PLEC DE PRESCRIPCIONS TÈCNIQUES

Subministrament de maquinari i programari i serveis professionals per a la Fase II de renovació tecnològica d'equips d'accés a la xarxa de comunicacions, amb destí a l'Hospital Clínic de Barcelona (HCB) i a la Fundació de Recerca Clínic Barcelona – Institut d'Investigacions Biomèdiques August Pi i Sunyer

EXPEDIENT 2025-95

Índex

1- OBJECTE DEL CONTRACTE

L'objecte del concurs és establir les condicions per a l'adquisició d'elements de maquinari i programari, així com els serveis professionals necessaris per realitzar una renovació tecnològica d'equips d'accés a la xarxa de comunicacions, tant la part cablejada com la WiFi, a la xarxa campus de l'Hospital Clínic de Barcelona (en endavant HCB) i Fundació Clínic per a la Recerca Biomèdica (en endavant FCRB). Aquesta renovació té com a objectiu seguir amb el model d'estandardització d'equipament iniciat a l'expedient 2024-92, substituint l'equipament dels edificis no inclosos en la mateixa, alhora que s'hi introdueixen serveis addicionals que aportin valor en l'àmbit operatiu dels entorns de xarxes campus.

S'espera que el present concurs presenti millores i noves prestacions que permetin operar, treballar i oferir serveis de valor afegit a la infraestructura de xarxa de l'HCB.

Tot i que es tracta d'un projecte global únic a nivell tècnic, a nivell econòmic caldrà presentar dues ofertes:

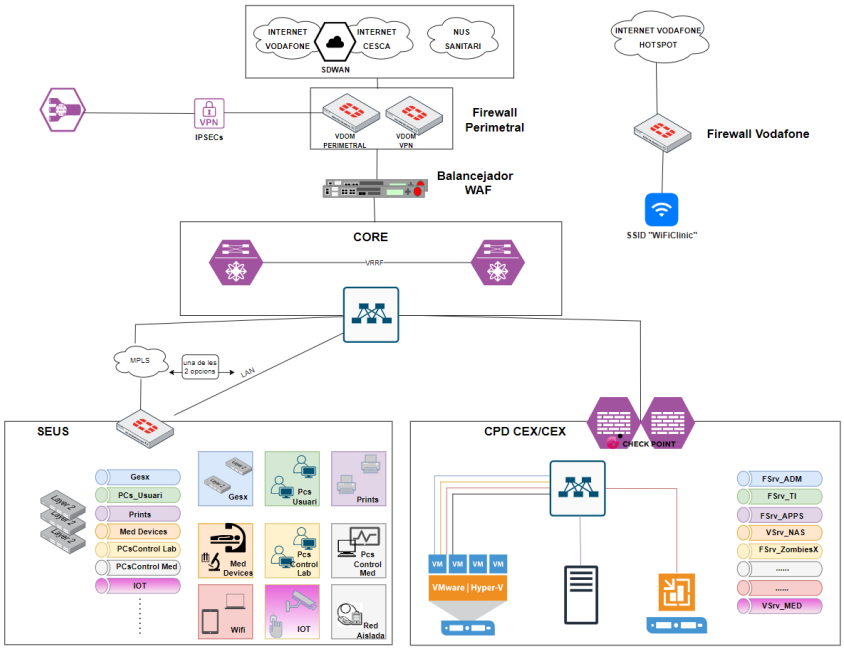
- La corresponent a part del projecte facturable a l'HCB.
- La corresponent a part del projecte facturable a FCRB.

En l'annex 3 i 4 s'indica quin equipament correspon a cadascun

2- INFRAESTRUCTURA DE LA XARXA CAMPUS

La xarxa campus està formada per 32 edificis en el moment de redacció d'aquest PPT, en la fase 1 de renovació, licitació 2024-92, es va substituir la electrònica de 18 edificis. En aquesta segona fase s'inclou edificis addicionals, 2 dels quals encara no estan ocupats però ho estaran durant el present any o el vinent.

A nivell general, l'esquema lògic és el següent:



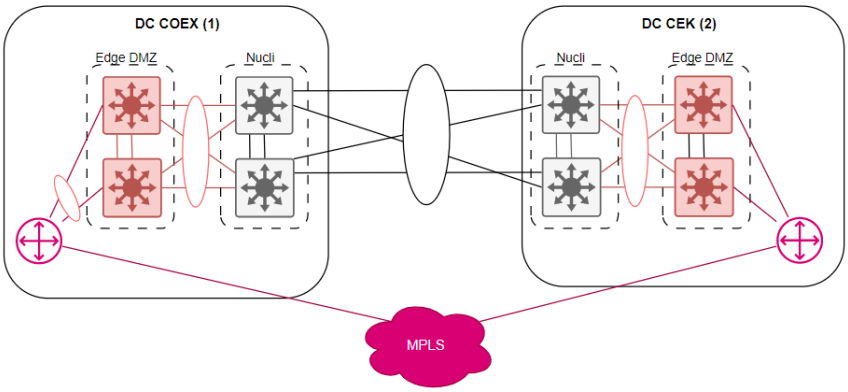
Depenent de la tipologia de seu, aquesta realitza una connexió a la xarxa troncal de l'HCB (core) de forma directa, utilitzant equips de distribució i/o utilitzant equips d'operador enllaçats amb tecnologia MPLS. La tipologia CPD es mostra en el diagrama però queda exclosa la renovació dins de l'abast d'aquesta licitació.

Totes les seus incloses dins l'abast disposen d'un Firewall local i equips d'accés amb autenticació 802.1x i MAB. En determinades seus, degut al seu dimensionament inclouen equips de distribució per tal d'enllaçar els equips d'accés amb connexions de fibra. Tots els commutadors d'accés i distribució, així com els punts d'accés WiFi són objecte de substitució dintre aquest PPT.

2.1- Xarxa troncal

La xarxa troncal de l'HCB està distribuïda entre dos Data Centers, el principal situat dintre de la seu COEX i el secundari situat dintre de la seu CEK. Com ja s'ha mencionat, totes les seus que conformen la xarxa campus tenen interconnexió a la xarxa troncal.

En el següent diagrama físic es mostren els elements més rellevants de la xarxa troncal i que han d'interactuar amb l'equipament objecte d'aquest PPT.



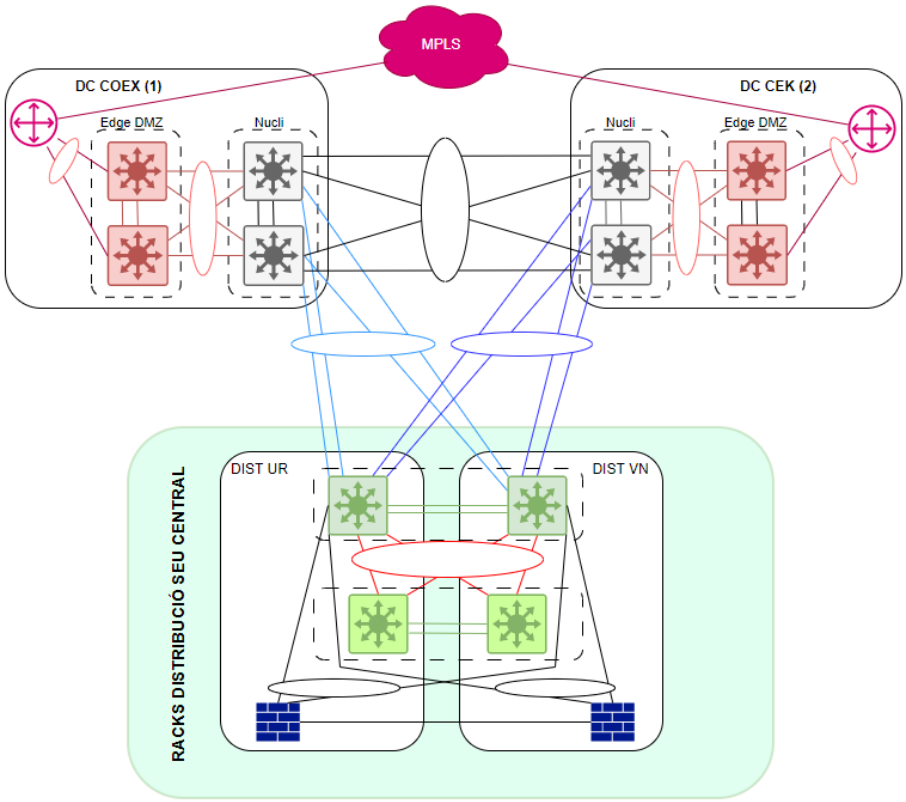
Els equips de "Nucli" són cisco N9K-C9336C-FX2, el equips "Edge DMZ" són cisco N9K-C93240YC-FX2.

2.2- Seus Hospital Clinic i CELLEX

La seu central compta amb dos espais físicament distants on es situa la capa de distribució de tots els raks d'accés de la pròpia seu i els de la seu CELLEX. Els equips de distribució actuals estan segregats en aquests dos espais per tal d'aportar redundància a la connectivitat, ambdues ubicacions tenen connectivitat entre elles mitjançant dues esteses de 24 parells de fibres monomode acabades amb connectors LC/PC.

Cadascun dels dos racks de distribució disposa d'una estesa de 24 parells de fibres monomode amb cada un dels data centers, acabades amb connectors SC/APC.

A continuació es mostra el diagrama de connexions entre els dos racks de distribució i la d'aquests amb la xarxa troncal en els dos data centers.



Els racks d'accés de la seu central, així com els de la seu CELLEX disposen d'una estesa de 4 parells de fibres contra cadascun dels racks de distribució, una de les esteses està realitzada amb fibra multimode i l'altre amb monomode (segons la distància), en ambdós casos acabada amb connectors LC/PC.

Els tallafocs locals es troben connectats als equips de distribució mitjançant la connexió d'un enllaç agregat de 2 ports 10G en cadascun dels tallafocs. Tot el tràfic generat a aquestes seus s'enruta i es filtra pels tallafocs locals de la seu central.

2.3- Seus COEX, Facultat i Rehabilitació

La seu COEX disposa d'un rack de distribució situat al data center principal ubicat al mateix edifici. La connexió entre els equips de distribució d'aquesta seu i la xarxa troncal de l'organització es realitza utilitzant fuetons de fibra, donat que la distància entre equips és de pocs metres.

Tots els racks d'accés d'aquesta seu, excepte el rack CEX_SdP i rack de rehabilitació, disposen d'una estesa de 4 parells de fibra multimode acabada amb connectors LC/PC amb el rack de distribució. Addicionalment el rack d'accés de la seu Facultat també depèn d'aquest rack de distribució, on arriba amb una estesa de 4 parells de fibra monomode acabada amb connectors LC/PC.

El rack d'accés CEX_SdP està enllaçat amb 2 esteses de parells de coure amb el rack CEX10.

El rack d'accés de la seu Rehabilitació està enllaçat amb 2 esteses de parells de coure amb el rack CEX0C de la seu COEX.

Els tallafocs locals es troben connectats als equips de distribució mitjançant la connexió d'un enllaç agregat de 2 ports 10G en cadascun dels tallafocs. Tot el tràfic generat a aquestes seus s'enruta i es filtra pels tallafocs locals de la seu COEX.

2.3- Seu Maternitat

A Maternitat existeix un rack de distribució per a tots els racks d'accés de la seu. Els racks MATHELIOS1, MATHELIOS2 i MATHELIOS3 arriben al de distribució amb una estesa de 4 parells de fibres monomode, la resta de racks d'accés de la seu ho fan amb una estesa de 4 parells de fibres multimode, en tots els casos els connectors són LC/PC.

