Departament d'Informàtica
Hospital de la Santa Creu i Sant Pau
Tel. 93 553 7430
informàtica@santpau.cat

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

Expedient OBE 24-573

1 Índex

2 Presentació

2.1 Introducció

Aquest és el plec de requeriments tècnics per a la compra d'un firewall perimetral i una sonda IOT que actualitzin i millorin la solució actual.

2.2 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.

2.3 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 5 anys de garantia i un mínim de 5 anys de manteniment, incloses les llicències i subscripcions necessàries.
- Seguiment de projecte.

2.4 Requeriments licitador

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

El contractista haurà de complir els següents criteris:

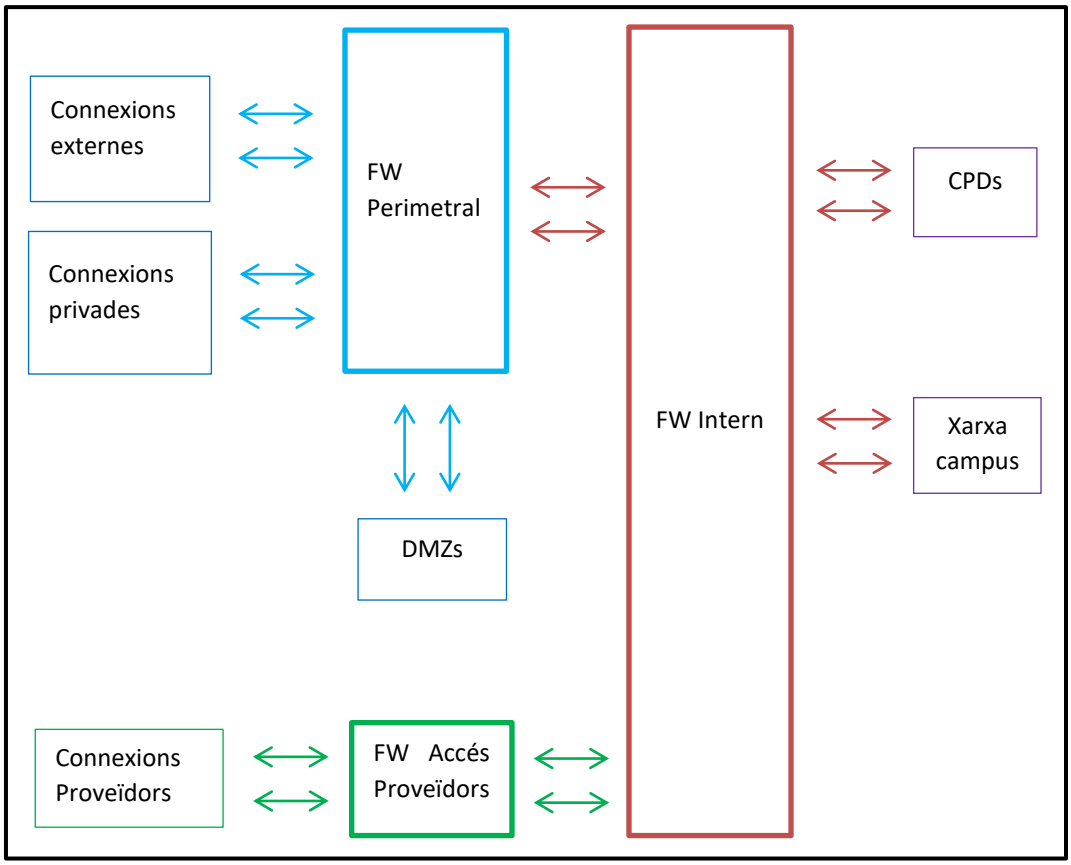
- Certificacions ISO: ISO 9001 o equivalent.
- Certificacions ISO: ISO 14001 o equivalent.
- Relació de partnership amb el fabricant dels productes presentats o alternativament una carta de validació del fabricant conforme el contractista està adequadament preparat per implantar aquest servei amb els seus productes. Aquest requeriment no és necessari si el licitador és el propi fabricant.
- Disposar d'un mínim de 1 tècnic amb la màxima certificació que atorgui el fabricant de la solució presentada amb capacitat d'acudir a l'hospital en un màxim de 2 hores quan sigui requerit (en cas d'incidència greu).
- Disposar d'un mínim de 3 tècnics certificats en la tecnologia presentada amb capacitat d'acudir a l'hospital en un màxim de 2 hores quan sigui requerit (en cas d'incidència greu).

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

3 Situació actual

3.1 Esquema lògic de la xarxa

En l'actualitat l'hospital disposa d'un sistema de seguretat de xarxa implementat segons el següent esquema:



L'equip a incorporar ha de substituir l'equip actual de protecció perimetral.

En el moment d'escriure aquests plecs l'equipament "FW Accés proveïdors" es troba en fase d'implementació, de manera que es preveu que en el moment d'executar aquest contracte el projecte hagi acabat i l'esquema en ús sigui l'esquema representat.

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

3.2 Dimensionament i prestacions

Internament hi ha prop de 4.000 usuaris actius, aproximadament 3.000 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.

La configuració actual filtra l'entrada i sortida des de la xarxa de l'hospital a 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 (a ampliar a 1Gbps) per aplicacions específiques, d'una connexió al "Nus sanitari" de 1 Gbps, 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.

