Plec de requeriments tècnics per a la licitació de la renovació de part de la xarxa de dades de la Fundació Privada del Hospital de la Santa Creu i Sant Pau

Gener 2026

Índex

1. Presentació

1.1 Objecte de la licitació

L'objecte de la licitació és la renovació parcial de l'equipament de xarxa de dades, i el manteniment i suport de tota la xarxa de dades de la Fundació Privada de l'Hospital de la Santa Creu i Sant Pau (en endavant Fundació), tant als pavellons del Recinte Modernista de l'Hospital de la Santa Creu i Sant Pau (en endavant RM) com de la seva seu a Reus.

A tots els efectes la implementació dels sistemes considerats en el present document es considerarà un projecte claus en mà i inclourà els serveis necessaris per a minimitzar el temps d'implementació.

Es fixen, a més, diversos objectius secundaris. El primer és reduir el nombre de tecnologies que han de gestionar els tècnics de comunicacions del RM amb la finalitat de facilitar un nivell de coneixement més profund dels elements que formen part de l'arquitectura de xarxa. A més, durant la vigència del contracte, es substituiran una part dels equipaments i es migrarà la seva funcionalitat a equipament més modern per garantir una total integració, compatibilitat i homogeneïtat del sistema per tal de facilitar l'administració i el manteniment posterior.

Finalment, es persegueix identificar millores tant en l'arquitectura de dades de de la Fundació com a les mesures de seguretat que puguin ser implantades en projectes futurs

1.2 Àmbit

L'àmbit del projecte és l'equipament de la xarxa de dades de la Fundació, tant dels pavellons del Recinte Modernista com de la seva seu a Reus. L'àmbit del projecte inclou:

- La integració del nou equipament als tallafocs actuals.
- Equipar dues sales tècniques ampliant equips existents per concentrar les connexions procedents dels diferents racks d'accés.
- La renovació d'una part dels equips d'accés cablejat a la xarxa de dades.
- La incorporació d'una nova capa de core a la xarxa.
- La renovació de garanties de l'equipament que no es substitueixi.

1.3 Abast del contracte

Forma part de l'abast del contracte:

- El subministrament de l'equipament nou detallat en aquest plec, subscripcions i material necessaris, amb les garanties que inclou SLAs garantits per a 5 anys (Annex 1).
- 5 anys de garantia que inclou SLAs garantits de l'equipament de xarxa que no es substitueixi (veure Annex 2).
- 5 anys de manteniment de tot l'equipament de xarxa del RM i de la seu de Reus, tant del el de nova adquisició com del que no es substitueix (veure Annex 1 i 2) des de la data del contracte.
- Dissenyar un pla de migració robust que permeti integrar sobre l'arquitectura de xarxa el nou equipament que substituirà l'actual.
- Instal·lació i configuració de l'equipament nou adquirit. En el cas dels racks d'accés s'inclouen els treballs de connexió del cablejat necessari a l'interior del racks.
- Posada en marxa i validació de la instal·lació.
- Documentació de la instal·lació.

- Registre de les incidències generades en el procés d'instal·lació i validació.
- Formació dels tècnics de suport designats per la Fundació.
- Planificació, coordinació i seguiment de projecte.

1.4 Objectius del projecte

Els objectius del projecte son:

- Renovar una part dels equips de xarxa de dades que actualment ja estan obsolets, amb les garanties corresponents.
- Renovar garanties de l'equipament no substituït.
- Mantenir homogeneïtat a la xarxa.
- Posar al dia tecnològicament les funcionalitats i característiques d'acord amb les possibilitats actualment disponibles en el mercat.

1.5 Terminis

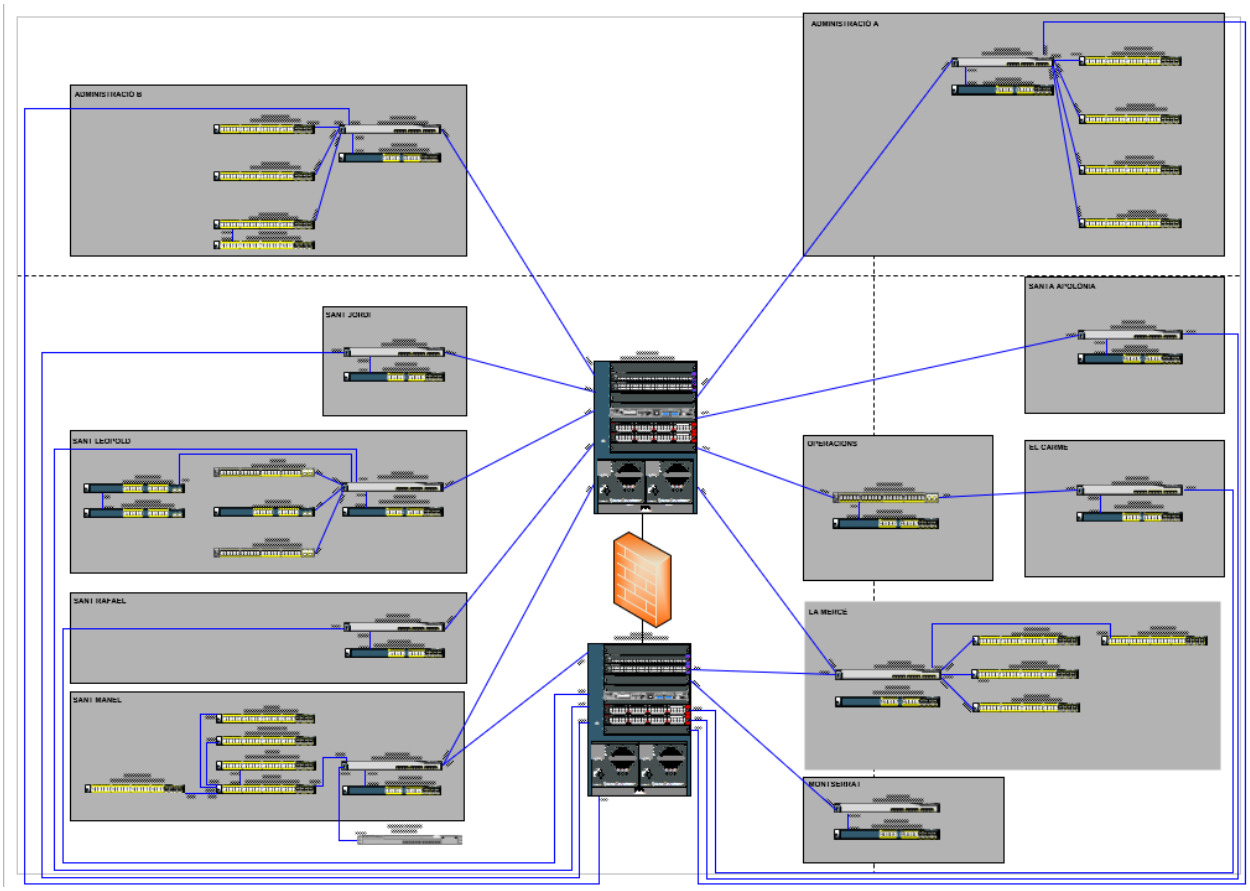
Termini màxim per a la instal·lació del nou equipament des de la data de signatura del contracte: 6 mesos.