Actualment els equips de distribució de Maternitat estan agregats a la xarxa troncal mitjançant dos circuits portadors d'1G per fibra monomode (un circuit per a cadascun dels data centers), però està previst que en un termini no gaire llunyà el circuit portador sigui substituït per accessos WAN basats en MPLS, en aquest cas la connectivitat probablement serà utilitzant 2 ports d'1G RJ-45 cap a cadascun dels routers d'operador que es realitzarien amb connectivitat als tallafocs locals.

Els tallafocs locals es troben connectats als equips de distribució mitjançant la connexió d'un enllaç agregat de 2 ports 10G en cadascun dels tallafocs. Tot el tràfic generat en aquesta seu s'enruta i es filtra pels tallafocs local.

2.4- Seus Plató, Plató 2 i Marc Aureli

A la seu Plató existeix un rack de distribució per a tots els racks d'accés de la mateixa seu, així com també per els dels edificis Plató 2 i Marc Aureli. Els racks d'accés estan units amb el de distribució amb una estesa de 4 parells de fibres multimode acabades amb connectors LC/PC.

Els equips de distribució de Plató estan agregats a la xarxa troncal mitjançant la connexió d'un enllaç agregat de 2 ports 10G amb cadascun dels tallafocs locals. A la vegada cadascun dels tallafocs disposa d'una connexió d'1G RJ-45 tant amb el router principal com el secundari de l'operador. Tot el tràfic generat en aquestes seus s'enruta i es filtra per aquests tallafocs.

Excepcionalment a l'edifici seu Plató 2, el rack HP222 depèn del rack HP221 y el rack HP241 del rack HP232, en ambdós casos existeixen 2 esteses de parells de coure entre els dos racks.

2.5- Seu Casanova 150

Aquesta seu també disposa d'un rack de distribució per a tots els racks d'accés, la connectivitat es realitza amb esteses de 4 parells de fibres multimode acabades amb connectors LC/PC en cada rack.

Els equips de distribució de Casanova 150 estan agregats a la xarxa troncal mitjançant la connexió d'un enllaç agregat de 2 ports 10G amb cadascun dels tallafocs locals. A la vegada cada un dels tallafocs disposa d'una connexió d'1G RJ-45 tant amb el router principal com el secundari de l'operador. Tot el tràfic generat en aquesta seu s'enruta i es filtra per aquests tallafocs.

2.6- Seu Londres 55 i Londres 57

Aquestes dues seus estan ubicades en edificis contigus, a Londres 55 hi ha 5 racks de planta enllaçats per fibra òptica multimode amb un rack de distribució situat al mateix edifici.

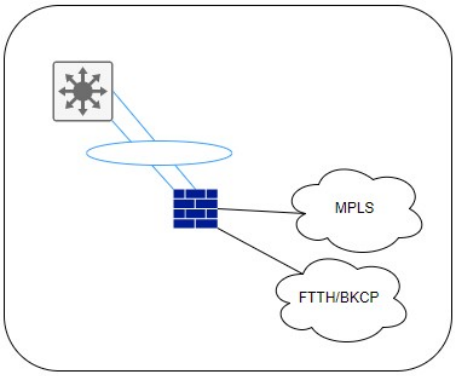
Pel que fa a Londres 57 consta de 2 racks de planta enllaçats per fibra òptica multimode al rack de distribució de Londres 55.

Aquestes seus encara no estan ocupades i no es disposa d'infraestructura, la previsió serà ocupar-les posteriorment a l'adjudicació de la licitació.

2.7- Resta de seus (Reina Amalia, Sant Just, Sant Pau i Tavern)

En la resta de seus incloses en l'annex 2 existeix un únic rack amb equips d'accés que s'agreguen a la xarxa troncal mitjançant una agregació de dos ports d'1G RJ-45 amb el tallafocs local, a la vegada cada un dels tallafocs disposa d'una connexió d'1G RJ-45 tant amb el router principal com el secundari de l'operador.

El diagrama d'aquestes seus, és el següent.



Seus: Reina Amalia, Sant Just, Sant Pau, Tavern

2.8- Xarxa WiFi

La solució actual en les seus objecte d'aquest PPT es basa en 2 controladores cisco WLC 5520 distribuïdes en els dos data centers, aquests gestionen els APs instal·lats en totes les seus mitjançant túnels CAPWAP.

Donat que el tràfic dels clients és processat per les controladores ubicades als data centers, el nivell 3 i servei de seguretat perimetral de les diferents xarxes IP utilitzades en els diferents SSIDs es realitza al tallafocs del data center.

Es treballa principalment amb 3 SSIDs, un amb una configuració enfocada a dispositius amb accés a la xarxa corporativa amb altes prestacions tant de connectivitat com de seguretat, un altre per a dispositius legacy que també requereixen accés a la xarxa corporativa però no suporten modes d'autenticació 802.1x, i un altre per oferir accés Internet a pacients i convidats de forma aïllada a la xarxa corporativa.

3- DESCRIPCIÓ DEL SUBMINISTRAMENT D'EQUIPAMENT I SERVEIS

La solució ha d'incloure el subministrament tant de maquinari com de programari, les empreses licitadores han d'oferir 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.

Donada la licitació de referència 2024-92 en la que es va iniciar la renovació tecnològica de l'electrònica d'accés dels diferents entorns campus gestionats per l'HCB i en la que la solució implantada va ser la del fabricant Fortinet, donada la necessitat d'estandarditzar una solució global en tots els entorns per tal de poder suportar les mateixes prestacions i aquestes es comportin i puguin ser gestionades de la mateixa manera, tot l'equipament de xarxa ofert com a resposta d'aquest PPT haurà de ser del mateix fabricant Fortinet.

Per tal de cobrir les necessitats, l'HCB requereix que es compleixi el següent:

- La solució ha de ser desplegada en mode "claus en mà", on s'inclogui el servei d'instal·lació del nou equipament, la substitució i retirada dels equips actuals, així com la reconnexió de tot el cablejat que dona servei als dispositius connectats.

- La solució proposada pels commutadors d'agregació ha de tenir alta disponibilitat, ha de ser robusta, tolerant a la fallida d'un element qualsevol dels que la composa sense que això suposi una degradació del servei ofert.

- Tot el maquinari ofert constituirà un mateix sistema, integrant-se al que l'HCB ja te implantat donant servei de connectivitat als ordinadors i resta d'equipament.

- S'ha d'incloure tot el llicenciament necessari per cobrir les funcionalitats sol·licitades en el PPT durant tota la durada del contracte.

- Cap dels equips oferts estarà a la llista de End-of-Sale del fabricant.

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, fent ús del formulari que figura a l'annex 2 la relació de productes de maquinari i programari així com la de llicències, que s'inclouran en el subministrament.

3.1- Elements de la xarxa cablejada

En aquest apartat es descriuen els 4 tipus d'equipament requerits per a la solució de xarxa cablatge, en l'annex 3 figuren tots els racks de comunicació on caldrà instal·lar algun dels elements d'aquest apartat, tipus i quantitat d'equipament necessari.

Les empreses licitadores hauran d'incloure a l'oferta tots els mòduls i/o connectors, així com el cablejat necessaris per establir els enllaços d'uplink, downlink i stack. S'utilitzarà sempre ports SFP per a aquesta finalitat per tal de no perdre ports destinats a connectar equipament d'accés.

3.1.1- Equips d'accés amb capacitats Full POE+ i uplinks 10G

Aquest tipus d'equip serà el model estàndard per utilitzar en tots els racks d'accés.

La capçalera pot estar formada per un únic equip en el rack de planta, o per 2 equips en stack dintre del rack de planta.

En el cas que un rack requereixi més de 2 equips, caldrà que els equips addicionals tinguin connectivitat d'uplink amb capacitat mínima de 10G de forma redundada amb 2 enllaços.

A les seus on es requeriran equips de distribució, aquests equips d'accés s'agregaran utilitzant 2 enllaços 10G quan actuïn de capçalera del rack de planta. En les seus on no hi ha capa de distribució (seus definides al punt 2.7), l'agregació al Firewall es realitzarà utilitzant mòduls SFP de 1G RJ45 per tal de reservar el màxim nombre de ports d'accés a la connectivitat de dispositius d'usuari.

Donada la limitació de profunditat d'un nombre reduït de racks, caldrà proposar 2 models diferents d'aquest tipus d'equip, un amb majors capacitats i dimensions pels racks on no hi ha aquesta limitació i un altre de menor dimensions i capacitats pels que si presenten limitació. En l'annex 3, als noms dels racks que tenen aquesta limitació s'ha afegit un caràcter "*".

3.1.2- Equips d'accés amb capacitats multigigabit

L'HCB requereix disposar d'equips amb capacitat mulitigigabit en racks on hi ha concentrada la connectivitat d'un nombre elevat d'APs WiFi o hi ha altres elements amb necessitat de connectivitat d'accés superior a 1Gbps.

Aquests equips actuaran com a equips capçalera dels racks formant un stack entre ells i connectant-se als equips de distribució inclosos en aquest PPT mitjançant una agregació de 2 enllaços (1 enllaç per cada membre de l'stack) de 25Gbps.

A més, aquests equips també han d'agregar fins a 3 equips d'accés amb capacitat full PoE+ i uplinks 10G definits al punt anterior, que formaran part del mateix rack d'accés per donar connectivitat als equips de planta.

Per tal de satisfer la necessitat d'alguns equips d'accés a planta dotats amb tarja de xarxa 10G, s'inclouran 6 mòduls SFP+ RJ45.

3.1.3- Equips de distribució amb enllaços 25G downlink

A la seu central es requereixen 2 equips de distribució amb capacitat d'enllaços downlink de 25G per tal d'agregar els equips d'accés descrits al punt anterior.

Donat que a la seu central la capa de distribució està formada per dos racks de comunicacions en ubicacions físiques diferents es muntarà un equip en cadascun d'aquests racks, els dos equips han de tenir la capacitat de muntar un stack mitjançant les línies de fibres existents entre els dos racks.

L'equipament s'haurà de connectar a la xarxa troncal de comunicacions de l'organització mitjançant 2 enllaços agregats de 4 membres cadascun (un agregat per a cada un dels dos data centers) de 100G.

Aquests equips de distribució hauran d'agregar una parella d'equips de distribució addicionals, els descrits en el proper punt, així com els firewalls locals de la seu central inclosos també en aquest PPT. La interconnexió entre aquests elements serà de 100G i amb redundància.

3.1.4- Equips de distribució amb enllaços 10G downlink

A la capa de distribució de la seu central es requereixen, a més dels 2 equips de distribució anteriorment mencionats, 2 equips de distribució addicionals amb capacitat d'enllaços downlink de 10G per tal d'agregar els equips d'accés descrits al punt 3.1.1.

Es muntarà un equip d'aquests tipus en cadascun dels 2 racks de distribució de la seu central, els dos equips han de tenir la capacitat de muntar un stack mitjançant les línies de fibres existents. Els equips hauran d'estar agregats als equips de distribució descrits en l'apartat anterior utilitzant una agregació de 4 ports 100G (2 ports de cada equip).

A la resta de seus on també es requereix una parella d'equips de distribució també els hi aplica aquest tipus d'equip, en aquests casos els dos equips s'ubicaran en un únic rack de distribució, també hauran de formar un stack entre ells i donar connectivitat redundant als equips d'accés i firewalls locals.

