

PLEC DE PRESCRIPCIONS TÈCNIQUES

**SUBMINISTRAMENT DE MAQUINARI I PROGRAMARI I SERVEIS PROFESSIONALS
PER A LA RENOVACIÓ TECNOLÒGICA D'EQUIPS D'ACCÉS A LA XARXA DE
COMUNICACIONS, AMB DESTÍ A L'HOSPITAL CLÍNIC DE BARCELONA**

Núm. d'exp. 2024-92

1- OBJECTE	3
2- INFRAESTRUCTURA DE LA XARXA CAMPUS	4
2.1- XARXA TRONCAL.....	4
2.2- SEUS CEK, CÒRSEGA 176, CÒRSEGA 180 I URGELL 216	5
2.3- SEU MALLORCA 183.....	5
2.4- RESTA DE SEUS.....	5
2.5- XARXA WIFI	7
3- DESCRIPCIÓ DEL SUBMINISTRAMENT.....	8
3.1- ELEMENTS DE LA XARXA CABLEJADA.....	9
3.2- ELEMENTS DE LA XARXA WIFI.....	9
3.3- EINA PER LA VISIBILITAT UNIFICADA I REGISTRES	10
4- GARANTIA	11
4.1- GARANTIA DE PRODUCTE.....	11
4.2- GARANTIA DE PROJECTE	11
4.3- GARANTIA POST PROJECTE.....	12
5- CONDICIONS DE SUBMINISTRAMENT, ENVIAMENT, RECEPCIÓ, INSTAL·LACIÓ I SUBSTITUCIÓ D'EQUIPS	13
5.1- INSTAL·LACIÓ I SUBSTITUCIÓ D'EQUIPS	14
5.2- SOSTENIBILITAT EN EL TRACTAMENT DELS EQUIPS I MATERIAL RETIRATS	15
6- SERVEIS D'IMPLANTACIÓ I CONFIGURACIÓ	16
6.1- DISSENY I PLANIFICACIÓ GENERAL	16
6.2- OPERATIVA DE SISTEMES.....	17
6.3- FORMACIÓ	17
6.4- DOCUMENTACIÓ	18
7- OFERTA TÈCNICA A LLIURAR.....	19
ANNEX 1 PPT – DECLARACIÓ RESPONSABLE DEL COMPLIMENT DELS REQUISITS IMPRESCINDIBLES.....	20
ANNEX 2 PPT – FORMULARI DE PRODUCTES QUE S'INCLOUREN EN EL SUBMINISTRAMENT	24
ANNEX 3 PPT – RELACIÓ RACKS/SEU, TIPUS I QUANTITAT DE NOU EQUIPAMENT REQUERIT	25
ANNEX 4 PPT – INVENTARI EQUIPAMENT TALLAFOCS PER SEU	26
ANNEX 5 PPT – REQUISITS GENERALS DE SEGURETAT PER A LA CONTRACTACIÓ DE SERVEIS I PRODUCTE SEGONS L'ENS.....	27
A5.1 - INTRODUCCIÓ I OBJECTIUS	27
A5.2 - ABAST	27
A5.3 - ASPECTES GENERALS DE SEGURETAT PER A LA CONTRACTACIÓ DE SERVEIS.....	27
A5.4 - ASPECTES GENERALS DE SEGURETAT PER A LA CONTRACTACIÓ DE PRODUCTES	31
A5.5 - RECORDATORI DOCUMENTACIÓ TÈCNICA EXIGIBLE	36
A5.6 - AVALUACIÓ D'IMPACTE.....	36

1- OBJECTE

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 seus concretes de l'Hospital Clínic de Barcelona (en endavant HCB) i entitats vinculades. Aquesta renovació té com objectiu l'estandardització d'equipament així com la substitució de l'equipament actual que ha arribat o està a punt d'arribar al seu final de vida útil marcat pel fabricant.