Termini de garantia i manteniment: 5 anys des de la data de posada en producció.

Terminis per activar les garanties de l'equipament que no es substitueix serà des de la data d'inici de contracte per 5 anys.

2. Descripció de la situació actual

2.1 Estructura actual de la xarxa de dades del RM



Actualment la xarxa de dades del RM té tres punts de concentració general principal al RM, en el Centre de Control A (CCA), Centre de Control B (CCB) i Centre de Control C (CCC) on estan connectats 12 búnquers de pavelló que donen servei als diferents racks de pavelló. Gairebé totes aquestes connexions estan redundades, utilitzant fibres que passen per 2 camins diferents i utilitzant equips concentradors diferents. Les fibres utilitzades són OM3.

Per permetre la connexió entre els 3 Centres de Control així com entre els 3 Centres de Control i els búnquers es disposa de mànegues de FO SingleMode

Entre els búnquers i els racks de pavelló hi han mànegues de FO MultiMode OM3.

El RM parteix per a aquest projecte d'una arquitectura de xarxa de dades existent en la qual es compta amb equipament Fortinet. amb 2 tallafocs, 68 commutadors i 87 punts d'accés sense fil. Com a resultat de la implantació del projecte es vol mantenir l'arquitectura de xarxa gestionada directament des del tallafocs i sobre la que s'han implementat un conjunt de eines de seguretat.

2.2 Estructura de dades de la seu a Reus

La seu de la Fundació a Reus disposa actualment d'un tallafocs Fortinet, integrat dins la mateixa arquitectura de seguretat corporativa que el Recinte Modernista. Aquest equip actua com a element

principal de protecció perimetral i gestiona les connexions remotes mitjançant VPN SSL i IPSec, assegurant la comunicació xifrada entre seus i l'accés segur dels usuaris remots.

El dispositiu proporciona funcionalitats avançades de seguretat de capa 7, com ara inspecció profunda de paquets (DPI), control d'aplicacions, filtratge web, detecció d'intrusions (IPS) i protecció antimalware amb sandboxing en el núvol. A més, permet la inspecció SSL del trànsit xifrat i l'aplicació de polítiques de seguretat granulars per usuari o servei.

La gestió del tallafocs es realitza de manera centralitzada des del Recinte Modernista. L'equip manté integració amb el model de seguretat corporatiu basat en Security Fabric.

3. Dimensionament de l'equipament a adquirir

3.1 Adquisició de tallafocs

Durant la vigència del contracte, la Fundació renovarà els dos equips de tallafocs del Recinte Modernista i l'equip de la seu de Reus en funció dels següents requeriments i característiques mínimes detallades en aquest apartat i segons els terminis establerts al punt 1.5.

A més, per garantir una total integració, compatibilitat i homogeneïtat de l'arquitectura ja instal·lada, els nous tallafocs hauran de ser del mateix fabricant que els commutadors de core, transport i accés instal·lats per tal de facilitar l'administració i el manteniment posterior.

3.1.1 Especificacions generals dels tallafocs

La proposta haurà d'incloure durant la totalitat de la duració del contracte, així com les possibles pròrrogues, totes les llicències i subscripcions necessàries per activar, en el cas que sigui necessari, totes les funcionalitats associades als requeriments obligatoris que es llisten a continuació.

Els equips tallafocs han de ser en format appliance d'un únic fabricant, quedant exclosos màquines virtuals ni servidors de propòsit general. Han de poder ser instal·lats en un rack estàndard de 19''.

Els dos equips físics per al Recinte Modernista han de ser de idèntiques característiques, redundats i en alta disponibilitat (HA, High availability). Han de permetre treballar en mode HA actiu-actiu i actiu-passiu. En el cas d'activar sistemes virtuals, aquests poden funcionar en qualsevol dels dos nodes, de forma que s'aconsegueixi un actiu-actiu.

L'equip per a Reus ha de ser físic. És un únic node.