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 amb xarxa gestionada per l'hospital**, com la seu del carrer Castillejos i el Centre de dia**.**
- 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:

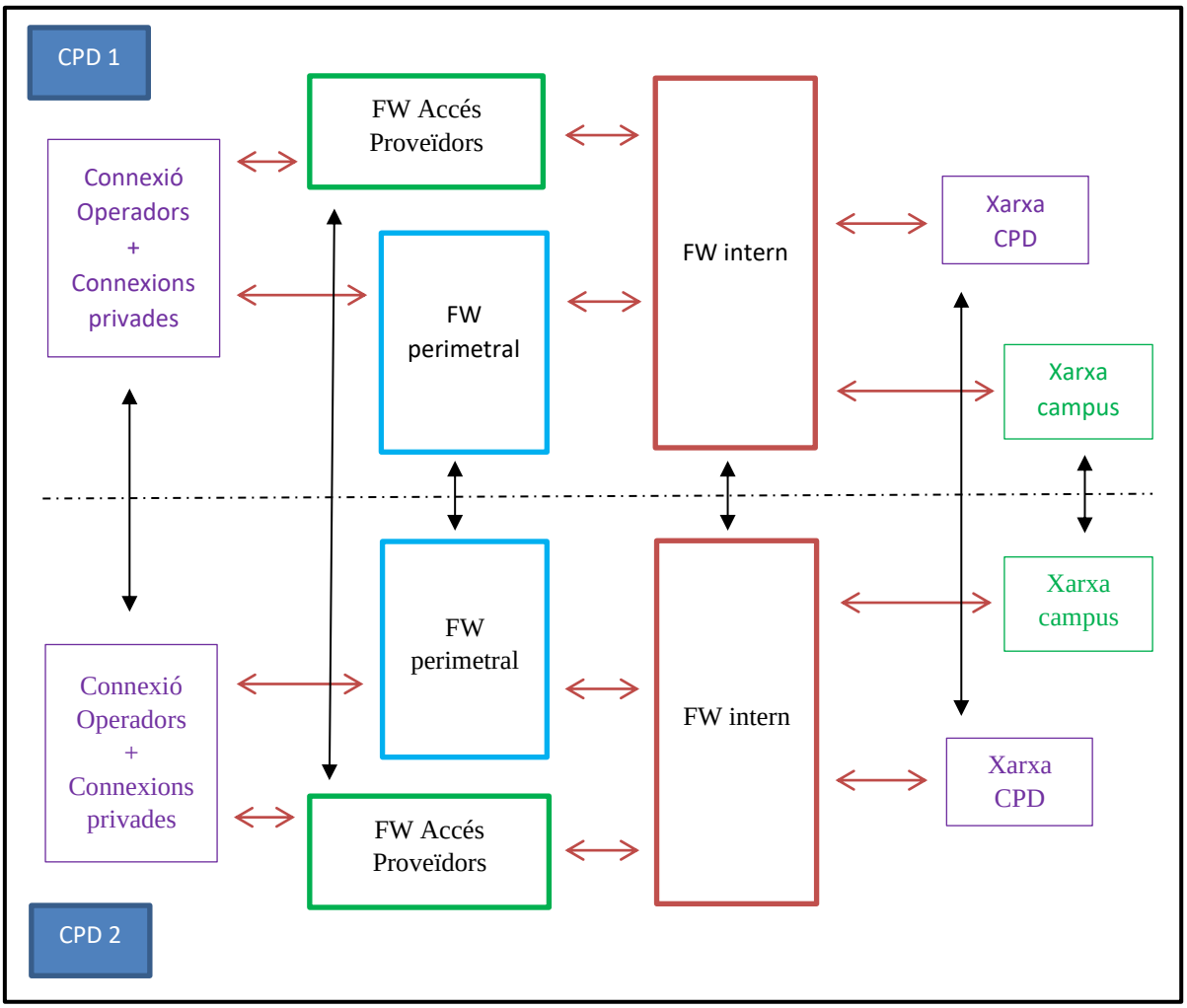
- Gestió via regles de les connexions autoritzades.
- Gestió de la configuració per aplicacions.
- Gestió de la configuració per usuaris.
- Filtratge de navegació web en funció de categories de classificació.
- Registre del tràfic de navegació, incorporant informació de classificació.
- Filtrar el tràfic de navegació i de correu per detectar i bloquejar software maliciós.
- 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 300 regles de configuració i l'altra amb aproximadament 100 regles.

3.3 *Esquema físic de xarxa*

Actualment l'esquema físic de xara es podria representar de la següent manera:



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.

Els Firewalls actuals a substituir són del fabricant Checkpoint i model 15400. Disposen de 10 interfícies 10/100/1000 BaseT i de 2 interfícies 10 Gb SFP+.

Els firewalls interns són Fortigate 2601F i disposen de boques de connexió QSFP28 a 100Gb, boques SFP28/SFP+ a 25 o 10Gb, i boques 10 Gb BaseT.

La connexió amb els operadors de comunicacions externes es realitza via boques 10 Gb BaseT o 1Gb BaseT.

Les connexions privades internes es connecten diferents enllaços 10 Gb SFP+ i connexions via el Firewall intern.

Els Firewalls accés proveïdors són Fortigate FG-200F.

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+. En el moment de redactar aquests plecs s'estan substituint per equips Cisco Nexus 9504 amb boques disponibles 10Gb basetT i 100Gb QSFP28.

La xarxa de campus actualment utilitza 3 equips concentradors 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.

4 Especificacions

4.1 Especificacions dels equips i programaris

4.1.1 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).