A la seus COEX (allotja el Data Center principal), els equips s'hauran de connectar a la xarxa troncal de comunicacions de l'organització mitjançant un enllaç agregat de 2 ports 100G. Així mateix també hauran de donar connectivitat redundant als firewalls locals de cadascuna de les seus.

3.2- Elements de la xarxa WiFi

Es requereix la substitució 1:1 dels APs actuals per equips amb capacitats de l'estàndard WiFi 7, els APs seran per ús en interiors i es requerirà que alguns d'ells suportin alta densitat d'usuaris per cobrir zones d'alta afluència de dispositius amb necessitats de connectivitat WiFi.

A l'annex 3 es detalla el número d'APs per rack. En el resum de APs totals es detalla quants són APs bàsics i quants d'alta densitat.

3.3- Elements tallafocs / controladors de switch i APs

Una necessitat addicional del projecte és la renovació dels tallafocs de la seu central, Maternitat i Casanova 150, on actualment hi ha una parella d'equips fortigate 500E, pels que Fortinet ja te anunciada data de final de suport al juliol de 2026.

Les licitadores han d'oferir nous equips proposant un model de desplegament en alta disponibilitat i complint amb els requisits indicats a l'annex 1.

3.4 Altres serveis inclosos en l'abast del contracte

3.4.1- Sistema de supervivència en cas de caiguda o pèrdua de connexió amb el NAC

Actualment tot l'equipament d'usuari és validat en la capa d'accés pel NAC corporatiu mitjançant 802.1x o MAB, i aquest retorna la VLAN d'accés al port de switch en funció de la política amb la que coincideix.

Es requereix implementar un mecanisme operatiu per tal que en cas que es perdi la connectivitat amb el NAC, els ports dels switchs mantinguin configurada la darrera VLAN d'accés que aquest ha assignat, i que en recuperar la connectivitat es restauri l'operativa habitual.

El mecanisme a implementar haurà de tenir la capacitat de consultar de forma recurrent la VLAN d'accés assignada pel NAC en tots els ports dels commutadors d'accés i, en cas de detectar que la VLAN assignada és diferent a la que el port aplica en cas de perdre la comunicació amb el NAC, haurà de modificar aquest paràmetre per tal que coincideixi amb l'assignació que ha fet el NAC.

És indispensable que la integració d'aquest mecanisme amb l'electrònica de xarxa de Fortinet sigui via l'eina de gestió centralitzada Fortimanager.

3.4.2- Generació automàtica d'evidències d'auditoria

Per tal de facilitar el compliment normatiu en vers a l'Esquema Nacional de Seguretat (ENS), les licitadores hauran d'incloure mecanismes que ajudin a obtenir de forma automatitzada evidències sol·licitades a les auditories que puguin ser extretes de la infraestructura de xarxa que l'HCB te desplegada amb tecnologia Fortinet. Les licitadores han de presentar una solució que com a mínim permeti generar les següents evidències:

- Validar el grau de compliment dels algoritmes utilitzats en les VPNs vers les recomanacions de l'ENS.
- Capacitat dels enllaços troncals, on es mostri capacitat total versus capacitat consumida.
- Registre d'actualitzacions de programari aplicades sobre els equips.
- Registre de revisions de configuracions i conformitat amb bastionat establert.

3.4.3- Alertes sobre vulnerabilitats de l'equipament

És necessari disposar d'un sistema que consulti diàriament les versions sobre les que treballa l'equipament desplegat contra bases de dades de vulnerabilitats (CVE), i generi informes i alertes en cas que hi hagi alguna coincidència per tal que aquestes siguin tractades el més aviat possible. Es tindrà en compte la flexibilitat a poder incloure elements addicionals.

3.5- Serveis de valor afegit

Addicionalment als punts anteriors, l'HCB té la necessitat d'incloure serveis que donin valor afegit, aquests serveis a l'oferta no són estrictament obligatoris, però donat l'interès de l'HCB en maximitzar el valor de la solució a nivell global, es valoraran positivament, sent sotmesos a judicis de valor.

A continuació es llisten els serveis als que les empreses licitadores hauran de donar resposta, es valorarà la versatilitat de les solucions proposades així com la flexibilitat a que aquestes puguin ser modificades o ampliades davant de noves necessitats futures.

3.5.1- Solució IPAM (IP Address Management)

Actualment l'HCB disposa d'un sistema IPAM estàtic registrat en l'aplicació Nautobot, on es donen d'alta les subxarxes IP utilitzades i després es registren les IPs utilitzades de forma manual, per altra banda s'utilitza la utilitat Netdisco que registra dinàmicament tots els equips connectats a la xarxa, obtenint adreça IP, adreça MAC i hostname però sense funcionalitat IPAM específica. Es valorarà la capacitat de la proposta d'incloure una integració via API entre Nautobot i Netdisco per tal que totes les subxarxes donades d'alta a Nautobot registrin automàticament i de forma periòdica la informació actualitzada present a Netdisco.

3.5.2- Solució d'impressió segura des de xarxa de convidats

L'HCB disposa de xarxes de convidats totalment aïllades de la xarxa corporativa amb només accés a Internet, principalment per a pacients, familiars, visitants i treballadors. Només es dona connectivitat a dispositius personals, no admetent la connexió d'equips corporatius propis de l'HCB.

Addicionalment, aquestes xarxes l'utilitza personal col·laborador extern que treballa en les dependències de l'HCB però no utilitza equipament corporatiu. Aquest personal actualment té la limitació de no poder imprimir, donat que la xarxa de impressió, per política de seguretat, no és visible des de la xarxa de convidats.

Es valorarà que l'oferta inclogui una solució que permeti l'ús de les impressores corporatives des de les xarxes de convidats, mantenint l'aïllament que hi ha en l'actualitat. La solució s'ha de basar en un sistema que actuï d'intermediari entre les dues xarxes, i permeti gestionar i limitar l'ús que en faran els usuaris.

4- GARANTIA

4.1- Garantia de producte

Atesa la naturalesa de la licitació, el període de garantia amb suport certificat pel fabricant haurà de ser obligatòriament per una duració mínima de 5 anys, incloent tot el maquinari i programari que inclogui l'oferta. De la mateixa manera, les subscripcions o llicenciaments requerits pel funcionament i compliment de totes les prestacions definides a l'oferta també han de tenir una durada mínima de 5 anys.

Els serveis prestats per l'HCB es consideren crítics i es presten ininterrompudament les 24 hores dels 7 dies de cada setmana i els 365 dies de l'any, pel que cal que es contempli un servei de suport per incidències per part del fabricant en format 24x7x4 (24 hores, 7 dies a la setmana , 4 hores de temps de resposta).

Per a incidències d'equips que requereixen un canvi de maquinari es requereix un SLA de:

- 8x5xNBD (8 hores, 5 dies a la setmana, de dilluns a divendres de 9 a 17 hores i un temps de resposta al dia següent) dels equips:
    - Equips de distribució .
    - Tallafocs.
- Per a la resta de maquinari inclòs no es defineix SLA.

4.2- Garantia de projecte

Durant el desplegament del projecte i fins el seu traspàs al servei d'operacions de l'HCB, l'adjudicatària es farà càrrec de tota la gestió d'incidències que es doni en qualsevol dels elements de la solució que hagi proposat a la seva oferta tècnica. Aquesta garantia serà addicional a la definida en el punt anterior.

Els serveis que ha d'incloure aquesta garantia són:

- Servei de suport en 24x7x4 (24 hores, 7 dies a la setmana, 4 hores de temps de resposta) i presencia in situ en el cas que la situació ho requereixi, per donar suport a incidents que provoquin caigudes de xarxa, problemes de connectivitat de dispositius o problemes de rendiment amb degradació de servei. El personal tècnic assignat per donar aquest suport hauran de tenir la capacitat tècnica adequada i haurà de conèixer la solució desplegada.
- Identificació, qualificació, diagnosi i escalat de les incidències a la fabricant.
- Gestionar la recepció de peces o equips avariats i realitzar la seva substitució.
- Informar i aplicar les accions requerides quan aparegui alguna vulnerabilitat crítica en qualsevol dels components de la solució.
- Actualització del programari davant noves versions publicades pel fabricant.
- Revisions de la salut del sistema.
- Analitzar i validar els diferents elements després de la instal·lació (configuracions, integracions amb altres elements), en base a aquest anàlisi presentarà riscos detectats i proposarà millores que comportin un guany de rendiment o aportin noves

funcionalitats.

- Servei d'atenció a qualsevol consulta tècnica per part de l'HCB on es doni resposta i solucions en la implementació o modificació de configuracions de les funcionalitats dels equips desplegats.

4.3- Garantia post projecte

S'estableix una garantia d'un any a comptar des del tancament del projecte, en el qual l'adjudicatària haurà de fer front a tasques de resolució de problemes i incidents derivats de la implantació.

Aquest concepte no podrà incórrer en costos de projecte donat que està estrictament lligat a la fiabilitat i qualitat de la implementació.

5- CONDICIONS DE SUBMINISTRAMENT, ENVIAMENT, RECEPCIÓ, INSTAL·LACIÓ I SUBSTITUCIÓ D'EQUIPS

S'entén per equip el conjunt complet de l'equip, màquina o aparell amb tots els accessoris imprescindibles per al seu funcionament, inclòs el programari. Els equips oferts es subministraran amb tots aquells dispositius o elements d'interconnexió, accessoris d'ancoratge o fixació necessaris per a un total i correcte funcionament i obtenció dels corresponents permisos i autoritzacions requerits per la legislació vigent.

Degut al volum d'equipament inclòs en la present licitació, l'HCB no pot garantir la disponibilitat d'espais logístics per al seu emmagatzematge. És per això que l'adjudicatària serà la responsable i haurà de gestionar múltiples lliuraments en base a la planificació de instal·lacions dels elements.

Els equips han d'anar convenientment embalats per tal que arribin en perfectes condicions. El cost de les gestions necessàries per garantir que l'equip es subministra en perfectes condicions, així com el cost dels desperfectes ocasionats en els equips durant en el seu transport fins al lloc de subministrament l'ha d'assumir l'empresa adjudicatària.

En concret, l'empresa adjudicatària es compromet a:

- Realitzar el transport dels equips fins al seu lloc d'ubicació final en les instal·lacions del centre on vagi destinat l'equip.

- Realitzar la retirada de l'embalatge.

- Realitzar la neteja de tots els residus i brutícia produïts per les tasques de desembalatge, recepció, trasllat, muntatge i instal·lació dels equips, per tal de deixar l'espai on s'han realitzat aquestes tasques en les mateixes condicions que es trobava abans de l'arribada dels equips.

L'empresa adjudicatària ha de facilitar el pes i el volum de tots els components embalats que configurin el conjunt de cada equip. De la mateixa manera, cada paquet ha de venir correctament identificat amb codis i textos a efectes de facilitar la seva localització i manipulació.

L'empresa adjudicatària ha d'estar capacitada per portar a terme els serveis de transport, lliurament, instal·lació i servei postvenda de tots els seus productes amb personal propi. En el cas que, alguns d'aquests serveis es subcontractin, l'empresa adjudicatària ho ha de comunicar prèviament a la realització dels serveis i per escrit a l'HCB per a la seva acceptació.

