

PLEC DE PRESCRIPCIONS TÈCNIQUES

**SUBMINISTRAMENT D'EQUIPAMENT DE SEGURETAT PERIMETRAL I SERVEIS PER PROTEGIR ELS ELEMENTS DE TI
HOSTATJATS ALS CENTRES DE PROCÉS DE DADES (CPD) I EQUIPAMENT IOT DE L'HOSPITAL CLÍNIC DE BARCELONA
(HCB)**

EXPEDIENT 2026-155

Índex

1	PRESENTACIÓ.....	3
1.1	Objecte i necessitat.....	3
1.2	Abast.....	3
1.3	Característiques de les empreses licitadores.....	3
2	SOLUCIÓ ACTUAL OBJECTE DE SUBSTITUCIÓ I CONTEXT.....	3
3	DESCRIPCIÓ DEL SUBMINISTRAMENT.....	4
3.1	Condicions d'enviament i recepció.....	5
3.2	Requeriments generals.....	5
3.3	Requeriments de la solució NGFW.....	6
3.4	Requeriments de la solució per a la gestió i operació del NGFW.....	6
3.5	Requeriments de la solució per a la sonda IOT.....	6
3.6	Garantia i manteniment de les solucions.....	7
4	SERVEIS PROFESSIONALS.....	7
4.1	Disseny i planificació.....	7
4.2	Operatives de sistemes.....	8
4.3	Desplegament de les solucions NGFW i de gestió, operació i recollida de logs.....	8
4.4	Desplegament de la solució IoT.....	9
4.4.1	Serveis gestionats IoT.....	10
4.5	Manteniment i suport avançat.....	10
4.5.1	Condicions generals.....	10
4.5.2	Manteniment i suport reactiu/correctiu.....	11
4.5.3	Manteniment i suport preventiu i evolutiu.....	11
4.5.4	Assessorament tècnic i suport d'administració avançada.....	12
5	TRANSFERÈNCIA DE CONEIXEMENT.....	12
5.1	Documentació.....	12
5.2	Formació.....	13
6	OFERTA TÈCNICA A LLIURAR.....	13
6.1	Solució proposada.....	13
6.2	Equip de projecte i metodologia.....	13
6.3	Proposta de serveis professionals.....	14
6.4	Traspàs de la instal·lació a la gestió continuada.....	14
	ANNEX 1 – DECLARACIÓ RESPONSABLE DEL COMPLIMENT DELS REQUERIMENTS.....	15
	ANNEX 2 – FORMULARI DE PRODUCTES HARDWARE, SOFTWARE, LICÈNCIES I MANTENIMENTS QUE S'INCLOURAN EN EL SUBMINISTRAMENT.....	17
	ANNEX 3 – CLÀUSULA DE SEGURETAT DE LA INFORMACIÓ.....	18

1 PRESENTACIÓ

1.1 Objecte i necessitat

L'objecte d'aquest plec és l'adquisició d'una solució de seguretat perimetral pels CPDs de l'HCB així com una sonda IOT, incloent hardware, llicenciament, aplicacions i serveis professionals associats.

La necessitat és substituir la solució actual degut a que entrarà en el seu fi de vida durant el proper any 2027 i dotar d'una sonda IOT que permeti visualitzar i gestionar la seguretat d'aquest tipus de dispositius.

1.2 Abast

L'abast d'aquesta licitació ha d'incloure:

- El subministrament de tot l'equipament, programari, subscripcions i qualsevol altre material o component necessari.
- Servei gestionat per a la solució IOT.
- Garantia, manteniment i suport.
- Gestió i seguiment del projecte.
- Migració de la solució actual a la nova.
- Anàlisi i optimització de polítiques.
- Disseny, planificació i desplegament de millores.
- Documentació.
- Formació.

La solució proposada haurà de complir els requisits tècnics mínims i imprescindibles recollits a l'Annex 1 d'aquest Plec. Tots els requisits inclosos en l'Annex 1 tenen la consideració de requisits mínims d'obligat compliment.

1.3 Característiques de les empreses licitadores

Per tal de garantir nivells de qualitat elevats en l'execució del projecte i posteriors serveis de manteniment i suport, les empreses licitadores hauran de complir i acreditar els següents requisits:

- Relació de partnership de màxim nivell amb el fabricant de l'equipament presentat.
- Disposar d'un mínim de 1 tècnic amb la màxima certificació que atorgui el fabricant de l'equipament presentat i que tingui possibilitat d'acudir a l'HCB en un màxim de 2 hores en cas d'incidència greu.
- Disposar d'un mínim de 3 tècnics certificats en la tecnologia presentada amb capacitat d'acudir a l'HCB en un màxim de 2 hores en cas d'incidència greu.
- Disposar d'un mínim de 1 tècnic amb certificació CCSE (Check Point Security Expert) o superior associada a l'equipament actual objecte de substitució en aquest plec.
- Complir amb la clàusula de seguretat de la informació descrita a l'annex 3 d'aquest PPT.