La solució per a les dues seus ha d'incloure funcionalitats de control d'aplicacions, IPS, Antimalware, Webfilter, Antispam i web application firewall. Totes aquestes funcionalitats han d'estar llicenciades per a la duració del contracte.

S'hauran de subministrar fonts d'alimentació redundants per a cada equip.

Els equips han de disposar de la funcionalitat de tallafocs virtual per tal de crear entorns completament diferencials. Ha d'incloure com a mínim 10 tallafocs virtuals per equip.

La solució de seguretat ha de permetre diferents modes de funcionament, podent-se combinar entre els diferents tallafocs virtuals:

- Mode transparent.
- Mode routed i/o mode sniffer.

S'haurà d'incloure a la proposta, dintre dels mateixos appliance, la funcionalitat d'auditoria pròpia del Sistema, que com a resultat tingui un indicador o valor numèric de risc, així com puntuació negativa per cada paràmetre auditat no complert. Aquests paràmetres que s'han de comprovar son com a mínim: política de seguretat sense ús en els últims 90 dies, política de contrasenyes dèbils i comprovació del llicenciament/suport.

La pròpia plataforma ha de tenir connectors automàtics amb l'objectiu d'integrar-se amb identitats terceres i poder recollir informació, adreçament ip, inventari d'objectes i etiquetes. Aquesta funcionalitat haurà d'estar suportada en els appliances de seguretat (sense necessitat de consola addicional). En concret es requereixen les següents:

- Cloud pública: Google Cloud, Azure, AWS, Oracle i AliCloud.
- Cloud privada: VMware NSX i ESXi, Openstack, Kubernetes, Cisco ACI i Nuage.
- Fonts d'identitat: Active directory i Radius.
- Fonts d'amaneces: Llistat d'ip, dominis i hash's de malware.

La mateixa solució de seguretat ha de permetre la creació d'automatismes per tal de:

- Davant la detecció d'un host compromès, els tallafocs enviïn (tots alhora): un email, una notificació tipus push a dispositius Iphone, poder banejar l'adreça ip, invocar funcions AWS Lambda, Google functions, Azure Functions i Webhook.
- Davant el canvi de configuració del tallafocs, un failover, reboot, actualització de firmes, de forma programada i qualsevol event del tallafocs, aquest enviï (tots alhora): un email, una notificació tipus push a dispositius Iphone e invocar funcions AWS Lambda, Google functions, Azure Functions, AliCloud Function, comanda per CLI i Webhook.

Capacitat de configuració de Proxy explícit per Interface, amb la funcionalitat de Proxy chaining en cas necessari, a més de capacitat de caching.

3.1.2 Especificacions particulars dels tallafocs

3.1.2.1 Centre de Control A (CCA)

Es demanarà la provisió del següent equipament o superior, per muntar- ne al Centre de Control A amb les següents característiques:

Unitats	Descripció	Codi
1	FortiGate-401F Hardware plus 5 Year 24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	FG-401F-BDL-950-60

3.1.2.2 Centre de Control B (CCB)

Es demanarà la provisió del següent equipament o superior, per muntar- ne al Centre de Control B amb les següents característiques:

Unitats	Descripció	Codi
1	FortiGate-401F Hardware plus 5 Year 24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	FG-401F-BDL-950-60

3.1.2.3 Seu a Reus

Es demanarà la provisió del següent equipament o superior, per muntar- ne al Centre de Control B amb les següents característiques:

Unitats	Descripció	Codi
1	FortiGate-121G Hardware plus 5 Year 24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	FG-121G-BDL-950-60

3.1.3 Rendiment

Els equips tallafocs tindran hardware específic (de tipus ASIC) per tal d'assegurar el rendiment requerit; en detall, ha de tenir un hardware específic per analitzar el tràfic a nivell 4 i un altre totalment diferent, a nivell 7.

El tallafocs disposarà de fins 36 / 36 / 27 Gbps de rendiment de tallafocs per paquets de 1518, 512 i 64 bytes en IPv4 ; i de 36 / 36 / 27 de rendiment de tallafocs per paquets de 1518, 512 i 64 bytes en IPv6.

El tallafocs ha de ser capaç de gestionar fins 8 Milions sessions concurrents. Així com a mínim 450.000 noves sessions per segon.

El tallafocs ha de tenir una latència de 2 µs (per paquets 64 byte UDP).

Ha de tenir capacitat per com a mínim de 10.000 polítiques de tallafocs.

A nivell 7, l'equip ha de disposar de com a mínim el següent rendiment:

- Rendiment IPS: 10 Gbps per tràfic Enterprise MIX.
- Rendiment NGFW (IPS i control d'aplicacions): 9.5 Gbps per tràfic Enterprise MIX.
- Rendiment amb Threat Protection (IPS, control d'aplicacions i motor antimalware actius): 7 Gbps per tràfic Enterprise MIX.

  Caldrà acreditar que aquestes tres últimes dades siguin amb logging actiu.

- Rendiment Inspecció SSL amb IPS: 8 Gbps mesurat amb diferents Ciphers.
- Rendiment per control d'aplicacions: 15 Gbps mesurat per http 64K.

3.1.4 Connectivitat i característiques físiques

Els tallafocs hauran de complir, com a mínim, les següents característiques físiques i de connectivitat:

- 1 port de consola RJ45 per a gestió fora de banda.
- 2 ports USB (1 tipus A i 1 tipus C) per a la connexió de dispositius externs, suport de càrrega de configuracions i firmware.
- 2 ports 10GE SFP+ per interconnexió d'alta velocitat.
- 12 ports GE RJ45 per connexions de xarxa.
- 8 ports GE SFP per connexions de fibra òptica.
- Instal·lació en rack estàndard de 19", amb un format de 1RU i kit de muntatge inclòs.
- Fonts d'alimentació redundants amb connexió hot-swap, garantint la continuïtat de servei.
- Consum màxim inferior a 250 W.
- Emmagatzematge intern SSD de fins a 240 GB per suportar funcions de logging local i serveis interns.
- Capacitat d'ampliació de ports mitjançant commutadors gestionats del mateix fabricant, integrables en una única plataforma de gestió.
- Ventiladors redundants amb control automàtic de velocitat.
- Nivell de soroll ≤ 60 dBA en condicions normals de funcionament.
- Compatibilitat total amb els mòduls d'expansió i llicències disponibles per a la sèrie FortiGate 400 i 100.

