



**SUBMINISTRAMENT, MIGRACIÓ I
IMPLANTACIÓ PER A LA RENOVACIÓ
D'UNA SOLUCIÓ HÍBRIDA DE
BALANCEIG DE TRÀNSIT I
SEGURETAT D'APLICACIONS PER A
L'HOSPITAL CLÍNIC**

Govern de la Seguretat

Índex

1	Objecte i necessitat.....	3
1.1.1	Antecedents i Estat Actual.....	3
1.2	Necessitat.....	3
2	Descripció del subministrament.....	4
2.1	Elements a subministrar.....	4
2.2	Característiques tècniques.....	5
3	Garantia i manteniment.....	5
4	Termini i lloc de lliurament.....	6
4.1	Termini.....	6
4.2	Lloc de lliurament.....	6
4.3	Documentació dels lliuraments.....	7
5	Planificació del Projecte d'implantació.....	7
6	Serveis d'implantació i configuració.....	7
6.1	Disseny i planificació.....	7
6.2	Estimació d'esforç i dedicació.....	7
6.3	Operativa de sistemes.....	8
6.4	Arquitectura de la solució.....	8
6.4.1	Integració en el Clúster Actual i Continuitat de Servei.....	8
6.4.2	Interconnexió amb el Servei SaaS.....	8
6.4.3	Interconnexió amb el núvol públic (Amazon Web Services - AWS).....	9
6.4.4	Mecanismes d'alta disponibilitat i contingència.....	9
6.5	Migració de zones DNS.....	10
6.5.1	Àmbit de la migració.....	10
6.5.2	Requisits tècnics d'execució.....	10
6.5.3	Validació i Proves de Resolució.....	10
6.5.4	Entregables Específics de la Migració DNS.....	10
6.5.5	Configuració d'Alta Disponibilitat i Commutació Automàtica (Multi-WAN).....	11
6.6	Funcionalitats addicionals.....	12
6.7	Mecanismes d'alta disponibilitat i/o contingència.....	12
6.7.1	Alta Disponibilitat de la Infraestructura Local (On-Premise).....	12
6.7.2	Contingència davant Fallada del Proveïdor de Comunicacions (Multi-WAN).....	13
6.7.3	Continuitat de Servei en Entorns Híbrids i Multi-Cloud.....	13
6.7.4	Procediments de Manteniment sense Interrupció.....	13
6.8	Formació i transferència de coneixement.....	13
6.8.1	Modalitat i Durada.....	13
6.8.2	Contingut del Programa Formatiu.....	13
6.8.3	Documentació i Suport a la Formació.....	14
6.9	Documentació de Final de projecte.....	14
6.9.1	Disseny de Detall i Arquitectura.....	14
6.9.2	Documentació de Configuració.....	15
6.9.3	Pla de Proves i Acta de Validació.....	15
6.9.4	Memòria de Migració DNS.....	15
6.9.5	Manuals d'Suport.....	15
6.9.6	Certificats i Evidències de Formació.....	16
6.9.7	Operatives Bàsiques de Explotació.....	16
6.10	Requisits Específics de la Instal·lació i Posada en Servei.....	16
7	Condicions d'Execució del Contracte.....	17
7.1	Acreditació de la Garantia i Suport.....	17
7.2	Seguretat de la Informació (ENS).....	17
7.3	Alliberament de Maquinari i Gestió de Residus (RAEE).....	17
7.4	Perfil del Personal i Confidencialitat.....	18

7.5	Continuïtat de Servei durant la Migració.....	18
7.6	Protecció de Dades de Caràcter Personal.....	18
8	Oferta Tècnica a lliurar.....	18
8.1	Relació i Descripció d'Elements a Subministrar.....	18
8.2	Metodologia de gestió de projectes.....	18
8.3	Metodologia de la posada en marxa i migració.....	19
8.4	Traspàs de la instal·lació a la gestió continuada.....	19
8.5	Proposta de formació i transferència de coneixement.....	19
8.6	Proposta de la qualitat de la documentació.....	19
8.7	Solvència tècnica mínima.....	19
8.7.1	Experiència prèvia en projectes similars.....	20
8.7.2	Capacitat tècnica de l'equip.....	20
8.7.3	Coneixement i compliment normatiu.....	20
8.7.4	Acreditació.....	20

1 Objecte i necessitat

L'Hospital Clínic de Barcelona (en endavant, HCB), com a institució de referència sanitària i infraestructura crítica, basa la seva operativa diària en una alta disponibilitat dels seus serveis digitals. Actualment, l'arquitectura de lliurament d'aplicacions se sustenta sobre una plataforma de balanceig de càrrega que gestiona dos ecosistemes diferenciats:

- Entorn de Publicacions Internes: Crític per a la comunicació entre sistemes d'informació hospitalària, accés a aplicacions internes clíniques i serveis de xarxa.
- Entorn de Publicacions Públiques: Punt d'exposició de serveis cap a l'exterior (portals de salut, APIs de tercers, aplicacions webs de pacients), on la seguretat perimetral és el factor determinant.

La infraestructura de hardware actual ha assolit el final del seu cicle de vida útil i sense més suport per part del fabricant a partir del 2027. Les limitacions de rendiment d'aquests equips, unides a la sofisticació de les amenaces actuals, fan necessària la transició cap a una arquitectura de microserveis en maquinari de nova generació i la integració de capacitats elàstiques al núvol.

L'objecte d'aquest contracte és el subministrament i la implantació d'una solució que renovi el maquinari local en fi de vida i assegurí la continuïtat de la subscripció SaaS al núvol interconnectats.

1.1.1 Antecedents i Estat Actual

L'arquitectura de lliurament d'aplicacions de l'Hospital Clínic ha evolucionat des de la seva posada en marxa el 2018 cap a un model de publicació centralitzat basat en tecnologia F5 o equivalent.

Actualment, l'entorn es dimensiona segons els següents nivells:

- Nivell Local (On-Premise): Dos nodes físics F5 BIG-IP i4600 distribuïts als CPD de CEX i CEK. Aquesta infraestructura gestiona la disponibilitat (LTM) i seguretat (WAF) de 254 Virtual Servers, que donen servei a 455 dominis d'aplicació i 415 nodes de backend.
- Nivell Cloud (SaaS): Integració amb la plataforma F5 Distributed Cloud (F5 XC) per a la protecció perimetral i DDoS. L'entorn està interconnectat amb el núvol d'AWS i la zona externa dels balancejadors físics, gestionant aplicacions corporatives crítiques amb polítiques de WAF, restricció geogràfica, detecció de bots i seguretat d'APIs.
- Configuració i Publicació: L'arquitectura es basa en una segregació lògica mitjançant tenants i particions, existint una connexió entre l'entorn físic i el núvol que resulta crítica per a la resiliència del servei assistencial

1.2 Necessitat

La necessitat administrativa rau en l'evolució cap a un model de gestió unificada i convergència tecnològica. Atès que l'Hospital ja opera amb tecnologies F5 en ambdós entorns, la solució objecte de aquest plec ha de mantenir la mateixa arquitectura i elements (SaaS i On-Prem) actuals per garantir:

1. Continuïtat Assistencial i migració amb impacte zero: Realitzar la migració dels 254 Virtual Servers i la lògica de polítiques existent sense reenginyeria de programari per a més de 450 aplicacions/serveis.