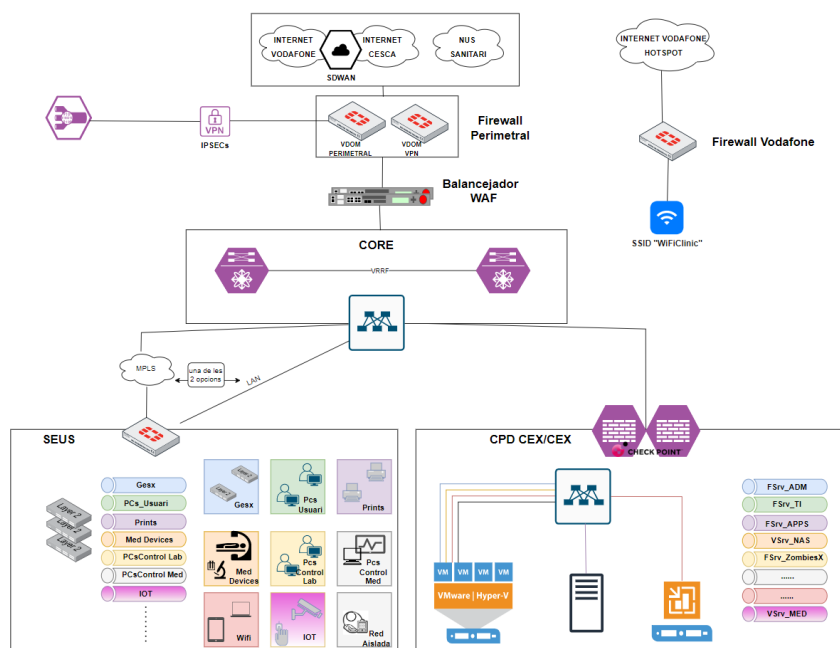
Les ubicacions descrites en el plec així com el número d'elements a instal·lar a cadascuna d'elles es consideren orientatives. El desplegament definitiu podrà ser variat d'acord amb les necessitats indicades l'HCB. No obstant l'anterior, el nombre total d'elements de cada tipologia no es veurà incrementat.

De la mateixa forma, s'espera que el present concurs presenti millores i noves prestacions que permetin operar, treballar i oferir un servei de connectivitat a la xarxa de l'HCB de la forma més òptima aprofitant els darrers avenços tecnològics.

2- INFRAESTRUCTURA DE LA XARXA CAMPUS

La xarxa campus està formada per 31 edificis en el moment de redacció d'aquest PPT, tot i que l'abast de la renovació es contempla només en 18, tots ells amb connectivitat a la xarxa troncal que hi ha distribuïda en dos *data centers*.

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.

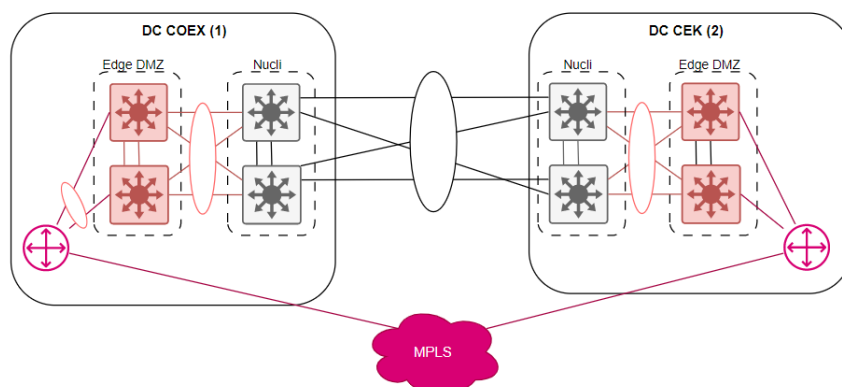
A nivell general, les seus incloses dins l'abast disposen actualment d'un equip que realitza el nivell 3 amb capacitats de tallafocs/enrutament i equips d'accés amb autenticació 802.1x i MAB. En una de les seus, degut al volum s'inclouen equips d'agregació per tal d'enllaçar els equips d'accés amb connexions de fibra cap a l'element de nivell 3. Tots els commutadors d'accés i distribució, així com els punts d'accés *WiFi* de les 18 seus mencionades són objecte de substitució dintre aquest PPT.