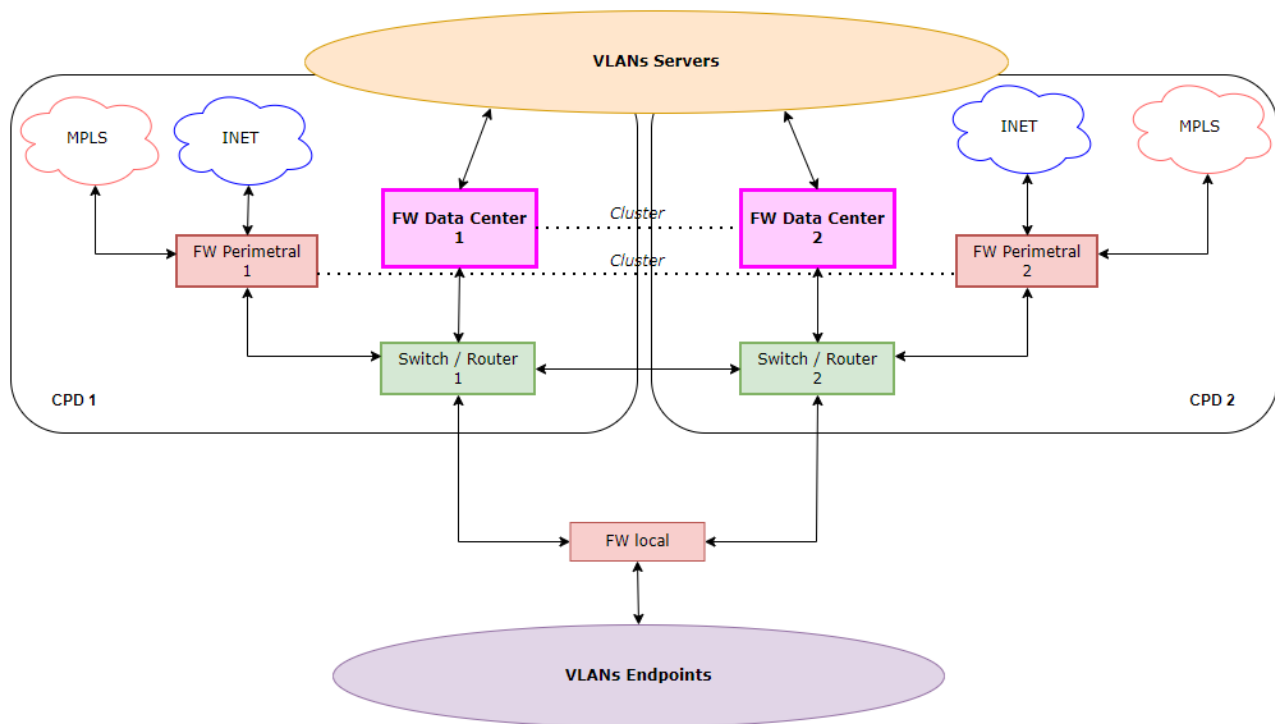
Tots aquests requeriments hauran de ser presentats. En el cas de les certificacions exigides en els punts anterior, aquestes hauran de ser presentades al sobre B.

2 SOLUCIÓ ACTUAL OBJECTE DE SUBSTITUCIÓ I CONTEXT

La solució de seguretat perimetral de Data Center actual està formada per una parella d'equips Checkpoint funcionant en alta disponibilitat actiu-passiu. La solució inclou dos servidors auxiliars en format virtual:

Servidor 1: Consola de gestió i logs d'activitat (SmartConsole).
 Servidor 2: Integració amb directori actiu (Identity Collector).

A nivell general l'arquitectura de xarxa dels Firewall de Data Center en relació amb els elements que ha de protegir i el seu encaix amb els principals elements de xarxa de l'Hospital és el següent:



Presenta una arquitectura en alta disponibilitat utilitzant 2 equips, cadascun dels quals està ubicat en un dels 2 CPDs de l'HCB formant un clúster actiu-passiu.

- La connectivitat entre elements de diferents CPDs es fa mitjançant FO monomode en distàncies inferiors a 1 Km.
- La connectivitat dels elements ubicats dintre del mateix CPD es fa mitjançant fuetons de FO multimode.
- Cadascun dels elements "Switch / Router" en cada CPD està format per dos equips físics, les connexions entre aquest elements i els firewalls es realitzen per agregació d'enllaços repartits en els dos equips.

A nivell de volumetria, el Firewall de Data Center té configurades aproximadament 2.500 polítiques i gestiona el nivell 3 de 70 xarxes IP diferents.

3 DESCRIPCIÓ DEL SUBMINISTRAMENT

El subministrament ha d'incloure el hardware, el software, el llicenciament i tots els elements addicionals necessaris per la posada en servei, així com els serveis professionals associats que s'hauran de desenvolupar en el marc del contracte durant el període establert de 5 anys.

Les empreses licitadores han de proposar un conjunt de productes que aportin les darreres millores tecnològiques del mercat, que siguin escalables i integrables en l'equipament de transmissió de dades de l'HCB.

3.1 Condicions d'enviament i recepció

El termini aplicable per fer la recepció de tots els components inclosos en aquest expedient és d'un màxim de 8 setmanes naturals, comptant a partir del dia en que s'ha emès la comanda per part de l'HCB. Les licitadores indicaran el termini de lliurament de tot el material i llicències.

Les ubicacions on es realitzarà la recepció s'acordaran prèviament amb l'HCB. Tots els lliuraments hauran d'anar acompanyats del corresponent albarà, incloent la següent informació:

- Número de comanda.
- Descripció del material.
- Nombre d'unitats que es lliuren.
- Models, números de sèrie i/o adreces MAC.

La recepció dels equips i programaris que formen part d'aquest expedient no es farà efectiva fins que l'adjudicatari no superi la posada en servei a plena satisfacció de l'HCB.

3.2 Requeriments generals

- El subministrament ha d'incloure, com a mínim, els següents components:

1. **Solució NGFW**
2. **Solució de gestió, operació i recollida de logs pels NGFW**
3. **Solució sonda IOT**

A elecció de les licitadores es poden afegir elements, components o solucions addicionals als estrictament requerits en el PPT per tal de donar resposta a alguna de les necessitats plantejades a l'apartat de serveis professionals, en aquest cas caldrà justificar-ho demostrant el valor que aporta al global del projecte, l'HCB no puntuarà per quantitat sinó per qualitat i valor aportat.

- Els tres components imprescindibles anteriorment citats han de ser del mateix fabricant per a facilitar la integració i operabilitat de l'HCB.
- L'equipament i tots els seus components seran totalment nous sense haver estat utilitzats prèviament.
- S'inclourà el llicenciament i subscripcions que cobreixin totes les funcionalitats i requeriments esmentats en aquest PPT durant tot el període contractat.
- Inclourà manteniment de hardware amb suport de fabricant per tot el període contractat.
- Actualitzacions de programari tant per correcció de problemes i vulnerabilitats detectades com per incloure millores evolutives dels productes durant tot el període contractat.
- S'inclourà els mòduls òptics, connectors i cablejat necessari per la posta en servei. Tots els mòduls òptics inclosos seran del mateix fabricant de l'equipament presentat.