2. Facilitar la convergència d'un model de gestió unificada de polítiques de WAF de seguretat. L'ús d'arquitectures homogènies permet minimitzar els costos de formació i, especialment, eliminar els riscos d'incompatibilitat tècnica entre plataformes i les possibles fallades de configuració que podrien comprometre l'estabilitat de les aplicacions assistencials crítiques de l'Hospital.
3. Mitigació i protecció avançada contra atacs de denegació de servei distribuïts (DDoS): Atesa la naturalesa crítica dels serveis assistencials de l'Hospital, la solució objecte d'aquest contracte ha d'incorporar mecanismes actius i integrats de detecció i mitigació d'atacs DDoS (tant a capa de xarxa/transport com a capa d'aplicació). Això és indispensable per garantir la disponibilitat ininterrompuda de la infraestructura davant d'anomalies de trànsit massives o atacs dirigits, assegurant el compliment de les directrius d'alta disponibilitat exigides pel sector salut.

Atès que la infraestructura actual es basa en tecnologia F5, la nova solució hardware haurà de permetre la integració nativa amb el clúster actual per fer un traspàs de configuracions i estats de sessió sense interrupció del servei.

Qualsevol solució que no garanteixi la compatibilitat nativa amb el parc instal·lat serà descartada, atès que comportaria un risc inacceptable de tall en el servei assistencial i un sobrecost econòmic i formatiu desproporcionat per a l'Hospital.

2 Descripció del subministrament

Per tal de garantir la continuïtat del servei durant la renovació tecnològica, la nova solució hardware ha de ser capaç d'interoperar de forma nativa amb els sistemes d'inspecció i balanceig existents, permetent la formació de clústers híbrids temporals per a la sincronització de configuracions i estats de sessió.

L'obsolescència dels equips actuals i la necessitat d'evolucionar cap a un model unificat de seguretat en el perímetre (SaaS) certificat en ENS Categoria ALTA justifiquen la present licitació. L'objectiu final és que la nova infraestructura local sigui plenament compatible amb la plataforma SaaS actual per permetre, en una fase posterior, la gestió centralitzada de totes les polítiques de publicació web, arquitectura tecnològica homogènia i seguretat de l'Hospital.

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

- Instal·lació i Retirada: Muntatge físic del nou equipament, així com la desconexió, desmuntatge i retirada de l'equipament substituït (incloent-hi la gestió de residus RAEE segons normativa vigent).
- Reconnexió i Configuració Híbrida: Configuració de la connectivitat i sincronització entre la infraestructura local i l'entorn cloud, garantint la persistència dels serveis i la seguretat perimetral.
- Migració i Desplegament: Traspàs de configuracions de l'entorn antic al nou i execució tècnica de les millores ofertes per les licitadores.
- Posada en Servei: Lliurament de la solució plenament operativa, verificada mitjançant proves de funcionament i amb tota la documentació tècnica de configuració i operació actualitzada.

2.1 Elements a subministrar

L'objecte és la provisió d'una solució integrada de disponibilitat i seguretat, consistent en:

- Dos sistemes físics de processament i balanceig de tràfic per a desplegament local (on-premise) amb funcionalitats WAF y balanceig LTM.
 - Pel que fa als balancejadors, cal incloure els transceptors tant dels balancejadors com els de l'electrònica a la qual aniran connectats (Switches Cisco Nexus). Tot el material subministrat haurà de ser de la mateixa empresa fabricant.

- [OPCIONAL] llicència de laboratori per testejar configuracions

Descripció	Quantitat
Balancejadors físics	2
Font d'alimentació extra balancejadors físics	2
Transceptor original SFP+ 10BASE-SR	8
Mòdul de WAF Avançat (Advanced Web Application Firewall) y LTM	2
[OPCIONAL] llicència de laboratori per testejar configuracions	1

- Subscripció durant 60 mesos a una plataforma de serveis de seguretat al núvol (SaaS) amb 2 load balancers i un paquet de 30M peticions WAF.

P/N	Descripció	Quantitat
F5-V-O-ADN-MSH-PUBLB	Distributed Cloud Mesh Globally Distributed Loadbalancer (/mth) ADN Org	2
F5-XC-ALL-WAF-ADD	Distributed Cloud WAF Add Requests (per Million requests, per month)	30

- Serveis professionals especialitzats per a la migració amb impacte zero i suport tècnic avançat.
- Manteniment integral 24x7x4 per al maquinari, incloent revisions preventives, evolutius, assessments de seguretat, substitucions i validacions tècniques per part del fabricant.

Descripció	Quantitat
Servei Premium del fabricant 24x7 als dos balancejadors	
Suport RMA Next-Business-Dayen tots dos balancejadors	
[OPCIONAL valorable] Revisions per part del fabricant TAP	21

En el Formulari que figura a l'Annex 3 del PPT, les empreses licitadores detallaran la relació de productes de maquinari (*Hardware*) i programari (*Software*) que s'inclouran en el subministrament.

En el Formulari que figura a l'Annex 4 del PPT, les empreses licitadores detallaran la relació de llicències incloses en el subministrament. Totes les llicències hauran de tenir una vigència mínima de 5 anys.

2.2 Característiques tècniques

Els elements a subministrar i els serveis objecte d'aquest contracte hauran de complir amb totes les característiques tècniques establertes a l'Annex 1 d'aquest PPT. El no compliment d'alguns dels requisits imprescindibles serà motiu d'exclusió.

3 Garantia i manteniment

L'oferta haurà d'incloure un mínim de 5 anys de garantia directa del fabricant, que contemplarà:

El servei s'haurà de prestar de forma ininterrompuda les 24 hores del dia, sota un nivell de servei (SLA) de 24x7x4, garantint una resposta tècnica en un temps màxim de 4 hores, els 7 dies de la setmana, durant tot l'any. Aquesta garantia inclourà el suport directe del fabricant de la solució oferta.

Per a la gestió d'incidències, s'aplicaran les següents condicions:

A. Incidències de Maquinari (Hardware):

- Substitució d'equips: El servei inclourà la provisió i substitució de l'equip complet o de les peces avariades mitjançant reemplaçament avançat. El canvi d'equipament estarà subjecte a la disponibilitat d'estoc propi o del fabricant.
- Mitigació en remot: Es realitzaran totes les accions tècniques necessàries de forma remota per minimitzar l'impacte de la incidència de la manera més immediata possible.
- Desplaçament tècnic (On-site): En cas d'averia greu o d'incidència amb un impacte crític en el servei que no pugui ser resolta remotament, el servei inclou obligatòriament el desplaçament de personal tècnic a les instal·lacions del client per a la substitució i posada en marxa de l'equipament avariament.

