

PLEC DE PRESCRIPCIONS TÈCNIQUES
SUBMINISTRAMENT D'ELECTRÒNICA DE XARXA CAMPUS PER UNA NOVA SEU EN
EL PCB

EXP: F25.044S

Índex

1- OBJECTE	3
2- INFRAESTRUCTURA DE XARXA DE LA NOVA SEU	3
3- DESCRIPCIÓ DEL SUBMINISTRAMENT	3
3.1- COMMUTADORS.....	4
3.2- PUNTS D'ACCÉS WIFI.....	4
3.3- TALLAFOCS.....	4
3.4- LLICÈNCIA FORTIMANAGER.....	4
4- GARANTIA	4
4.1- GARANTIA DE PRODUCTE	4
4.2- GARANTIA DE PROJECTE	5
4.3- GARANTIA POST PROJECTE	5
5- CONDICIONS DE SUBMINISTRAMENT, ENVIAMENT, RECEPCIÓ, INSTAL·LACIÓ I SUBSTITUCIÓ D'EQUIPS.....	5
5.1- INSTAL·LACIÓ D'EQUIPS	6
5.1.1- Horaris	6
5.1.2- Identificació i etiquetatge.....	7
5.1.3- Condicionament dels racks.....	7
6- SERVEIS D'IMPLANTACIÓ I CONFIGURACIÓ	7
6.1- DISSENY I PLANIFICACIÓ GENERAL	7
6.2- OPERATIVA DE SISTEMES	8
6.3- FORMACIÓ	8
6.4- DOCUMENTACIÓ	9
7- OFERTA TÈCNICA A LLIURAR	9
ANNEX 1 PPT – REQUISITS GENERALS DE SEGURETAT PER A LA CONTRACTACIÓ DE SERVEIS I PRODUCTE SEGONS L'ENS.....	11
A1.1 - INTRODUCCIÓ I OBJECTIUS.....	11
A1.2 - ABAST	11
A1.3 - ASPECTES GENERALS DE SEGURETAT PER A LA CONTRACTACIÓ DE SERVEIS	11
A1.3.1 - Requisits per a la contractació de serveis	11
A1.3.2 – Subcontractació	11
A1.3.3 - Requisits del servei de subministrament i configuració d'elements de xarxa.....	12
A1.3.4 - Requisits del servei de desenvolupament de programari	12
A1.3.5 - Serveis al núvol	14
A1.3.6 - Excepcions	14
A1.4 - ASPECTES GENERALS DE SEGURETAT PER A LA CONTRACTACIÓ DE PRODUCTES.....	14
A1.4.1 - Primera opció – “Certificació del producte al catàleg de productes i serveis de seguretat de les tecnologies de la Informació i comunicació”	15
A1.4.2 - Segona opció – certificació internacional del producte	15
A1.4.3 - Tercera opció – auditoria de seguretat.....	15
A1.4.4 - Quarta opció – declaració de responsabilitat legal i qüestionari de seguretat	15
A1.5 - RECORDATORI DOCUMENTACIÓ TÈCNICA EXIGIBLE	20
A1.6 - AVALUACIÓ D'IMPACTE	20

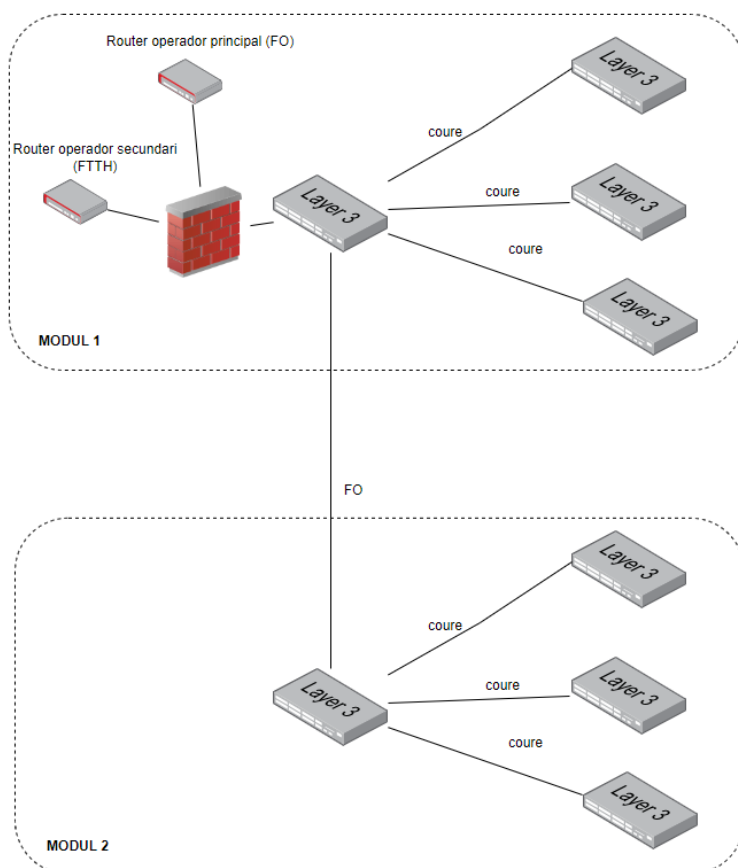
1- OBJECTE

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 nova dotació d'equips d'accés a la xarxa de comunicacions a un nova seu de la Fundació Clinic (endavant FCRB) i que ha de formar part de la xarxa CAMPUS CLINIC com qualsevol altre seu de les que ja es disposen amb accés WAN corresponen.