El subministrament i desplegament de la solució s'executarà sota la modalitat de "claus en mà", assumint l'adjudicatària la responsabilitat integral de la posada en marxa operativa. Aquesta modalitat inclou obligatòriament:

- **Instal·lació i retirada:** Muntatge físic del nou equipament, així com la desconexió, desmuntatge i retirada de l'equipament substituït (incloent-hi la gestió de residus RAEE segons normativa vigent) i reconexions de cablejat.
- **Migració i desplegament:** Trasllat de configuracions de l'entorn antic al nou i execució tècnica de les millores ofertes pel licitador, així com el desplegament de components auxiliars inclosos dintre de la solució.

- **Posada en servei:** Lliurament de la solució plenament operativa, verificada mitjançant proves de funcionament i amb tota la documentació tècnica de configuració i operació actualitzada.

Els elements a subministrar hauran de complir amb les característiques tècniques establertes a l'annex 1, el no compliment d'algun dels requisits imprescindibles serà motiu d'exclusió.

El licitador detallarà fen ús del formulari que figura a l'annex 2 la relació d'elements que inclou en el subministrament.

3.3 Requeriments de la solució NGFW

Es requereixen 2 equips físics en format appliance, dissenyats específicament per a aquesta funció, no admetent servidors de propòsit general. Presentaran una arquitectura de processament en paral·lel en una sola passada (SP3) per a un alt rendiment alhora que incorpora funcions i innovacions tecnològiques.

La solució proposada ha d'operar en alta disponibilitat amb connectivitat 100 Gbps redundada amb el core de comunicacions de l'HCB, oferint perfils de seguretat avançats i aportar connectivitats d'alt rendiment entre usuaris i aplicacions.

Donada la criticitat de l'entorn de Data Center es requereix que el fabricant proposat aparegui classificat en el quadrant de líders en el darrer informe de Gartner "Magic Quadrant for Hybrid Mesh Firewalls" (agost de 2025 en el moment de la redacció d'aquest plec). Com que el sistema de seguretat perimetral de Data Center licitat es muntarà en cadena amb el sistema de seguretat perimetral per connexions externes existent de Fortinet, no s'admetran solucions del mateix fabricant que ja tenim degut a que es vol garantir protecció de doble fabricant.

3.4 Requeriments de la solució per a la gestió i operació del NGFW

Haurà de proporcionar capacitat per a:

- Gestió centralitzada dels NGFW
- Recol·lecció, emmagatzematge i explotació de logs

Permetent disposar de visibilitat i administració centralitzada oferint una protecció integral dels actius allotjats al Data Center davant incidents de ciberseguretat en temps real.

La solució no podrà estar basada en els recursos hardware dels Firewalls, es requereix independència de hardware per tal que en cap cas una sobrecarrega en la gestió i operació pugui penalitzar el rendiment del pla de dades dels Firewalls destinats a prestar servei. La solució estarà basada en hardware virtualitzat propi de l'HCB.

Es valorarà que la solució es pugui dividir en dos o més components separant la funció de gestió de la funció de processament/emmagatzematge de logs, amb capacitat d'escalabilitat independent, garantint el rendiment en un entorn amb alt volum d'esdeveniments.

3.5 Requeriments de la solució per a la sonda IOT

L'Hospital es vol dotar de capacitats de visió de l'estat dels dispositius IoT (OT/IoT/IoMT) i les vulnerabilitats associades de forma sistemàtica i automatitzada, per la qual cosa es demana un component que aporti aquestes capacitats.

Aquest component es basarà en una sonda integrada en/amb el propi Firewall capaç d'analitzar el tràfic entrant en, com a mínim, tres ports de xarxa amb capacitat de 10 Gbps.

La càrrega de processament associada a les funcionalitats principals de la solució és realitzarà al núvol del fabricant, de manera que el processament requerit per la sonda inclosa al Firewall no penalitzi el rendiment del pla de dades dels mateixos.

L'explotació de les dades recollides i generades per la solució estaran recollides en una aplicació que donarà el fabricant en format SaaS.

3.6 Garantia i manteniment de les solucions

Tots els elements subministrats a la oferta com a resposta a les tres solucions que ha d'incloure la oferta amb caràcter obligatori, definits en el punt 3.2, ha de quedar cobert amb garantia i contracte de manteniment del fabricant durant tota la durada del contracte, quedant inclòs:

- Substitució d'equips: provisió i substitució de l'equip complet o de les peces avariades mitjançant reemplaçament avançat amb una SLA de 24x7xNBD.
- Accés a TAC o servei equivalent de fabricant, tant per part del personal tècnic de l'adjudicatari a càrrec dels serveis professionals com el propi personal tècnic de l'HCBC amb una SLA de 24x7x4.
- Dret a actualitzacions, pegats i noves versions de software tant per la necessitat de resoldre incidències com per evolució.

4 SERVEIS PROFESSIONALS

En aquest apartat es detallen els serveis professionals tant associats a la posada en servei de les solucions incloses en aquesta licitació com a serveis post posada en producció. Aquest servei inclouen el disseny, planificació, gestió de canvis i execució de totes les activitats i tasques necessàries per desplegar les solucions deixant-les plenament productives d'acord a les necessitats i requeriments de l'HCBC, així com els serveis de suport i manteniment post posada en producció.

Totes les configuracions, parametritzacions o aspectes relacionats amb els dissenys i posada en servei en el marc d'aquesta licitació que puguin tenir impacte en qualsevol de les dimensions de la seguretat de la informació hauran de complir de manera obligatòria amb els requisits establerts a l'Esquema Nacional de Seguretat (ENS) per a sistemes classificats en nivell alt. Les propostes presentades hauran de mostrar molt clarament la mesura en que el seu plantejament va alineat amb aquest marc de referència normatiu.