A l'annex 2 hi ha un llistat de *racks* de comunicació de les seus 18 seus. El *rack* on la columna "tipus" és "DIST" correspon a la seu on es disposa d'equips de distribució, quan la columna "dependència" sigui diferent a la de "edifici" indica que l'accés a la xarxa troncal es a través d'un *rack* d'una altra seu.

2.1- Xarxa troncal

La xarxa troncal de l'HCB està distribuïda entre dos *data centers*, el principal situat dins de la seu COEX i el secundari situat dintre de la seu CEK. Com ja s'ha mencionat anteriorment, 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 CEK, Còrsega 176, Còrsega 180 i Urgell 216

La seu CEK disposa d'un *rack* de distribució situat al *data center* secundari 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 disposen d'una estesa de 4 parells de fibra multimode acabada amb connectors LC/PC amb el *rack* de distribució. Addicionalment els *racks* d'accés de les seus Còrsega 176 i Urgell 216 també depenen d'aquest *rack* de distribució, on arriben amb una estesa de 4 parells de fibra monomode acabada amb connectors LC/PC.

El *rack* d'accés de la seu Còrsega 180 està enllaçat amb 4 esteses de parell de coure amb el de Còrsega 176.

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 CEK.

2.3- Seu Mallorca 183

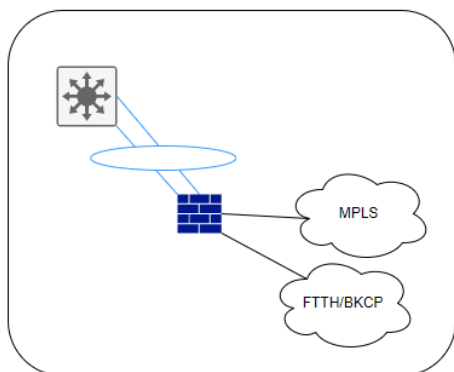
En aquesta seu es disposa d'un *rack* d'accés/distribució unit per quatre esteses de parells de coure amb cada un dels dos *racks* d'accés del mateix edifici.

L'equip que actua de distribució també ho fa d'accés, l'agregació a la xarxa troncal es realitza mitjançant una agregació de dos ports d'1G RJ-45 amb el tallafocs local. A la vegada el tallafocs disposa d'una connexió d'1G RJ-45 tant amb el rúter principal com el secundari de l'operador. Tot el tràfic generat en aquesta seu s'enruta i es filtra per aquest tallafocs.

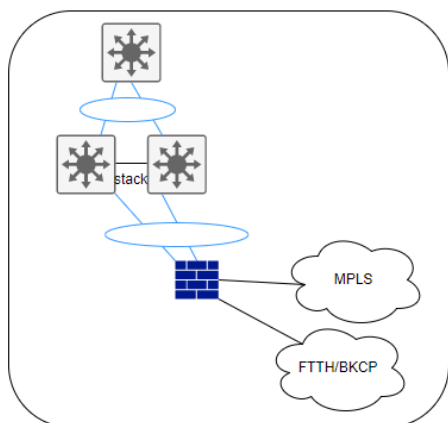
2.4- Resta de seus

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 rúter principal com el secundari de l'operador.

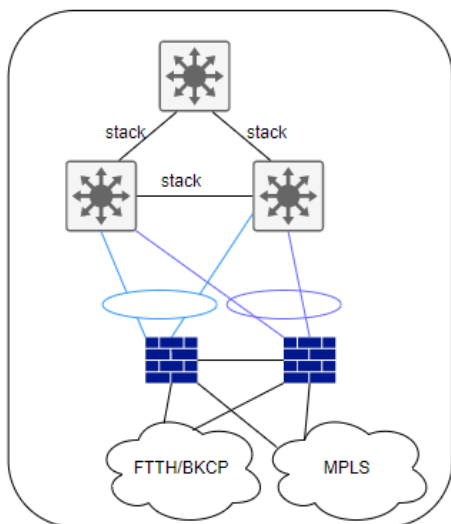
El diagrama d'aquestes seus, segons es disposi d'un o més equips de capçalera i/o un o dos tallafocs és el següent.