B. Incidències de Programari (Software):

- Actualitzacions de manteniment: S'inclou el suport i l'accés a noves versions de manteniment o menors (minor releases) seguint les recomanacions i millors pràctiques del fabricant.
- Suport remot: Gestió i resolució remota d'errors de programari per garantir la continuïtat del servei.
- Revisions periòdiques: semestrals de la salut del sistema que permeti detectar aspectes a corregir o millorar, incloent informació rellevant a la detecció de vulnerabilitats per part de fabricant. Es lliurarà un informe amb els problemes identificats. L'adjudicatària es farà càrrec de les tasques i accions associades a la resolució d'aquests problemes, com podrien ser canvis de configuració o aplicar actualitzacions

C. Configuració i Consultoria:

- Resolució de problemes: El servei cobreix la resolució de problemes derivats de la configuració dels equips i les seves funcionalitats.
- Assessorament tècnic del fabricant: S'inclouen en l'abast les consultes sobre l'estat del servei, així com l'assessorament tècnic per a modificacions, optimitzacions o canvis en l'arquitectura de la solució per part del fabricant.

4 Termini i lloc de lliurament

4.1 Termini

El termini aplicable per fer els lliuraments de tots els materials inclosos en aquest expedient és d'un màxim de 8 setmanes naturals, comptant a partir del dia en què s'ha emès la comanda per part de l'HCB. El licitador indicarà el termini de lliurament de tot el material i llicències.

4.2 Lloc de lliurament

El subministrament dels balancejadors i altres elements es realitzarà en les ubicacions que es detallen en l'annex 2 del PPT.

En tots els casos, els lliuraments es realitzaran dins dels horaris que indiqui la Direcció de Sistemes d'Informació de l'HCB.

4.3 Documentació dels lliuraments

Els articles 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/o adreces MAC dels materials
- Import unitari i import total

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

5 Planificació del Projecte d'implantació

Caldrà iniciar la planificació de la implantació de la solució com a màxim 15 dies després de la formalització del contracte.

6 Serveis d'implantació i configuració

6.1 Disseny i planificació

Es proposaran una sèrie de reunions amb el personal de TI de l'Hospital amb l'objectiu de dissenyar i planificar les diferents fases d'implantació que s'acordin.

La planificació haurà d'incloure totes les tasques necessàries per assolir les funcionalitats requerides incloent calendari d'implantació i recursos necessaris, no podent superar els tres mesos de durada.

6.2 Estimació d'esforç i dedicació

Amb l'objectiu de facilitar una adequada comprensió de l'abast dels serveis professionals associats al projecte, s'estableix una estimació orientativa de l'esforç necessari.

La durada prevista del projecte d'implantació és de vuit (8) setmanes. Considerant un equip multidisciplinari i les diferents fases del projecte (anàlisi, disseny, implantació, migració, proves i posada en servei), es preveu una dedicació global estimada de l'ordre de 377 hores.

Aquesta estimació:

- Té caràcter orientatiu i no vinculant
- Inclou la participació de diferents perfils tècnics especialitzats
- No limita la responsabilitat de l'adjudicatari de dimensionar els recursos necessaris

Les licitadores hauran d'incloure en la seva oferta:

- El desglossament detallat d'hores per fase
- La dedicació per perfil professional
- La planificació temporal dels treballs

L'adjudicatària serà la responsable de garantir el compliment dels terminis i nivells de servei establerts, independentment de l'estimació indicada.

6.3 Operativa de sistemes

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

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

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

6.4 Arquitectura de la solució

La solució proposada s'haurà de basar en una arquitectura híbrida d'alt rendiment i disponibilitat, dissenyada per gestionar fluxos de tràfic de forma unificada entre el centre de dades local de l'Hospital, la plataforma de seguretat en el perímetre (SaaS) i entorns de núvol públic de AWS.

6.4.1 Integració en el Clúster Actual i Continuïtat de Servei

Per garantir una transició amb impacte zero en l'operativa assistencial, l'arquitectura haurà de complir els següents requisits d'integració:

- Interoperabilitat Nativa: Els nous nodes físics s'hauran d'integrar funcionalment amb el clúster de balanceig actualment en servei. Aquesta integració ha de permetre la sincronització d'estats de sessió, taules de persistència i configuracions lògiques entre la plataforma existent i la nova infraestructura.
- Migració sense Interrupció: El disseny de l'arquitectura ha de permetre un desplaçament progressiu del tràfic des dels equips antics cap als nous. És condició indispensable que aquest procés no provoqui cap desconexió ni degradació dels serveis actius, mantenint la persistència de les sessions d'usuari en aplicacions crítiques durant tota la fase de transició.

6.4.2 Interconnexió amb el Servei SaaS

L'arquitectura ha d'estendre les capacitats d'inspecció i balanceig local cap a una plataforma de seguretat en el perímetre (SaaS) sota els següents paràmetres:

- Publicació de Servidors Interns: La solució ha de permetre la interconnexió segura d'aplicacions allotjades en servidors interns de l'Hospital amb els nodes de la xarxa SaaS. El tràfic destinat a publicacions web externes haurà de ser inspeccionat en el perímetre (SaaS) abans de ser lliurat de forma segura a la infraestructura local.
- Sincronització d'Objectes i Polítiques: Es requereix una arquitectura que garanteixi l'homonímia i l'intercanvi dinàmic d'objectes de seguretat (signatures WAF, llistes de reputació d'IPs, polítiques de mitigació de bots) entre l'entorn on-premise i el núvol (cloud), assegurant una postura de seguretat coherent en tots els punts d'entrada.
- Capacitat i Rendiment: La solució garantirà la publicació de serveis a través de la seva infraestructura sense establir limitacions d'ample de banda. El cabal haurà de ser elàstic i suficient per absorbir els pics de demanda de l'organisme, garantint una latència mínima i la integritat de les dades en trànsit.
- Integració Nativa amb Infraestructura de Gestió de Trànsit: El servei SaaS haurà de disposar de mecanismes d'integració nativa amb l'equipament de gestió de trànsit i lliurament d'aplicacions F5 BIG-IP (o tecnologia equivalent) actualment desplegat al centre de dades de l'organisme.
- Mecanismes de Service Discovery: El sistema haurà de ser capaç de realitzar un descobriment dinàmic de serveis allotjats darrere dels *Virtual Servers* de la infraestructura local. Aquesta integració permetrà utilitzar aquests objectes com a nodes de destinació final (*pool members* o *backends*) de forma automatitzada, assegurant que qualsevol canvi en la disponibilitat o topologia dels serveis locals es reflecteixi en temps real en la publicació externa del SaaS.

- **Seguretat i Visibilitat:** Aquesta interconnexió haurà de suportar l'intercanvi d'estats de salut (*Health Checks*) i el manteniment de la persistència de sessió, assegurant que el flux de trànsit des de la infraestructura del proveïdor cap a la destinació final al centre de dades sigui xifrat i transparent per a la gestió de xarxa de l'organisme.
- **Normalització i Estandardització de la Nomenclatura d'Objectes:** L'adjudicatària haurà d'implementar una política de nomenclatura estandarditzada i coherent per a tots els elements configurats a la plataforma SaaS. Això inclou, de manera enunciativa però no limitativa: noms d'objectes de xarxa, polítiques de seguretat WAF (Web Application Firewall), regles de filtrat, perfils d'acceleració, nodes i certificats.