Els equips vindran acompanyats del corresponent albarà. L'albarà inclourà la següent informació:

- Número de comanda
- Descripció del Material
- Nombre d'unitats que es lliuren
- Models, números de sèrie i adreces MAC dels equipaments

El termini de garantia dels equips ha de començar a comptar a partir de la data d'instal·lació de l'equip.

5.1- Instal·lació i substitució d'equips

La instal·lació consistirà en gestionar i realitzar la substitució de l'equipament actual per l'adquirit en el present PPT en tots els edificis, racks i plantes especificats a l'annex 3.

Les tasques associades en els racks de comunicació inclouen la gestió de totes les connexions de cablejat, tenint en compte que totes les connexions actives existents dels dispositius de planta hauran de mantenir-se actives després de la substitució, mantenint la mateixa assignació de VLAN i mode d'assignació (estàtic o dinàmic). Actualment gairebé tots els ports dels commutadors estan configurats per fer un control d'accés mitjançant 802.1x i MAB, en la fase de planificació de la migració de l'electrònica de cada rack l'adjudicatària haurà de revisar les configuracions de l'equipament actual per tal de detectar ports amb configuracions especials o entrades estàtiques a la taula DHCP snooping que s'hagi de traslladar a la configuració dels nous equips.

Les tasques associades a les plantes on s'haurà de substituir els APs inclouen la seva localització fent ús dels plànols facilitats per l'HCB, retirada dels ancoratges de fixació actuals i muntatge dels nous.

L'equipament substituït així com el material associat (cablejat elèctric, de stack, mòduls òptics, etc.), haurà de ser retirat i caldrà gestionar el seu trasllat, rebuig o tractament de residus d'acord a les indicacions del personal designat per l'HCB.

5.1.1- Horaris

Els horaris d'instal·lació s'encaixaran fora de les jornades laborals de les àrees afectades per tal de no interrompre l'activitat professional. Això implica que els horaris hauran de ser de tardes, vespres o matinades de dies laborables o qualsevol hora en caps de setmana o festius, sempre acordat prèviament amb els serveis afectats, l'horari concret per a cada instal·lació serà indicat per l'HCB. Només en casos excepcionals, on tinguem el consentiment dels serveis afectats, es podrà realitzar en horari laboral. Les instal·lacions que afectin a àrees que donin servei 24x7 caldrà planificar-les en horari de menor impacte possible.

5.1.2- Identificació i etiquetatge

Tot els equips lliurats i/o instal·lats hauran d'etiquetar-se amb una identificació única en la part frontal, s'utilitzarà una etiqueta permanent que resisteixi temperatures elevades. L'etiqueta haurà d'estar en una part visible per tal que una vegada instal·lat sigui identificable fàcilment pel personal de l'HCB que el gestiona.

En el cas dels APs, a més de l'etiqueta identificativa de l'equip, haurà d'incloure una segona etiqueta que identifiqui la línia informàtica que ocupa.

La codificació de les etiquetes serà lliurada per l'HCB. Les empreses licitadores inclouran el material necessari per l'etiquetat dintre de l'oferta.

5.1.3- Condicionament dels racks

Els serveis d'instal·lació inclosos en la substitució d'equips haurà de contemplar criteris d'ordre i facilitar les posteriors operatives de manipulació d'elements del rack. Per complir amb aquest propòsit cadascun dels commutadors es muntarà amb un passafils horitzontal a sobre i un altre a sota. El de sobre s'utilitzarà per pentinar els fuetons que es connectin a la filera de ports ethernet de sobre i el de sota per pentinar els fuetons que es connectin a la filera de ports ethernet de sota. S'utilitzaran també els passa fils verticals per conduir el cablatge pels laterals i deixar la part operativa del rack lliure d'obstacles. S'aprofitaran els passafils existents però caldrà preveure que en alguns casos poden requerir-se nous passafils, caldrà identificar aquesta necessitat en la fase de planificació de la instal·lació per tal d'incloure el material

necessari en el moment de la substitució d'equips. Per tal que el resultat sigui òptim es valoraran les opcions que incloguin retirada de tots els elements actuals (electrònica i cablatge) i muntatge del nou equipament i reconnexió de cablatge partint d'un rack buit i lliure d'obstacles, a la vegada que es considerarà que el procés minimitzi talls de servei .

5.2.- Sostenibilitat en el tractament dels equips i material retirats

Les ofertes hauran d'incloure criteris de sostenibilitat en el procés de substitució d'equipament, components o altres materials, retirant els equips vells substituïts i gestionar-ne els residus d'acord amb la normativa aplicable en matèria de residus.

Per facilitar aquest procés l'HCB disposa de zones on dipositar els equips i material de rebuig, serà obligatori que l'adjudicatari les utilitzí de forma responsable amb les instruccions precises sobre el seu ús.

6- Serveis d'implantació i configuració

La planificació de la implantació de la solució s'iniciarà, com a màxim, 15 dies després de la formalització del contracte.

Tota l'activitat associada a la implantació de la solució tecnològica objecte d'aquest plec, així com la seva gestió, correrà a càrrec de l'adjudicatària, i s'haurà de coordinar amb l'equip intern en les diferents actuacions i fases del projecte per tal de garantir la continuïtat del servei actual i garantir la seva transició.

Aquests serveis han d'incloure dissenys, instal·lacions, configuracions, migracions, integració amb la xarxa existent de l'HCB, desplegament de serveis de valor afegits inclosos en la oferta, posada en servei i gestió de canvis.

6.1- Disseny i planificació general

Es proposaran una sèrie de reunions amb el personal de TI de l'Hospital amb l'objectiu de dissenyar amb detall la configuració de la solució i planificar les diferents fases d'implantació. Per a això caldrà una fase inicial d'estudi del disseny lògic actual de les xarxes campus a migrar i proposar un nou disseny en base al mode de funcionament i noves capacitats de l'equipament adquirit. Cal que s'incloguin les següents fites, tenint en compte que aquestes ja han sigut tractades prèviament en la implantació d'equipament Fortinet que l'HCB ja té desplegat i majoritàriament serà suficient en estendre el que ja hi ha definit:

- Hardering dels equips.
- Integració de la seguretat i els equips d'accés.
- Pla de naming/normalització de l'equipament.
- Definició i disseny de VLANs / Adreçaments.
- Arquitectura WiFi (SSIDs, grups, perfils, visualització de les ubicacions dels APs sobre plànols carregats a la plataforma de gestió o controladors, etc.).
- Revisió i redefinició, si cal, dels perfils de seguretat.
- Migració de les configuracions actuals a la nova plataforma.
- Integració amb la solució NAC de l'HCB (OpenNAC Enterprise), mirant d'aprofitar l'alta disponibilitat de nodes radius disponibles pel NAC vs 1 sol node actiu en la plataforma Fortinet.
- Integració amb l'eina de gestió unificada Fortimanager, tenint en compte:
    - Gestió unificada de tallafocs, commutadors i APs.
    - Creació de plantilles que permetin una administració unificada.
    - Configuracions automatitzades pel desplegament de nous equips.
    - Copies de seguretat.

- Configuració SDWAN de les xarxes corresponents a seus on es realitza substitució de tallafocs, configuració que haurà de ser exportable per medi de plantilla a qualsevol altre equip.

- Proposta de gestió d'esdeveniments a identificar, notificacions i automatitzacions de processos a l'eina de gestió de logs centralitzada Fortianalyzer existent.

- Detalls tècnics de funcionament, esquemes lògics, etc.

- Proposta detallada d'implantació de cadascun dels serveis de valor afegit inclosos.

Es requerirà tractar amb especial cura el disseny de la seu Hospital Clínic, destacant la comunicació d'aquest amb els dos data center a través d'enllaços propis, definit a l'apartat 2.2. Actualment hi ha una comunicació de capa 3 utilitzant un enllaç de nivell 2 (utilitzant VLAN de transport), es requereix que es transformi aquest enllaç de nivell 2 a nivell 3 tenint en compte les implicacions d'implementar-la tant a nivell de la nova infraestructura de campus com de l'existent al data center del fabricant Cisco.

La planificació haurà d'incloure totes les tasques necessàries per implantar tan les funcionalitats requerides per l'HCB com les proposades per les licitadores per implementar les funcionalitats de valor afegit. S'inclourà 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'adjudicatària i validat per l'HCB abans de portar-lo a terme.

6.2- Operativa de sistemes

Tots els elements han de quedar integrats a la plataforma de monitorització de l'HCB de la mateixa manera que ho està l'equipament Fortinet ja desplegat, l'adjudicatària revisarà el sistema de monitorització actual conjuntament amb l'equip tècnic de l'HCB per tal de validar-lo. En cas que sigui necessari, l'adjudicatària facilitarà els scripts, OIDs o checks necessaris per monitoritzar l'estat operatiu i de rendiment de tots els equips instal·lats.

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 copies de seguretat de l'HCB.

6.3- Formació

La licitadora ha d'incloure formació per a la correcta administració de la solució implementada, i com a mínim, el següent temari:

- Coneixement de la infraestructura desplegada.

- Administració/Configuració bàsica dels equips i aplicacions que formen part de la solució.

- Troubleshooting bàsic de la infraestructura.

- Realització de copies de seguretat i restauració de les mateixes.

Aquesta formació serà per a 6 persones i es durà a terme quan l'equip de seguiment del projecte ho determini.

6.4- Documentació

La documentació generada en el lliurament de la instal·lació, com a mínim inclourà els següents punts:

- Diagrama de xarxa amb tots els elements de la solució i altres elements amb els que s'integra.
- Document de disseny de la solució on hi constin tots els elements que formen part.
- Pla de proves de la instal·lació efectuades.
- Particularitats de la integració amb elements de la infraestructura de xarxa actual (Commutadors, tallafocs, NAC, eines de gestió, etc.).
- Manuals d'explotació segons metodologia HCB.
- Manuals de Troubleshooting.
- Document gràfic on hi constin les fotografies de tots els racks de comunicacions on s'apreciï l'estat anterior i posterior a la substitució d'equips.
- Inventari d'instal·lació en format full de càlcul on consti el nom de host, número de sèrie, identificador i ubicació on ha quedat instal·lat cadascun dels equips. En el cas dels APs s'afegirà informació de la línia informàtica utilitzada, la informació d'ubicació haurà de mantenir relació amb els punts marcats sobre plànol de planta que també s'entregarà com a documentació d'inventari.

7- OFERTA TÈCNICA A LLIURAR

La oferta tècnica que es lliurarà en el sobre B ha d'incloure els següents punts indexats:

- Resum executiu.
- Disseny general on es presentarà el disseny de la proposta tècnica. Ha d'incloure amb el màxim nivell de detall el conjunt de materials objecte de la licitació incloent maquinari, programari, llicències, adaptadors òptics, cablatge, conversors, etc. No poden faltar esquemes d'arquitectura i disposició de l'equipament amb el màxim de detall.
- Propostes dels serveis de valor afegit on es descriguin les funcionalitats que dotaran les solucions i quedi clar l'abast de la implantació proposada.
- Proposta d'implantació on es definirà el procés de migració des del model actual al proposat i la forma en què es produirà la substitució de l'equipament i desplegament de serveis de valor afegit.
- Proposta inicial de planificació que inclourà el desglossat del projecte en termes de tasques, fites i terminis. La proposta tindrà especialment en compte el nivell de detall referent a la substitució d'equipament en els racks d'accés. Aquesta proposta haurà de servir de base a la que es definirà dins del projecte d'implantació.
- Presentació de l'equip de projecte per perfils i experiència en projectes similars.
- Detall del cap de projecte que liderarà la implantació d'inici a fi, acreditant experiència en projectes d'aquest tipus i dimensions així com coneixements en les tecnologies objecte d'aquest plec.
- Detall dels perfils de l'equip tècnics que formarà part de l'equip de projecte, indicant també la seu de treball.
- Metodologia de gestió de projectes, gestió de canvis i gestió de riscos.
- Model de seguiment del projecte amb els interlocutors assignats per l'HCB.
- Traspàs de la instal·lació a la gestió continuada dels serveis del client.
- Proposta de formació.