- Cal incloure les òptiques, connectors, cables de connexió, i tot el que sigui necessari per a la implantació.
- Les connexions es realitzaran a la més alta velocitat possible i sempre per duplicat.
- Les òptiques utilitzades (SFP, SFP+, SP28) seran les oficials del fabricant de l'equipament.
- Per connectar els equips entre CPDs es disposa de cablejat de FO Monomode. La distància d'aquestes fibres és inferior a 500 metres.

- 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.

- Serveis in-situ.

4.1.2 Requeriments equipament

4.1.2.1 Fabricant

- El sistema es considera molt crític per a l'interès de l'hospital i es requereix fabricant classificat en el quadrant de líders en el darrer informe (desembre 2022 en el moment d'escriure aquests plecs) de Gartner "Magic Quadrant for Network Firewalls".
- El sistema es muntarà en cadena amb el sistema ja existent de protecció interna, i es desitja garantir protecció de doble fabricant, de manera que **no es permeten** equips del fabricant del sistema intern actual, Fortinet.

4.1.2.2 Arquitectura

- Solució de Nova generació (NGFW) que protegeix d'amenaces de dia zero:
  - Anàlisi profund de webs, fitxers, atacs no prèviament coneguts.
  - Base de dades de webs, fitxers i atacs ja analitzats.
  - Inclou detecció d'atacs altament evasius.
  - Desplegament de noves signatures en temps real.

- Aplicació de polítiques de seguretat via capa 7:
  - Anàlisi continu de confiança per usuari, aplicació i dispositiu.
  - User-ID, App-ID, Device-ID integrats com a base del model de gestió.
  - Reconeixement automàtic d'aplicacions.
  - Protecció sense afectació al rendiment.
  - Procés paral·lel en una sola passada.

- Es requereixen equips físics per a la funció de gateway de dades:
  - 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 1 unitat de Rack.
  - CPUs dedicades a configuració, logging i reporting independents de les CPUs dedicades a procés de seguretat.

  - Per a funció sandbox és permet l'ús de recursos del fabricant en el núvol.

- Possibilitat de configuració dels equips en mode sniffing, transparent, capa 2, i routing capa 3.

- 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 d'integració amb altres sistemes gestors d'identitats i gestors d'infraestructures per recollir informació, identificacions i inventaris.
  - Integració amb directori actiu per aplicació de polítiques basades en usuari.
  - Integració amb Directori Actiu per validació de connexions externes, túnels ipsec i https.
  - Integració amb sistemes radius per gestió de la doble validació en l'autentificació.
  - Compatibilitat amb sistema de doble factor existent Fortinet FortiAuthenticator.
  - Publicació de portal captiu sol·licitant usuari autoritzat pels intents de connexió que realitzin usuaris no autoritzats.
  - Integració amb mòduls HSM de tercers per a l'emmagatzematge de claus criptogràfiques.

- Totes les funcions de xarxa apropiades:
  - Routing OSPF, BGP
  - PIM sparse mode
  - NAT
  - IEEE 802.1Q
  - PPPoE
  - 802.3ad
  - Multicast
  - Jumbo frames
  - Suport de IPv6 amb les mateixes funcionalitats que IPv4
  - Altres prestacions habituals

- Suport de
  - 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.
  - Anàlisi de tràfic https.
    - Intercepció d'aquest tràfic per poder aplicar les funcionalitats del firewall.
    - Compliment normatiu: capacitat de configuració de quin tràfic s'analitza i quin no, que com a mínim permeti evitar interceptar el tràfic privat del tipus "ciutadà – organismes públics", "ciutadans – bancs", ... i similars.

- Arquitectura gestió
  - Suport a RBAC (Role Based Access Control). Perfils per a gestió diferenciada i delegada.
  - Administració tant via entorn CLI com via entorn Web.

- Funcions d'administració i de recol·lecció de logs en equips completament independents.
- Per a les funcions d'administració i recol·lecció de logs es permeten equips virtualitzats instal·lats in-situ a l'hospital.
- Es permet la utilització del núvol per a les funcions de sandbox.
- Accés via SNMP per control de disponibilitat i capacitat.

- 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.

4.1.2.3 Funcionalitats

- Es requereix
  - Prestacions de xarxa gestionades pel Firewall.
  - Prestacions SDWAN.

  - Visibilitat i control d'aplicacions. Polítiques i regles per aplicació.
  - Integració i identificació d'usuaris. Polítiques i regles per usuari.
  - Polítiques i regles per dispositiu.
  - Polítiques i regles segons horari o calendari.

  - Protecció davant d'atacs de denegació de servei
  - Protecció davant vulnerabilitats
  - Protecció davant software maliciós. Inclou sandboxing.

  - Filtratge d'URLs
  - Seguretat DNS
  - Protecció de dades sensibles (DLP), encara que no necessàriament llicenciat.

  - Detecció i prevenció d'amenaces en dispositius IoT

  - VPNs sobre IPSEC i sobre SSL

- Prestacions de xarxa gestionades pel firewall
  - Policy Routing
  - QoS per aplicació, usuari o URL

- Prestacions SDWAN
  - Capacitat de creació d'overlay per a connectar seus remotes sense equipament addicional
  - Capacitats d'autoprovisionament
  - Best Path selection
  - QoS
  - Link Status

- Control d'aplicacions. Polítiques i regles de gestió per aplicacions.

