Expedient: 0889/25
Entitat: EDP Salut Sant Joan de Reus – Baix Camp
Tipus: mixt
Procediment: obert
Tràmit: ordinari
Objecte: Contractació de la renovació de la infraestructura de seguretat datacenter i perimetral i la renovació del manteniment de la infraestructura de comunicacions centrals

PLEC DE PRESCRIPCIONS TÈCNIQUES

EXPEDIENT 0889/25

CONTINGUT

1. INTRODUCCIÓ

El present plec inclou les especificacions tècniques per a la contractació del projecte de renovació de la infraestructura de seguretat perimetral-datacenter i renovació del manteniment hardware, software i les llicències de la arquitectura actual de Core Network del CPD de Hospital Sant Joan de Reus

El Departament TIC de la Entitat de Dret Públic Salut Sant Joan de Reus – Baix Camp, en endavant SSJRBC, obre un procés de concurrència d'ofertes per tal de seleccionar les més òptimes, i satisfer així, les seves necessitats.

2. OBJECTIU DEL CONCURS

A continuació es descriuen els objectius principals del present plec.

2.1. Objectius del Concurs

- Renovació de la infraestructura de seguretat perimetral per assegurar els accessos a la xarxa pública
- Renovació de la infraestructura de seguretat interna per assegurar els accessos entre les diferents xarxes de la xarxa interna.
- Renovació del manteniment software, hardware i llicencies de la infraestructura Core Network del CPD de HUSJR

3. DIVISIO DEL CONCURS EN LOTS

Atenent als diferents tipus de necessitats de les empreses que concorren a la licitació, els serveis de comunicacions i seguretat s'han agrupat en 2 lots.

- **LOT 1 – SEGURETAT DATACENTER I PERIMETRAL**

El Lot 1: 'Seguretat datacenter i perimetral ' contempla:

- Instal·lació i posta en marxa d'un element de seguretat de nivell 7 OSI per a gestionar l'accés de tots els centres de la EDP salut Sant Joan Reus-Baix Camp a la xarxa pública (Internet).
- Instal·lació i posta en marxa d'un element de seguretat de nivell 7 OSI per a gestionar els accessos des de les diferents VLAN's de la xarxa de Hospital Sant Joan de Reus
- Serveis de manteniment per a la infraestructura.

- **LOT 2 – INFRAESTRUCTURA DE COMUNICACIONS CENTRALS**

El Lot 2: "Infraestructura de comunicacions centrals" contempla:

- Renovació del manteniment software, hardware i llicencies de la infraestructura Core Network del CPD de HUSJR

4. LOT1 - SEGURETAT DATACENTER I PERIMETRAL

4.1. OBJECTE

L'objecte de la present licitació és la renovació de la plataforma de seguretat interna i perimetral, **serveis de subscripció, suport tècnic i manteniment, posta en marxa i migració ,** actualment basada en dos nodes Palo Alto PA-3220.

El motiu de la renovació es la finalització del cicle de vida i suport de l'actual equipament, en el període en que es planteja el nou contracte.

I es per aquest motiu que la proposta serà un nou equipament, que ha de garantir:

- **Migració transparent** de l'arquitectura actual a la nova, garantint que les connexions actuals amb els diferents proveïdors assistencials de la entitat no es vegi afectada per el canvi de tecnologia. Un canvi radical implicaria una reconfiguració de totes les connexions, amb el risc de desconnexions que podrien posar en risc la continuïtat del servei.
- **Migració efectiva,** on les regles actualment configurades que garanteixen la segmentació de la xarxa de la EDP, puguin ser exportades des de la infraestructura actual i importades a la nova, sense necessitat de realitzar canvis.
- **Integracions amb SOC** que gestiona les alertes de Ciberseguretat, actualment en producció, com a empresa del sector sanitari.

Com a entitat del sector salut, gestionem dades de categoria especial segons el RGPD. La disponibilitat dels sistemes i la integritat de la informació són crítiques. Atès que les subscripcions actuals dels tallafocs (Firewalls) estan properes a la seva caducitat, és imperatiu garantir:

- La protecció contra amenaces avançades
- El filtratge de continguts i control d'aplicacions.
- Increment de la capacitat de processament derivat de les noves necessitats a les que donar resposta dins del sector.
- Garantir la continuïtat del negoci.

El present plec fixa els requisits, les obligacions i les solucions tecnològiques que hauran de complir les ofertes presentades.