Seus: Rosselló 132, Casanova 153, Provença 156, Cornellà



Seus: Borrell 303, Manso, Enric Granados 86, Urgell 204, Rosselló 138



Seus: Còrsega 173, Granollers

Mencionar el cas especial de les seus:

- **Rosselló 140.** Aquesta seu connecta mitjançant una estesa de 2 parells de fibres multimode acabades amb connectors ST amb l'equip d'accés capçalera de la seu Rosselló 138.

- **Rosselló 132.** Aquesta seu es divideix en 2 plantes, la planta del segon pis connecta amb la del primer mitjançant l'estesa de dos parells de core.
- **Casanova 155.** Aquestes dues seu, connecta mitjançant una estesa de 4 parells de fibres multimode acabades amb connectors LC/PC amb l'equip d'accés capçalera de la seu Casanova 153.

2.5- Xarxa WiFi

La solució actual es basa en 2 controladores cisco WLC 5520 distribuïdes en els dos *data centers*. Aquests gestionen la totalitat dels 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

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.

Actualment l'HCb necessita un nou enfocament per oferir una connectivitat segura i d'alt rendiment entre usuaris i aplicacions. La solució proposada ha de permetre disposar de visibilitat, administració i protecció de forma centralitzada per assolir una protecció extrem a extrem i poder donar una resposta automatitzada a qualsevol amenaça, oferint una protecció integral davant incidents de ciberseguretat en temps real.

Igualment, la solució ha de disposar d'un anàlisi centralitzat impulsat per intel·ligència artificial (IA) i la prevenció automatitzada.

També ha de permetre l'automatització de processos per tal de simplificar les implementacions mitjançant plantilles centralitzades amb desplegament automàtic mitjançant Zero Touch Provisioning (ZTP) tant a commutadors com a APs.

La solució ha de ser capaç de mantenir una postura de seguretat sòlida en tots els entorns de xarxa de les seues objectes d'aquest PPT, permetent aplicar polítiques de capa 7 amb funcionalitats addicionals de seguretat (IPS, AV...) entre dos clients ja sigui en el tràfic nord-sud (diferents segments de xarxa) com en el tràfic est-oest (mateix segment de xarxa i domini de broadcast).

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 reconexió 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 compona sense que això suposi una degradació del servei ofert.
- Tot el maquinari ofert constituirà un mateix sistema que donarà servei de connectivitat als ordinadors i resta d'equipament de la companyia. Per maximitzar les prestacions de baixa latència, màxim rendiment i facilitar la gestió, tot el maquinari ofert haurà de ser del mateix fabricant. Tot el material, connectors i adaptadors necessaris inclosos, ha de ser nou i original del fabricant.
- Per tal de garantir una total integració i homogeneïtat amb l'equipament de seguretat actual de cada seu (gestionar i aplicar polítiques unificades, monitorització, etc.) es requereix una plataforma o via única d'operació de l'equipament de xarxa cablejada i WiFi amb els equips de Nivell3/tallafoc de cada seu, es pot consultar un llistat en l'annex 4. Quedaran excloses totes les solucions que no facin servir la pròpia gestió webGUI del tallafocs, com integracions via API i similars que no siguin del mateix fabricant del maquinari.
- S'haurà 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 haurà d'estar 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.

Les licitadores detallaran, fent ús del formulari que figura a l'Annex 2 la relació de productes de maquinari i Programari així com de llicències que s'inclouran en el subministrament.

3.1- Elements de la xarxa cablejada

En aquest apartat es descriuen els 2 tipus d'equipament requerits per a la solució de xarxa cablejada. A 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.

Els licitadors hauran d'incloure a l'oferta tots els mòduls i/o connectors, així com el cablatge necessaris per establir els enllaços d'*uplink*, *downlink* i *stack* d'acord amb el disseny de connectivitat entre elements que presentin.