Aquesta normalització haurà de complir els següents criteris:

- **Definició Prèvia:** La convenció de noms haurà de ser proposada per l'adjudicatària i validada pels responsables tècnics de l'organisme abans de l'inici de la configuració.
- **Traçabilitat:** Els noms han de permetre identificar clarament la funció, l'entorn (producció, preproducció, etc.) i el servei associat.
- **Documentació:** La guia d'estil i la llista completa d'objectes normalitzats hauran de formar part obligatòria dels lliurables finals del projecte (segons el punt 6.8). Qualsevol desviació d'aquest estàndard durant l'execució serà motiu de correcció per part de l'adjudicatària sense cost addicional per a l'HCB.

6.4.3 Interconnexió amb el núvol públic (Amazon Web Services - AWS)

Atès que l'HCB estén part dels seus serveis cap a entorns de núvol públic, la solució proposada ha de contemplar:

- **Connectivitat Multi-Cloud:** La plataforma ha de facilitar la interconnexió lògica i el balanceig de càrrega cap a instàncies i serveis allotjats al núvol d'Amazon (AWS).
- **Arquitectura de xarxa unificada:** La solució ha de permetre la gestió de serveis distribuïts, garantint que el flux de tràfic entre el CPD local, els serveis SaaS i els recursos en AWS es realitzi sota un esquema d'encaminament optimitzat, xifrat i monitoritzat centralitzadament, complint en tot moment amb els requisits de seguretat de l'ENS Categoria ALTA.

6.4.4 Mecanismes d'alta disponibilitat i contingència

L'arquitectura es dissenyarà per eliminar qualsevol punt únic de fallada:

- **Redundància física i lògica:** Els nodes físics operaran en configuració d'alta disponibilitat activa/passiva.
- **Resiliència del pla de control:** En cas d'indisponibilitat temporal del servei SaaS o dels enllaços cap al núvol públic, els nodes locals hauran de mantenir la capacitat de gestió de tràfic i seguretat per a tots els serveis interns de l'Hospital.

6.5 Migració de zones DNS

L'adjudicatària serà la responsable integral de la planificació, execució i validació de la migració de les zones DNS institucionals de l'Hospital Clínic de Barcelona cap al Distributed Cloud. Aquest servei és crític per assegurar la resolució de noms i la disponibilitat dels serveis web, correu electrònic i aplicacions de tercers durant i després del procés de renovació tecnològica.

6.5.1 Àmbit de la migració

La migració comprèn la totalitat dels registres i configuracions de les següents zones DNS:

- **clinic.cat**
- **clinicbarcelona.org**

6.5.2 Requisits tècnics d'execució

El procés de migració haurà de complir estrictament amb els punts següents:

- Auditoria prèvia i consolidació: realització d'un inventari exhaustiu de tots els registres DNS actuals (A, AAAA, CNAME, MX, TXT, SRV, etc.). S'hauran d'identificar registres obsolets o orfes abans d'iniciar el traspàs.
- Transició amb impacte zero: la migració s'ha de dissenyar per evitar qualsevol finestra d'indisponibilitat en la resolució de noms. L'adjudicatària haurà d'ajustar els temps de vida dels registres (TTL) prèviament a la migració per permetre canvis dinàmics i reversions immediates en cas d'error.
- Integració amb la solució híbrida: configuració de la delegació de zones cap a la nova plataforma (On-Premise i SaaS) assegurant la compatibilitat amb esquemes de DNSSEC (Domain Name System Security Extensions) si l'Hospital així ho requereix, per garantir la integritat i l'autenticitat de les respostes DNS.
- Sincronització de registres: assegurar que qualsevol canvi realitzat en la infraestructura de balanceig (noves IPs de Load Balancers) es reflecteixi de forma automàtica o coordinada en les zones DNS migrades.

6.5.3 Validació i Proves de Resolució

Després de la migració, l'adjudicatària haurà de realitzar proves de validació des de múltiples xarxes externes i eines de diagnòstic global per assegurar:

- La correcta propagació dels nous registres.
- La resolució exacta de serveis crítics (Webs, Mail, VPN).
- L'absència de latències anòmales en la resposta dels servidors de noms.

6.5.4 Entregables Específics de la Migració DNS

Com a part de la documentació final del projecte, s'haurà de lliurar:

- Pla de Migració DNS: Document detallat amb l'estratègia de tall, gestió de TTLs i pla de contingència (Rollback).
- Informe de Validació: Acta de proves de resolució satisfactòria després de la migració de cada zona.
- Manual de Gestió i operativa DNS: Instruccions per al personal de l'Hospital sobre com realitzar altes, baixes i modificacions de registres en la nova plataforma.

6.5.5 Configuració d'Alta Disponibilitat i Commutació Automàtica (Multi-WAN)

A. Escenari de Connectivitat On-Premise

La infraestructura local de l'Hospital disposa d'una arquitectura de doble entrada WAN per a la publicació de serveis:

- Ruta Principal (Primary): Connectivitat a través del proveïdor Vodafone.
- Ruta de Respatller (Backup/Secondary): Connectivitat a través del proveïdor CESCA.

B. Lògica de Monitoratge i Failover Automàtic

La solució proposada ha de configurar el servei SaaS per actuar com a orquestrador intel·ligent del trànsit sota els següents requisits funcionals:

- Monitoratge de Salut (Health Checks): S'implementaran monitors de salut constants des dels nodes de la xarxa SaaS cap a les adreces IP públiques de totes dues WAN. Aquests monitors verificaran no només la disponibilitat de la xarxa, sinó també la resposta de l'aplicació a nivell de Capa 7.
- Detecció de Fallada i Commutació (Automated Failover): En cas que el sistema detecti una caiguda o degradació del servei en l'entrada de Vodafone, la plataforma haurà de modificar de forma automàtica la lògica d'encaminament (o la resolució IP del backend a la xarxa SaaS) per redirigir la totalitat del trànsit de les aplicacions cap a l'entrada de CESCA.
- Transparència d'Usuari: Aquest procés de commutació s'ha de realitzar de forma immediata i automàtica, minimitzant l'impacte en la sessió de l'usuari final i evitant la necessitat d'intervenció manual per part dels administradors de l'Hospital.
- Lògica de Reversió (Failback): El sistema haurà de monitorar la recuperació de la línia principal (Vodafone). Un cop validada l'estabilitat d'aquesta ruta durant un temps definit, el trànsit haurà de retornar de forma controlada a la seva entrada preferent.

C. Requisits de Configuració Backend

L'adjudicatària serà responsable de:

- Configurar els *Origin Pools* corresponents en la plataforma SaaS per a cada aplicació, contemplant ambdues adreces IP d'entrada.
- Definir les polítiques de prioritat i pes de trànsit per assegurar que l'ús de la WAN secundària sigui estrictament en escenaris de contingència.
- Assegurar que els certificats SSL i les polítiques de seguretat WAF es mantinguin íntegres i idèntiques independentment de la ruta WAN utilitzada per a l'accés al *backend*.

6.6 Funcionalitats addicionals

- Descobriment d'APIs i Protecció de Dades: La solució ha de permetre el descobriment automàtic d'APIs, la validació d'esquemes (Swagger/OpenAPI) per evitar injeccions en els endpoints i el bloqueig de fuga de dades sensibles (emascarament de dades de salut en les respostes de l'API).
- Automatització i Orquestració: La plataforma ha d'oferir una API REST completa i ser compatible amb eines d'automatització tipus Terraform o Ansible. Ha de permetre el desplegament de configuracions mitjançant plantilles declaratives (tipus AS3 o equivalent) per assegurar l'homogeneïtat entre els entorns de test i producció.