4.2. ARQUITECTURA ACTUAL

2 equips PAN 3220, i les següents llicències:

- Threat Prevention
- Wildfare
- URL Filtering
- Virtual System extra (5)
- Globalprotect
- Serveis de suport del fabricant

4.3. REQUERIMENTS DE LA SOLUCIÓ

La infraestructura que realitzarà les tasques de Firewall perimetral i de primera barrera de seguretat estarà ubicada al Datacenter de Hospital Sant Joan de Reus i haurà de complir els següents requeriments, pel que fa referència a funcionalitats, hardware, serveis i rendiment, sense perdre cap de les funcionalitat indicades en el punt anterior:

4.3.1. Característiques de la solució

- Solució en alta disponibilitat en actiu-actiu i actiu-passiu
- Routing entre VLAN's
- Agregació enllaços de manera que es comportin com un de sol, tant a l'hora d'identificar una zona com a l'hora d'aplicar una política
- Protocols dinàmics de Routing OSPF,BGP i capacitat de routing basats en aplicacions SD-WAN.
- Suport per NAT, PAT, inclòs NAT Transparent.
- Polítiques de routing basades en ip o xarxa origen.
- Filtratge entre VLAN's a nivell aplicació.
- Suport HTTP/2
- Modalitats TAP, mirror i transparent per a les interfícies per inspecció del transit.
- Suport per a standard 802.1Q, 801.AX, 802.3ad
- QoS per aplicació, usuari, URL
- Gestió de túnels VPN-SSL , VPN IPSec i x-auth VPN-SSL

- Identificació usuaris per integració amb LDAP (Active Directory)
- Autenticació usuaris basada el LDAP, Kerberos, SSO, TACACS, RADIUS, BBDD local per accessos VPN.
- Aplicació de polítiques basades en usuaris i grups de LDAP
- Suport a OCSP i llistes de revocació de certificats
- Suport a integració a mòduls HSM de tercers
- Capacitat per a la identificació de microserveis SaaS.
- Identificació aplicacions en túnels encriptats SSL entrada i sortida
- Identificar aplicacions fora dels ports TCP standard.
- Capacitat per a identificar trànsit desconegut, categoritzar per al seu anàlisi i crear polítiques per a la seva gestió.
- Capacitat per a crear firmes personalitzades per identificar aplicacions propietàries.
- Agrupar aplicacions per categories
- Creació de regles de qualitat de servei segon us de les aplicacions
- Utilització de la identificació aplicacions com a criteri per a la selecció de perfils de protecció de vulnerabilitats, de manera que s'apliquin només aquelles signatures específiques segona aplicació en us.
- Anàlisi predictiu DNS per bloqueig amenaces de C2,DGA o substracció de dades per tunelització DNS.
- Capacitat per a analitzar el trànsit DNS en temps real per detectar atacs de Fast-Flux, dominis generats estratègicament i atacs basats en l'edat del domini mitjançant ML.
- Capacitat per a inspeccionar trànsit SSL
- Suport natiu i accelerat per maquinari per desxifrar i inspeccionar trànsit TLS 1.3 i el protocol QUIC sense degradació dràstica del rendiment.
- Capacitat per desxifrar trànsit SSL i SSH a qualsevol port.
- Capacitat identificar aplicació real dins túnel SSL
- Capacitat per a bloquejar sessions SSL que no puguin ser desxifrades
- Capacitat anàlisi de trànsit de xarxa.
- Protecció davant atacs per denegació de servei DoS
- Capacitat per a detectar i bloquejar escanejos de xarxa
- Proteccions SYN Flood, UDP Flood, ICMP Flood, ICMP Flood, inundacions
- Protecció IDS i IPS davant vulnerabilitats, permetent aplicar polítiques al tràfic generat tant des de Internet com des de la LAN.
- Filtratge segons categories de risc

- Filtratge per URL, essent possible que les llistes siguin estàtiques o dinàmiques i que puguin ser aplicades a les diferents regles.
- Detecció d'equips compromesos a la xarxa local fent us de fitxers de signatures.
- Identificació de fitxers, inclosos els comprimits
- Identificació de fitxers per tipus MIME, essent possible l'aplicació a les regles generades.
- Identificació de fitxers per patrons , essent possible l'aplicació a les regles generades
- DLP, capacitat de cerca de patrons, cadenes concretes, amb la finalitat d'evitar falsos positius.
- Identificació enviament de credencials cap a l'exterior.
- Identificació de vulnerabilitats per identificador CVE
- Bloqueig de amenaces – incloent malware, exploits i spyware – a qualsevol port TCP/UDP, sense importar la tècnica d'evasió utilitzada.
- Filtratge per polítiques antivirus amb capacitat de bloqueig, quarantena i enviament del adjunt a serveis externs per anàlisi
- Filtratge per polítiques antivirus sobre protocols de xarxa
- Filtratge per polítiques antivirus sobre usuaris, segments de xarxa, aplicacions.
- Capacitat prevenció en temps real.
- Capacitat per aturar codi maliciós completament desconegut i atacs de phishing en temps real, utilitzant models d'aprenentatge automàtic dins del mateix firewall, sense haver d'esperar el veredicte d'un Sandbox extern.
- Capacitat per a generar firmes automàtiques un cop analitzat el fitxer a la Sandbox i distribuir-les als tallafocs
- Capacitat per a pujar fitxers de forma manual a Sandbox i comprovar estat anàlisi.
- Estaran inclosos els fitxers tipus EXE, DLL, PDF, APK, JAVA, entre altres.
- Creació informes predefinits / personalitzats fent us dels fitxers de traça sense utilitzar equipament extern. Informes automatitzats.
- SNMP per a la recollida de fitxers de traça i enviaments a tercers syslog
- Accés per a la gestió del dispositiu per WEB i CLI
- Suport Jumbo Frames (MTU 9192)
- Autentificació multifactor.
- Capacitat per aplicar polítiques d'accés basades en el principi de mínim privilegi i en l'avaluació contínua de l'estat de l'usuari, el dispositiu i el context de connexió, amb revocació o limitació d'accés quan es detectin anomalies.".
- Funcionalitats per optimitzar l'enrutament de sortida cap a aplicacions SaaS (ex. Office 365, sistemes