Partim de la situació on els troncats, la gestió i la monitorització de la xarxa ja està en funcionament i per tant s'han d'estendre les polítiques i les configuracions d'acord al que ja està definit en altres seus.

2- INFRAESTRUCTURA DE XARXA DE LA NOVA SEU

La infraestructura lògica de xarxa a la nova seu, ubicada al PCB (Parc Científic de Barcelona), haurà de ser la següent:



Es tracta de dues oficines (mòdul 1 i mòdul 2) interconnectades amb FO monomode. Cadascun dels 4 switch de cada mòdul està ubicat en un rack diferent (4 per mòdul), en un d'ells s'ubicarà el Firewall que ha de donar accés a les a la seu principal ubicada a Hospital Clinic per medi de un accés MPLS principal i un accés Internet FTTH secundari.

3- DESCRIPCIÓ DEL SUBMINISTRAMENT

Tots els equips subministrats han de ser entregats en mode "claus en mà" on s'inclougui el servei d'instal·lació, configuració i interconnexió/integració amb la seu central.

Per tal de mantenir la homogeneïtat i estandardització de l'equipament que actualment es desplega a tot el campus Clínic, d'on aquesta nova seu formarà part, l'equipament ha de ser del fabricant Fortinet, i inclourà els següents elements:

3.1- Commutadors

Es subministraran 9 equips FS-148F-FPOE, 1 d'ells s'utilitzarà com equip de backup en cas d'averia, i un més de similar que es valorarà més endavant amb l'adjudicatari. S'inclouran 4 mòduls FN-TRAN-SFP+LR per tal de realitzar la interconnexió dels dos mòduls.

3.2- Punts d'accés Wifi

Es subministraran 8 equips FAP-231K-E i un més de similar que es valorarà més endavant amb l'adjudicatari.

3.3- Tallafocs

Es subministraran 2 equips FG-121G-BDL-950-60. S'inclouran 2 mòduls FN-CABLE-SFP+1 per la interconnexió amb un dels commutadors i un "Firewall petit per cobrir necessitats d'oficina max 10 usuaris"

3.4- Llicència Fortimanager

Donat que els firewalls hauran de gestionar-se amb el Fortimanager de la seu central, l'oferta haurà d'incloure una llicència per ampliar el número d'equips suportats actualment.

4- GARANTIA

4.1- Garantia de producte

Atesa la naturalesa de la licitació (per ampliar la xarxa del en el CAMPUS CLINIC), 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 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 tallafocs.
- Per als equips commutadors i punts d'accés WiFi no es defineix SLA.

4.2- Garantia de projecte

Durant el desplegament del projecte i fins el seu traspàs al servei d'operacions del FRCB, l'adjudicatari 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 FRCB 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 de el tancament del projecte, en el qual l'adjudicatari 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, FRCB no pot garantir la disponibilitat d'espais logístics per el seu emmagatzematge. És per això que l'adjudicatari serà el 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'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 FRCB 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 d'equips

La instal·lació consistirà en gestionar i realitzar la instal·lació de l'equipament adquirit en el present PPT en els mòduls que té FRCB al edifici del PCB. Les tasques associades en els racks de comunicació inclouen la gestió de totes les connexions de cablejat. Per a la instal·lació dels punts d'accés WiFi, la FCRB facilitarà les ubicacions precises.

5.1.1- Horaris

Els horaris d'instal·lació podran ser en horari laboral normals però sempre avisant prèviament i acordant les activitats i els horaris el personal de FRCB (que a la vegada a de validar-ho amb el PCB).

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 FRCB-IDIBAPS 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 FRCB. Els licitadors inclouran el material necessari per l'etiquetat dins de l'oferta.

5.1.3- Condicionament dels racks

Els serveis d'instal·lació inclosos en la instal·lació ha d'incloure criteris d'ordre, facilitant les posteriors operatives de manipulació d'elements del rack. Per complir amb aquest propòsit cada un dels commutadors es muntarà incloent elements passafils horitzontals que permetin pentinar els fuetons.