- **Monitoratge i Quadres de Comandament:** Capacitat de generació de quadres de comandament (dashboards) visuals que mostrin en temps real el mapa d'amenaques, el rendiment dels servidors de backend (latència d'aplicació) i l'estat de salut dels enllaços WAN. Ha de permetre el drill-down per identificar quina aplicació específica està patint una degradació de servei.

6.7 Mecanismes d'alta disponibilitat i/o contingència

L'adjudicatària haurà de dissenyar i implementar una arquitectura d'alta disponibilitat (HA) i contingència que garanteixi la continuïtat del negoci i la disponibilitat dels serveis assistencials de l'Hospital Clínic les 24 hores del dia, els 7 dies de la setmana. Aquesta arquitectura haurà de cobrir tant els nodes físics locals com la interconnexió amb els serveis al núvol.

6.7.1 Alta Disponibilitat de la Infraestructura Local (On-Premise)

La solució local s'haurà de configurar sota un esquema de redundància total, complint els següents requisits:

- **Configuració de Clúster d'Alta Disponibilitat:** Els dos nodes físics operaran de forma conjunta en un grup de dispositius (Device Group) sota una modalitat actiu/passiu, assegurant que, davant una fallada de maquinari o programari en el node principal, el node secundari assumeixi la totalitat del trànsit en un temps inferior a un segon.
- **Sincronització d'Estat:** El sistema permetrà l'edició i el desplegament d'objectes, Virtual Servers i polítiques en el node actiu, romanent aquests canvis en estat local fins que l'administrador del sistema executi de forma manual l'ordre de sincronització cap al node passiu del clúster.
- **Supervisió d'Objectes i Enllaços:** S'implementarà un monitoratge multinivell que inclogui:
 - **Monitors de Gateway:** Per detectar caigudes en els encaminadors de sortida.
 - **VLAN Failover:** Per reaccionar davant fallades en els enllaços físics o interfícies de xarxa.
 - **Monitors d'Aplicació Avançats:** Capaços de validar no només la connectivitat IP, sinó l'estat real de l'aplicació mitjançant la cerca de cadenes de text específiques en les respostes HTTP/S.

6.7.2 Contingència davant Fallada del Proveïdor de Comunicacions (Multi-WAN)

Com a mecanisme de contingència crític, la solució haurà de gestionar la redundància dels enllaços de comunicacions de l'Hospital:

- **Gestió Intel·ligent d'Enllaços:** La plataforma ha d'orquestrar el trànsit entre les entrades dels proveïdors Vodafone (Principal) i CESCA (backup) per a la publicació d'aplicacions web corporatives
- **Commutació Dinàmica via SaaS:** S'utilitzarà la intel·ligència de la xarxa distribuïda al núvol per detectar, mitjançant sondes de salut globals, la indisponibilitat de la ruta principal. Davant un esdeveniment de caiguda, la solució haurà de redirigir de forma automàtica el trànsit de les aplicacions crítiques cap a la ruta de respall, actualitzant de forma dinàmica la resolució DNS o l'encaminament cap al backend local.

6.7.3 Continuïtat de Servei en Entorns Híbrids i Multi-Cloud

L'arquitectura de contingència s'estendrà cap als serveis allotjats a Amazon Web Services (AWS) i la pròpia xarxa SaaS:

- Aïllament de Fallades al Perímetre: La plataforma SaaS haurà de disposar de mecanismes d'autoprotecció que, davant d'atacs massius de denegació de servei (DDoS), aïllin el trànsit maliciós en els nodes d'entrada globals, evitant que la saturació arribi a la infraestructura local de l'Hospital.

6.7.4 Procediments de Manteniment sense Interrupció

Tots els mecanismes d'HA han de permetre la realització de tasques de manteniment (actualització de pegats de seguretat, canvis de maquinari, etc.) de forma transparent. El sistema haurà de permetre el pas forçat de trànsit al node passiu (*forced-offline*) per intervenir el node principal sense degradar el servei ni provocar desconnexions en les sessions dels usuaris.

6.8 Formació i transferència de coneixement

L'adjudicatària haurà de realitzar una formació tècnica i un traspàs d'operativa dirigit al personal tècnic de l'Hospital Clínic. L'objectiu d'aquesta formació és garantir que l'equip de sistemes, seguretat i xarxes del centre disposi de la capacitat necessària per a la gestió, explotació i resolució de problemes de primer nivell de la nova solució híbrida.

6.8.1 Modalitat i Durada

La formació s'ajustarà als següents paràmetres:

- Durada mínima: Un mínim de 3 mitges jornades de formació.
- Metodologia: Sessions remotes mitjançant plataforma de videoconferència corporativa.
- Horari: Dins de l'horari d'oficina (de dilluns a dijous de 9:00h a 18:30h, i divendres de 9:00h a 14:30h).
- Abast tecnològic: La formació cobrirà tant la nova plataforma de maquinari com l'entorn desplegat de seguretat en el núvol.

6.8.2 Contingut del Programa Formatiu

El contingut de la formació es dividirà en els següents blocs temàtics:

A. Coneixement de la infraestructura i arquitectura:

- Presentació detallada de l'entorn desplegat: arquitectura física i lògica.
- Ús de quadres de comandament i revisió de versions de programari.
- Visualització de serveis disponibles i estat de salut de la plataforma.

B. Administració i Configuració de Sistemes:

- Administració bàsica dels equips: gestió de xarxes, perfils i adreçament.
- Sincronització de configuracions entre els nodes del clúster local.
- Gestió i creació d'usuaris amb diferents nivells d'accés i rols (RBAC).

C. Gestió de Serveis i Publicacions:

- Desplegament i publicació de nous serveis balancejats (Virtual Servers).
- Creació i configuració d'entorns de *routing* i configuració aïllats.
- Configuració de pàgines de manteniment personalitzades per als serveis desplegats.

D. Seguretat Aplicativa i Serveis Cloud:

- Activació i securització de nous serveis mitjançant WAF (Web Application Firewall).
- Gestió de serveis de DNS i interconnexió amb el servei SaaS.

- Interacció amb el tràfic web mitjançant l'ús d' *scripting* estructural del fabricant.

E. Operativa, Manteniment i Resolució de Problemes:

- Procediment de realització de còpies de seguretat (*backups*) i restauració.
- Procediments d'actualització dels equips i descàrrega de noves signatures d'amenaques.
- Habilitació i gestió de sistemes de monitorització.
- Anàlisi avançada de *logs* per a l'auditoria i detecció d'errors.
- Troubleshooting bàsic: eines de diagnòstic i mètodes de resolució d'incidències comunes.

6.8.3 Documentació i Suport a la Formació

Com a part de la prestació d'aquest servei, l'adjudicatària haurà d'entregar:

- Documentació de suport utilitzada durant les sessions (presentacions, guies ràpides).
- Enregistrament de les sessions formatives per a consulta futura per part del personal del Hospital.
- Acta de finalització de la formació signada per ambdues parts, on es detalli la relació d'assistents i els temes tractats.