Barcelona,

David Vidal Fernández
Direcció de Sistemes d'Informació

ANNEX 1 PPT – DECLARACIÓ RESPONSABLE DEL COMPLIMENT DELS REQUISITS IMPRESCINDIBLES

El/la Sr./Sra....., en nom i representació de l'empresa ..... DECLARA que els equips i solucions que ofereix compleixen amb els requeriments tècnics obligatoris que es relacionen tant a l'apartat 3 com en aquesta declaració, i amb tota la normativa aplicable a la tipologia d'equip subministrat .

	Requisits tècnics imprescindibles
	Característica
	Commutadors d'accés amb capacitats Full POE+ i uplinks 10G
1	Plataforma hardware en format appliance de 1U
2	Ha de disposar de connexió especifica per a configuració, manteniment i monitorització
3	48 ports RJ45 GE (10/100/1000) POE (802.3af/at), 4 ports 10 GE SFP+
4	Memòria del sistema de 1GB
5	Flash de 256MB
6	Buffer de 4MB
7	176 Gbps d'ampla de banda
8	262 milions de paquets per segon (mpps)
9	Latència de xarxa inferior a 1 µs
10	Capacitat d'emmagatzematge de fins a 32.000 MAC Address
11	Suport de fins a 4.000 VLANs
12	Suport d'agregació d'enllaços
14	Doble font d'alimentació
	Commutadors d'accés amb capacitats Full POE+ i uplinks 10G amb limitació de profunditat
1	Plataforma hardware en format appliance de 1U
2	Profunditat màxima de 31 cm
3	48 ports RJ45 GE (10/100/1000) POE (802.3af/at), 4 ports 10 GE SFP+
4	Memòria del sistema de 512MB
5	Buffer de 2MB
7	176 Gbps d'ampla de banda
8	260 milions de paquets per segon (mpps)
9	Latència de xarxa inferior a 1 µs
10	Capacitat d'emmagatzematge de fins a 32.000 MAC Address
11	Suport de fins a 4.000 VLANs
12	Suport d'agregació d'enllaços
	Commutadors d'accés amb capacitat multigigabit
1	Plataforma hardware en format appliance de 1U
2	Ha de disposar de connexió especifica per a configuració, manteniment i monitorització
3	32 ports RJ45 1/2,5 GE PoE(802.3 af/at/bt type 4), 16 ports RJ45 1/2,5/5 GE PoE(802.3 af/at/bt type 4), 8 ports 10/25 GE SFP+/SFP28
4	Memòria del sistema de 4GB
5	Flash de 32MB
6	Buffer de 8MB

7	Disc dur de 32GB SSD
8	720 Gbps d'ampla de banda
9	1.071 milions de paquets per segon (mpps)
10	Latència de xarxa inferior a 1 µs
11	Capacitat d'emmagatzematge de fins a 64.000 MAC Address
12	Suport de fins a 4.000 VLANs
13	Suport de tants grups d'agregació d'enllaços com ports físics disponibles
14	Capacitat d'agregar el 100% dels ports físics en un sol grup d'agregació d'enllaços
15	Doble font d'alimentació
	Commutadors de distribució amb enllaços 25G downlink
1	Plataforma hardware en format appliance de 1U
2	Ha de disposar de connexió especifica per a configuració, manteniment i monitorització
3	48 ports 1/10/25GE SFP28, 8 ports 40/100 QSFP28, 2 ports 1/10GE SFP+
4	Memòria del sistema de 8GB
5	Flash de 8GB
6	Buffer de 32MB
7	Disc dur de 32GB SSD
8	4.000 Gbps d'ampla de banda
9	4.000 milions de paquets per segon (mpps)
10	Latència de xarxa inferior a 1 µs
11	Capacitat d'emmagatzematge de fins a 96.000 MAC Address
12	Suport de fins a 4.000 VLANs
13	8 Cues/Port
14	Suport de 48 grups d'agregació d'enllaços
15	Capacitat d'agregar el 100% dels ports físics en un sol grup d'agregació d'enllaços
16	Doble font d'alimentació
	Commutadors de distribució amb enllaços 10G downlink
1	Plataforma hardware en format appliance de 1U
2	Ha de disposar de connexió especifica per a configuració, manteniment i monitorització
3	48 ports 1/10GE SFP+, 6 ports 40/100 QSFP28
4	Memòria del sistema de 8GB
5	Flash de 128GB
6	Buffer de 12MB
7	Disc dur de 128GB SSD
8	1.760 Gbps d'ampla de banda
9	1.518 milions de paquets per segon (mpps)
10	Latència de xarxa inferior a 800 ns
11	Capacitat d'emmagatzematge de fins a 144.000 MAC Address
12	Suport de fins a 4.000 VLANs
13	8 Cues/Port
14	Suport de 48 grups d'agregació d'enllaços
15	Capacitat d'agregar el 100% dels ports físics en un sol grup d'agregació d'enllaços
16	Doble font d'alimentació
	Funcionalitats comunes a tots els commutadors
1	Suport IPv4 i IPv6

2	Unicast/Multicast
3	VLAN 802.1Q
4	LACP per a l'agregació de ports
5	Gestió i administració
6	Possibilitat de gestionar a través d'una consola centralitzada, amb accés mitjançant RADIUS
7	Possibilitat de tornar a una configuració anterior (Rollback)
8	Suport de SNMP
9	DHCP Snooping amb capacitat de mantenir la taula de bindings generada en cas de caiguda o falta de subministrament elèctric, de manera que un cop es reprengui el servei les connexions dels endpoints no es vegi afectada
10	IP Source Guard
11	DAI (Dynamic ARP Inspection)
12	Qualitat de Servei (QoS): Per Queue Traffic Shaping i Per Port Traffic Shaping
13	Monitorització de tràfic via SPAN i RemoteSPAN (Nivell 2)
14	Autenticació 802.1x i MAB
15	Mínim de 1023 VLAN configurables
16	Capacitat de detecció automàtica dels dispositius connectats en cada port. Cada switch alimentarà de forma automàtica la base de dades de dispositius dels tallafocs mitjançant integració nativa del propi fabricant
17	Automatismes per a que els tallafocs puguin posar en quarentena a dispositius infectats o maliciosos bloquejant de forma automàtica a nivell de port d'accés en el switch
	Funcionalitats solució WiFi
1	Identificació y control d'aplicacions mitjançant inspecció a nivell 7 amb més de 7500 aplicacions reconegudes per aplicar tant seguretat, com control d'ample de banda
2	Funcions de UTM amb antivirus, filtratge de contingut web, IPS, filtratge de email, sandbox integrat, DLP i control d'accés per DNS. Aquestes funcions s'han de poder fer mitjançant tant inspecció profunda SSH/SSL com per inspecció de certificat
3	Seguretat wireless mitjançant WIDS: • Unauthorized Device Detection • Rogue/Interfering AP Detection • Ad-hoc Network Detection and Containment • Wireless Bridge Detection • Weak WEP Detection • MAC OUI Checking
4	Supressió automàtica i contenció de Rogue APs connectats a la LAN i/o emetent SSIDs malintencionats
5	Punts d'accés amb capacitat d'agregar almenys 512 clients connectats a una mateixa radio
6	Solució en alta disponibilitat sense temps d'error i recuperació immediata
7	Tots els APs han de disposar de 3 radios i una BLE/Zigbee. Una radio ha de funcionar a la freqüència de 2.4GHZ, una altra a 5GHz i la tercera a 6GHz
8	Tots els APs han de disposar de tecnologia 802.11be Wi-Fi 7
9	APs d'alta densitat amb les següents prestacions: • 4x4 MU-MIMO • Capacitat de Data Rate: • Radio 1: 1148 Mbps • Radio 2: 8648 Mbps • Radio 3: 11530 Mbps • Dues interfícies 100/1000/2,5G/5G Multigigabit Ethernet • Alimentació mitjançant un port 802.3bt o dos ports 802.3at
10	APs de planta amb les següents prestacions:

	• 2x2 MU-MIMO • Capacitat de Data Rate: • Radio 1: 668 Mbps • Radio 2: 2882 Mbps • Radio 3: 5765 Mbps • Una interfície 100/1000/2,5G/5G Multigigabit Ethernet • Alimentació mitjançant un port 802.3at
11	Disposar de múltiples opcions de connectivitat incloses en els controladors wireless sense necessitat d'afegir elements addicionals. • Autenticació estàndard WPA2/WPA3 • Autenticació d'usuari mitjançant portal captiu personalitzable • Autenticació de dispositius mitjançant claus compartides dinàmiques, de forma que en un SSID puguin distribuir-se diferents claus compartides a dispositius o grups de dispositius
12	Connectivitat d'usuaris mitjançant tunelització fins al controlador o als ports LAN on es connecta l'AP. La connectivitat als ports LAN on es connecta l'AP ha de poder configurar-se de forma flexible, mitjançant les següents opcions: • Bridge amb un SSID concret de l'AP • Bridge amb la interfície LAN connectada al switch • NAT amb la interfície LAN connectada al switch
13	S'ha de poder realitzar perfilat dels dispositius mitjançant signatures integrades o mitjançant la integració amb un servei de base de dades de perfils
14	Es podrà aplicar diferents criteris d'accés a la xarxa sense fils en funció de: • Fabricant del hardware • Tipus de dispositiu • Sistema operatiu • Família de dispositiu • Adreça MAC o grup d'adreces MAC
15	Els punts d'accés han de poder realitzar les funcions de monitorització i captura de tràfic per a poder realitzar el perfilat des del controlador wireless
16	Quan s'apliqui una regla de control d'accés, el controlador podrà aplicar les següents funcions: • Assignació de VLAN • Aplicar polítiques de seguretat NGFW específiques • Aplicar polítiques de QoS i traffic shaping • Accés autenticat mitjançant portal captiu
	Tallafocs seu Clínic
1	Plataforma hardware en format appliance de 2U
2	NGFW Throughput de 34Gbps
3	SSL Inspection Throughput de 29Gbps
4	Ha de suportar la gestió de fins a 300 Fortiswitch i fins a 2048 FortiAPs en mode tunel
5	6 ports 100G QSFP28/40G QSFP+, 16 ports 25G SFP28/10G SFP+, 18 ports 1G/10G RJ45, 2 ports 1G RJ45
	Tallafocs seu Maternitat
1	Plataforma hardware en format appliance de 1U
2	NGFW Throughput de 7Gbps
3	SSL Inspection Throughput de 7 Gbps
4	Ha de suportar la gestió de fins a 64 Fortiswitch i fins a 128 FortiAPs en mode tunel
5	8 ports 10G SFP+, 8 ports 5G RJ45, 10 ports 1G RJ45, 4 ports 1G SFP
	Tallafocs seu Casanova 150
1	Plataforma hardware en format appliance de 1U
2	NGFW Throughput de 3.1 Gbps
3	SSL Inspection Throughput de 3 Gbps