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 FRCB, 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 FRCB 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'inclouin les següents fites:

- Integració amb Fortimanager aplicant totes les configuracions de forma centralitzada, tenint en compte:
 - Gestió unificada tallafocs, commutadors i APs.
 - Creació de plantilles que permetin una administració unificada.
 - Configuracions automatitzades pel desplegament de nous equips.
 - Còpies de seguretat.
- Definició de xarxes, interfícies de xarxa, adreçaments IP segons indicacions de FRCB en base a un model ja definit en altres seus.
- Integració amb la solució NAC de FRCB.

- Disseny de SDWAN que garanteixi la màxima eficiència d'ús de les línies d'accés principal (MPLS) i secundaria (Internet FTTH). La solució ha de contemplar accés a seu central per enllaç MPLS principal i en cas de caiguda utilitzar una VPN mitjançant l'accés Internet. La solució ha de ser escalable a qualsevol altre seu gestionada des de Fortimanager,
- Detalls tècnics de funcionament, esquemes lògics, etc.

La planificació haurà d'incloure totes les tasques necessàries per implantar tan les funcionalitats requerides per FRCB (i que ja existeixen dins de la xarxa CAMPUS CLINIC) com les proposades pel licitador que siguin d'interès per FRCB, incloent un calendari d'implantació i recursos necessaris atenent a les prioritats i complexitats de FRCB.

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 FRCB abans de portar-lo a terme.

6.2- Operativa de sistemes

Tots els elements han de quedar integrats a la plataforma de monitorització de Campus CLINIC, 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 del Campus Clinic 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 cluster.
- Caigudes de serveis o equipament hardware.

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 del Campus Clinic.

6.3- Formació

El licitador ha d'incloure formació per a la correcta administració de la solució implementada, amb un mínim de 1 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.
- Pla de proves de la instal·lació efectuades.
- Manuals d'exploració.
- 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, convertors, etc.
- Proposta d'implantació on es definirà el procés d'instal·lació del model proposat,
- Proposta inicial de planificació que inclourà el desglossat del projecte en termes de tasques, fites i terminis.
- 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 tècnics amb les seves certificacions sobre la solució proposada, indicant també la seu de treball. Es valorarà la quantitat de tècnics certificats i les seves certificacions.

- 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.
- Model de seguiment del projecte amb els interlocutors assignats per FRCB.
- Traspàs de la instal·lació a la gestió continuada dels serveis del client.
- Proposta de formació.

ANNEX 1 PPT – REQUISITS GENERALS DE SEGURETAT PER A LA CONTRACTACIÓ DE SERVEIS I PRODUCTE SEGONS L'ENS

A1.1 - 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 FRCB en compliment dels requisits exigits per l'Esquema Nacional de Seguretat (ENS en endavant).

A1.2 - Abast

Tractar tots els serveis i productes que necessitin ser desplegats o integrats a la infraestructura IT de FRCB. 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.

A1.3 - 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 FRCB 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.

A1.3.1 - 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 FRCB, 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 A7.4 "Aspectes generals de seguretat per a la contractació de productes"

FRCB 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.

A1.3.2 – 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 FRCB, per la qual cosa el contingut del present annex resultarà així mateix d'aplicació a la cadena de subministrament del proveïdor.

En aquest sentit, FRCB 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.

A1.3.3 - 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
--------	---------------------------------------	-----------	-------------	-------------	-----------

A1.3.4 - 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
--------	--	-----------	-------------	-------------	-----------

A1.3.5 - 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.

A1.3.6 - 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'FRCB-IDIBAPS i el proveïdor, com està pensat s'organitzi i es doni suport a cadascuna de les mesures.

A1.4 - 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'FRCB-IDIBAPS compleix les directrius de seguretat mínimes, la plataforma haurà de complir algun dels següents requisits per ordre de rellevància:

A1.4.1 - 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.

A1.4.2 - 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)

A1.4.3 - 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)

A1.4.4 - 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 annex 4 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.***
 - Seràn 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 corregeixen 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 la FRCB-IDIBAPS. En cas que algun d'aquests requisits no apliqui s'hauran d'exposar els motius.

A1.5 - 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

A1.6 - 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 la FRCB-IDIBAPS per detectar els riscos derivats del tractament de dades personals.

ANNEX 2 PPT

**DECLARACIÓ RESPONSABLE SOBRE EL COMPLIMENT DELS REQUISITS TÈCNICS
ESSENCIALS**

F25.044S

El/la Sr./Sra. _____, amb NIF núm. _____, com a representant legal de l'empresa _____,
amb CIF núm. _____, amb residència en _____, carrer _____, núm. _____,

DECLARA,

Que coneix i compleix estrictament les condicions i requisits essencials que s'exigeixen
als plecs de prescripcions tècniques (PPT), per poder participar en el procés
d'adjudicació del contracte de " _____ ", i que es compromet a executar-lo amb estricta
subjecció als requisits i condicions estipulats als plecs i en l'oferta presentada.

I perquè així consti, signa aquesta declaració responsable, a _____, el _____ de _____,
de 2025.

Identificació i signatura del representant legal