sanitaris al núvol) basant-se en la latència, el jitter i la pèrdua de paquets dels enllaços ISP en temps real.

- Identificació i control del trànsit cap a aplicacions SaaS (Shadow IT), amb capacitat per bloquejar la pujada de dades sensibles a instàncies personals
- L'arquitectura de processament de la solució ha de ser capaç d'executar les funcions d'identificació d'aplicacions, control d'usuaris i prevenció d'amenaces avançades en un únic cicle d'inspecció de flux de dades, garantint que el rendiment de la inspecció a Nivell 7 no es degradi de forma acumulativa en activar múltiples subscripcions de seguretat de forma simultània
- La solució haurà d'oferir descobriment, classificació, perfilat i avaluació de risc de dispositius IoMT/IoT/OT mèdics, amb capacitat d'identificar automàticament tipus de dispositiu, fabricant, model i atributs tècnics rellevants per a la segmentació i aplicació de polítiques de seguretat
- El tallafocs i la solució de seguretat IoMT hauran de provenir del mateix fabricant, per garantir la integració nativa de les polítiques de seguretat, evitar dependències entre múltiples vendors i assegurar una responsabilitat única en cas d'incidència de seguretat
- La solució de visibilitat IoT haurà d'operar sense requerir el desplegament d'agents programari en els dispositius finals ni sondes de hardware dedicades de captació (appliances analitzadors de tràfic addicionals), aprofitant el propi pla de control del tallafocs per al descobriment del parc tecnològic. El sistema ha de demostrar la capacitat de catalogació automatitzada a partir de l'anàlisi de tràfic passiu des del moment de la seva connexió
- El sistema ha d'incloure interfícies d'explotació de dades orientades a entorns d'enginyeria clínica o biomèdica que permetin correlacionar l'inventari IoMT de forma nativa amb: les declaracions de seguretat dels fabricants de hardware sanitari (estàndard MDS2), bases de dades oficials d'alertes sanitàries o retirades de producte (com les notificacions de la FDA o equivalents de forma automatitzada) i mètriques d'activitat de la connectivitat de dispositius crítics de suport vital.
- La solució haurà d'incorporar un motor d'identitat en núvol per a la integració amb proveïdors d'identitat empresarials (IdP), compatible amb estàndards SAML 2.0 i SCIM, que permeti la sincronització d'identitats sense duplicació de tasques operatives

4.3.2. Hardware

- 10 - Interface Ethernet1/2,5/10/25 GbE
- 10 - Interface 1/10 GB (SFP/SFP+)
- 4 Port 25G (SFP28)
- Interface OOB
- Disc dur SSD
- Interface consola RJ45

- Arquitectura hardware dedicada per a gestió (Interface dedicat amb alta disponibilitat), separada de la dedicada al servei.
- Font alimentació redundada

4.3.3. Serveis

- Subscripció Advanced Thread Prevention
- Subscripció Advanced URL Filtering
- Subscripció Advanced Wildwire
- Subscripció Advanced DNS Security
- Subscripció Advanced SD-WAN
- Subscripció Device Security – IOT
- Subscripció Prisma Access Agent
- Subscripció 5 Extra VS
- Serveis de manteniment del hardware i software
- Serveis de suport per incidències de "Ciber-seguretat"
- El servei de manteniment del maquinari de la solució es prestarà en modalitat 24x7

Tots aquest serveis hauran de ser vigents en tota la durada del contracte.

4.3.4. Rendiment

- Rendiment mínim acreditat pel fabricant, amb funcionalitats de seguretat habilitades i sota condicions de prova publicades a fitxa tècnica, per garantir la capacitat operativa de l'entorn.
- Rendiment en càrrega amb funcionalitats habilitades de IPDS/IPS major 7 Gbps
- Rendiment VPN – IPSEC major de 5 Gbps
- Capacitat per a crear més 100.000 sessions per segon
- Nombre màxim de sessions total 1.250.000

5. LOT 2 – INFRAESTRUCTURA DE COMUNICACIONS CENTRALS

5.1. INTRODUCCIÓ

L'objecte d'aquest lot és la renovació del manteniment de la infraestructura de comunicacions centrals (CORE Network) del CPD de l'Hospital Sant Joan de Reus. Els elements inclosos en aquest lot, amb el detall d'equipament i dates de finalització de contracte, es descriuen a l'Annex 1 del quadre de característiques.