- El tràfic s'analitzarà a nivell 7. El motor de classificació que s'utilitzarà per identificar el trànsit serà en base a l'aplicació (nivell 7 de la pila TCP), i no només el port. Així, l'aplicació no ha de formar part d'un filtre que s'apliqui posteriorment, sinó que ha de ser l'element d'identificació inicial i basar la resta de l'anàlisi en el seu context.
- Identificació de totes les aplicacions habituals. Capacitat per identificar i controlar, de manera nativa, sense llicències ni mòduls addicionals que puguin afectar al rendiment, un mínim de 3.600 aplicacions actives actuals (com ara, Webex, Sharepoint, Whatsapp, Facebook, Spotify, Teams, Bit Torrent, SAP, Oracle, GMail, Last.Fm...).
- 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 independent del port que facin servir. Identificació d'intents de simulació d'una aplicació que no és.
- 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 concretes.
- Control granular de les diferents funcionalitats dins de les aplicacions. Identificar aspectes com transferències de fitxers, correu electrònic, xat...
- Identificació de l'intercanvi de fitxers efectuat dins de les aplicacions.
- Creació de signatures específiques per a aplicacions personalitzades.
- Identificació i suport de tràfic VoIP.
- Identificar, classificar i gestionar sistemàticament el trànsit desconegut. La solució ha de ser capaç d'identificar el trànsit desconegut, categoritzar-lo per a la seva anàlisi i gestionar-lo en base a polítiques. A més, ha de ser possible prendre captures PCAPs automàticament del trànsit desconegut, així com generar signatures personalitzades per identificar-lo en cas que sigui trànsit desitjat.

- Polítiques i regles de gestió per usuaris.
  - Polítiques per usuari, independents de la ubicació i del mecanisme d'identificació.
  - Identificació d'usuaris transparent a través de la integració amb directoris LDAP, incloent-hi l'Active Directory de Microsoft.
  - Utilització d'usuaris i grups de Directori Actiu en les regles d'autorització de tràfic.
  - API XML per a la identificació d'usuaris, que permetrà injectar usuaris après des d'altres sistemes, facilitant així la integració amb altres mecanismes d'autenticació via scripting (com ara, sistemes 802.1x, Radius, …).
  - El Sistema de Seguretat integrarà un recopilador de syslog (tant TCP com UDP) per poder aprendre usuaris que han estat validats en altres sistemes d'autenticació. Aquesta funcionalitat permetrà als administradors redirigir els esdeveniments de syslog d'autenticació contra el servei de syslog del Sistema de Seguretat, que comptarà amb un sistema de parsing automàtic dels logs per extreure i aprendre d'aquests la tupla usuari-IP. Aquest mecanisme permet integrar les funcions d'identificació d'usuaris pràcticament de manera transparent amb qualsevol sistema d'autenticació que generi esdeveniments de syslog.
  - Serveis d'autenticació basada en LDAP (incloent NTLM), Kerberos (inclosa la funció de Single Sign On), Radius i base de dades local al Sistema de Seguretat per als accessos VPN i per a l'accés a aplicacions.
  - Capacitat d'integració nativa amb serveis d'autenticació MFA (Okta, PingID, RSA, Duo...).
  - Possibilitat de connectar els firewalls a un servei central d'autenticació al núvol que integri tots els sistemes d'autenticació de l'organització, evitant haver de configurar tots aquests sistemes en tots els firewalls.

- Capacitat d'utilitzar MFA per a l'accés VPN d'un, diversos o tots els usuaris.
- Capacitat per crear grups dinàmics amb membres actualitzats a través d'una API XML.

- Protecció Dos.
  - Detecció i mitigació d'atacs de DoS. S'ha de comptar almenys amb els següents tipus de protecció: SYN Flood, UDP Flood, ICMP Flood, protecció davant d'inundacions per noves sessions o protecció per atacs de desbordament per límits de sessions establertes, essent possible en cada cas establir els llindars necessaris per activar aquestes proteccions.
  - Capacitat de llistes d'IPs malicioses ofertes pel fabricant, que s'actualitzin i mantinguin automàticament i es posin a disposició per a l'ús al firewall de manera nativa.

- Protecció davant vulnerabilitats
  - S'han de poder aplicar polítiques tant de detecció com de prevenció (mode IDS o IPS) davant possibles exploits de vulnerabilitats que es detectin en el trànsit ja sigui entrant o sortint d'Internet, realitzant l'anàlisi en una única passada per a tot tipus d'amenaces.
  - En la protecció davant de vulnerabilitats, el criteri a utilitzar és la identificació de l'aplicació per poder aplicar perfils de vulnerabilitats ajustats a aquesta aplicació, de manera que no es vegi afectat el rendiment de l'equip.
  - Els perfils de detecció i protecció davant de vulnerabilitats han de permetre aplicar-se tant al trànsit originat des de la xarxa interna com al trànsit originat des d'Internet, i ha de ser possible l'aplicació de detecció i protecció davant de vulnerabilitats especificant si són vulnerabilitats que s'apliquen als clients, als servidors o a ambdós indistintament.
  - Les vulnerabilitats han d'estar categoritzades per tipus i per nivells de risc, de manera que l'aplicació de perfils de protecció en el trànsit es pugui realitzar en base a aquestes categories.
  - S'ha de poder usar la identificació CVE de vulnerabilitats per a l'aplicació de perfils de protecció específics.
  - Ús de la identificació d'aplicacions com a criteri per seleccionar els perfils de protecció de vulnerabilitats, de manera que s'apliquin només aquelles signatures específiques segons l'aplicació que s'està utilitzant.
  - Capacitat de creació de signatures de IPS a partir de la informació d'una signatura de Snort i s'ha de permetre importar de manera automàtica un llistat de regles de Snort.
  - Suport en línia de Deep Learning i anàlisi al núvol.
  - Prevenció de Command and Control desconegut basat en Machine Learning des del núvol.