6.9 Documentació de Final de projecte

L'adjudicatària tindrà l'obligació de lliurar una documentació tècnica completa i detallada un cop finalitzada la implantació i abans de la signatura de l'acta de recepció de conformitat.

Aquesta documentació haurà de permetre a l'HCB conèixer, gestionar i evolucionar la solució de forma autònoma.

La documentació final del projecte inclourà, com a mínim, els següents blocs:

6.9.1 Disseny de Detall i Arquitectura

- Topologia de xarxa: Esquemes detallats de la interconnexió física i lògica dels nous nodes amb el core de xarxa del Hospital.
- Disseny Híbrid: Mapa d'interconnexió entre la infraestructura on-premise, el servei SaaS (Distributed Cloud) i els entorns de núvol públic (AWS).
- Disseny Multi-WAN: Detall de la lògica de monitorització i encaminament dinàmic per a les entrades de Vodafone i CESCA.
- Matriu de Fluxos: Llistat de ports i protocols habilitats per a la gestió i el tràfic de serveis.
- Normalització i Estandardització de la Nomenclatura d'Objectes.

6.9.2 Documentació de Configuració

- Configuració de Maquinari: Detall dels tenants/particions creats, assignació de recursos (CPU/Memòria) i configuració de la capa Host.
- Inventari d'Objectes: Llistat complet de Virtual Servers, Pools, Nodes, Profiles i certificats SSL instal·lats durant el projecte.
- Lògica de Programació: Còpia íntegra i documentada de tots els scripts en llenguatge TCL o altre llenguatge i creades durant el projecte.

- Polítiques de Seguretat: Detall de les polítiques WAF aplicades, nivells de bloqueig i excepcions configurades per a cada aplicació.

6.9.3 Pla de Proves i Acta de Validació

- Proves d'Alta Disponibilitat: Resultats de les proves de failover manual i automàtic del clúster local.
- Proves de Contingència WAN: Informe de validació de la commutació automàtica entre proveïdors d'Internet davant de caigudes simulades.
- Proves de Rendiment: Resultats dels tests de càrrega i inspecció SSL realitzats per validar els llindars de rendiment exigits.

6.9.4 Memòria de Migració DNS

- Informe de Resolució: Acta de validació de la resolució externa i propagació dels dominis clinic.cat i clinicbarcelona.org.
- Manual de Gestió DNS: Guia específica per a la realització de canvis, altes i baixes de registres en la nova plataforma.

6.9.5 Manuals d'Suport

- Guia d'Administració: Procediments per a la gestió d'backups.
- Pla de Suport i Manteniment: Directori de contactes, procediment d'obertura d'incidències 24x7 i calendari de manteniments preventius per als 5 anys de contracte.

6.9.6 Certificats i Evidències de Formació

- Materials Formatius: Còpia de les presentacions i materials utilitzats durant les sessions de transferència de coneixement.
- Enregistraments: Arxius de vídeo de les sessions formatives realitzades de forma remota.
- Acta de Formació: Llistat d'assistents i temari tractat signat per l'adjudicatària i les persones responsables de l'Hospital.

6.9.7 Operatives Bàsiques de Explotació

- Gestió de publicacions: Procediments per a les altes, baixes i modificacions de Virtual Servers, Pools i nodes de backend.
- Seguretat d'aplicacions (WAF): Operativa per a l'anàlisi de logs, gestió d'excepcions de firmes (falsos positius) i actualització de polítiques de seguretat.
- Restriccions de tràfic: Configuració de bloquejos geogràfics, llistes de reputació d'IP i control d'accessos basat en perfils.
- Gestió d'usuaris i accessos: Procediment d'alta i baixa d'administradors i definició de rols de gestió (RBAC).

- Manteniment de certificats: Guia per a la renovació i instal·lació de certificats SSL/TLS i les seves claus corresponents.
- Auditoria i Reporting: Procediment per a l'extracció de logs d'activitat i generació d'informes de compliment de l'ENS.

6.10 Requisits Específics de la Instal·lació i Posada en Servei

Els elements hardware redundants s'instal·laran en els dos CPD diferenciats de l'Hospital (CPD de Consultes Externes i Edifici CEK), situats a una distància inferior a 1 km.

L'equipament es connectarà localment a l'electrònica del CPD on s'instal·larà mitjançant les interfícies de fibra òptica d'alta velocitat (SFP28 a 25G o SFP+ a 10G) subministrades en aquest expedient, assegurant la compatibilitat amb el core de xarxa existent.

Pel que fa a la posada en servei, s'establirà un procediment de transició controlada basat en les següents fases:

1. Instal·lació i Sincronització Inicial: Un cop realitzada la configuració base dels nous xassís i els seus entorns lògics (tenants/particions), es procedirà a la interconnexió física i lògica dels nous balancejadors amb els equips antics. Aquesta interconnexió és obligatòria per permetre la sincronització manual de les configuracions actuals, objectes de xarxa, certificats i regles de scripting, minimitzant així el risc d'errors en el traspàs de dades.
2. Integració de la Solució Híbrida: Es configurarà el túnel de connectivitat segura i la lògica de publicació entre els balancejadors físics i la plataforma de seguretat en el núvol (SaaS), habilitant la visibilitat dels servidors interns des de la vora de la xarxa i la interconnexió amb el núvol d'Amazon (AWS) mitjançant una configuració que garanteixi l'alta disponibilitat.
3. Migració Esglaonada solució hardware: Els serveis es migraran mitjançant sincronització del clúster dels antics balancejadors als nous. Atès que la majoria formen part del Servei Assistencial en producció, s'utilitzarà la capacitat del clúster híbrid per validar cada servei abans del tall definitiu.
4. Migració de 10 aplicacions públiques de l'entorn onprem a l'entorn cloud.

La posada en servei dels elements objecte d'aquest expedient es considerarà assolida en el moment que:

- Tots els sistemes (físics i cloud) estiguin operatius, perfectament configurats i amb la lògica de canvi d'IP automàtica Multi-WAN (Vodafone/CESCA) validada, a plena satisfacció de l'Hospital Clínic.
- S'hagi completat la migració de les zones DNS i la resolució de noms funcioni correctament per a tots els dominis institucionals.
- S'hagi dut a terme la formació tècnica segons el programa detallat al punt 6.7.
- El proveïdor hagi lliurat tota la documentació del projecte indicada en el punt 6.8 d'aquest plec.
- S'hagi certificat la retirada i l'esborrat segur del maquinari antic.

7 Condicions d'Execució del Contracte

Més enllà de les obligacions generals, l'adjudicatària haurà de complir amb les següents condicions específiques d'execució:

7.1 Acreditació de la Garantia i Suport

Al llarg del primer mes de vigència del contracte, l'adjudicatària haurà d'aportar la documentació oficial del fabricant que acrediti la contractació dels serveis de suport i garantia directa segons el nivell **24x7x4** especificat al punt 3, incloent les millores tècniques presentades en l'oferta.

7.2 Seguretat de la Informació (ENS)

Atesa la naturalesa dels serveis assistencials de l'Hospital Clínic, la solució i l'empresa adjudicatària han de complir amb l'Esquema Nacional de Seguridad (ENS) en categoria ALTA.