Per a l'HCBC l'èxit del projecte radica en la qualitat i rigor dels serveis professionals, és per això que seran objecte d'avaluació mitjançant **judicis de valor** en base al grau de detall, qualitat tècnica, metodologia i adequació de la proposta presentada pel licitador a les expectatives i requeriments plantejats. El licitador haurà de descriure a la seva oferta:

- L'abast detallat dels serveis i qualitat de la proposta.
- La metodologia d'execució.
- El pla de treball i fases.
- Impacte en la continuïtat del servei.
- Els recursos assignats.
- Els lliurables previstos.
- Millores aportades.

La dedicació estimada per als serveis professionals d'implantació de la solució és de 440 hores de treball especialitzat, incloent tasques de direcció de projecte, arquitectura tècnica, configuració, migració, proves, posada en marxa, documentació i transferència de coneixement. Els licitadors hauran de preveure els recursos necessaris per garantir l'execució completa dels treballs descrits en aquest PPT.

4.1 Disseny i planificació

Es proposaran una sèrie de reunions amb el personal de TI de l'Hospital amb l'objectiu de dissenyar amb detall l'arquitectura física i lògica, integracions amb infraestructura i serveis de l'HCBC, així com les configuracions i operatives que s'aplicaran. Cal que s'incloguin les següents fites:

- Integració a la xarxa de l'HCB.
- Bastionat dels equips.
- Pla d'estandardització i normalització per a la nomenclatura d'objectes i polítiques fent ús dels camps de dades disponibles amb l'objectiu de facilitar:
 - Identificar fàcilment conjunts de polítiques associades a entorns, serveis o projectes
 - Realitzar cerques eficients per nom i text descriptiu dels camps de dades
- Definició dels perfils de seguretat a desplegar i aplicar.
- Migracions de les configuracions actuals a la nova plataforma.
- Proposta de gestió d'events a identificar, notifikacions i automatització de processos a l'eina de gestió de logs.
- Aplicació de millores.

La planificació haurà d'incloure totes les tasques necessàries per implantar tan les funcionalitats requerides com les proposades pel licitador que siguin d'interès per l'HCB, incloent un calendari d'implantació i recursos necessaris atenent a les prioritats i complexitats de l'HCB.

La planificació també haurà d'incloure un pla de proves funcionals amb la finalitat de detectar debilitats o punts no contemplats en el disseny inicial i així poder aplicar les correccions que es considerin necessàries. El pla de proves haurà de ser entregat per l'adjudicatari i validat per l'HCB abans de portar-lo a terme.

4.2 Operatives de sistemes

L'adjudicatària es comprometrà a treballar conjuntament amb la persona assignada de l'Àrea de TI per tal d'integrar la infraestructura objecte d'aquest expedient en el sistema de monitorització de l'Hospital (sistema basat en plataforma Check_MK). Com a mínim les alertes que s'integraran han de ser:

- Elements indicatius d'una imminent fallida, com pot ser consum de CPU o memòria elevat, espai de disc insuficient, estat del cluster.
- Caigudes de serveis o equipament hardware.

També caldrà coordinació de la mateixa manera per tal d'establir els mecanismes de còpia de seguretat i restauració de tots els elements del sistema, que s'integraran amb la plataforma de Backups de l'Hospital.

4.3 Desplegament de les solucions NGFW i de gestió, operació i recollida de logs

El focus principal consisteix en la posada en producció del nou Firewall realitzant la migració de la solució actual. La migració s'haurà de realitzar posant les dues solucions en paral·lel sense que hi hagi cap interferència entre elles i sigui possible commutar entre una solució i l'altre ja sigui pel 100% del tràfic processat (una sola intervenció) o pel tràfic associat a interfícies de xarxa determinats (diverses intervencions fins assolir el 100%). Els aspectes a valorar seran:

- Optimitzacions prèvies a la migració sobre la solució actual, com per exemple identificar i descartar elements en desús o adaptació d'elements que per diferència tecnològica sigui necessari.
- Facilitat i flexibilitat en que les dues solucions poden conviure en paral·lel alhora que es fan canvis i aquests es repliquen sense que impliquin cap tall de servei ni suposin una càrrega extra en quant a tasques de configuració al personal de TI de l'HCB.
- Facilitat d'identificació d'objectes i polítiques en la nova solució, evitant que un canvi tecnològic comploqui i dificulti aquesta tasca.

Abans de planificar la migració final, moment en que la nova solució entri en producció i l'actual deixi de processar tràfic, s'haurà d'haver realitzat les següents tasques:

- Definició de perfils d'administrador.
- Integració amb AD corporatiu.
- Arquitectura de desxifrat SSL/TLS per tal que els perfils de seguretat de capa 7 funcionin adequadament.
- Operativa de sistemes tant de monitorització com de backup per a tots els components que ho requereixin
- Solució de gestió, operació i recollida de logs plenament operativa.

- Realització de pla de proves pactat per tal de validar funcionalitats, fiabilitat i robustesa de la nova solució. L'objectiu serà minimitzar el risc de possibles impactes operatius.

Adicionalment al procés de migració, l'HCB desitja aplicar millores en 3 línies, per a les quals els licitadors hauran de proposar com aplicar-les i els recursos que hi dedicaran, s'haurà d'indicar la funcionalitat en la que es basaran i raonar el seu plantejament. Les 3 línies de millora són:

1. **Enfortir la postura de seguretat.** Fent ús de les capacitats d'aplicar capes de seguretat de la solució, caldrà proposar perfils de seguretat segons diferents fluxes de xarxa:
 - **Tràfic entre equips interns.** L'objectiu serà evitar que un atacant o malware ja present a un equip es propagui entre equips de la xarxa interna.
 - **Tràfic sortint cap a Internet.** S'ha de poder donar els accessos necessaris per a les operatives dels servidors i altres equipaments (actualitzacions, integracions amb tercers, serveis de còpia al núvol, etc.) assegurant que no s'accedeix a llocs maliciosos o es descarrega fitxers que contenen malware.
 - **Tràfic entrant a serveis publicats a Internet.** L'HCB disposa de diversos serveis exposats a Internet: serveis web, DNS, correu o SFTP. Són serveis especialment crítics i sensibles que requereixen un alt nivell de protecció.