6. PROJECTE DE SERVEIS

Els licitadors hauran de presentar un projecte de serveis per a cada un dels lots, segons necessitat, que serà indicada en cada un dels apartats. A continuació es detallen cada un dels apartats del projecte.

6.1. SERVEI DE MIGRACIÓ

Només per a LOT 1
Els licitadors indicaran en la seva proposta tècnica el pla de migració proposat, considerant:

- L'adjudicatari serà l'encarregat del muntatge, posada en marxa i la configuració de l'arquitectura exposada en aquest plec de prescripcions tècniques.
- Haurà de garantir-se la mínima afectació dels serveis als usuaris en el procés de migració. En cas de ser necessari la instal·lació d'elements temporals pel procés de migració, els costos aniran a càrrec del nou proveïdor.
- Per aquesta tasca serà necessari presentar un pla de migració detallat on quedarà identificat molt clarament quines son les finestres de no disponibilitat del sistema.
- Les migracions es realitzaran en l'horari fixat per HUSJR amb la finalitat de minimitzar la indisponiblitat. Aquests horaris poden ser nits i cap de setmana en cas que la criticitat del centre així ho requereixi.
- Haurà d'indicar-se el pla de proves previst per la certificació dels serveis instal·lats.
- No es considerarà el projecte per entregat fins que el rendiment no sigui l'esperat per el departament de IT.

6.2. SERVEI DE MONITORITZACIÓ

- El servei de monitorització de l'arquitectura consistirà en la monitorització proactiva de la disponibilitat i la operativitat de tots els elements adquirits en el projecte.
- El servei de monitorització es realitzarà les 24 del dia i els 365 de l'any.
- La monitorització es podrà fer tant des del centre de serveis gestionats de l'empresa licitadora, o bé des

del servei de monitorització que gestiona el Departament TIC (plataforma Nagios). En el cas que sigui des de les dependències de l'empresa licitadora, el Departament TIC haurà de tenir visibilitat de la plataforma de gestió en mode lectura.

- El licitador aportarà les eines necessàries hardware i software, i les línies de comunicacions que li permetin dur a terme les tasques de monitorització i solució de les incidències remotament.
- El Departament TIC posarà a disposició del licitador la plataforma de virtualització existent a l'Hospital Sant Joan de Reus per a hostatjar els servidors necessaris per oferir el servei de monitorització.
- La comunicació de les incidències originades des del servei de monitorització i la seva resolució es notificarà al CAU que gestiona el Departament TIC per correu electrònic i en cas de no disponibilitat de la plataforma de correu per via telefònica.
- La infraestructura de la plataforma de monitorització haurà de complir requeriments d'alta disponibilitat.
- Els protocols d'actuació i els llindars dels nivells d'alerta per a cada un dels elements actius del projecte es pactaran entre l'adjudicatari i el Departament TIC abans de l'inici del servei. L'adjudicatari haurà de redactar un documents amb la descripció dels procediments i les tasques pactades a realitzar.
- L'adjudicatari haurà de presentar documentació del pla d'implantació del projecte de monitorització. Es requerirà detall de les fases i durada del projecte. En el cas que puguin generar indisponiblitat del servei caldrà detallar les finestres de tall per tal de minimitzar l'impacte en el servei i concretar els horaris de les actuacions.
- Un cop iniciat el servei l'adjudicatari haurà de generar informes periòdics amb el detall de l'estat del servei, incidències i actuacions realitzades. Aquests informes seran pactats abans d'iniciar el servei de monitorització.

6.3. MANTENIMENTS

- Requereix tenir actiu contracte de manteniment amb el fabricant en tot l'equipament subministrat per l'adjudicatari durant la vigència del contracte.
- L'adjudicatari haurà d'entregar la documentació on s'acredita que l'equipament està al corrent de pagament de manteniment.

6.4. SERVEIS DE SUPORT TÈCNIC

- Els model de serveis de suport tècnic van destinats a complimentar les tasques que es realitzen a l'àrea tècnica del Departament TIC. Les tasques encomanades al servei de suport tècnic estaran dins del context del manteniment, gestió i actualització de l'equipament software i hardware de seguretat.
- Els protocols d'actuació i els llindars dels nivells d'alerta per a cada un dels elements actius de la xarxa

es pactaran entre el adjudicatari i el Departament TIC abans de l'inici del servei. L'adjudicatari haurà de redactar un document amb la descripció dels procediments i les tasques pactades a realitzar.