3.1.2- 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 la seu CEK, on es requeriran equips de distribució, aquests equips d'accés s'agregaran utilitzant 2 enllaços 10G quan actuïn de capçalera del *rack* de planta.

3.1.4- Equips de distribució amb enllaços 10G downlink

A la capa de distribució de la seu CEK es requereixen 2 equips d'aquest tipus funcionant en *stack* i alta disponibilitat per tal d'agregar els equips d'accés descrits en el punt anterior i els *firewalls* locals de seu.

Els equips s'hauran de connectar a la xarxa troncal de comunicacions de l'organització mitjançant un enllaç agregat de 2 ports 100G.

3.2- Elements de la xarxa WiFi

Es requereix la substitució 1:1 dels APs actuals per equips amb capacitats de l'estàndard *WiFi* 6E.

La solució *WiFi* proposada ha d'oferir una arquitectura única des d'on es pugui realitzar una gestió unificada, control d'accés i seguretat NGFW aplicat a tot l'entorn LAN/WAN i *WiFi*. Aquesta gestió unificada ha de permetre poder segmentar la infraestructura en diferents controladors *wireless* que tinguin la configuració centralitzada en únic punt.

La proposta ha de ser sòlida des del punt de vista de seguretat, connectivitat, experiència d'usuari i control d'accés. A la taula de l'annex 3 es detalla el número d'APs per seu.

3.3- Eina per la visibilitat unificada i registres

En l'actualitat, l'HCB disposa d'un Fortianalyzer 400E com a eina per la visualització i anàlisi de l'estat de la xarxa i fluxes de tràfic. És la voluntat d'aquest plec actualitzar aquesta eina per tal de suportar les noves càrregues estimades.

La solució proposada ha de proporcionar les capacitats i funcionalitats pròpies d'una eina d'informes i registres, totalment extern a l'equipament maquinari de seguretat, per ampliar les capacitats de visibilitat, gestió d'alarmes i esdeveniments que proporcionen les diferents plataformes, així com d'altres dispositius de tercers compatibles amb Syslog.

La solució proposada ha de suportar les mateixes funcionalitats que la solució actual i, com a mínim, afegir les següents capacitats:

- Creació de Playbooks il·limitats.
- Mapeig d'incidents de seguretat en la matriu de MITRE ATT&CK.
- Desplegament de paquets per la detecció de *malware*.

4- GARANTIA

4.1- Garantia de producte

Atesa la naturalesa de la licitació, el període de garantia certificada pel fabricant haurà de ser obligatòriament per una duració de 5 anys, incloent maquinari i programari. De la mateixa manera, les subscripcions o llicenciaments requerits pel funcionament i compliment de totes les prestacions definides a la 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
 - Controladors *WiFi* en el cas que la solució els contempli.
 - Equip de visibilitat unificada i registres.
- 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 del 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 en 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 8x5x4 (8 hores, 5 dies a la setmana, de dilluns a divendres de 9 a 17 hores i un temps de resposta en 4 hores) i presència 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. Els tècnics assignats per donar aquest suport hauran de tenir la capacitat tècnica adequada i hauran de conèixer la solució desplegada.
- Identificació, qualificació, diagnosi i escalat de les incidències al 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 despleats.

4.3- Garantia post projecte

S'estableix una garantia d'un any a comptar des de el 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 el seu emmagatzematge. És per això que l'adjudicatària serà la responsable i haurà de gestionar els 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'haurà 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 de lliurament de l'albarà o 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, altres mecanismes de seguretat presents que també caldrà conservar o proposar alternatives per aconseguir el mateix propòsit són: bloqueig de la comunicació entre equips del mateix segment ("protected port"), "DHCP Snooping", "IP source guard" i "ARP inspection", en la fase de planificació de la migració de la electrònica de cada *rack* l'adjudicatari 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 matinalades dels 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.

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. Els licitadors 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 cada un 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 passa fils existents però caldrà preveure que en alguns casos poden requerir-se nous passa fils, caldrà identificar aquesta necessitat en la fase de planificació de la instal·lació per tal d'incloure el material necessari, que serà proporcionat per l'HCB.