Per al tràfic amb origen o destí la xarxa Internet, altres serveis propis desplegats a núvols públics (AWS i Azure) i equipament final d'usuari ubicat a les plantes dels diferents edificis, cal tenir en compte que el Firewall de data center es una capa de seguretat perimetral addicional a la solució existent basada en Fortinet. Adicionalment també es disposa d'un WAF basat en tecnologia F5 per a la publicació de Webs.

2. **Integrar la infraestructura de virtualització i clouds públics** per facilitar la gestió de polítiques. Hi ha gran interès en poder aplicar polítiques basades en etiquetes i metadades de l'entorn de virtualització VMware corporatiu i clouds públics AWS i Azure, de manera que la posada en producció de nous sistemes sigui més flexible i redueixi la càrrega de treball associada a la configuració de polítiques de seguretat en el Firewall.
3. **Gestió i operació de la solució.**
 - **Gestió de canvis.** A l'HCB s'apliquen canvis constantment als firewalls per tal de donar resposta a nous projectes o requeriments, aquest canvis s'apliquen tant per personal extern de serveis gestionats com per personal intern. Es valorarà que dins la solució es proposi i s'implementi un procediment que permeti establir un circuit d'aprovació de canvis així com mecanismes de publicació i traçabilitat dels mateixos oferint el màxim nivell de detall.
 - **Eliminar objectes en desús.** És habitual que amb el pas del temps es donin de baixa productes o serveis que tenen polítiques i objectes associats al Firewall, tot i que hi ha procediments per tramitar la baixa, aquests es basen en escalats manuals que no sempre es gestionen correctament deixant configuracions residuals no desitjades. Es desitja dotar una tasca, a poder ser automatitzada, de revisió d'aquestes configuracions amb la proposta d'accions corresponents.
 - **Generació de documentació en format autoservei.** Dins l'activitat que realitza el personal de TI que gestiona els firewalls, és habitual rebre peticions sobre quines polítiques tenen aplicades certs servidors o equipament concret, també revisar logs d'accés, amb l'objectiu de validar si es compleixen els requisits de comunicacions necessaris o per afegir a la documentació dels projectes. Per tal de donar resposta a aquesta necessitat alhora que s'elimina la dependència en el personal especialitzat que gestiona els Firewalls, es desitja disposar d'una utilitat basada en web que permeti a usuaris autoritzats i sense coneixements de gestió de firewalls, generar-se ells mateixos la informació que necessiten sense haver de disposar de visibilitat completa sobre tota la configuració o logs. L'ús ha de ser simple, introduint una IP o nom d'equip, el sistema ha de generar una taula on es presenti la informació de polítiques de seguretat on l'element introduït figurei com a origen o destí i els darrers logs d'accés. Cal que els licitadors que presentin

aquesta millora descriguin clarament capacitats i limitacions posant exemples dels resultats que s'obtingrien segons el tipus de dada introduït per l'usuari.

4.4 Desplegament de la solució IoT

La solució d'IoT s'haurà d'activar i deixar configurada per a poder visualitzar, analitzar i gestionar totes les alertes associades als dispositius de IoT de l'hospital, entenent IoT com OT, IoT, IoTMT.

S'haurà d'analitzar el model organitzatiu actual de l'hospital i etiquetar dels actius crítics per tal de fer una gestió correcta de la configuració i gestió de les alertes posteriors. En fase de desplegament s'haurà de visualitzar tots els dispositius IoT de l'hospital, etiquetats i agrupats correctament per tal de poder fer una gestió de les vulnerabilitats de forma prioritzada.

S'haurà d'establir un pla de desplegament que incorpori les següents funcions:

- Inventari i classificació d'actius identificats per l'eina.
- Agrupament i perfilat dels dispositius.
- Etiquetat dels actius crítics.
- Integració amb la electrònica de xarxa (múltiples fabricants).
- Definició i escalat d'alertes de forma automàtica.
- Creació de tots els dashboards personalitzats necessaris.
- Segons l'estructura organitzativa, definir i implementar els diferents perfils d'accés a l'eina.
- Generar la documentació associada a la instal·lació, configuració, operacions sobre l'eina i processos de gestió que esdevinguin del projecte.
- Recomanacions i implementacions de polítiques de seguretat en funció dels comportaments dels dispositius.

4.4.1 Serveis gestionats IoT

A banda de les funcionalitats i desplegament requerit per a la visualització dels dispositius IoT es demana un servei gestionat recurrent de les alertes d'aquesta funcionalitat durant els 5 anys de contracte.

L'àmbit d'aquest servei ha de contemplar la gestió centralitzada de les alertes, amb una dedicació parcial de recursos per a la revisió i reporting, així com el lideratge d'un comitè nou a conformar on traslladar i fer seguiment de les alertes identificades.

Es requerirà:

- Col·laborar en l'inventari de dispositius IoT en base a la informació del tràfic detectat per la solució, aportant idees i solucions per al manteniment òptim.
- Conformar conjuntament amb l'HCB el comitè de gestió d'actius IoT.
- Generar i mantenir el model de governança de la seguretat dels dispositius IoT.
- Revisió periòdica setmanal de les alertes de la consola.
- Anàlisis i reporting mensual de les alertes de forma prioritzada.
- Seguiment mensual de les accions acordades amb els diferents actors que han de resoldre les alertes
- Convocar les sessions mensuals del comitè, liderar-les i fer les actes.
- Realitzar semestralment l'anàlisi de riscos de l'àmbit IoT.
- Detecció de possibles anomalies en el comportament de xarxa dels dispositius.
- Detecció i visibilitat d'amenaques desconegudes als dispositius IoT a partir del seu comportament en xarxa.
- Prevenció d'amenaques conegudes als dispositius IoT.
- Fomentar la creació polítiques als tallafocs utilitzant la informació d'inventari descoberta (tipus de dispositiu, fabricant i model).