- El desenvolupament de les activitats de serveis gestionats que es preveu en aquesta contractació s'haurà de cenyir a l'ús de les millors pràctiques generalment acceptades en el sector, i que en el cas de les entitats licitadores s'identifiquen amb el marc metodològic ITIL en la seva versió 3.
- Els serveis de suport tècnic operaran de manera coordinada amb el Departament TIC.
- Les intervencions per part de l'adjudicatari en qualsevol de les àrees seran liderades i tutelades per membres del Departament TIC, tant si és en mode presencial com en remot.
- L'objectiu final es garantir la continuïtat de servei durant les 24 hores del dia, 7 dies a la setmana.
- L'adjudicatari serà l'encarregat de reportar la incidència al fabricant de software i hardware en els casos on l'equipament estigui sota manteniment o garantia. Realitzarà el seguiment de la incidència, verificarà el bon funcionament un cop resolta i generarà informe de les tasques realitzades.
- Un cop iniciat el servei l'adjudicatari haurà de generar informes periòdics amb el detall del estat del servei, nombre d'incidències i actuacions realitzades, nivell d'acompliment dels SLA's, percentatge d'incidències obertes des de la plataforma de monitorització. Aquests informes seran pactats abans d'iniciar el servei de monitorització.
- Les actualitzacions de software i hardware alliberades pels fabricants de l'arquitectura proposada hauran de ser instal·lades per l'adjudicatari dins del marc del contracte de serveis de suport.
- La ubicació del servei de suport tècnic estarà ubicat dins del territori espanyol i l'idioma utilitzat serà català o castellà.

6.5. GESTIÓ DEL SERVEI SUPORT TÈCNIC

- L'adjudicatari posarà a disposició del Departament TIC un interlocutor únic per a tasques de gestió de servei (operació, supervisió i seguiment).
- Es requerirà atenció personalitzada en el centre de gestió del proveïdor en horari 8x5
- Fora de l' horari 8x5 personalitzat l'adjudicatari haurà d'oferir el suport necessari per garantir la prestació del servei.
- Les peticions de suport tècnic només les podran sol·licitar el personal Departament TIC, o les persones designades a aquests efectes per cadascuna de les entitats licitadores.

6.6. PLA – OFICINA TÈCNICA DE IMPLANTACIÓ

Només per a LOT 1

Durant la implantació dels serveis, l'adjudicatari destinarà un equip de professionals dedicats al projecte (Oficina Tècnica d'Implantació).

Aquest equip estarà liderat per un cap de projecte, amb experiència demostrada suficient, que serà l'interlocutor tècnic únic amb el Departament TIC durant la implantació.

L'Equip de Treball proposat pels licitadors per l'execució de la implantació dels serveis, serà el que el licitador estimi necessari per la bona execució del projecte, estant format com a mínim pels següents perfils clau:

- Cap de Projecte.
- Responsable de la implantació / prestació del servei.

En tot cas, serà responsabilitat de l'adjudicatari, l'adequació del nombre de recursos en funció de la fase d'implantació i assumpció de l'abast segons planificació pactada, per tal de garantir l'èxit en el termini màxim establert.

A tal efecte, els licitadors hauran d'indicar en la seva proposta tècnica els recursos que integrin l'Equip de Treball proposat per la implantació del projecte, incloent el número de recursos i perfils proposats, la dedicació per perfils i per recursos, i els rols que exerciran durant el transcurs de la implantació del servei.

Durant la fase de execució i posada en marxa, l'oficina tècnica d'implantació ha de fer-se càrrec de:

- Direcció d'implantació i posada en marxa dels serveis.
- Planificació de la posada en marxa i validació del pla de migració, planificació global d'activitats / responsabilitats, planificació temporal de trasllat i implantació, període de proves i test, formació, etc.
- Implantació i posada en marxa de tots els serveis
- Desinstal·lació dels productes a substituir si fos el cas.
- Identificar les accions a realitzar per la implantació de cadascun dels serveis: requeriments i adequació d'infraestructures, etc.
- Establir, conjuntament amb Departament TIC, el calendari detallat de les actuacions.
- Establir els protocols i formats de comunicació amb Departament TIC pel seguiment del projecte.
- Direcció tècnica durant la implantació.
- Identificació de riscos i propostes correctives, replantejos, etc.
- Coordinació del pla de formació tècnica, tant a personal operatiu com tècnic.
- Coordinació i acceptació del pla de proves i test.
- Suport i coordinació d'activitats en la posada en marxa de cada centre.
- Establir el procediment de seguiment i coordinació: reunions de coordinació i seguiment, seguiment amb direcció del projecte, elaboració i distribució d'actes de reunions,…
- Reunions de seguiment de la implantació.
- Suport tècnic i resolució de problemes durant la implantació.
- Recepció provisional de la documentació.
- Posada en marxa.

- Elaboració dels procediments de posada en marxa
- Supervisió dels processos de posada en marxa
- Presentació de documents de seguiment d'implantació, informes de identificació de riscos i propostes de millora, memòria tècnica detallada de la configuració.

6.7. CALENDARI

Només per a LOT 1

La totalitat dels serveis hauran d'estar operatius com a màxim en els següents terminis, respectant els compromisos vigents de la entitat.
Aquesta es reserva el dret a modificar el calendari proposat pel adjudicatari dins d'aquests terminis màxims.

- 4 mesos posteriors a la data de formalització del contracte per tots els serveis o la data que s'indiqui a tal efecte en el contracte.