3.1.5 Gestió

La gestió ha de ser de fàcil ús i intuïtiva.

Capacitat de gestió dels equips mitjançant accés via web (https) i terminal (ssh) per la total configuració de les polítiques de seguretat de la plataforma.

Quedaran excloses aquelles solucions que requereixin una plataforma de gestió externa per gestionar i administrar la solució.

Tots els canvis efectuats en els tallafocs han de ser aplicats de forma immediata, sense necessitat de compilar o similar.

Creació de diferents tipus d'usuari per l'administració podent aplicar diferents rols o perfils, així com definir xarxes d'origen confiables. Es necessari també la possibilitat de crear usuaris de tipus REST-API.

Suport de SNMP i sFlow.

Exportació de logs vía SYSLOG, FTP, SCP i TFTP.

3.1.6 Networking

Suport de protocols RIP v1/v2, OSPF, ISIS, BGP, WCCP i Multicast per IPv4 e IPv6, Routing basat en política o PBR.

Suport Dual Stack IPv4 e IPv6 simultàniament.

Network address translation NAT IPv4, NAT64 i NAT66.

DHCP server / DHCP Relay /DNS Server / DNS Proxy / NTP Server.

802.1Q VLANs i Point-to-Point Protocol over Ethernet (PPPoE).

802.3ad Capacitat de crear enllaços LACP per l'agregació de ports.

Capacitat de balanceig de servidors a nivell 4 per tots els serveis, com també possibilitat de fer SSL off-loading pel tràfic HTTPS.

Cal que la solució de seguretat tingui capacitats integrades de SD-WAN, en concret:

- Balanceig intel·ligent de connexions físiques i lògiques, indiferentment del tipus de connexió WAN (MPLS, 3G/4G, FTTH, VPN, etc..).
- El número mínim de connexions físiques i lògiques que es poden afegir a l'SD-WAN ha de ser de 256.
- Verificació de la disponibilitat d'Internet per cadascuna de les línies, per protocols http, ping i TWANP. El numero de chequejos ha de ser de com a mínim 100.
- Verificació de paràmetres de qualitat en temps real: jitter, packet loss i latència per línia.

- Configuració de polítiques de SD-WAN intel·ligent basat en origen (usuaris AD i direcció IP), en el destí (direcció IP, aplicacions i/o serveis d'Internet/aplicacions) i en la línia amb millor qualitat d'aquell moment basat en valors de jitter, packet loss, latència, tràfic de pujada/baixada o ampla de banda, així com una combinació per pesos.
- En el cas de necessitat de llicenciament o subscripcions per activar aquestes funcionalitats, caldrà que aquestes estiguin incloses en la proposta durant la duració completa del contracte.

Suport d'VXLAN i VXLAN VTEP per l'extensió de xarxes de nivell 2 entre xarxes de nivell 3.

El sistema proposat ha de tenir una funcionalitat integrada de Traffic Shaping tant de trànsit sortint com a entrant sent capaç de reservar ample de banda i marcar el trànsit amb DSCP. Aquest traffic shaping ha de basar-se en aplicacions i URLs a nivell global de perfil o per ip.

3.1.7 Alta disponibilitat (tallafocs Recinte Modernista)

La funcionalitat d'alta disponibilitat ha d'estar disponible sense necessitat de llicencia.

Suport HA tipus Actiu – Passiu, Actiu - Actiu i mode mixta. El mode mixte implica poder tenir tallafocs virtuals actius i passius de forma barrejada, es a dir, el màster de certs tallafocs virtuals sigui la primera unitat de tallafocs, mentre que la segona unitat de tallafocs es màster de la resta de tallafocs virtuals alhora.

La transferència de servei d'un equip a l'altre s'ha de poder fer sense talls, ni pèrdua de les connexions tcp, ni aturada de servei.

Les configuracions s'han de traspassar de manera automàtica entre els dos equips.

Capacitat de funcionament en mode actiu/actiu sincronitzant sessions entre els dos nodes però mantenint adreçament IP diferenciat en les interfícies de cada node del clúster.

En el cas de necessitat de llicenciament o subscripcions per activar l'alta disponibilitat, caldrà que aquestes estiguin incloses en la proposta durant la duració completa del contracte.

3.1.8 Visibilitat

Els equips tallafocs han de poder generar topologies gràfiques físiques i lògiques, amb la integració d'altres tallafocs del fabricant, per tal de poder ser capaç de veure en un extrem a extrem que esta passant en tota la xarxa.

Funcionalitat de consolidació de logs amb diferents nivells d'agrupació, en concret: per origen, destí, aplicació, amenaça, websites i polítiques per a la seva visualització.

Aquesta visualització ha de ser tipus "Drill-down", és a dir, poder seleccionar uns dels objectes agrupats i anar filtrant el resultat en base a aquesta selecció, fins a saber el detall complet.

Aquests requeriments hauran de poder acomplir-se des de la mateixa GUI dels appliances, en temps real, i sense necessitat d'una consola central de gestió.