La dedicació aproximada prevista per a aquestes tasques és de 16 hores mensuals. Així mateix, es preveu la possibilitat d'incrementar aquest volum d'hores durant l'execució del contracte, d'acord amb les necessitats del servei i en els termes establerts a l'apartat de modificacions previstes. A aquest efecte, s'estableix un criteri d'adjudicació que valorarà la tarifa horària aplicable a les hores addicionals que, si escau, puguin ser objecte de la modificació contractual.

4.5 Manteniment i suport avançat

L'adjudicatari haurà d'oferir serveis de manteniment i suport avançat addicionals als contractats al fabricant, descrits en el punt 3.6 del PPT, durant tot el període de contractació.

4.5.1 Condicions generals

- En general el servei es realitzarà en remot per minimitzar l'impacte de les incidències de la manera més immediata possible sempre que es donin les circumstàncies necessàries per fer-ho en aquest format, però en cas que no sigui possible, sigui quin sigui el motiu, o en cas que la naturalesa o criticitat de l'incident ho requereixi, el servei ha d'incloure obligatòriament la opció de desplaçament del personal tècnic a càrrec de l'incident a les instal·lacions de l'HCB per tractar-la insitu.
- L'adjudicatari actuarà com a punt únic de contacte per la gestió d'incidents involucrin o no al fabricant, tot i això si l'HCB ho requereix podrà accedir directament als serveis del fabricant.
- Per a totes les actuacions que calgui planificar dintre del servei caldrà:
 - Presentar un document amb la planificació a validar i aprovar per l'HCB.
 - Execució dintre de les finestres acordades amb l'HCB per minimitzar possibles impactes.
- Per tal de facilitar i agilitzar la resolució de les incidències, l'adjudicatària es comprometrà a treballar i col·laborar tant amb personal propi de l'HCB com amb personal d'empreses col·laboradores o que també ofereixen serveis de TI a l'Hospital.

4.5.2 Manteniment i suport reactiu/correctiu

Els serveis prestats per l'HCB es consideren crítics i es presten ininterrompudament les 24 hores dels 7 dies de la setmana i els 365 dies, pel que cal que es contempli un servei de suport a incidències en format 24x7 amb diferents temps de resposta segons criticitat.

Els tècnics de l'HCB assumiran el primer nivell d'atenció a incidents, els serveis requerits en la contractació han de donar resposta a un suport expert quan aquest primer nivell requereixi un escalat, els serveis contractats també inclourà la gestió d'actualitzacions per donar resposta a vulnerabilitats o problemes reconeguts pel fabricant.

Serveis inclosos:

- Recepció i gestió d'incidències.
- Diagnòstic i resolució de problemes.
- Escalat al fabricant quan sigui necessari i gestió dels casos oberts amb aquest.
- Gestió de RMA i substitució de maquinari defectuós.
- Gestió i aplicació d'actualitzacions.
- Suport a incidents crítics de seguretat.
- Seguiment de casos oberts fins el seu tancament.
- Comunicació periòdica de l'estat de les incidències.

El temps de resposta requerit és el següent.

Criticitat	Descripció	Temps de resposta	Temps escalat a fabricant (en cas de necessitat)
Molt alta	Servei caigut o impacte greu	30 minuts	1 hora
Alta	Degradació significativa	1 hora	2 hores
Mitja	Afectació parcial no greu	4 hores	1 dia laborable
Baixa	Sense impacte considerable	1 dia	Segons necessitat

4.5.3 Manteniment i suport preventiu i evolutiu

Inclou totes les activitats orientades a mantenir el sistema actualitzat, segur i optimitzat amb l'objectiu de minimitzar riscos operatius i de seguretat mitjançant revisions periòdiques i tasques proactives.

Serveis inclosos:

- Detecció i anàlisi de vulnerabilitats presents en qualsevol dels components.
- Revisar i validar els components de la infraestructura per a garantir un rendiment òptim.
- Revisions de la configuració per assegurar que la instal·lació i polítiques definides compleixen amb les bones pràctiques definides pel fabricant.
- Revisar la utilització de polítiques i objectes analitzant si cal plantejar accions conseqüents.
- Analitzar mètriques i presentar informes amb les dades més rellevants.
- Generació d'informes amb el detall de tasques realitzades i conclusions o resultats derivats.
- Suggeriment de millores de forma proactiva.
- Reunions de seguiment amb el personal de l'HCB.

La periodicitat d'aquest manteniment serà trimestral.

Així mateix, es preveu una dedicació estimada de 20 hores anuals de serveis especialitzats per a l'execució de les activitats de manteniment preventiu i evolutiu descrites en aquest apartat.

4.5.4 Assessorament tècnic i suport d'administració avançada

Inclou l'accés a especialistes per resoldre dubtes i rebre suport tècnic en tasques d'administració avançada, aquest servei ha de cobrir necessitats puntuals que es puguin donar durant la vigència del contracte on el personal tècnic de l'HCB requereixi suport expert.

Serveis inclosos:

- Recepció i gestió de peticions.
- Consultes sobre arquitectura.
- Consultes sobre bones pràctiques.
- Consulta sobre configuracions.
- Interpretació d'alertes de seguretat.
- Revisió de propostes de canvi.
- Anàlisis d'impacte de noves necessitats.

5 TRANSFERÈNCIA DE CONEIXEMENT

L'adjudicatari haurà de garantir la transferència de coneixement necessària per assegurar que el personal tècnic de l'organització disposa de la informació, documentació i capacitat adequades per operar, administrar, supervisar i evolucionar la infraestructura de seguretat objecte del contracte.

5.1 Documentació

Inclou una documentació tècnica completa i detallada de les solucions incloses i desplegades a la oferta. La documentació inclourà com a mínim els següents blocs:

- **Documentació de disseny i arquitectura**
 - Esquema de la solució implantada.
 - Topologia de xarxa associada al Firewall i sonda IOT.
 - Configuracions d'alta disponibilitat.
 - Integracions amb altres sistemes.