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 utilitzi 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'adjudicatari, 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, 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 la xarxa 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:

- Hardening 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.).
- Definició dels perfils de seguretat a desplegar i aplicar.
- Migració de les configuracions actuals a la nova plataforma.
- Integració amb la solució NAC de l'HCB.
- Proposta de gestió i operació 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.
 - Còpies de seguretat.
- Disseny bàsic de SDWAN que permeti la evolució cap a una arquitectura full SDWAN.
- Proposta de gestió d'events a identificar, notificacions i automatitzacions de processos a l'eina de gestió de logs.

- Detalls tècnics de funcionament, esquemes lògics, etc.

La planificació haurà d'incloure totes les tasques necessàries per implantar tan les funcionalitats requerides per l'HCB 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.

6.2- Operativa de sistemes

Tots els elements han de quedar integrats a la plataforma de monitorització de l'HCB, l'adjudicatari facilitarà els scripts, OIDs o checks necessaris per monitoritzar l'estat operatiu i de rendiment de tots els equips instal·lats i col·laborarà en el procés d'implantació i validació. En aquest sentit serà necessari un treball conjunt amb l'equip tècnic de l'HCB que garanteixi la generació d'alertes de qualsevol anomalia que pugui donar-se en els equips instal·lats. Cada alerta establerta haurà de tenir documentat i procedimentat el pla d'acció operatiu per a la seva gestió o resolució. 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 i estat de clúster.
- Caigudes de serveis o equipament maquinari.

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

6.3- Formació

Les licitadores hauran d'incloure formació per a la correcta administració de la solució implementada, amb un mínim de 2 jornades.

Aquesta formació haurà d'incloure 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 còpies 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.
- Particularitats de la integració amb elements de la infraestructura de xarxa actual (Commutadors, tallafocs, NAC, eines de gestió, etc.).
- Pla de proves de la instal·lació efectuades.
- 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

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

- Resum executiu.
- Declaració signada corresponent a l'annex 1 del PPT.
- Formulari de productes corresponent a l'annex 2 del PPT.
- Disseny general on es presentarà 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, requeriments d'energia i de connectivitat, etc. així com la descripció de la solució proposada referent a arquitectura de connexió entre elements, detalls tècnics de funcionament com el temps de convergència en la fallida dels components significatius, esquema de la disposició de tots els elements amb el màxim de detall, etc.
- 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 actual pel del nou escenari.
- Integració de la solució en les operatives de sistemes de l'HCB referent a monitorització i backup.
- Presentació de l'equip de projecte per perfils i experiència en projectes similars. Aquest haurà de incloure un 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. Es presentaran també les certificacions del personal tècnic que participarà respecte de la solució proposada i la que actualment té implantada l'HCB.
- Proposta inicial de planificació que inclourà el desglossament 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.
- Referències de projectes similars que garanteixin l'experiència de l'empresa en la implantació de les solucions i tecnologies que oferta en aquest plec.
- Metodologia de gestió de projectes, gestió de canvis i gestió de riscos i seguiment amb els interlocutors assignats per l'HCB.
- Traspàs de la instal·lació a la gestió continuada dels serveis del client, ha d'incloure formació i documentació.

Es recorda que en aquest sobre no es pot incloure informació inclosa en el sobre A, ni característiques valorades en el sobre C, fer-ho serà motiu d'exclusió.