3.1.9 Seguretat

Capacitat de definir polítiques de seguretat IPv4/v6 utilitzant els següents paràmetres de coincidència:

- Com a origen (totes les opcions):
  - Capacitat de definir una i/o més d'una Interface d'origen, incloent "any". Així com també "zones".
  - Capacitat d'utilitzar direccions ip, rangs i/o xarxes, FQDN, països, serveis d'internet i direccions ip's reconegudes com origen de xarxes TOR, proxies anònims (aquestes direccions han d'actualitzar-se automàticament), així com els objectes exportats dels connectors esmentats a l'apartat de caracterisques generals de l'equip.
  - Capacitat d'utilitzar usuaris/grups locals o AD.
  - Capacitat per declarar horaris o "schedule" tant per dia/hora com a data màxima de venciment.
  - Capacitat de selecció del servei a utilitzar.

- Com a destí:
  - Capacitat de definir una i/o més d'una Interface de destí, incloent "any". Així com també "zones".
  - Capacitat d'utilitzar direccions ip, rangs i/o xarxes, així com objectes FQDN, països i serveis d'internet.

Capacitat de definir polítiques de seguretat IPv4/v6 utilitzant la següent parametrització:

- S'ha de poder seleccionar quin tràfic s'analitzarà a nivell 4 i quin a nivell 7, per política, sense excepció.
- La configuració del NAT sortint s'ha de poder configurar dintre de cadascuna de les polítiques de seguretat, de forma granular.
- Les diferents funcionalitats de seguretat avançades de nivell 7 s'activaran de forma individual a nivell de política, mai a nivell global. A més aquestes es gestionaran amb perfils per tal de ser granulars en els permisos. Aquestes funcionalitats son: antivirus, webfilter, DNS filter, Web Application Firewall, Control d'aplicacions, IPS, i DLP.
- Decidir a nivell de política quin tràfic SSL serà desxifrat pel seu anàlisis i quin només a nivell de certificat.
- A nivell de logging, cal que la solució permeti activar el logging de només nivell 7, o tant de nivell 4 més nivell 7. Cal també fer captura de packets en la pròpia política.

Capacitat de creació de regles de DoS a nivell 3 i 4, podent aplicar umbrals per serveis publicats on poder filtrar per direccions ip o països per: ip_src_session, ip_dst_session, tcp_syn_flood, tcp_port_scan, tcp_src_session, tcp_dst_session, udp_flood, udp_scan, udp_src_session, udp_dst_session, icmp_flood, icmp_sweep, icmp_src_session, icmp_dst_session, sctp_flood, sctp_scan, sctp_src_session i sctp_dst_session.

Per tal d'evitar l'accés de xarxes botnet, els tallafocs han de tenir una base de dades de reputació dinàmica que bloquegi els accessos a nivell d'Interface.

Visualització del número d'usos i quantitat de tràfic de cada regla de seguretat, de forma àgil tant en la pròpia secció de polítiques de seguretat, això com també dintre de la configuració de cada política . També cal veure l'ultima vegada que se ha utilitzat.

3.1.10 Control d'aplicacions

Capacitat per identificar un mínim de 1.900 aplicacions actives actuals (incloent aplicacions web 2.0), com per exemple distingir Facebook, d'una sub-aplicació Facebook-chat o post.

La solució ha de classificar les aplicacions en diferents categories i subcategories, per poder aplicar regles d'acord amb aquestes categories / subcategories (control granular dins de l'aplicació).

Aplicar tècniques d'identificació d'aplicacions a tots els ports TCP / UDP i no només en els més comuns.

Capacitat per identificar les aplicacions sota túnels HTTPS.

Capacitat per identificar aplicacions Industrials com Modbus.

Capacitat de creació de firmes d'aplicacions per un reconeixement personalitzat. Es obligatori que en aquelles aplicacions customitzades, també siguin analitzades per motors de protecció (IPS i antimalware).

3.1.11 IPS

Capacitat per protegir tant servidors com clients amb un mínim de 10000 firmes d'IPS, agrupades per categoria, severitat, objectiu i protocol. Davant la identificació d'un atac per IPS, cal que el tallafocs capturi el tràfic en un arxiu pcap per tal d'evidenciar-ho i fer un estudi posterior.
Capacitat per identificar patrons d'atacs basats en comportament o rated-base, per tal de bloquejar intents d'atacs un cop superat un umbral d'ús en un temps determinat.
Capacitat de creació de firmes d'IPS per un reconeixement personalitzat.

3.1.12 Antimalware

Capacitat de detecció de malware (virus, grayware, worns, etc…) basat en firmes conegudes o mètodes avançats de detecció.

Suport de sandboxing en el cloud, amb un tamany mínim de fitxer de 100 MB indistintament del tipus de fitxer.

Capacitat per l'eliminació del contingut dinàmic (macros, javascript, URL) explotable dintre de documents ofimàtics i pdf, que es distribueixen per protocols SMTP, IMAP i http.

Capacitat de comprovació de si es tracta d'un fitxer bo o dolent, en funció del hashing i comparat amb la BBDD del fabricant. Així com bloquejant mitjançant malware de repositoris externs de threat inteligence.

3.1.13 Webfilter

Capacitat de categoritzar més de 250 milions de pàgines web en més de 60 categories web per tal d'aplicar: block, monitor i aplicació de cuotes de temps o tràfic per categoria.

Suport de protocols http v1.0, 1.1 i 1.2.

La base de dades de categories web caldrà consumir-se com un servei cloud en temps real i no podrà basar-se únicament en llistats locals per tal de tenir la categorització de les url's el més actualitzat possible.

Suport per restringir l'accés a Youtube i Google en mode "safe search".