6.8. FASES DE IMPLANTACIÓ

Només per a LOT 1

El procés de posta en marxa constarà de les següents fases:

- **Solució tècnica:** Un cop formalitzat el contracte, l'entitat contractista es posarà en contacte amb el departament TIC de SSJRBC per tal de fer una coordinació i calendarització dels terminis i adequació de la implantació de la infraestructura oferta a les necessitats de l'entitat. El contractista presentarà la solució final del disseny, arquitectura, tecnologia, dimensionat, esquemes, pla d'implantació, pla de proves, pla de formació, pla de emergència i pla de qualitat.

- **Aprovació del projecte per part de l'EDP SSJRBC:** Una vegada rebut el projecte, l'EDP SSJRBC l'analitzarà i podrà realitzar propostes de modificació que hauran de ser incloses per part del contractista en 7 dies a partir de la seva comunicació, lliurant el projecte definitiu.

- **Execució i posta en marxa:** Una vegada lliurat i validat per l'EDP SSJRBC el projecte definitiu, s'iniciaran els processos d'execució i posta en marxa.

- **Test i proves:** El contractista realitzarà els tests necessaris d'acord amb el pla de proves presentat. Aquestes es realitzaran d'acord amb la normativa vigent. L'EDP SSJRBC podrà realitzar proves addicionals, amb el suport del personal i mitjans de l'adjudicatari, sense cap cost. No es consideraran superades les proves sense l'acceptació per part de l'EDP SSJRBC.

- **Acceptació:** Realitzades amb èxit les proves i lliurada tota la documentació, l'EDP SSJRBC procedirà a l'acceptació. A partir del moment de l'acceptació, el proveïdor podrà iniciar a facturar el projecte segons es detalla a continuació.

  Lliurament de documentació en format electrònic, inclourà les versions finals del projecte executiu amb els resultats de les proves de test realitzades. El contractista acordarà un model de documentació i etiquetat amb l'EDP SSJRBC. La instal·lació s'hauran d'etiquetar segons el model acordat.

6.9. NIVELLS DE CERTIFICACIÓ

Respecte els dos lots, els licitadors han d'estar en possessió dels nivells de certificació específics amb el producte proposat i haurà d'aportar les acreditacions corresponents:

- Condició de distribuïdor homologat. La condició de distribuïdor homologat és una condició per a l'execució del contracte. Els licitadors, en fase de presentació d'oferta, han de presentar una declaració de responsable mitjançant la qual faran constar que, en cas de ser proposats adjudicataris del contracte, disposaran de la certificació de distribuïdor oficial emès pel fabricant; en el moment de l'inici de l'execució del contracte, el contractista haurà d'aportar l'acreditació d'aquesta condició, és a dir, la certificació. Es necessària aquesta certificació atès que es tracta d'una renovació de la infraestructura actual que es disposa del fabricant actual i s'ha de garantir un correcte manteniment d'aquesta amb empreses especialitzades que tinguin aquesta certificació; la compatibilitat amb la infraestructura actual es necessària, en cas contrari, es perdrien funcionalitats ja implantades o suposaria inversions addicionals injustificades.

- L'empresa contractista haurà d'acreditar que el fabricant de la solució proposada dona compliment als estàndards internacionals de seguretat en el desenvolupament del seu programari, tals com ISO/IEC 27001, SOC 2 Type II, o equivalents.

  Amb l'objectiu de garantir un nivell de seguretat de la informació i protecció de dades personals en l'allotjament i gestió de la plataforma, el contractista haurà d'acreditar de forma obligatòria que el servei del contracte està certificat d'acord amb la norma ISO/IEC 27001, SOC 2 Type II o equivalent atès que aquests instruments son els únics que garanteixen que el proveïdor disposa d'un mínim de seguretat en els seus processos, control d'accés i gestió de vulnerabilitats, entre d'altres.

  En el moment d'iniciar l'execució del contracte, el contractista haurà d'aportar l'acreditació d'aquesta condició.

6.10 COMPLIMENT AMB CERTIFICACIÓ ENS SSJRBC

L'EDP SSJRBC té categoritzats els seus sistemes d'informació en el Nivell Baix de l'Esquema Nacional de Seguretat (ENS), d'acord amb el RD 311/2022. Les solucions aportades pels licitadors no podran implicar una degradació d'aquest nivell de seguretat. A tal efecte, qualsevol component de la solució que impliqui el tractament, transmissió o emmagatzematge de dades fora de les instal·lacions de l'Hospital — incloent serveis de telemetria, anàlisi de fitxers en sandbox, actualitzacions de signatures o intel·ligència d'amenaces en núvol — haurà de complir els següents requeriments:

- a) Les dades tractades fora de les instal·lacions hauran de residir i processar-se dins de l'Espai Econòmic Europeu (EEE), o en un país amb decisió d'adequació reconeguda per la Comissió Europea d'acord amb l'article 45 del RGPD.

- b) El contractista haurà d'acreditar documentalment, mitjançant certificació del fabricant o contracte de nivell de servei, que és tècnicament possible restringir el flux de dades a la regió europea i que aquesta restricció estarà activa durant tota la vigència del contracte. En el moment d'iniciar l'execució del contracte, el contractista haurà d'aportar l'acreditació d'aquesta condició.