- **Documentació de configuració**
 - Integració amb altres sistemes o components.
 - Estandardització de nomenclatures.
 - Relació de perfils de seguretat.
 - Configuracions específiques rellevants.
 - Adequacions a l'ENS contemplades en les configuracions aplicades.
- **Documentació d'operació**
 - Procediments d'arrencada i aturada dels equips.
 - Procediments de verificació dels components.
 - Procediment d'actuació davant problemes coneguts.
 - Procediment de recuperació davant fallides.
- **Documentació dels plans d'intervenció durant el desplegament i migració**
- **Documentació de validació**
 - Validacions del correcte funcionament de tots els components.
 - Plans de proves i resultats realitzats per validar els mecanismes d'alta disponibilitat.
 - Validacions de que les configuracions dels mòduls de seguretat aplicats responen correctament.

La documentació haurà de lliurar-se en format editable i estàndard (Word, Excel, Visio, etc.), aquesta serà propietat de l'HCB.

5.2 Formació

L'adjudicatari haurà de realitzar una formació tècnica i un traspàs de coneixement dirigit al personal tècnic de l'Hospital Clínic. El temari cobrirà com a mínim els següents punts:

- **Infraestructura desplegada**
 - Arquitectura desplegada a nivell físic i lògic.
 - Components principals i relació entre ells.
 - Integracions amb altres sistemes.
- **Administració i configuració dels equips i aplicacions**
 - Ús de les eines de gestió i bones pràctiques.
 - Creació i gestió de polítiques de seguretat.
- **Troubleshooting bàsic**
 - Eines i mètodes de diagnòstic per a la resolució d'incidències.
 - Monitoratge en temps real.
 - Resolució de problemes comuns.

6 OFERTA TÈCNICA A LLIURAR

Els licitadors hauran de lliurar una oferta tècnica que descrigui detalladament la solució proposada i la metodologia prevista per la seva implantació. Aquesta memòria haurà de permetre avaluar la qualitat tècnica de l'oferta, el grau d'adequació als requeriments i el valor afegit aportat pel licitador.

Haurà d'estar estructurada com a mínim en els apartats següents:

6.1 Solució proposada

- Descripció general de la solució oferta.
- Relació detallada dels equips, llicències, subscripcions i components inclosos.
- Característiques tècniques de la plataforma.

- Arquitectura de la solució.
- Esquema d'interconnexió i alta disponibilitat.
- Integració amb els sistemes existents.

6.2 Equip de projecte i metodologia

- Identificació dels perfils professionals assignats.
- Funcions, responsabilitats i dedicació de cada perfil.
- Certificacions tècniques i acreditacions de fabricant.
- Experiència acreditada en projectes similars.
- Metodologia de gestió del projecte.
 - Model de governança.
 - Organització de reunions de seguiment.
 - Gestió de riscos.
 - Gestió de canvis.
 - Mecanismes de control i seguiment.

6.3 Proposta de serveis professionals

- Abast dels serveis professionals en el context de compliment amb el PPT i millores.
- Implantació
 - Fases del projecte.
 - Pla de migració i posada en servei.
 - Pla de contingència i reversió.
 - Pla de validació i proves.
- Manteniment i suport.
 - Cobertura.
 - Recursos tècnics assignats.
 - Procediments d'atenció a incidències i peticions o consultes.
 - Model d'escalat.
- Serveis gestionats IOT.
 - Model de gestió.
 - Activitats incloses i periodicitat.

6.4 Traspàs de la instal·lació a la gestió continuada.

- Procediment de transició entre la fase d'implantació i la fase d'explotació.
- Proposta de formació i perfil de l'instructor.
- Proposta de la documentació i format d'entrega.
 - Estructura dels documents.
 - Exemples o models de documentació utilitzats.

AVÍS IMPORTANT: segons el que estableix el Plec de Clàusules Administratives Particulars (PCAP), la memòria tècnica no podrà contenir cap informació relativa a criteris d'adjudicació valorables mitjançant fórmules o criteris automàtics. La inclusió d'informació corresponent a criteris avaluable automàticament pot comportar l'exclusió en aquesta licitació.

ANNEX 1 – DECLARACIÓ RESPONSABLE DEL COMPLIMENT DELS REQUERIMENTS

El/la Sr/Sra, en nom i representació de l'empresa declara que els equips i solucions que ofereix com a resposta als 3 components que obligatòriament ha d'incloure el submissament compleixen amb els requeriments tècnics descrits tant en els diferents apartats del PPT com en les taules de requisits d'aquest annex, havent marcat aquelles que presenten opcions, i amb tota la normativa aplicable a la tipologia d'equip subministrat.

- **Solució NGFW**

REQUISITS TÈCNICS MÍNIMS IMPRESCINDIBLES	
	Hardware
1	Format per muntar en rack estandard de 19"
2	8 ports Ethernet 1G/2.5G/5G/10G
3	12 ports 1G/10G (SFP/SFP+)
4	4 ports 25G (SFP28)
5	4 ports QSFP28 40G/100G
6	Disc dur redundat SSD per al sistema operatiu amb capacitat mínima de 480GB
7	Port dedicat per a gestió fora de banda
8	Port dedicat per a Alta Disponibilitat
9	Port de consola RJ45
10	Fonts d'alimentació redundants
11	4 òptiques SFP+ LR 10G
12	4 òptiques QSFP SR 100G BIDI
	Capacitats i rendiment
1	52 Gbps de Firewall throughput amb inspecció de capa 7, identificació d'aplicacions i logging activat utilitzant paquets de 64 KB amb tràfic mixt
2	35 Gbps de Threat Prevention throughput amb serveis de control d'aplicacions, IPS, Antivirus, Antispyware, AntiMalware, filtratge de URL, seguretat DNS, file blocking i logging actius utilitzant paquets de 64 KB amb tràfic mixt
3	20 Gbps de IPSEC VPN Throughput
4	270 mil sessions noves per segon
5	Capacitat total de sessions de 5 milions
6	10 sistemes virtuals