Suport de rating per imatges per URL.

Suport per a la creació de llistes blanques/negres externes sense necessitat de llicencia.

3.1.14 Altres funcionalitats de nivell 7

Altres funcionalitats de nivell 7 que la proposta ha d'incloure son:

- DLP.
- DNS Filter.
- ICAP.
- Web application firewall.

3.1.15 VPN

El sistema de seguretat haurà de complir, com a mínim, amb els següents requisits relacionats amb la funcionalitat VPN:

- Compatibilitat completa amb estàndards de la indústria per a VPN, sense necessitat de maquinari addicional, incloent:
  - IPSec VPN (IPv4 i IPv6) amb suport d'encriptació avançada AES-256, IKEv2 i autenticació robusta.
  - SSL VPN (tant en mode túnel com en mode portal web) amb suport per accés remot segur des de navegadors i clients FortiClient.
  - GRE sobre IPSec, PPTP i L2TP per compatibilitat amb entorns heterogenis.
- Capacitat de connexions VPN simultànies:
  - Suport per a fins a 20.000 usuaris VPN IPSec simultanis.
  - Suport per a fins a 10.000 usuaris SSL VPN simultanis sense necessitat de llicència addicional.
- Rendiment VPN:
  - IPSec VPN throughput ≥ 20 Gbps (paquets de 512 bytes).
  - SSL VPN throughput ≥ 7 Gbps, amb inspecció de trànsit xifrat.
- Funcionalitats avançades de VPN:
  - Suport per VPN concentrator amb capacitat d'agregació de túnels i balanceig per paquet, permetent sumar amplada de banda entre seus.
  - Capacitat d'integració amb autenticació multifactor (2FA) nativa del fabricant, mitjançant tokens mòbils, SMS o correu electrònic, també aplicable a l'accés a la GUI d'administració.
  - Possibilitat d'integració amb serveis externs d'identitat (Active Directory, Radius, LDAP, SAML).
  - Suport per túnels VPN dinàmics amb detecció automàtica de peers i reconfiguració sense interrupció del servei.

- Gestió i seguretat VPN:
  - Gestió centralitzada de túnels VPN des de la mateixa GUI/CLI de l'appliance sense requerir plataformes externes.
  - Monitoratge i diagnosi en temps real del trànsit VPN, amb visibilitat de sessions, usuaris i alertes d'incidències.
  - Capacitat de generar logs detallats de connexions, intents fallits i trànsit xifrat, exportables via SYSLOG.

3.1.16 Controladora d'accés segur integrada

El sistema ha de ser capaç d'actuar com controladora de punts d'accés wireless així com de commutadors del mateix fabricant.

La capacitat mínima de punts d'accés ha de ser de 512, i de commutadors de 64.

En el cas de necessitat de llicenciament o subscripcions per activar l'alta disponibilitat, caldrà que aquestes estiguin incloses en la proposta durant la duració completa del contracte.

La gestió dels APs i commutadors es farà des de la mateixa interfície gràfica i CLI des de la qual es gestiona el tallafocs.

3.1.17 Logging i Reporting

Pel logging i reporting caldrà instal·lar una màquina virtual per que els tallafocs enviïn en temps real els logs generats, amb l'objectiu de que sigui una:

- Eina de monitoreig a temps real del trànsit filtrat pels diferents mòduls dels equips.
- Eina de monitoreig històric externa als dispositius, emmagatzematge de logs, reports, del tràfic analitzat pels equips amb capacitat de fer informes de 6 mesos aproximadament (incloure llicenciament i suport necessari durant tota la durada del contracte).
- Reports i alarmes en funció de adreces, ports, protocols.
- Reports i alarmes en funció de usuaris i/o grups d'usuaris (AD/LDAP).
- Poder analitzar, correlacionar i fer informes de la informació de seguretat de manera centralitzada.
- Panell de control amb vista general d'usuaris destacables, aplicacions, destinacions, llocs web, vulnerabilitats, etc.
- Models d'informes preconfigurats, editables, modificables i exportables.
- Gestió d'events amb generació d'alertes automàtiques a administradors.
- Visor de logs en temps real o històric, que permeti distingir-los entre trànsit, events i seguretat.
- Visió de logs per dispositiu, dominis d'administració o agregats.
- Capacitat de filtratge i granuralitat d'anàlisi de logs.
- Dissenyador d'alertes comprensible .
- Possibilitat de generació d'alertes per nivells de seguretat, events específics, accions o destinacions i nombre d'events en un determinat temps.
- Capacitat de cercar alertes històriques.

- Notificació d'alertes per correu electrònic, SNMP o syslog.
- Rotació de logs recopilats automàtica amb enviament d'històrics a d'altres sistemes per email, FTP, HTTP, etc.
- Visibilitat dels logs en format TXT descarregables.
- Vista comparada de patrons de trànsit i amenaces.
- Anàlisi exhaustiva de totes les activitats relacionades amb el trànsit i els dispositius.
- Elaboració d'informes sobre totes les activitats de trànsit i de dispositius.

3.2 Adquisició de commutadors

Durant la vigència del contracte, la Fundació renovarà 3 equips de commutadors, tots ells ubicats en el Recinte Modernista en funció dels següents requeriments i característiques mínimes detallades en aquest apartat i segons els terminis establerts al punt 1.5.

A més, per garantir una total integració, compatibilitat i homogeneïtat de l'arquitectura ja instal·lada, els nous commutadors hauran de ser del mateix fabricant que els commutadors de core, transport i accés instal·lats per tal de facilitar l'administració i el manteniment posterior.