- L'empresa licitadora, haurà d'aportar el Certificat de Conformitat amb l'ENS (categoria ALTA) en el sobre B de la seva oferta (Veure PCAP).
- En el cas dels serveis en el núvol (SaaS), el proveïdor de la plataforma també haurà d'acreditar la certificació ENS Categoria Alta.

7.3 Alliberament de Maquinari i Gestió de Residus (RAEE)

L'adjudicatària serà el responsable de la retirada dels equips que s'han de substituir.

Aquesta gestió inclou:

- Esborrat segur de dades: Abans de la retirada física, l'adjudicatària realitzarà un esborrat segur de tota la informació i configuracions dels discos (segons estàndards tipus NIST 800-88 o similar) i lliurarà el certificat corresponent.
- Gestió RAEE: L'adjudicatària actuarà com a gestor de residus d'aparells elèctrics i electrònics, lliurant a l'Hospital el certificat oficial de tractament de residus segons la normativa vigent.

7.4 Perfil del Personal i Confidencialitat

Les empreses licitadores hauran d'adscriure els mitjans personals següents com a mínim:

- Cap de projecte expert en implantacions similars, amb 5 d'anys d'experiència mínima i com a mínim un projecte d'implantació amb els mateixos components i mateix càrrec.
- Enginyer de seguretat Sènior expert en els productes de F5 objectes d'aquest plec, amb 5 anys d'experiència, com a mínim un projecte d'implantació amb els mateixos components.

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

- Relació de partnership amb el fabricant de l'equipament presentat
- Disposar d'un mínim de 1 tècnic adscrit al projecte que haurà de disposar de certificacions oficials vigents del fabricant (nivell expert) per a les tecnologies objecte de la licitació F5 centrades en l'administració de BIG-IP, ASM i Distributed Cloud .
- Disposar almenys de 1 tècnic adscrit al projecte que haurà de disposar de certificacions oficials vigents en tecnologia de xarxes CISCO a nivell professional per a la interconnexions i configuracions dels balancejadors a nivell de xarxa

- **Confidencialitat:** Tot el personal que hagi d'intervenir en la instal·lació o el manteniment haurà de signar un compromís de confidencialitat específic amb l'Hospital Clínic, donat l'accés potencial a infraestructures crítiques.

Aquests mitjans personals i materials formaran part de la proposta presentada per les licitadores i, per tant, del contracte que se signi amb l'empresa adjudicatària. Per aquest motiu, hauran de ser mantinguts per l'empresa adjudicatària durant tot el temps de realització de la prestació. Qualsevol variació respecte a ells haurà de ser comunicada. El seu incompliment podrà ser causa de resolució del contracte o d'imposició de penalitats de conformitat amb el que estableix el PCAP.

7.5 Continuïtat de Servei durant la Migració

L'adjudicatària té l'obligació d'executar la migració garantint la continuïtat del servei assistencial. Qualsevol intervenció que pugui suposar un risc per a la producció haurà de ser comunicada amb antelació i aprovada pels responsables de l'Hospital, realitzant-se fora de l'horari de màxima activitat assistencial si fos necessari.

7.6 Protecció de Dades de Caràcter Personal

L'adjudicatària haurà de complir amb el Reglament General de Protecció de Dades (RGPD) i la LOPDGDD, signant el corresponent contracte d'encarregat de tractament de dades en cas que tingui accés a informació sensible durant les tasques de suport o migració.

8 Oferta Tècnica a lliurar

L'oferta tècnica que les empreses licitadores han de lliurar en el sobre corresponent de la licitació, ha d'incloure obligatòriament els següents punts indexats i detallats. Aquesta memòria ha de permetre avaluar la solvència tècnica de la proposta i el rigor en l'execució del projecte:

8.1 Relació i Descripció d'Elements a Subministrar

Com a primer apartat obligatori de la proposta, el licitador haurà d'incloure una memòria detallada i un inventari formal que respongui directament a les necessitats del Punt 2.1 (Elements a subministrar).

Aquesta secció ha de desglossar de forma transparent:

- **Components de Hardware i Software:** Detall dels equips de balanç de trànsit físics, llicències virtuals, mòduls de seguretat i accessoris ofertats. S'haurà d'especificar el fabricant, model, versió de programari/firmware y la quantitat exacta d'unitats proporcionades, garantint que compleixen o superen les capacitats especificades en el plec.
- **Conformitat amb el Formulari de Productes:** Tota la informació tècnica descrita en aquest apartat haurà de mantenir una coherència del 100% amb les dades indexades a l'Annex 3 (Formulari de Productes Hardware i Software) i a l'Annex 4 (Formulari de Llicències) de la seva proposta.

8.2 Metodologia de gestió de projectes

- **Pla de Projecte:** Descripció de la metodologia de treball (ex: Waterfall, Agile o similar) i cronograma detallat per fites, des de la signatura del contracte fins a la recepció definitiva.
- **Equip de Treball:** Organigrama del personal adscrit al projecte, detallant rols (Cap de Projecte, Enginyers d'Implantació) i les seves certificacions oficials vigents del fabricant.

- Pla de Comunicació i Riscos: Definició dels canals de comunicació amb l'Hospital Clínic i matriu de riscos amb els corresponents plans de mitigació, especialment durant les fases de migració assistencial.

8.3 Metodologia de la posada en marxa i migració

- Estratègia de Migració Híbrida: Detall tècnic de com s'executarà la interconnexió entre els equips antics i els nous, així com la integració amb la plataforma SaaS i AWS.
- Migració DNS: Metodologia específica per al traspàs de les zones *clinic.cat* i *clinicbarcelona.org*, detallant la gestió de TTLs i la validació de la propagació.
- Configuració Multi-WAN: Explicació de la implementació de la lògica de commutació automàtica entre Vodafone i CESCA per 5 subdominis crítics.
- Pla de Rollback: Descripció dels procediments de reversió immediata en cas d'incidència durant qualsevol fase del desplegament.

8.4 Traspàs de la instal·lació a la gestió continuada

- Procediment de Traspàs: Detall de com es realitzarà el pas de la fase de "Projecte" a la fase de "Suport i Manteniment".
- Gestió d'Incidències: Descripció del flux d'atenció per al suport 24x7x4 i les eines d'escalat cap al fabricant.
- Manteniment Preventiu: Proposta del calendari i metodologia per a les revisions semestral de salut del sistema, actualització de firmes i neteja d'aplicacions no operatives, dels punts 3A, 3B i 3C.

8.5 Proposta de formació i transferència de coneixement

- Pla Formatiu: Detall de les sessions proposades segons els requeriments del punt 6.7 d'aquest plec (3 mitges jornades, temari, materials i metodologia remota).
- Perfil de l'Instructor: Acreditació de l'experiència i certificacions del personal que impartirà la formació.

8.6 Proposta de la qualitat de la documentació

- Catàleg d'Integrables: Índex de continguts que inclourà el document de Disseny i el manual d'Explotació, segons el que s'especifica al punt 6.8.
- Exemples d'Informes: Proposta de format per als informes de salut trimestrals i les actes de validació de migració.

