de la Santa Creu i Sant Pau.*