3.2.1 Centre de Control B

Es demana la incorporació d'un equip FortiSwitch FS-148F-POE amb la finalitat de fer funcions de concentrador de connectivitat entre els Centres de Control i els diferents búnquers del RM, dins d'una arquitectura de xarxa gestionada de manera centralitzada.

Aquest equip permetrà la connectivitat ethernet gigabit i PoE+ a nivell d'accés, i disposarà de connexions uplink de 10 GbE per a enllaç amb la xarxa troncal de l'organització, així com una interfície dedicada per a configuració, manteniment i monitorització remota.

L'equip disposarà, com a mínim, de les següents característiques tècniques:

- 48 ports 10/100/1000Base-T RJ45, amb suport PoE+ (IEEE 802.3at).
- 4 uplinks 10 GbE SFP+ per connexió a backbone o agregació.
- 1U d'alçada (format rack estàndard).
- Switching capacity: 176 Gbps.
- Throughput: fins a 130 Mpps (millor esforç).
- MAC address table: 16K entrades.
- Latència: inferior a 3 µs (en forwarding a capa 2).
- VLANs suportades: fins a 4.000 (802.1Q).
- Link Aggregation (LAG): fins a 32 grups amb múltiples ports per grup (802.3ad).
- QoS amb 8 cues per port.
- Packet buffers: 1.5 MB (shared).
- Memòria DRAM: 512 MB.
- Emmagatzematge intern (Flash/NAND): 1 GB.

3.2.2 Centre de Control A

Es demana la incorporació d'un equip FortiSwitch FS-124G-FPOE amb la finalitat de fer funcions de concentrador de connectivitat entre els Centres de Control i els diferents búnquers del RM, dins d'una arquitectura de xarxa gestionada de manera centralitzada.

Aquest equip permetrà la connectivitat ethernet gigabit i PoE+ a nivell d'accés, i disposarà de connexions uplink de 1 o 10 GbE per a l'enllaç amb la xarxa troncal de l'organització, així com una interfície dedicada per a configuració, manteniment i monitorització remota.

L'equip ofert disposarà, com a mínim, de les següents característiques tècniques:

- 24 ports 10/100/1000Base-T RJ45, amb suport PoE+ (IEEE 802.3at).
- 4 uplinks SFP, dos dels quals poden funcionar a 10 GbE (SFP+), i dos a 1 GbE (SFP).
- 1U d'alçada (format rack estàndard).

- Switching capacity: fins a 56 Gbps.
- Throughput: fins a 83.3 Mpps.
- MAC address table: fins a 16.000 adreces.
- Latència: inferior a 3 µs en entorns capa 2.
- VLANs suportades: fins a 4.000 (802.1Q).
- Link Aggregation (LAG): fins a 32 grups, amb múltiples ports per grup (IEEE 802.3ad).
- QoS amb 8 cues per port, per a priorització de tràfic.
- Packet buffers: 1 MB (shared).
- Memòria DRAM: 256 MB.
- Emmagatzematge intern (Flash): 128 MB.

3.2.3 Pavelló del Carme

Es demana la incorporació d'un equip FortiSwitch FS-124G-FPOE amb la finalitat de fer funcions de concentrador de connectivitat entre els Centres de Control i els diferents búnquers del RM, dins d'una arquitectura de xarxa gestionada de manera centralitzada.

Aquest equip permetrà la connectivitat ethernet gigabit i PoE+ a nivell d'accés, i disposarà de connexions uplink de 1 o 10 GbE per a l'enllaç amb la xarxa troncal de l'organització, així com una interfície dedicada per a configuració, manteniment i monitorització remota.

L'equip ofert disposarà, com a mínim, de les següents característiques tècniques:

- 24 ports 10/100/1000Base-T RJ45, amb suport PoE+ (IEEE 802.3at).
- 4 uplinks SFP, dos dels quals poden funcionar a 10 GbE (SFP+), i dos a 1 GbE (SFP).
- 1U d'alçada (format rack estàndard).
- Switching capacity: fins a 56 Gbps.
- Throughput: fins a 83.3 Mpps.
- MAC address table: fins a 16.000 adreces.
- Latència: inferior a 3 µs en entorns capa 2.
- VLANs suportades: fins a 4.000 (802.1Q).
- Link Aggregation (LAG): fins a 32 grups, amb múltiples ports per grup (IEEE 802.3ad).
- QoS amb 8 cues per port, per a priorització de tràfic.
- Packet buffers: 1 MB (shared).
- Memòria DRAM: 256 MB.
- Emmagatzematge intern (Flash): 128 MB.

3.2.4 Especificacions generals dels commutadors

Tot el maquinari ofert constituirà un mateix sistema que donarà servei de connectivitat al RM que, per maximitzar les prestacions de baixa latència, màxim rendiment i facilitar la gestió dels mateixos, tot el hardware ofert haurà de ser del mateix fabricant. Tot el material, connectors i adaptadors necessaris inclosos, ha de ser nou i original del fabricant.

Per tal de garantir una total integració i homogeneïtat amb l'equipament de seguretat (gestionar i aplicar polítiques directament des del tallafocs) i gestionar els commutadors des de l'equip de seguretat (també des del tallafocs), tots els commutadors ofertats han de poder ser gestionats pels tallafocs actuals i una vegada substituïts, pels nous. Quedaran excloses totes les solucions que no puguin ser gestionades des dels tallafocs actuals.