- Protecció davant software maliciós
  - 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.
  - S'han de poder aplicar polítiques que permetin aplicar el motor d'antivirus sobre protocols com ftp, http, imap, pop3, smb/cifs o smtp, definint per a cadascun d'aquests protocols l'acció a realitzar (permetre els fitxers, descartar els fitxers, desconnectar la sessió o registrar mitjançant logs) davant la detecció del fitxer maliciós pel motor d'antivirus.
  - El tallafocs ha de permetre l'aplicació de polítiques d'antivirus de manera granular, permetent, per exemple, l'aplicació d'aquestes polítiques a certs usuaris de determinats grups o a certs segments de xarxa amb determinat direccionament o a certes aplicacions.

- El mòdul d'antimalware ha de disposar d'un motor d'anàlisi estàtic basat en algorismes de Machine Learning que permetin identificar mostres malicioses desconegudes en temps real sense necessitat de haver d'esperar al veredicte del mòdul de Sandboxing.

- 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.
  - Els fitxers desconeguts s'identifiquen al tallafocs i s'envien al sistema de detecció de malware al núvol segons l'aplicació, el tipus de fitxer, la direcció del flux o l'usuari.
  - El sistema d'anàlisi d'amenaces al núvol ha d'estar ubicat a la Unió Europea, i ha d'acreditar el compliment de les normatives europees en matèria de protecció de dades.
  - El sistema de detecció al núvol ha d'executar el fitxer enviat utilitzant una sandbox virtual per determinar qualsevol comportament maliciós. El sistema també ha de ser capaç de generar signatures automàticament basades en l'activitat observada i distribuir-les als tallafocs.
  - L'administrador del Sistema de Seguretat ha de ser capaç d'accedir a aquesta sandbox per veure l'estat dels fitxers inspeccionats, així com també pujar fitxers manualment a la mateixa.
  - S'han d'inspeccionar com a mínim fitxers EXE, DLL, PDF, APK, Java, Office de Microsoft, Mach-O i DMG de OS-X.
  - Inspecció de fitxers de script JScript, VBScript i PowerShell Script.
  - Gestionar la confidencialitat de manera que sense pujar fitxers a la sandbox, es puguin rebre, de manera contínua, les noves defenses.
  - La Sandbox ha de disposar de certificacions oficials d'organismes de defensa o països OTAN (SOC2, FedRAMP...).
  - Temps de resposta del servei Sandbox màxim de 5 minuts.
  - El servei de sandbox ha de proporcionar algoritmes d'anàlisi estàtics dels fitxers executables i scripts de PowerShell utilitzant Machine Learning que permetin donar veredictes en temps real per a la majoria de les mostres desconegudes. Aquest algoritme d'anàlisi estàtic ha d'analitzar patrons en els fitxers com el compressor utilitzat, l'assemblador, entropia, i altres característiques estàtiques del fitxer.

- Filtratge d'URLs. Classificació incorporada i automatitzada del tràfic de navegació web.
  - Capacitat de realitzar el filtratge per URL o per categoria d'URL. S'oferirà un sistema de filtratge que inclogui la categorització d'URLs per part del fabricant, així com la seva actualització automàtica. S'inclourà també un mecanisme per poder sol·licitar canvis en la categorització de les URLs.
  - Possibilitat de configurar el filtre de URL multicategoria, és a dir, categoritzar una URL fins a 4 categories diferents basades en el seu contingut, el domini al qual pertany, etc., i així poder establir polítiques que permetin l'accés però limitin les possibilitats de navegació.
  - Disposar d'un motor d'anàlisi estàtic basat en algoritmes d'aprenentatge automàtic que sigui capaç de prevenir l'accés a URLs de phishing i la descàrrega de fitxers JavaScript desconeguts en temps real en el moment que passen pel tallafoc i sense haver d'esperar pel veredicte del mòdul de sandboxing.
  - Ha de suportar la inspecció o no del trànsit xifrat SSL basant-se en aquestes categories.
    - Desxifrat de trànsit SSL i SSH sobre qualsevol port.
    - Capacitat per identificar les aplicacions reals dins dels túnels SSL.

- Ha de tenir la possibilitat de bloquejar les sessions SSL que no es poden desxifrar o aquelles amb certificats de servidor no fiables.
- Suport de desxifrat de trànsit TLS1.3 i HTTP/2, incloent un registre dedicat per a aquest trànsit, facilitant així el seu anàlisi.
- Suport de categorització en línia basat en Deep Learning i lliurat des del núvol.
- Expansió de la inserció de la capçalera HTTP.
- Anàlisi de dominis basat en Machine Learning.
- Motor per a desofuscar java-script.
- Motors d'anàlisi estàtic i dinàmic.
- Anàlisi recursiva de Deep Learning.