- **Solució per a la gestió i operació**

REQUISITS TÈCNICS MÍNIMS IMPRESCINDIBLES	
	Plataforma
1	Arquitectura de gestió i col·lecció de logs independents sobre infraestructura virtual basada en VMWare
2	Permet ampliar capacitat de processament i emmagatzematge
	Capacitats
1	Capacitat de gestionar fins a 25 firewalls sense ampliació de llicència
2	Gestió centralitzada de múltiples dispositius
3	Capacitat d'auditoria i traçabilitat de canvis efectuats
4	Visibilitat i monitorització
5	Quadres de comandament gràfics i personalitzables
6	Recollida centralitzada de logs, cerca i correlació d'esdeveniments de seguretat, conservació d'històrics amb capacitat mínima de retenció d'un any per a auditories i anàlisis
7	Generació d'informes predefinits i personalitzats
8	Correlació i detecció d'amenaces
8	Control d'accés d'administració basat en rol (RBAC) i registre de totes les accions administratives
9	Integració amb eines ITSM, SIEM i plataformes d'automatització

10	APIs per automatitzar desplegaments i canvis de configuració
11	Suport de grups d'adreces dinàmics per adaptar polítiques de forma dinàmica
12	Integració amb infraestructures virtualitzades basades en VMware, així com entorns de núvol públic, incloent com a mínim plataformes AWS i Azure. Aquesta integració haurà de permetre la descoberta automàtica de màquines virtuals, instàncies i recursos desplegats en els diferents entorns, així com la seva classificació mitjançant atributs dinàmics, etiquetes o metadades pròpies de cada plataforma oferint una sincronització periòdica amb les fonts d'informació. La solució haurà de ser capaç d'utilitzar aquesta informació per a la definició i aplicació de polítiques basades en etiquetes, sense dependència exclusiva d'adreces IP estàtiques.

- **Solució IoT**

REQUISITS TÈCNICS MÍNIMS IMPRESCINDIBLES	
	Capacitats
1	Descobriments automàtics de dispositius IOT, OT, IoMT i IT tradicionals
2	Classificació basada en IA i Machine Learning analitzant fins a 200 paràmetres. La plataforma ha de ser capaç de perfilar perfectament els equips identificant dades com: • Fabricant • Model • Tipus de dispositiu • Sistema Operatiu • Funció del dispositiu
3	Inventari enriquit d'actius, per a cada equip descobert s'han d'obtenir els atributs: • Adreça IP • MAC • VLAN • Ubicació • Fabricant • Firmware • Vulnerabilitats associades • Criticitat de l'actiu
4	Avaluació continua de vulnerabilitats i detecció d'anomalies en base al comportament de xarxa.
5	Prevenició d'amenaques conegudes als dispositius IoT.
6	Detecció i visibilitat d'amenaques desconegudes als dispositius IoT a partir del seu comportament en xarxa.
7	Gestió de l'avaluació del risc i control de les amenaces a partir del comportament que tenen els dispositius comparant-lo amb el comportament dels mateixos i permetent aplicar polítiques que només permetin els fluxos autoritzats.
8	Integració amb plataformes corporatives: • SCCM i Intune de Microsoft, d'on recollirà tota la informació registrada. • Sistemes de control d'accés (NAC) o sistemes de gestió d'infraestructura de xarxa per obtenir informació de localització física dels dispositius (switch/port/VLAN).
9	Integració amb arxius MDS2 (Manufacture Disclosure Statement for Medical Device Security)
10	Classificacions de FDA (Food and Drug Administration)

ANNEX 2 – FORMULARI DE PRODUCTES HARDWARE, SOFTWARE, LICÈNCIES I MANTENIMENTS QUE S'INCLOURAN EN EL SUBMINISTRAMENT

En aquest formulari es recull la relació detallada d'elements inclosos a la oferta. Si el licitador ho considera oportú pot incloure alguna columna addicional per facilitar o ampliar la informació associada als articles.

Tipus d'element	Fabricant	Part Number	Descripció	Quantitat

ANNEX 3 – CLÀUSULA DE SEGURETAT DE LA INFORMACIÓ

L'objecte d'aquest contracte ha estat categoritzat, d'acord amb l'article 40 del Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguridad (ENS), amb categoria ALTA. En conseqüència, l'empresa adjudicatària ha d'acreditar, amb caràcter obligatori, la disposició d'una Certificació de Conformitat amb l'ENS en categoria ALTA, vigent i emesa per una entitat de certificació acreditada per l'Entitat Nacional d'Acreditació (ENAC), o per un organisme d'acreditació equivalent en el marc de la Cooperació Europea per a l'Acreditació (EA), de conformitat amb el que estableixen la disposició addicional tercera i l'article 38 del citat Reial Decret.

Aquesta certificació ha de cobrir, com a mínim, l'abast dels sistemes i serveis directament relacionats amb l'objecte del contracte, ha de trobar-se en vigor durant tota la durada de la prestació i ha de ser objecte d'auditoria de renovació, com a mínim, cada dos anys, de conformitat amb l'article 31 del Reial Decret 311/2022, essent obligació de l'adjudicatari mantenir-la actualitzada i comunicar a l'HCBC, de manera immediata, qualsevol modificació, suspensió, no renovació o revocació que la pugui afectar.

Per acreditar aquest compliment, l'adjudicatari ha de presentar còpia de la certificació vigent, juntament amb el certificat d'acreditació de l'entitat certificadora, en el tràmit de requeriment de documentació establert a l'article 150.2 de la LCSP que es dirigirà a l'empresa que hagi presentat la millor oferta. L'empresa licitadora no podrà al·legar, en cap cas, que el sistema, servei o equipament ofert no assoleix la categoria ALTA per eximir-se d'aquesta obligació, atès que la categorització és pròpia de l'objecte del contracte i no de la solució tècnica presentada. En cas de no disposar de la certificació exigida, de no complimentar adequadament el requeriment, o de no complir amb els requeriments sol·licitats, s'aplicarà el que estableix el mateix article 150.2.