4	Ha de suportar la gestió de fins a 48 Fortiswitch i fins a 64 FortiAPs en mode tunel
5	4 ports 10G SFP+, 18 ports 1G RJ45, 8 ports 1G SFP
	Funcionalitats comunes a tots els tallafocs
1	Doble font d'alimentació
2	Ha de disposar de discs locals.
3	L'alta disponibilitat ha de permetre la transferència de servei d'un equip a l'altre sense talls ni pèrdua de les connexions tcp. Les configuracions s'han de traspassar de manera automàtica entre els dos equips.
4	Capacitat de funcionament en mode actiu/actiu sincronitzant sessions entre els dos nodes però mantenint adreçament IP diferenciat en les interfícies de cada node del clúster
5	Suport de protocols RIP v1/v2, OSPF, ISIS, BGP, WCCP i Multicast per IPv4 e IPv6, Routing basat en política o PBR i funcionalitats avançades SD-WAN
6	Suport de VRFs (múltiples taules de Routing) i multiVRF Routing (per BGP i OSPF)
7	Suport Dual Stack IPv4 e IPv6 simultàniament
8	Network address translation NAT IPv4, NAT64 i NAT66
9	DHCP server / DHCP Relay /DNS Server / DNS Proxy / NTP Server
10	802.1Q VLANs i Point-to-Point Protocol over Ethernet (PPPoE)
11	802.3ad Capacitat de crear enllaços LACP per l'agregació de ports
12	Capacitat de balanceig de servidors a nivell 4 per tots els serveis, com també possibilitat de fer SSL off-loading pel tràfic HTTPS
13	Suport d'VXLAN i VXLAN VTEP per extensió de nivell 2 sobre xarxes de nivell 3
14	Capacitat de protecció anti DoS (Denegació de Servei) implementada per hardware contra atacs volumètrics
15	Suport de QoS per hardware incloent traffic shaping i queuing
16	S'ha de poder seleccionar quin tràfic s'analitzarà a nivell 4 i quin a nivell 7, per política
17	Funcionalitats de antivirus, webfilter, DNS filter, Web Application Firewall, Control d'aplicacions, IPS, i DLP
18	Capacitat de creació de regles de DoS a nivell 3 i 4, podent aplicar umbrals per serveis publicats on poder filtrar per direccions ip o països
19	Capacitat de definir polítiques a nivell d'interfície per tal de denegar tràfic i no ser processat per la política de seguretat global. S'han de poder utilitzar direccions IP, països, així com rangs i xarxes ip com a origen
20	Per tal d'evitar l'accés de xarxes botnet, els tallafocs han de tenir una base de dades de reputació dinàmica que bloquegi els accessos a nivell d'interfície
21	Visualització del número d'usos i quantitat de tràfic de cada regla de seguretat, de forma àgil tant en la pròpia secció de polítiques de seguretat, així com també dintre de la configuració de cada política. També cal veure l'ultima vegada que s'ha utilitzat
22	Capacitat per identificar un mínim de 4400 aplicacions actives actuals (incloent aplicacions web 2.0), com per exemple distingir Facebook, d'una sub-aplicació Facebook-chat o post. La solució ha de classificar les aplicacions en diferents categories i subcategories, per poder aplicar regles d'acord amb aquestes categories/subcategories (control granular dins de l'aplicació)
23	Capacitat per identificar les aplicacions sota túnels HTTPS
24	Capacitat per identificar aplicacions Industrials com Modbus
25	Capacitat de creació de firmes d'aplicacions per un reconeixement personalitzat. Es obligatori que en aquelles aplicacions customitzades, també siguin analitzades per motors de protecció (IPS i antimalware)
26	Capacitat per protegir tant servidors com clients amb un mínim de 11.000 signatures d'IPS, agrupades per categoria, severitat, objectiu i protocol. Davant la identificació d'un atac per IPS, cal que el tallafocs capturi el tràfic en un arxiu pcap per tal d'evidenciar-ho i fer un estudi posterior
27	Capacitat per identificar patrons d'atacs basats en comportament o rated-base, per tal de bloquejar intents d'atacs un cop superat un umbral d'ús en un temps determinat
28	Capacitat de creació de firmes d'IPS per un reconeixement personalitzat

29	Capacitat de detecció de malware (virus, grayware, worns, etc…) basat en firmes conegudes o mètodes avançats de detecció
30	Suport de sandboxing en el cloud
31	Capacitat per l'eliminació del contingut dinàmic (macros, javascript, URL) explotable dintre de documents ofimàtics i pdf, que es distribueixen per protocols SMTP, IMAP i HTTP
32	Capacitat de comprovació de si es tracta d'un fitxer bo o dolent, en funció del hashing i comparat amb la BBDD del fabricant. Així com bloquejar malware mitjançant repositoris externs de threat inteligence
33	Capacitat de categoritzar més de 250 milions de pàgines web en més de 60 categories web per tal d'aplicar: block, monitor i aplicació de cuotes de temps o tràfic per categoria. Suport de protocols http v1.0, 1.1 i 1.2. La base de dades de categories web caldrà consumir-se com un servei cloud en temps real i no podrà basar-se únicament en llistats locals per tal de tenir la categorització de les URL's el més actualitzat possible. Suport per restringir l'accés a Youtube i Google en mode "safe search". Suport de rating per imatges per URL. Suport per a la creació de llistes blanques/negres externes sense necessitat de llicencia
34	DNS Filter. Capacitat de categoritzar domins DNS en més de 60 categories per poder realitzar intercepció del tràfic DNS amb les següents accions: block, monitor i redirect (redirigir les consultes cap a un portal web cloud o personalitzat de bloqueig). La base de dades de categories dns caldrà consumir-se com un servei cloud en temps real i no podrà basar-se únicament en llistats locals per tal de tenir la categorització de les url's el més actualitzat possible. Suport per a la creació de llistes blanques/negres externes sense necessitat de llicencia
35	Els equips han de disposar de la funcionalitat de Firewalls virtuals per tal de crear entorns completament diferencials, incloent com a mínim 10 Firewalls virtuals. En el cas d'activar sistemes virtuals, aquests han de poder funcionar en qualsevol dels dos nodes
36	Funcionalitats de control d'aplicacions, IPS, Antimalware amb Cloud Sandbox inclós, Webfilter, DNS Filter, Antispam, protecció anti DoS i Web Application Firewall
38	Hauran de disposar de la funcionalitat d'auditoria pròpia del sistema, que com a resultat tingui un indicador o valor numèric de risc, així com puntuació negativa per cada paràmetre auditat no complert. Aquests paràmetres que s'han de comprovar seran com a mínim: política de seguretat sense ús en els últims 90 dies, política de contrasenyes dèbils i comprovació del llicenciament/suport
39	La pròpia plataforma ha de tenir connectors automàtics amb l'objectiu d'integrar-se amb identitats terceres i poder recollir informació, adreçament ip, inventari d'objectes i etiquetes. Aquesta funcionalitat haurà d'estar suportada en els appliances de seguretat (sense necessitat de consola addicional). En concret es requereixen les següents: • Cloud pública: Google Cloud, Azure, AWS, Oracle i AliCloud. • Cloud privada: VMware NSX i ESXi, Openstack, Kubernetes, Cisco ACI i Nuage. • Fonts d'identitat: Active directory i Radius. • Fonts d'amaneces: Llistat d'ip, dominis, URLs i hash's de malware customitzats.
40	Davant la detecció d'un host compromès, els tallafocs han de tenir la capacitat d'enviar un email, una notificació tipus push, poder banejar l'adreça ip, invocar funcions AWS Lambda, Google functions, Azure Functions i Webhook
41	Davant el canvi de configuració del tallafocs, un failover, reboot, actualització de firmes de forma programada i qualsevol event, els tallafocs han de tenir la capacitat d'enviar un email, una notificació tipus push a dispositius i invocar funcions AWS Lambda, Google functions, Azure Functions, AliCloud Function, comanda per CLI i Webhook

Signatura
Iloc i data

ANNEX 2 PPT – FORMULARI DE PRODUCTES MAQUINARI I PROGRAMARI QUE S'INCLOURAN EN EL SUBMINISTRAMENT

En aquest formulari, es recull la relació detallada d'articles inclosos en la solució proposada:

Fabricant	Part Number	Descripció	Quantitat

ANNEX 3 PPT – RELACIÓ RACKS PER SEU AMB EL TIPUS I QUANTITAT DE NOU EQUIPAMENT REQUERIT

Edifici	Rack	Accés Multigigabit	Accés Full PoE+	Distribució 10G	Distribució 25G	APs WiFi
Casanova 150	CPD	0	0	2	0	0
Casanova 150	Planta -1	0	2	0	0	5
Casanova 150	Plata 1	0	1	0	0	2
Casanova 150	Plata 2	0	1	0	0	2
Casanova 150	Plata 3	0	1	0	0	3
Casanova 150	Plata 4	0	1	0	0	2
Casanova 150	Plata 5	0	1	0	0	2
COEX	CPD	0	0	2	0	0
COEX	CEX0R	0	2	0	0	4
COEX	CEX0C	0	3	0	0	7
COEX	CEX-1C	0	2	0	0	3
COEX	10A	1	2	0	0	6
COEX	10B	0	3	0	0	1
COEX	CEX1C	0	2	0	0	3
COEX	CEX3C	0	3	0	0	10
COEX	CEX3R	0	3	0	0	0
COEX	CEX5C	0	4	0	0	10
COEX	CEX5R	0	3	0	0	2
COEX	SdC	0	1	0	0	1
COEX - Rehabilitació	26* (depèn de CEX1C)	0	1	0	0	0
COEX - Facultat S8N-1	FMS8-1	0	1	0	0	4
Hospital Plato - COEX	HP222 (depèn de HP221)	0	1	0	0	0
Hospital Plato - COEX	HP232	0	1	0	0	2
Hospital Plato - COEX	HP241 (depèn de HP232)	0	1	0	0	1
Hospital Plato - COEX	HP201	0	1	0	0	5
Hospital Plato - COEX	HP211	0	1	0	0	4
Hospital Plato - COEX	HP221	0	1	0	0	5
Hospital Plato	HP11	0	2	0	0	7
Hospital Plato	HP103	0	1	0	0	0
Hospital Plato	CPD core	0	0	2	0	0
Hospital Plato	CPD access	0	2	0	0	0
Hospital Plato	HP111	0	1	0	0	1
Hospital Plato	HP113	0	2	0	0	1
Hospital Plato	HP131	0	3	0	0	16
Hospital Plato	HP151	0	2	0	0	11