- Filtratge DNS
  - Capacitat per detectar i prevenir de manera automàtica i dinàmica les sol·licituds DNS malicioses associades amb dominis de malware, a les quals el tallafocs ha de respondre automàticament amb una IP falsa en lloc del servidor autoritatiu (DNS sinkholing). La base de dades de dominis maliciosos ha d'estar alimentada per les següents fonts:
    - Sistema de sandbox per trobar nous dominis C2 (Command & Control).
    - DNS passius i telemetries.
  - El servei que gestioni els veredictes dels dominis DNS ha d'estar al núvol per assegurar que el nombre de dominis gestionats sigui il·limitat i pugui escalar-se. Aquest servei eliminarà la necessitat de gestionar actualitzacions dinàmiques al tallafocs.
  - Ha de tenir la capacitat per detectar atacs basats en DNS:
    - Atacs que utilitzen Algorismes de Generació de Dominis (DGA)
      - Els DGA són programes integrats en el malware per generar ràpidament quantitats massives de noms de domini que el malware utilitza per rebre instruccions o robar dades (generalment anomenats "comandament i control" o C2).
      - Els atacants utilitzen DGA per poder canviar ràpidament els dominis que estan utilitzant per als atacs de malware. Els atacants fan això perquè el programari de seguretat i els proveïdors actuen ràpidament per bloquejar i eliminar dominis maliciosos que utilitza el malware. Els atacants van desenvolupar DGA específicament per contrarestar aquestes accions.
      - En el passat, els atacants mantenien una llista estàtica de dominis maliciosos; els defensors podien fàcilment prendre aquesta llista i començar a bloquejar i eliminar aquests llocs. En utilitzar un algorisme per construir la llista de dominis, els atacants també fan que sigui més difícil per als defensors saber o predir quins dominis s'utilitzaran que si tinguessin una llista simple de dominis. Per obtenir aquesta llista de dominis que utilitzarà el malware, els defensors han de descodificar l'algorisme, la qual cosa pot ser difícil.
      - Molts DGA estan dissenyats per utilitzar centenars o fins i tot milers de dominis. I aquests dominis solen estar actius només per períodes de temps limitats.
    - Atacs que encapsulen túnels de comandament i control en trànsit DNS
      - El trànsit DNS cap a Internet es permet en totes les organitzacions per poder tenir accés a recursos a Internet. Els atacants poden "camuflar-se" com consultes DNS vàlides i amagar les seves accions en petits "fragments" que semblen ser part del flux normal de DNS.
      - Els atacants aconsegueixen dividir les seves instruccions en fragments de mida molt petita que es poden integrar en un trànsit aparentment vàlid. Aquests

fragments després es llegeixen al destí i es torna a muntar aquests fragments en una llista completa d'instruccions per a la següent etapa de l'atac.

- El túnel de DNS també es pot utilitzar per "fragmentar" dades confidencials i extreure-les lentament de l'organització en sol·licituds DNS vàlides, que seran muntades posteriorment al costat de l'atacant.
- La identificació del túnel DNS requereix inspeccionar el trànsit DNS en temps real amb anàlisi profund.

- Dominis de Retorn (Callback Domains)
  - Malware i dominis C2.
  - Prevenció d'amenaces de DNS en l'ús de servidors intermediaris de xarxes de bots basades en DNS.
  - Dominis de flux ràpid.
  - DGA aleatoris.
  - DGA de diccionari: Detecció i prevenció d'atacs basats en dominis maliciosos que utilitzen paraules conegudes.
- Dominis d'Alt Risc (High Risk Domains)
  - Grayware.
  - Dominis registrats recentment.
  - Dominis estacionats.
  - Evitació de servidors intermediaris.
  - DNS dinàmic.
  - Detecció predictiva.
  - Dominis caducats de manera estratègica.
- Atacs als Registres DNS
  - Domain Squatting.
  - Dangling DNS.
  - Zones DNS compromeses.
  - Wildcard DNS.
  - Camuflatge CNAME.
- Atacs basats en el protocol DNS
  - Reversió DNS.
  - Atac NXNS.
- Canals encoberts
  - Tunelització DNS.
  - Tunelització DNS molt lenta.
  - Infiltració de DNS.
  - Detecció i prevenció de tunels C2 basats en DNS amb moviment lent.

- DLP Prevenció de pèrdua de dades (no necessàriament llicenciat)

- Es requereix que els tallafocs disposin de la possibilitat de **contractar en el futur** un servei de DLP en un format al núvol i que cobreixi el moviment de fitxers a través del tallafocs.
    - El servei de DLP ha d'estar integrat nativament al firewall sense necessitat de desplegar ni configurar equips addicionals.
    - Suport de DLP basat en fitxers.
    - S'ha de gestionar l'inventari de documents classificant-los automàticament en funció de la seva tipologia mitjançant algoritmes de machine learning.
    - S'han de poder realitzar les accions de resposta necessàries per assegurar que es redueixin al màxim els riscos d'extracció i exposició de les dades.
- Es requereix que els tallafocs tinguin, de manera nativa, capacitat de controlar quin tipus de fitxers circulen per la xarxa, inclosos els fitxers comprimits.
- Es requereix capacitat de controlar els fitxers en funció del seu tipus i de pujades i baixades basant-se en el context de l'aplicació (per exemple, no poder pujar fitxers a aplicacions de correu, però sí a aplicacions de compartició de fitxers).
- Registre d'informació rellevant. Filtratge de les connexions a registrar.

- Detecció i Prevenció d'amenaces en dispositius IoT. S'ha de permetre als tallafocs:
    - Funcionalitat aportada pel mateix fabricant dels equips principals, amb suport de fabricant integrat.
    - La solució d'IOT aportarà les següents integracions:
        - Integració amb SCCM, d'on recollir tota la informació registrada.
        - Integració amb switchos i APs Cisco, inclosa la informació CDP i LLDP.
        - Integració amb SNMP, per saber a quin switch i port estan connectats els equips.
        - Integració amb Cisco Wireless Lan Controllers per integrar la informació recollida.
    - Manteniment d'un inventari, avaluació del risc i control de les amenaces als dispositius IoT a partir del trànsit que es veu als mateixos tallafocs i en una sonda addicional incorporada expressament per a la funció.
    - Descobrir un inventari de dispositius IoT instal·lats, identificant el tipus de dispositiu, fabricant i model.
        - Analitzar fins a 200 paràmetres de cada equip connectat per establir tipus, proveïdor i model, quedant cada equip completament perfilat.
        - Avaluació dels riscos específics de cada dispositiu, permeten aplicar polítiques que només permetin els fluxos autoritzats.
    - Avaluació de riscos de cadascun dels dispositius a partir del comportament que tenen, comparant-lo amb el comportament normal dels mateixos.
    - Detecció de possibles anomalies en el comportament de xarxa dels dispositius a partir d'una línia base de xarxa.
    - Detecció i visibilitat d'amenaces desconegudes als dispositius IoT a partir del seu comportament en xarxa.
    - Prevenció d'amenaces conegudes als dispositius IoT.
    - Possibilitat de crear polítiques als tallafocs utilitzant la informació d'inventari descoberta (tipus de dispositiu, fabricant i model).