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 <i>hardware</i> en format appliance de 1U
2	Ha de disposar de connexió específica 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 de 8 grups d'agregació d'enllaços
13	Capacitat d'agregar el 100% dels ports físics en un sol grup d'agregació d'enllaços
14	Doble font d'alimentació
Commutadors de distribució amb enllaços 10G downlink	
1	Plataforma <i>hardware</i> en format appliance de 1U
2	Ha de disposar de connexió específica 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 punts d'accés han de tenir com a mínim 2 ports ethernet i suportar LACP
8	Tots els APs han de disposar de 3 radios suportant les freqüències de 2.4GHz, 5GHz i 6GHz respectivament.
9	Tots els APs han de disposar de tecnologia 802.11ax Wi-Fi 6E
10	APs de planta amb les següents prestacions: 2x2 MU-MIMO - Capacitat de Data Rate: - Radio 1: 574 Mbps - Radio 2: 1201 Mbps - Radio 3: 2401 Mbps - Una interfície 100/1000/2500 Base-T i una interfície 10/100/1000 Base-T RJ45 - 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	El controlador wireless haurà de disposar de funcionalitats de control d'accés dinàmic en funció del dispositiu o tipus de dispositiu connectat
14	S'ha de poder realitzar perfilat dels dispositius mitjançant signatures integrades o mitjançant la integració amb un servei de base de dades de perfils
15	Es podrà aplicar diferents criteris d'accés a la xarxa sense fils en funció de: • Fabricant del maquinari • Tipus de dispositiu • Sistema operatiu • Família de dispositiu • Adreça MAC o grup d'adreces MAC
16	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
17	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 autènticat mitjançant portal captiu
Eina per la visibilitat unificada i registres	
1	Plataforma <i>hardware</i> en format appliance de 3U
2	Capacitat de recepció de registres via Syslog
3	Capacitat analítica de 60.000 logs/sec sostinguts
4	Suport RAID 0/1,1s/5,5s/6,6s/10/50/60
5	Fonts d'alimentació redundants intercanviables en calent
6	Emmagatzemament total de 64 TB (16 discos de 4TB) i 56 TB en RAID
7	Discs reemplaçables en calent
8	2 interfícies Gigabit Ethernet, 2 interfícies 25GE SFP28
9	Suport IPv6 per a la gestió de la plataforma i recepció de registres.
10	Permetre la integració a través de l'API REST.
11	Poder agrupar els diferents elements que envien registres en contextos d'administració diferents.
12	Suport RADIUS, LDAP i TACACS+ per a l'autenticació dels usuaris d'administració.
13	El sistema emmagatzemarà els registres en una base de dades SQL, que podrà ser consultat amb comandes SQL.
14	Suport de sincronització horària amb el protocol NTP
15	Cal disposar d'una interfície gràfica per a la consulta de registres, permetent realitzar cerques
16	Suport d'enviament de Traps SNMP v.1/v.2
17	Ha de permetre l'exportació manual o automàtica de registres a través de FTP, SFTP, SCP
18	Capacitat d'importació de logs prèviament exportats

19	Permetre la generació d'un conjunt d'informes fàcilment personalitzats, permetent analitzar, informar i emmagatzemar esdeveniments de seguretat, tràfic, contingut web i missatges per al compliment de les polítiques de l'organització.
20	Permetre realitzar un anàlisi en temps real i històric del tràfic generat a l'entorn. La informació serà presentada consolidada, permetent centrar l'activitat a les tasques més crítiques. Entre altres vistes ha de disposar de vistes de Top Orígens, Top Amenaces, Top Aplicacions, etc.
21	Analitzar la informació de forma granular, aplicant filtres a nivell global, de domini administratiu, de dispositiu o domini virtual. De igual forma ha de poder fer agrupacions dels elements prèviament citats amb l'objectiu de mostrar la informació seleccionada en el gràfic o el dashboard que composin el perfil en funció del conjunt de dispositius seleccionats.
22	Permetre definir diferents vistes personalitzades per a cada dispositiu monitoritzat, de manera que es mostri la informació específica en cada situació i en temps real.
23	Mitjançant la gestió d'esdeveniments ha de generar alertes que permetin monitoritzar i rebre notificacions d'una activitat específica a la xarxa. S'ha de poder configurar les alertes pel nivell de gravetat establint un límit per damunt del qual s'enviarà el detall de l'esdeveniment d'alerta a una adreça de correu electrònic, servidor SNMP o servidor de Syslog. Així mateix, cal poder cercar un text genèric als registres de manera que el sistema envii una alerta quan una nova entrada al registre contingui la cadena de text especificada.
24	L'eina ha d'incloure diferents informes predefinits, permetent, a més, afegir informes addicionals gràcies a les seves eines d'elaboració de consultes a la base de dades i composició de gràfics. Al mateix temps s'ha de programar l'execució automàtica d'un informe, per rebre'l en el correu electrònic en format PDF.