Hospital Plato	HP1S2	0	1	0	0	1
Hospital Plato	HP101	0	1	0	0	2
Hospital Plato	HP102	0	1	0	0	1
Hospital Plato	HP104	0	1	0	0	0
Hospital Plato - Marc Aureli	HPM	0	2	0	0	5
Tavern	HPTA	0	1	0	0	2
Maternitat	AN-1	0	3	0	0	8
Maternitat	PO0	0	4	0	0	8
Maternitat	LL1	0	2	0	0	0
Maternitat	LL0 (CPD)	0	0	2	0	0
Maternitat	LL0 (acces)	0	2	0	0	8
Maternitat	LL3	0	2	0	0	11
Maternitat	PO1	0	2	0	0	5
Maternitat	PO2	0	3	0	0	6
Maternitat	HEL1	0	3	0	0	7
Maternitat	HEL2	0	2	0	0	9
Maternitat	HE3	0	4	0	0	6
Reina Amalia	RAM101*	0	1	0	0	3
Sant Pau	SPAU	0	1	0	0	3
Sant Just	SJ	0	1	0	0	3
Seu central	DISTUR	0	0	1	1	0
Seu central	DISTVN	0	0	1	1	0
Seu central	1511A	0	2	0	0	3
Seu central	1411A	0	2	0	0	3
Seu central	76	0	3	0	0	5
Seu central	901A	0	3	0	0	0
Seu central	0	0	1	0	0	0
Seu central	31A	0	2	0	0	0
Seu central	62	0	1	0	0	1
Seu central	81A	0	1	0	0	2
Seu central	Seguretat	0	1	0	0	0
Seu central	101A	0	1	0	0	0
Seu central	141A	0	4	0	0	0
Seu central	161A	0	3	0	0	2
Seu central	1051A	0	2	0	0	0
Seu central	103	0	4	0	0	0
Seu central	1101A	0	2	0	0	0
Seu central	1111A	2	0	0	0	21
Seu central	1121A	2	2	0	0	18
Seu central	1131A	0	2	0	0	0
Seu central	1141A	2	1	0	0	21
Seu central	1151A	0	4	0	0	0
Seu central	1201A	0	4	0	0	0
Seu central	1211A	2	1	0	0	23

Seu central	1221A	2	1	0	0	11
Seu central	1241A	2	0	0	0	18
Seu central	31	0	4	0	0	1
Seu central	31A	0	2	0	0	0
Seu central	311A	2	1	0	0	23
Seu central	321A	2	2	0	0	20
Seu central	331A	0	3	0	0	0
Seu central	341A	2	1	0	0	24
Seu central	351A	0	4	0	0	1
Seu central	361A	0	3	0	0	2
Seu central	371A	0	4	0	0	11
Seu central	372A	0	1	0	0	0
Seu central	302A	0	1	0	0	1
Seu central	230	0	2	0	0	0
Seu central	4	0	1	0	0	0
Seu central	401A	0	3	0	0	0
Seu central	402A	0	1	0	0	0
Seu central	411A	2	0	0	0	27
Seu central	421A	2	0	0	0	19
Seu central	422A	0	3	0	0	1
Seu central	431A	0	3	0	0	1
Seu central	441A	2	0	0	0	20
Seu central	442A	0	4	0	0	5
Seu central	451A	0	3	0	0	0
Seu central	461A	0	2	0	0	1
Seu central	471A	0	1	0	0	3
Seu central	501A	0	3	0	0	1
Seu central	511A	2	1	0	0	28
Seu central	521A	2	1	0	0	20
Seu central	531A	0	2	0	0	0
Seu central	551A	2	0	0	0	0
Seu central	611A	0	3	0	0	5
Seu central	601A	0	5	0	0	1
Seu central	612A	0	2	0	0	22
Seu central	621A	2	1	0	0	22
Seu central	631A	0	2	0	0	0
Seu central	641A	2	3	0	0	20
Seu central	731A	0	4	0	0	0
Seu central	741A	2	1	0	0	22
Seu central	751A	0	3	0	0	0
Seu central	771A	0	1	0	0	0
Seu central	851A	0	1	0	0	0
Seu central	901A	0	3	0	0	0
Seu central	911A	0	3	0	0	0
Seu central	971A	0	2	0	0	6

Seu central	1301A	0	1	0	0	2
Seu central	1311A	0	2	0	0	2
Seu central	1351A	0	3	0	0	1
Seu central - CELLEX	CEL42	0	2	0	0	8
Seu central - CELLEX	CEL44	0	2	0	0	4
Seu central - CELLEX	CEL62	0	2	0	0	4
Seu central - CELLEX	CEL64	0	2	0	0	4
Londres 55-57	CPD	0	0	2	0	0
Londres 57 - CAPSBE	Planta Baixa	0	2	0	0	4
Londres 57 - CAPSBE	Planta Altell	0	2	0	0	3
Londres 55	Planta Baixa	0	1	0	0	3
Londres 55	Planta Altell	0	1	0	0	3
Londres 55	Planta 1	0	2	0	0	4
Londres 55	Planta 2	0	2	0	0	4
Londres 55	Planta 3	0	2	0	0	4
Londres 55	Planta 4	0	2	0	0	4
Londres 55	Planta 5	0	2	0	0	4
STOCK		2	10	0	0	35

Resum del total d'equipament per tipus i assignació a Lot:

	Equips d'accés Multigigabit	Equips d'accés 10G Full PoE	Equips de distribució 10G	Equips de distribució 25G	APs WiFi
Total	39	270	12	2	736
1 - HCB	39	235	10	2	630
2 - FCRB	0	35	2	0	106

* Racks amb limitació de profunditat (corresponent a 1 HCB)

** 5 APs del total hauran de suportar alta densitat d'usuaris (corresponent a 1 HCB)

ANNEX 4 PPT – INVENTARI EQUIPAMENT TALLAFOCS PER SEU

Seu	Tallafocs
Seu central	Fortigate 500E*
Casanova 150	Fortigate 500E*
Maternitat	Fortigate 500E*
COEX	Fortigate 600E
Hospital Plato	Fortigate 600E
Tavern	Fortigate 60F
Reina Amalia	Fortigate 60F
Sant Pau	Fortigate 60F
Sant Just	Fortigate 60F
Londres 55	Fortigate 100F**

* Model que haurà de ser substituït dintre la present licitació dintre de 1 hcb.
** L'equip no està en producció, a la espera de desplegar la seu.

ANNEX 5 PPT – REQUISITS GENERALS DE SEGURETAT PER A LA CONTRACTACIÓ DE SERVEIS I PRODUCTE SEGONS L'ENS

A5.1 - Introducció i objectius

Aquest annex té com a objectiu informar dels requisits de seguretat que haurà de complir qualsevol servei i/o producte amb característiques IT o OT que es vulgui implantar a l'HCB en compliment dels requisits exigits per l'Esquema Nacional de Seguretat (ENS en endavant).

A5.2 - Abast

Tractar tots els serveis i productes que necessitin ser desplegats o integrats a la infraestructura IT de l'HCB. En el cas de productes, es consideraran dins de l'abast tant els sistemes de TI com els OT, IOT i IOMT.

Aquest annex pretén incloure tant la casuística de compliment com la de no compliment de la legalitat vigent, en aquest cas respecte de l'ENS.

A5.3 - Aspectes generals de seguretat per a la contractació de serveis

Davant del procés de contractació i incorporació d'un servei cal seguir en tot moment el principi de professionalitat, segons l'article 16 de l'ENS:

- La seguretat dels sistemes d'informació estarà atesa i serà revisada i auditada per personal qualificat, dedicat i instruït en totes les fases del cicle de vida: planificació, disseny, adquisició, construcció, desplegament, explotació, manteniment, gestió d'incidències i desmantellament.
- Les organitzacions que prestin serveis a l'HCB han de comptar amb professionals qualificats i amb uns nivells idonis de gestió i maduresa en els serveis prestats.
- Es determinaran els requisits de formació i experiència necessària del personal per al desenvolupament del lloc de treball.

A5.3.1 - Requisits per a la contractació de serveis

Cal que l'empresa que prestarà el servei presenti certificat de conformitat amb l'ENS relatiu al servei que es pretén prestar. Per defecte es sol·licitarà per a la provisió de serveis que sustentin les activitats principals de l'HCB, un certificat de Nivell ALT.

Aquest requisit aplica a qualsevol implantació d'infraestructura d'IT i OT, por per exemple xarxes, emmagatzemament, servidors, dispositius de còpies de seguretat i altres elements d'infraestructura. Aplica tanmateix al desplegament d'elements de programari específics de suport a la infraestructura tecnològica o de suport a negoci.

Qualsevol component o producte subministrat dins el servei caldrà que compleixi els criteris indicats a l'apartat A7.4 "Aspectes generals de seguretat per a la contractació de productes"

L'HCB podrà requerir del proveïdor, a més a més del certificat de conformitat amb l'ENS del servei a contractar, el detall de la declaració d'aplicabilitat i mesures utilitzades per garantir que els components proveïts garanteixin els requisits de l'ENS.

A5.3.2 – Subcontractació

L'entitat proveïdora del servei haurà de disposar d'una documentació que detalli clarament els elements que formen part de la cadena de subcontractació, així com les implicacions derivades de qualsevol canvi o modificació que pugui patir algun esglaó d'aquesta cadena. El proveïdor haurà d'assegurar que els sistemes d'informació de les empreses subcontractades són conformes amb l' ENS pel que fa als serveis que afectin a l'HCB, per la qual cosa el contingut del present annex resultarà així mateix d'aplicació a la cadena de subministrament del proveïdor.

En aquest sentit, l'HCB podrà requerir del prestador, a més de la corresponent certificació de conformitat amb l' ENS, el detall de la declaració d'aplicabilitat i, si s'escau, de les mesures compensatòries i complementàries de vigilància utilitzades.

A5.3.3 - Requisits del servei de subministrament i configuració d'elements de xarxa

Es presenten els requisits específics per aquest tipus de servei, segons ENS, nivell ALT:

- **Configuració final del subministrament d'equips de xarxa:**

mp.com	Protecció de les comunicacions		BAIX	MITJÀ	ALT
mp.com.1	Perímetre segur	Categoria	aplica	aplica	aplica
mp.com.2	Protecció de la confidencialitat	C	aplica	+ R1	+ R1 + R2 + R3
mp.com.3	Protecció de la integritat i de la autenticitat	I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
mp.com.4	Separació en fluxos d'informació a la xarxa	Categoria	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4

- **Documentació general del sistema segons:**

op.pl.2	Arquitectura de Seguridad	Categoria	aplica	+ R1	+ R1 + R2 + R3

- **Protecció dels Serveis que suporti el sistema:**

mp.s.2	Protecció de serveis i aplicatius web	Categoria	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3

A5.3.4 - Requisits del servei de desenvolupament de programari

Es presenten els requisits específics per a aquest tipus de Servei, segons ENS, nivell ALT:

- Desenvolupament Mitjançant Metodologia de Desenvolupament de Programari Segur:

mp.sw	Protecció de les aplicacions informàtiques	Dimensió	BAJO	MITJÀ	ALT
mp.sw.1	Desenvolupament de programari	Categoria	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4

mp.sw.2	Acceptació i posada en servei	Categoria	aplica	+ R1	+ R1

Requisits.

- [mp.sw.1.1] El desenvolupament d'aplicacions es realitzarà sobre un sistema diferent i separat del de producció, no havent d'existir eines o dades de desenvolupament en l' entorn de producció, ni dades de producció en el de desenvolupament.

  Reforç R1-Mínim privilegi.

- [mp.sw.1.r1.1] Les aplicacions es desenvoluparan respectant el principi de mínim privilegi, accedint únicament als recursos imprescindibles per a la seva funció, i amb els privilegis que siguin indispensables.

  Reforç R2-Metodologia de desenvolupament segur.

- [mp.sw.1.r2.1] S'aplicarà una metodologia de desenvolupament segur reconeguda que:
  a) Tindrà en consideració els aspectes de seguretat al llarg de tot el cicle de vida.
  b) Inclourà normes de programació segura, especialment: control d'assignació i alliberament de memòria, desbordament de memòria (*overflow*).
  c) Tractarà específicament les dades usades en proves.

  Permetrà la inspecció del codi font.