- c) En cap cas les dades de configuració, polítiques de seguretat, logs o informació sobre la xarxa interna de SSJRBC podran ser accessibles per a tercers ubicats fora de l'EEE sense autorització expressa i prèvia de l'EDP.

Exposat tot l'anterior, l'empresa contractista es farà responsable que la configuració final desplegada a la infraestructura de l'Hospital permeti el compliment de les mesures organitzatives i tècniques requerides per l'Esquema Nacional de Seguretat (ENS) en categoria Baixa, d'acord amb el RD 311/2022, que és el nivell de categorització declarat per l'EDP SSJRBC. La solució ofertada no podrà implicar una degradació d'aquest nivell de seguretat.

Els licitadors, en fase de presentació d'oferta, han de presentar una declaració de responsable mitjançant la qual faran constar que la solució tecnològica oferta dona compliment als les mesures organitzatives i tècniques requerides per l'Esquema Nacional de Seguretat (ENS) en categoria Baixa que disposa l'entitat Salut Sant Joan de Reus – Baix Camp.

6.11 NIVELLS DE SERVEI

La qualitat del servei prestat pel adjudicatari es controlarà mitjançant els indicadors de nivell de servei.

En les seves propostes els licitadors han d'incloure:

- Metodologia per garantir el compliment dels compromisos (especificar matriu d'escalat).
- Procediments de càlcul dels ANSs per part dels licitadors.

Els nivell de servei exigits es referenciaran segons aquesta classificació:

- Crític P1: Impacte per a tots els usuaris. Incomunicació entre les diferents xarxes del centre. Afectació en els pacients.
- Greu P2: Impacte per alguns usuaris. Indisponiblitat o degradació d'alguna xarxa virtual, servei. Afectació en els pacients.
- Lleu P3: Impacte en algun usuari puntual. No assistencial, sense afectació per al pacient.

Temps de resolució de les incidències.

Tipus	Temps
Crític P1	1 Hores
Greu P2	4 Hores
Lleu P3	24 Hores

Temps de resolució per a peticions

Tipus	Temps
Prioritària	8 Hores
No prioritària	72 ores

6.12 FORMACIO

<u>Només per a LOT 1</u>

Serà responsabilitat de l'adjudicatari formar al personal de HUSJR en les noves tecnologies i plataformes tecnològiques que siguin implantades, en cas que apliqui, per garantir un coneixement bàsic sobre les seves característiques i funcionament així com en aquells processos operatius i de gestió que requereixin la participació del personal de Departament TIC. Addicionalment s'haurà de proveir informació de les eines de gestió i control implantades a les que HUSJR pugui accedir per realitzar tasques de monitorització i gestió.

Els licitadors indicaran en les seves propostes el pla de formació a impartir inclòs en la seva proposta detallant: cursos, participants, metodologia, calendari, continguts, etc.

El pla de formació haurà de ser aprovat per Departament TIC, que serà l'encarregat d'establir les directrius

pel disseny del pla de formació definitiu del personal, així com coordinar el mateix. La formació es realitzarà abans de la posada en marxa dels serveis en horaris, grups i format convingut amb HUSJR.

6.13 LLICENCIAMENT

- L'oferta haurà d'estar dimensionada per a cobrir les llicencies en tota la durada del contracte.

6.14 DEVOLUCIÓ DEL SERVEI

Per tal de no afavorir la posició dominant dels proveïdors que donen actualment els serveis objecte del contracte o per evitar que puguin realitzar un mal ús de la seva posició, tant en aquest procés de licitació com el que tindrà en la futura renovació en concursos posteriors, els proveïdors actualment implantats i els que en resultin elegits, pel fet de presentar-se al present concurs, accepten i estaran obligats a:

Facilitar tota la informació tant tècnica com administrativa necessària per a la realització del traspàs en un termini màxim de 4 setmanes des de la seva sol·licitud.
No dificultar el procés de canvi, ni degradar els ANS pactats.

En cas d'incompliment d'aquestes obligacions, HUSJR podrà aplicar les següents penalitzacions, sense perjudici d'altres sancions derivades de les pèrdues de servei o econòmiques que es puguin derivar:
10% de la facturació mensual corresponent a la totalitat dels serveis contractats per HUSJR del lot adjudicat per cada setmana de retard en facilitar la informació a "l'adjudicatari entrant".
El doble de les penalitzacions establertes en el present plec, per aquells ANS i serveis que siguin d'aplicació.

HUSJR podrà sol·licitar al proveïdor adjudicatari de la present licitació, amb antelació a la data de terminació del contracte, la continuïtat de la prestació dels serveis per un període pactat de fins a 6 mesos amb l'objectiu d'assegurar el traspàs global dels serveis.

7 REQUERIMENTS GENERALS

Addicionalment als requeriments de cada servei, hi ha un conjunt de requeriments, vinculats no tant a les tecnologies sinó als serveis associats, que són comuns a tots els serveis, i que l'adjudicatari haurà de satisfer segons la següent relació de requeriments.