Signatura
lloc i data

ANNEX 2 PPT – FORMULARI DE PRODUCTES QUE S'INCLOUREN EN EL SUBMINISTRAMENT

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

Fabricant	Part Number	Descripció	Quantitat

ANNEX 3 PPT – RELACIÓ RACKS/SEU, TIPUS I QUANTITAT DE NOU EQUIPAMENT REQUERIT

Les ubicacions descrites així com el número d'elements a instal·lar a cadascuna d'elles es consideren orientatives. El desplegament definitiu podrà ser variat d'acord amb les necessitats indicades l'HCB. No obstant l'anterior, el nombre total d'elements de cada tipus no es veurà incrementat.

Rack	Tipus	Edifici	Dependencia	Equips d'accés	Equips de distribució	APs WiFi de planta
BOR303	Accés	Borrell 303	Borrell 303	3	0	9
CAS 153	Accés	Casanova 153	Casanova 153	1	0	3
CAS 155	Accés	Casanova 155	Casanova 153	1	0	2
CDM	Accés	Manso	Manso	2	0	5
CBK_CPD	DIST	CEK	CEK	0	2	0
CBK-1	Accés	CEK	CEK	4	0	9
CBK0	Accés	CEK	CEK	2	0	5
CBK1	Accés	CEK	CEK	3	0	12
CBK2	Accés	CEK	CEK	2	0	12
CBK3	Accés	CEK	CEK	3	0	12
CBK4	Accés	CEK	CEK	2	0	12
CBK5	Accés	CEK	CEK	2	0	12
URG216	Accés	Urgell 216	CEK	2	0	2
COR173	Accés	Corsega 173	Corsega 173	2	0	3
COR176	Accés	Corsega 176	CEK	1	0	3
COR180	Accés	Corsega 180	Corsega 176	1	0	3
COR59	Accés	Cornella	Cornella	1	0	2
EG86	Accés	Enric Granados 86	Enric Granados 86	2	0	2
GRA	Accés	Granollers	Granollers	3	0	6
MLL42S	Accés	Mallorca 183	Mallorca 183	1	0	3
MLL420	ACCES / DIST	Mallorca 183	Mallorca 183	2	0	4
MLL421	Accés	Mallorca 183	Mallorca 183	2	0	3
PRO156	Accés	Provença 156	Provença 156	1	0	2
UR204	Accés	Urgell 204	Urgell 204	2	0	2
ROS132-22	Accés	Rossello 132	Rossello 132	1	0	1
ROS132-11	Accés	Rossello 132	Rossello 132	1	0	2
ROS138_7	Accés	Rossello 138	Rossello 138	2	0	4
ROS140_19	Accés	Rossello 140	Rossello 138	2	0	3
ESTOC				7	0	12
				Total Equips d'accés	Total Equips de distribució	Total APs WiFi
				58	2	150

ANNEX 4 PPT – INVENTARI EQUIPAMENT TALLAFOCS PER SEU

Seu	Tallafof/N3
Borrell 303	FG60F
Casanova 153	FG60F
Casanova 155	Depèn de Casanova 153
CEK	FG200F (clúster)
Cornella	FG60F
Còrsega 173	FG60F (clúster)
Còrsega 176	Depenen de CEK
Còrsega 180	Depenen de Còrsega 176
Enric Granados 86	FG60F
Granollers	FG60F (clúster)
Mallorca	FG60F
Manso	FG60F
Provença 156	FG60F
Rosselló 132	FG60F
Rosselló 138	FG60F
Rosselló 140	Depenen de Rosello-138
Urgell 216	Depenen de CEK
Urgell 204	FG60F

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, 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 A5.4 "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	Dimensió	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	Categoria	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

Adicionalment 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**.

Adicionalment 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'ofertant 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 relatiu 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.