S'haurà de tenir en compte la guia de Desenvolupament Segur del CCN quan es tractin de desenvolupaments Web "CCN-STIC-812 Guia de Seguretat en Entorns i Aplicacions Web" així com la guia relativa a desenvolupament segur "CCN-CERT Recomanacions sobre desenvolupament segur"

Reforç R3-Seguretat des del disseny.

- [mp.sw.1.r3.1] Els següents elements seran part integral del disseny del sistema:
  a) Els mecanismes d' identificació i autenticació.
  b) Els mecanismes de protecció de la informació tractada.
  c) La generació i tractament de pistes d' auditoria.

Reforç R4-Dades de proves.

- [mp.sw.1.r4.1] Preferiblement, les proves prèvies a la implantació o modificació dels sistemes d' informació no es realitzaran amb dades reals. En cas que fos necessari recórrer a dades reals es garantirà el nivell de seguretat corresponent.

  Reforç R5-Llista de components programari.

- [mp.sw.1.r5.1] El desenvolupador elaborarà i mantindrà actualitzada una relació formal dels components programari de tercers emprats en l' aplicació o producte. Es mantindrà un històric dels components utilitzats en les diferents versions del programari. El contingut mínim de la llista de components, que contindrà, almenys, la identificació del component, el fabricant i la versió emprada.

- Protecció de les Comunicacions en el Desenvolupament:

Caldrà que el desenvolupament tingui en compte el compliment del requisits relatius a les comunicacions:

mp.com	Protecció de les comunicacions	Dimensió	BAIX	MITJÀ	ALT
mp.com.2	Protecció de la confidencialitat	C	aplica	+ R1	+ R1 + R2 + R3
mp.com.3	Protecció de la integritat i de l'autenticitat	I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
mp.com.4	Separació en fluxos d'informació a la xarxa	Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4

Documentació general del sistema segons:
El desenvolupament ha d'incloure una descripció de la seva arquitectura de sistemes, si escau i la manera en que compleix els requisits d'arquitectura de seguretat.

op.pl.2	Arquitectura de Seguretat	Categoria	aplica	+ R1	+ R1 + R2 + R3

- Protecció dels Serveis desenvolupats:
Caldrà que el desenvolupament tingui en compte el compliment del requisits relatius a la protecció de serveis i aplicatius web.

mp.s.2	Protecció de serveis i aplicacions web	Categoria	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3

A5.3.5 - Serveis al núvol

Addicionalment si el servei ofert es tracta de serveis al núvol l'adjudicatari haurà de:

- Complir les guies del CCN-STIC (Centre Criptològic Nacional) ja siguin en modalitat IaaS, PaaS o SaaS vigents aplicables en funció de la modalitat relatives a la gestió, manteniment, configuració, administració, disseny i explotació
- Realitzar auditories de proves de penetració.
- Ser transparent en quant a facilitar informació relativa al servei i infraestructures prestada.
- Utilitzar xifratge de dades i gestionar les claus d'acord amb les guies del CCN-STIC.
- Facilitar una avaluació d'impacte associada al servei que es presta.

A5.3.6 - Excepcions

Com a excepció, **si l'entitat licitadora no disposés dels requisits anteriors**, s'acceptarà el disposar de la certificació sobre l'abast del servei mitjançant la ISO 27001.
No obstant això, en cas que aquesta sigui l'opció escollida, l'empresa proveïdora **haurà de presentar el pla d'adequació a l'Esquema Nacional de Seguretat en nivell Alt**.

Addicionalment es requerirà una declaració d'aplicabilitat segons els requisits de l'Annex II de l'ENS per conèixer com compleix la solució aportada cadascun dels requisits, si li aplica o no i en cas d'haver-hi responsabilitats creuades entre l'HCB i el proveïdor, com està pensat s'organitzi i es doni suport a cadascuna de les mesures.

A5.4 - Aspectes generals de seguretat per a la contractació de productes

Els dispositius que conformen el sistema han de tenir una configuració de seguretat adequada per garantir el control del flux definit d'entrada i sortida de la informació. Els dispositius presents a la xarxa que disposin d'algun tipus d'emmagatzematge temporal o d'informació permanent proporcionaran la funcionalitat necessària per eliminar informació dels suports d'informació.

Per garantir que el producte o productes implantats a l'HCB compleix les directrius de seguretat mínimes, la plataforma haurà de complir algun dels següents requisits per ordre de rellevància:

A5.4.1 - Primera opció – "Certificació del producte al catàleg de productes i serveis de seguretat de les tecnologies de la Informació i comunicació"

Si el producte ja està a la llista "Guia de Seguretat de les TIC CCN-STIC 105" caldrà remetre el certificat corresponent emès per entitat equivalent.

A5.4.2 - Segona opció – certificació internacional del producte

El producte o la solució amb qualsevol característica IT haurà d'estar certificada en alguna homologació nacional o internacional de seguretat.

Llistat de Certificacions admissibles:

- **Common Criteria CC/CEM v3.1** (CC= Common Criteria for Information Technology Security Evaluation): EAL3
- **SOGIS MRA v3** (Senior Officers Group for Information Systems, Mutual Recognition Agreement), per:
    - Smartcards and Similar Devices - Aquest domini tècnic està relacionat amb les targetes intel·ligents i dispositius similars.
    - Hardware Devices with Security Boxes - Aquest domini tècnic està relacionat amb productes compostos per una o més plaques de circuit imprès on gran part de la funcionalitat de seguretat requerida depèn del seu embolcall físic (l'anomenada caixa de seguretat)

A5.4.3 - Tercera opció – auditoria de seguretat

Disposar d'un informe d'auditoria de seguretat de la informació aportat per una entitat certificada en el camp de la seguretat de la informació amb certificació ISO 27001 o ENS, amb els resultats recents com a màxim de sis mesos, en què no es detectin riscos ni vulnerabilitats de nivell crític ni alts.

Aquesta auditoria ha de ser del tipus caixa blanca, presentant contra quins marcs de seguretat s'han realitzat, presentant un resum executiu del resultat i haurà d'indicar segons els criteris de l'article 19 de l'ENS i els criteris de la Guia "CCN-STIC 140 Taxonomia de referència per a productes de seguretat TIC", si es considera:

- Favorable
- Favorable amb NO confirmades (en tal cas incloure Pla d'Accions Correctives)

A5.4.4 - Quarta opció – declaració de responsabilitat legal i qüestionari de seguretat

S'haurà d'emplenar un formulari associat a les característiques del producte o productes oferts per conèixer el grau de compliment de seguretat que ofereix i el pla d'acció que prendrà l'oferent per solucionar-lo en cas de no complir els requisits.

Aquest formulari haurà d'anar acompanyat d'una declaració de responsabilitat signada per l'apoderat de l'entitat proveïdora avalant la veracitat de les dades proporcionades per part del proveïdor relatius al nivell de compliment dels requisits de seguretat del producte.

S'hauran d'aportar per a cada apartat els detalls i evidències suficients per corroborar el compliment del requisit. Els aspectes per valorar són els següents:

- ***El producte incorpora canals de comunicació fiables i segurs:*** *cal establir canals de comunicació segurs entre les parts utilitzant algoritmes i protocols segons la guia CCNSTIC-807 (ex.: HTTPS/TLS 1.2 o superior, IPSEC, etc.).*

Compleix requisits: *SI ☁ NO ☁*
En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

- ***El producte s'executa sobre una plataforma fiable:*** *incloent-hi el sistema operatiu o qualsevol entorn d'execució i dependència sobre el qual s'utilitzi. Les versions de les plataformes i productes relacionats han de ser les recomanades per les guies de seguretat CCN-STIC.*
    - *Seran admissibles, encara que no recomanables, versions que estiguin properes al final del seu cicle de vida i que encara tinguin suport amb actualitzacions de seguretat, amb el compromís d'evolucionar a versions superiors suportades.*
    - *En cap cas no s'acceptaran versions o dependències sense suport del fabricant o fora del seu cicle de vida.*

Compleix requisits: *SI ☁ NO ☁*
En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

- ***El producte té capacitat antiexplotació:*** *Depenent de l'àmbit del producte s'autoprotegirà quan estigui en execució, per exemple: protecció contra atacs de força bruta, protecció contra manipulacions, protecció contra manipulació de fitxers, etc. El producte ha d'estar configurat amb els permisos més restrictius, sense permisos d'accés a fitxers de manera anònima i protegir els accessos no autoritzats.*

Compleix requisits: *SI* ☁ *NO* ☁
En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

- ***El producte tindrà actualitzacions periòdiques per evitar vulnerabilitats i obsolescència:*** *El desenvolupament del producte serà actualitzat pel proveïdor durant el cicle de vida d'aquest i comunicarà les actualitzacions evolutives o que corregeixin vulnerabilitats conegudes a fitxers i protegir els accessos no autoritzats.*

Compleix requisits: *SI* ☁ *NO* ☁
En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

- ***El producte aporta restriccions d'accés a àrees restringides:*** *El producte ha de controlar l'accés a la interfície de gestió i control d'usuaris amb accés restringit mitjançant sessions no manipulables.*

Compleix requisits: *SI* ☁ *NO* ☁
En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

- ***El producte no permet la possibilitat d'injecció de codi:*** *El producte ha de controlar que els paràmetres rebuts per part de l'usuari siguin correctes i no permetin la injecció de codi o manipulació de dades.*

Compleix requisits: *SI* ☁ *NO* ☁
En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

- ***El producte us permet assegurar una política de contrasenyes robustes:*** *El producte ha de contenir un sistema de control i gestió d'autenticació mitjançant contrasenyes segures i/o certificats digitals.*

Compleix requisits: *SI* ☁ *NO* ☁

En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

- ***El producte incorpora un mètode de xifratge:*** *El producte ha de contenir un sistema de xifratge que garanteixi la protecció de dades sensibles.*

Compleix requisits: *SI* ☁ *NO* ☁
En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

- ***El producte permet utilitzar usuaris d'administració nominals:*** *El producte ha de treballar amb usuaris nominals i no es permetran comptes genèrics o compartits.*

Compleix requisits: *SI* ☁ *NO* ☁
En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

- ***El producte incorpora capacitat d'auditoria:*** *El producte ha de permetre el control de sessions, la traçabilitat de les accions dels usuaris i administradors.*

Compleix requisits: *SI* ☁ *NO* ☁
En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

Un cop rebudes les evidències i les respostes a cadascun dels punts, en cas d'incompliment de tres o més requisits que apliquin a la solució proposada es considerarà el producte com a no vàlid. Quan no es compleixin un o dos punts, l'adjudicatari haurà de donar solució en temps d'implantació en coordinació de l'equip tècnic de l'HCB. En cas que algun d'aquests requisits no apliqui s'hauran d'exposar els motius.

A5.5 - Recordatori documentació tècnica exigible

Es recorda que qualsevol producte amb connexions de TI ha d'incorporar com a documentació:

- Guies d'Instal·lació Segura
- Llistat de Components programari i maquinari que el constitueixen
- Proposta de Pla d'actualitzacions per cobrir elements obsolets de programari

A5.6 - Avaluació d'impacte

Per complir els requisits que es desprenen de la legislació de protecció de dades personals vigent, en cas que, per tipologia de dades personals, finalitat, emplaçament de l'adjudicatari, quantitat de dades, nova tecnologia o qualsevol circumstància que aconselli realitzar una avaluació d'impacte sobre la privadesa, es traslladarà a l'adjudicatari l'obligació de realitzar aquesta avaluació, seguint les indicacions del delegat de protecció de dades de l'HCB per detectar els riscos derivats del tractament de dades personals.