- 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.

4.1.2.4 Gestió i reporting

- Gestió i reporting via consola gràfica, que resulti intuïtiva, amigable, i poc propensa a errors.
- Llicència per a un mínim de 25 dispositius.

- Actualitzacions
    - Actualitzacions automatitzades dels continguts de seguretat: actualització automatitzada de signatures i patrons IDS i IPS, classificació urls, adreces de xarxes TOR o de proxis anònims, classificació DNS, tràfic privat usuaris (bancs, organismes públics), xarxes botnets, identificació d'aplicacions, signatures antivirus, "checksums de fitxers malware", reputació anti-spam.
    - Disponibilitat de les noves versions que es vagin publicant en el període subscrit.

- Accés:
    - Accés via https i via CLI.

- Gestió de la configuració:
    - Funcionalitats integrades al tallafocs: les capacitats de gestió, administració, gestió de registres i informes han de ser components natius al tallafocs, sense necessitat d'adquirir altres elements de maquinari o programari per disposar d'aquestes funcionalitats.
    - Auditoria de configuracions, incloent la cerca de diferències entre diferents fitxers de configuració.
    - La solució de gestió ha de ser capaç de correlacionar automàticament esdeveniments desconnectats que quan es reuneixen al llarg d'un període de temps per a un mateix equip o usuari indiquen que aquest equip ha estat probablement compromès. Per exemple, una vulnerabilitat des d'un kit d'explotació, juntament amb un accés posterior a un domini maliciós que acaba finalment amb una descàrrega de programari maliciós, ha de generar un esdeveniment correlacionat que indiqui el compromís, a més dels tres esdeveniments individuals.
    - La solució ha de suportar informes totalment personalitzables per a tots els registres sobre l'equip mateix (sense necessitat, per tant, d'utilitzar un equip secundari per a aquestes tasques).
    - Utilitzant les funcionalitats incloses al dispositiu, els administradors han de ser capaços de generar informes personalitzats. A més, ha de ser possible extreure tant els informes predefinits com els personalitzats mitjançant una API XML, que permetrà la integració amb sistemes externs.
    - La solució ha de ser capaç de realitzar de manera automàtica una anàlisi del comportament diària, basada en tots els registres, a la recerca d'equips que puguin formar part de botnets desconegudes. El resultat serà un informe que inclourà totes les màquines susceptibles d'haver estat reclutades per a noves botnets, així com els comportaments que han tingut i que les fan considerar infectades.
    - Disponibilitat de mapa geogràfic per identificar l'origen i destí dels fluxos i amenaces que entren i surten de la xarxa.
    - Capacitat per consumir indicadors de compromís de tercers i incorporar-los automàticament als tallafocs. S'han de poder consumir com a mínim llistes d'IP, URLs i DNS.

- Tant la interfície gràfica com la documentació oficial del producte (guia d'usuari) han d'estar disponibles com a mínim en castellà.
- Eina del fabricant que faciliti la posada en marxa dels següents escenaris:
  - Migració: possibilitat de "traduir" fitxers de configuració de tallafocs Paloalto, Cisco, Checkpoint, Fortinet, Forcepoint, a polítiques de capa 7. Un cop traduïts, podem seleccionar quines polítiques ens interessa exportar al tallafocs.
  - Greenfield: per desplegaments des de zero, deixant inicialment una política de any-any allow i mitjançant mecanismes d'aprenentatge automàtic, identificar totes les aplicacions i proposar polítiques basades en el comportament i ús d'aquestes aplicacions.
- Eina d'optimització de polítiques integrada al tallafoc, de manera que ens guiï i faciliti la millora de les configuracions basades en regles no utilitzades, polítiques a modificar segons l'ús de les aplicacions, etc.
- Poder programar en el temps des de la consola l'enviament de configuracions als tallafocs.
- Actualitzacions automàtiques, programables, per a les signatures d'aplicació, IPS, Antivirus i AntiSpyware.
- Millora de les operacions mitjançant coneixement basat en l'aprenentatge automàtic per a un millor perfil de seguretat i per evitar errors humans en la configuració.
  - Prediccions basades en l'aprenentatge automàtic i detecció d'anomalies.
  - Recomanacions de configuració basades en les millors pràctiques.
  - Creació de tiquets de manera automàtica i senzilla.
  - Alertes de manera proactiva sobre l'estat de salut i la seguretat del NGFW.
  - Avís sobre vulnerabilitats conegudes de programari, fi de vida i caducitat de llicències.
  - Visualització i informes sobre l'eficàcia de la seguretat.
- La solució proposada ha de disposar de mecanismes que injectin automàticament, en els firewalls, llistes dinàmiques provinents de bases de dades de tercers (per exemple, serveis anti-phishing, llistes de dominis maliciosos, serveis antispam, serveis d'identificació de nodes TOR, avisos de CERTs, etc.). Aquestes fonts han de ser rebudes de manera automàtica, processades i injectades en els firewalls a través de STIX, TAXI, JSON, llistes dinàmiques, etc., sense intervenció humana.
- Capacitat de gestió totalment integrada tant de la sonda IOT com dels equips perimetrals.