8.7 Solvència tècnica mínima

Amb l'objectiu de garantir la capacitat d'execució del contracte, els licitadors hauran d'acreditar la seva solvència tècnica mitjançant el compliment dels requisits següents:

8.7.1 Experiència prèvia en projectes similars

- Almenys tres (3) projectes executats en els darrers cinc (5) anys.
- Projectes desenvolupats en entorns d'alta disponibilitat i criticitat, preferentment en l'àmbit sanitari o equivalent.
- Els projectes hauran d'incloure tecnologies de balanceig de càrrega i seguretat aplicativa (WAF).

8.7.2 Capacitat tècnica de l'equip

- Disponibilitat de personal tècnic amb certificacions oficials vigents del fabricant de la solució ofertada o certificacions equivalents.
- Experiència demostrable en la implantació i operació d'entorns híbrids (on-premise i cloud).

8.7.3 Coneixement i compliment normatiu

- Experiència acreditada en projectes subjectes al compliment de l'Esquema Nacional de Seguretat (ENS) en categoria ALTA.
- Experiència en entorns amb requisits de protecció de dades de caràcter personal (RGPD i normativa associada).

8.7.4 Acreditació

La documentació acreditativa dels requisits anteriors haurà d'incloure's en l'oferta tècnica presentada pel licitador, i podrà ser objecte de verificació per part de l'òrgan de contractació.

AVÍS IMPORTANT: La incorporació d'informació relativa a preus, imports econòmics o qualsevol característica que hagi de ser valorada mitjançant criteris automàtics (Criteris de Valoració del Sobre C) en aquesta memòria tècnica (Sobre B), comportarà l'exclusió automàtica de la licitadora, segons el que estableix el Plec de Clàusules Administratives Particulars (PCAP).

David Vidal Fernández

Director de Sistemes d'Informació
Hospital Clínic de Barcelona

Annex 1 PPT- Declaració responsable del compliment dels requisits imprescindibles

La persona sota signant, en representació de l'empresa, declara sota la seva responsabilitat que la solució proposada compleix íntegrament tots i cadascun dels requisits tècnics imprescindibles establerts en el Plec de Prescripcions Tècniques, i en particular els recollits a l'Annex 1. Així mateix, declaro conèixer que el no compliment d'algun dels requisits indicats comportarà l'exclusió de la licitació, de conformitat amb el que estableix el Plec.

Requisits tècnics imprescindibles	
Característica	
Bloc A: Solució SaaS (Infraestructura de Vora)	
ID	Requisit Tècnic
A.1	Infraestructura Global Anycast: Desplegament en PoPs distribuïts geogràficament amb adreçament IP ANYCAST per a l'optimització de latència i protecció DDoS.
A.2	Independència de Núvol Públic: Els PoPs no poden executar-se sobre núvols públics de tercers (ex. AWS, Azure, GCP) per garantir el control total de l'SLA.
A.3	Seguretat ENS Alta: Certificació de conformitat amb l'Esquema Nacional de Seguretat (ENS) Categoria Alta (RD 311/2022).
A.4	Nodes Privats (Hybrid Cloud): Capacitat de desplegar nodes de programari a les instal·lacions del client (on-premise o tenants privats) gestionats des de la consola única cloud.
A.5	Serveis DNS i Ports: DNS primari/secundari sense límit de peticions i publicació de serveis HTTP en ports no estàndard.
A.6	Protecció Avançada: Inclusió de capacitats proactiva d'intel·ligència que permetin reconèixer atacs pertanyents a campanyes d'atacs cibernètics organitzats, capacitat de detectar IP malicioses en funció de la seva reputació amb almenys 11 categories que permetin diferenciar els accessos des de Proxys anònims/Tor, Botta Discovery i protecció d'APIs.
Bloc B: Equipament Físic (On-Premise)	
ID	Requisit Tècnic
B.1	Integració Arquitectura Hospital Clínic: Integració nativa en els clústers actuals per a una migració transparent de polítiques i objectes.
B.2	Alta Disponibilitat (HA): Mecanismes de failover manual/automàtic amb supervisió de components crítics (VLAN trunks, gateways, pools).
B.3	Xifrat Post-Quàntic: Suport i implementació d'algoritmes de xifrat resistent a la computació quàntica en la versió ofertada.
B.4	Gestió de Logs: Emmagatzematge local (SSD 480GB) i enviament massiu via Syslog/High-speed logging amb baix impacte en CPU/RAM.
B.5	Dual Stack IPv4/IPv6: Funcionalitat de Gateway IPv6 a IPv4 (i viceversa) amb ús simultani d'ambdós protocols.
B.6	Lògica Programable: Suport de scripting estructurat (tipus TCL o equivalent) per a la manipulació de tràfic en nivells OSI 2-7 i consultes a APIs externes.
B.7	Optimització de Tràfic: Compensació hardware (20 Gbps), Caché HTTP (Gzip) i optimització nativa per a protocols S3.
Bloc C: Seguretat WAF y Protecció d'Aplicacions	

ID	Requisit Tècnic
C.1	Homogeneïtat de Firmes: Nomenclatura de firmes WAF idèntica entre la solució Cloud i On-premise per facilitar la gestió de falsos positius.
C.2	Protecció OWASP i Avançada: Defensa contra SQLi, XSS, Cookie Poisoning, Força Bruta i segrest de sessions.
C.3	Detecció de Bots i Proactivitat: Defensa proactiva contra bots i aprenentatge automàtic (Machine Learning) del comportament de l'aplicació.
C.4	Integració Antivirus: Capacitat d'integració amb motors AV externs mitjançant protocol ICAP.
C.5	Catàleg CPSTIC: La solució ha d'estar inclosa en el Catàleg de Productes de Seguretat TIC del CCN amb categoria Alta.
Bloc D: Capacitats de Rendiment i Connectivitat (Hardware)	
ID	Requisit Tècnic
D.1	Throughput L4/L7: Mínim 40 Gbps en Capa 4 i 30 Gbps en Capa 7.
D.2	Connexions Concurrents: Capacitat per mantenir almenys 38.000.000 de connexions concurrents L4.
D.3	Transaccional: Mínim 1.300.000 peticions HTTP L7 per segon.
D.4	Acceleració SSL/ECDSA: Almenys 30k transaccions RSA/sec i 14k transaccions ECDSA P-256/sec.
D.5	Interfícies Físiques: 4x 25/10/1 Gbps (SFP+), 4x 10/1 Gbps (Coure), Gestió OOB i Consola Sèrie.

Annex 2 PPT- Adreça de lliurament dels elements del contracte

Els APs es lliuraran a les ubicacions que s'indiquen al a següent taula:

Equipament	Adreça de Lliurament	Quantitat
Balancejador 1	Centre de procés de dades de Consultes Externes (CEX, situat al Carrer Rosselló 161 de Barcelona): Soterrani -1 - CPD	1
Balancejador 2	Edifici CEK (situat al Carrer Rosselló 149-153 de Barcelona) Soterrani -1 - CPD	1

Annex 3 PPT – Formulari de Productes Hardware i Software que s'inclouran en el subministrament

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

Fabricant	Part Number	Descripció	Quantitat

Annex 4 PPT – Formulari de Llicències que s'inclouran en el subministrament

En aquest formulari, es recull la relació detallada de llicències incloses en la configuració proposada:

Element HW/SaaS on s'apliquen	Part Number	Descripció	Quantitat	Tipus (nominals, concurrents,..)	Durada (mesos)