7.11 ACTITUD PROACTIVA

En tots els àmbits dels serveis a contractar es demana una permanent actitud proactiva per part de l'adjudicatari, és a dir, es desitja que l'adjudicatari dels serveis sigui un veritable soci tecnològic de la entitat. Això implica entre altres:

- Informar nous serveis que puguin ser d'interès o adients.
- Accions proactives tant de manteniment preventiu com de manteniment correctiu.
- Informar a la entitat amb l'antelació suficient de la necessitat d'adequació de les infraestructures que puguin estar obsoletes i que donin suport als serveis, permetent i facilitant així la presa de decisions, sense que la informació rebuda suposi un compromís de cap tipus per part de HUSJR.

Com a mínim amb una periodicitat anual, es realitzarà una reunió entre els responsables de la entitat i el adjudicatari, on l'adjudicatari presentarà un informe de nous serveis o millores en els disponibles aparegudes en el període, així com un informe de les millores o avantatges que aquestes representarien per a SSJRBC. Aquests informes no suposaran un compromís de cap tipus per part de SSJRBC. Aquesta reunió no substituirà les reunions periòdiques de seguiment dels serveis contractats establertes en els requeriments tècnics.

7.12 OBLIGACIONS DE L'ADJUDICATARI EN SEGURETAT

- El proveïdor adjudicatari haurà de garantir la seguretat, disponibilitat, confidencialitat i integritat dels serveis gestionats a SSJRBC mitjançant el compliment de les següents normes bàsiques:
- Complir amb els estàndards i polítiques de seguretat de SSJRBC
- Garantir la confidencialitat, integritat i disponibilitat de la informació emmagatzemada.
- Informar a SSJRBC sobre la seva política de seguretat així com de la implementació i seguiment per part de la seva organització.
- Informar per escrit a SSJRBC tan aviat com es detectin riscos reals o potencials de seguretat en la seva xarxa o en l'equipament del client.
- Garantir que tota la informació transmesa per SSJRBC no és emmagatzemada, duplicada o interceptada, extrem a extrem en la seva xarxa.
- Accés a qualsevol equipament de xarxa i/o sistemes d'informació mitjançant un control d'accés lògic, garantint la restricció als usuaris autoritzats.
- Garantir l'estricta aplicació de les normes de seguretat per part del seu personal.
- Definir normes de seguretat que siguin respectades en tots els centres operatius, garantint la seva aplicació mitjançant controls periòdics i auditories realitzades per organitzacions externes.
- Executar totes les operacions de servei seguint procediments escrits que contemplin les normes de seguretat.

Degut a la importància dels serveis objecte del contracte, els adjudicataris hauran de garantir la confidencialitat de la informació i de les configuracions dels sistemes de SSJRBC als que donin servei així com el compliment de la legislació vigent en matèria de protecció de dades de caràcter personal.

7.13 RELACIÓ EDP SSJRBC – ADJUDICATARI

La relació entre l'EDP SSJRBC i l'empresa contractista complirà els següents requeriments:
El contractista que presti serveis a l'EDP SSJRBC haurà de disposar d'una única interfície tipus "finestra única" a través de la qual es realitzaran totes les gestions.

Aquesta atenció serà personalitzada, permanent i àgil. Des d'aquest únic punt d'entrada es canalitzaran totes les sol·licituds, reclamacions i altres comunicacions realitzades per l'EDP SSJRBC. L'atenció, tant tècnica com comercial, serà personalitzada. Els recursos encarregats de l'atenció comercial hauran de tenir els coneixements tècnics i aptituds personals adequades a la magnitud d'un client com l'EDP SSJRBC. L'EDP SSJRBC podrà sol·licitar, de forma justificada, el canvi de comercial que es realitzarà en un termini màxim de 15 dies. El contractista ha de garantir la continuïtat de l'atenció comercial i tècnica personalitzada, durant els períodes de vacances, amb el mateix nivell de servei. La resolució d'incidències haurà de contemplar procediments de relació excepcionals, a banda del canal estàndard, per atendre problemes urgents o d'emergència.

El sotasignat declara que, l'elaboració i la informació continguda en el present document, ha sigut duta a terme d'acord amb el seu criteri tècnic i tot garantint la lliure concurrència, segons el disposat a la Llei 9/2017, de 8 de novembre, de contractes del sector públic.

El que signo als efectes oportuns,

A Reus, amb data de signatura digital

Juli Ferrer Espax
Cap de Tecnologies de la Informació i Comunicació
EDP Salut Sant Joan de Reus – Baix Camp

Amb la signatura del present document, el sotasignat declara que no existeix conflicte d'interès en la seva actuació professional. Així mateix, declara que coneixen les seves obligacions, que consten al Codi ètic i de bones pràctiques en la contractació pública i licitacions de l'Entitat de Dret Públic (EDP) Salut Hospital Universitari Sant Joan de Reus – Baix Camp (SSJRB)