4.1.2.5 Dimensionament mínim

Capacitat	Requeriments
Nombre màxim de **sessions** concurrents: (valor mínim)	1,4 milions
Connectivitat (mínim per equip)	12 x 10/5/2,5/1 Gb RJ45 10 x 10/1 Gb SFP+ 4 x 25/10/1 Gb SFP28 1 x 1 Gb RJ45 gestió 2 x 1 Gb alta disponibilitat 1 x consola RJ45 1 x micro-USB
Disc mínim, redundat, per equip	480 GB SSD
Instàncies multidomini (firewalls virtuals) (mínim llicenciat)	11
Òptiques incorporades, per equip	2 òptiques SFP 10G LR per a fibra monomode 2 òptiques SFP 10G SR per a fibra multimode. 2 òptiques SFP28 25G per a fibra multimode.

Rendiment (Valors nominals mínims en condicions de laboratori)	Valor mínim
Nombre màxim de sessions	1.400.000
Nombre màxim de **noves sessions per segon**: (valor mínim)	145.000
Rendiment amb control nivell 7 i control per aplicacions	9,5 Gbps
Rendiment IPS + control d'aplicacions + motor antimalware	5,8 Gbps
Throughput de VPN IPSEC: (valor mínim)	5,6 Gbps

Sonda addicional IOT fora de línia	Requeriments
Llicència	Segons funcionalitat requerida
Connectivitat (mínim per equip)	8 x 5/2,5/1 Gb RJ45 4 x 1 Gb RJ45 10 x 10/1 Gb SFP+ 1 x 1 Gb RJ45 gestió 2 x 1 Gb alta disponibilitat 1 x consola RJ45
Òptiques incorporades, per equip	4 òptiques SFP+ 10 Gb multimode

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

La configuració a implantar activarà totes les funcionalitats indicades, excepte la funcionalitat DLP, que com s'ha indicat no requereix ni llicenciament ni implantació inicial.

4.2 Especificacions dels serveis

4.2.1 Abast dels serveis

4.2.1.1 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 per al funcionament normal de l'hospital.

Segueixen especificacions més detallades dels punts enumerats.

4.2.1.2 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.

4.2.1.3 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 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.
  - Utilització d'eines de migració, i revisió manual per evitar dificultats.
  - Elaboració d'un joc de proves de validació del funcionament, que inclogui la validació de les funcionalitats crítiques per a l'hospital.
- 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.

4.2.1.4 Posada en funcionament

- Posada en funcionament amb el mínim tall de servei possible.
  - En el moment de la posada en funcionament execució d'un joc de proves que confirmi el funcionament de les necessitats més crítiques de l'hospital i l'efectivitat de la solució.
- 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 la posada en funcionament amb un pla de proves.
  - La validació de la posada en funcionament inclourà la realització d'un pla de proves elaborat prèviament que confirmarà el funcionament de totes les prestacions que es considerin crítiques. Si no s'aconsegueix la correcta execució del pla de proves en el termini pactat prèviament s'executarà el pla de tornada enrere i es repetirà l'operació un cop solucionades les dificultats.
- 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.

4.2.1.5 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.

4.2.1.6 Manteniment reactiu

4.2.1.6.1 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.
- Els serveis de 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, conductius i evolutius no estan inclosos en aquesta licitació, excepte les actualitzacions de firmware, que l'hospital podrà sol·licitar de forma justificada.

4.2.1.6.2 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.
- S'inclouen tots els aspectes: hardware, software i configuració.
- S'inclou la substitució del hardware avariat.
- 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.

4.2.1.6.3 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.

4.2.1.6.4 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.

4.2.1.7 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	Esforç continuat fins a la resolució
	Penalització per cada hora de retard en el temps de resposta o resolució d'una incidència.	30€
	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.	30€
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	30€
Límit màxim de penalitzacions		
	L'import màxim de possibles penalitzacions	10% de l'import d'adjudicació contracte

4.2.2 Condicions dels serveis

4.2.2.1 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

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

4.2.2.2 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.

4.2.2.3 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.

4.2.2.4 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.
- La valoració dels serveis inclourà un **mínim de 10 jornades** d'implementació.

4.2.2.5 Coneixement especialitzat

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

4.2.2.6 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.

4.2.2.7 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.

4.2.2.8 Calendari

- El calendari laboral utilitzat serà el de Barcelona.

4.2.2.9 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 del contractista (llicències, línies, maquinari, programari, ...) no suposaran cap cost addicional per a l'Hospital.

4.2.2.10 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 a la prestació dels serveis.

4.2.2.11 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.

4.2.2.12 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...

Aquesta contractació es faria per jornades senceres.

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 seguretat cibernètica, amb formació d'enginyer, amb formació especialitzada en els productes oferts, i amb una experiència en l'àrea mínima de 2 anys.

L'hospital no s'obliga a contractar aquests esforços necessàriament via aquest procediment.

4.3 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 <u>processos de compra i instal·lació</u> 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 <u>processos de manteniment</u> 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 <u>report</u> amb la informació:
    - Nombre d’incidències, temps mig de resolució, compliments d’SLA.

5 Signatura

Barcelona, a 11 de juny del 2024,

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 la persona competent.*

***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.*