Es demana el compliment de les següents especificacions:

- Tots els equips i programaris seran de marca registrada.
- Tot el hardware i software ha de ser nou, sense utilització prèvia.
- Tot el hardware i software ha de ser vigent, trobar-se en període de comercialització del producte, sense que el fabricant n'hagi anunciat la discontinuïtat o la substitució per nous models.
- Tot el hardware i software ha de disposar d'un mínim de 5 anys de suport del fabricant un cop anunciat el fi de la comercialització del producte. Aquest suport ha d'incloure la reparació o substitució d'equips avariats, i el suport i resolució de dificultats amb el programari "firmware" dels equips i el programari de gestió.
- Tot el hardware i software s'ha de gestionar des d'una única plataforma de gestió, que implementi les necessitats de configuració i de monitoratge descrits.
- En el lliurament de les implementacions realitzades caldrà presentar documentació exhaustiva del resultat final.
- Si en el període de vigència de l'acord es publiquessin noves normatives catalanes, estatals, o internacionals, el licitador s'obliga al seu compliment.
- Els equips tindran format i accessoris adequats pel muntatge en rack estàndard de 19" d'amplada i 600 mm o 1000 mm de fons, incloent espai necessari per connexions, cables i similars. Provisió dels accessoris necessaris pel muntatge en el rack.
- Els equips s'alimentaran amb fonts d'alimentació AC 220V i 50Hz.
- Cables alimentació
- No es permeten fonts d'alimentació externes als equips.
- Es requereix suport de tots els estàndards habituals de mercat.
- Cal incloure tot el llicenciament necessari per a totes les opcions demanades.
- Subministrament de tots els materials i accessoris necessaris per a la interconnexió dels equips entre els equips d'accés amb els equips de core. Això inclou les òptiques, els cables de connexió de FO, els mòduls i cables específics, els cables d'alimentació, els cables d'stack, els cables de consola, ... i qualsevol altre element que resulti necessari. Això inclou tot el cablatge necessari per a la instal·lació dels equips (excepte els cables RJ necessaris per connectar les preses del cablejat de pavelló als commutadors d'accés).
- Les òptiques (transceivers) necessàries en els equips commutadors, (GBIC, SFP, SFP+, QSFP, QSFP+, ...) seran del mateix fabricant que el fabricant dels equips. No s'admeten òptiques compatibles ni reacondicionades ("refurbished").
- Tots els equips han de ser de gamma empresarial, que garanteixin prestacions i robustesa òptimes per a un entorn d'alta criticitat. No s'admeten equipaments pensats per al mercat SMB (empresa petita) o SOHO (small office home office).
- Tots els equips subministrats procediran del canal formal de distribució i manteniment que tingui el fabricant al país.
- Tots els equips seran completament gestionables des del propi tallafocs, en remot, via les eines subministrades en la proposta o via les eines ja existents al RM.
- El projecte inclou la implementació d'un model de gestió automatitzada via un paradigma Security Fabric i la implementació d'un model de seguretat proporcionat per la pròpia xarxa.
- El programari que es subministri en modalitat de subscripció es subministrarà de manera que s'inclogui un mínim de 5 anys de subscripció.
- En qualsevol lloc on s'anomeni una normativa estàndard cal entendre que també s'accepta com a vàlida una normativa posterior que actualitzi i millori la normativa indicada.
- L'equipament proposat haurà de complir amb criteris d'eficiència energètica i sostenibilitat, conforme als estàndards Energy Star o equivalentes, i disposar de components reciclables o de baix impacte ambiental.

3.3 Adquisició d'equipament addicional durant la vigència del contracte

Durant la vigència del contracte, la Fundació podrà requerir la incorporació d'equipament addicional de xarxa de dades per a ampliacions, substitucions o adaptacions derivades de necessitats operatives o d'evolució tecnològica.

Per atendre aquestes necessitats, s'estableix una partida econòmica específica destinada a la compra d'aquest nou equipament, que serà gestionada dins del mateix contracte i sota les condicions següents:

- Aquesta partida tindrà caràcter sota demanda de la Fundació, amb un import màxim determinat al pressupost de licitació.
- L'equipament que s'adquireixi haurà de ser plenament compatible i integrable amb l'arquitectura de xarxa i seguretat existent, mantenint la coherència amb el model de gestió centralitzada i de seguretat.
- Els elements adquirits podran incloure, entre d'altres: commutadors, punts d'accés, mòduls òptics, accessoris, components de seguretat o llicències de programari.
- L'adjudicatari serà responsable de la subministració, instal·lació, configuració, validació i documentació tècnica de tot l'equipament que s'adquireixi amb càrrec a aquesta partida.
- Haurà d'integrar-lo dins dels sistemes de monitoratge, gestió i seguretat existents, assegurant la seva operativitat completa i la seva inclusió dins del pla de manteniment.
- L'adjudicatari haurà de garantir la cobertura de garantia i manteniment de tot el nou equipament, en els mateixos termes que la resta d'equipament del contracte, fins a la finalització de la seva vigència.
- Cada adquisició haurà de ser autoritzada prèviament per la Fundació, mitjançant una petició formal que especifiqui el material, import i justificació tècnica.
- L'import corresponent es deduirà de la partida econòmica reservada a aquesta finalitat.
- L'adjudicatari no podrà imputar cap altre cost addicional derivat de la instal·lació, configuració o manteniment d'aquest equipament addicional.
- Les noves adquisicions hauran d'incloure's dins dels informes de seguiment i manteniment periòdics que estableix el present plec.

4. Renovació de garanties de l'equipament que no es substitueix

Formarà part de l'abast del contracte la renovació de les garanties per a 5 anys i dels serveis de suport i manteniment dels equips de xarxa de dades que no es substituiran amb equipament nou d'acord amb el següent inventari:

Marca	Model	Unitats
Fortinet	FortiSwitch 548D-FPOE	2
Fortinet	FortiSwitch 448E-FPOE	31
Fortinet	FortiSwitch 424E-FPOE	20
Fortinet	FortiSwitch 108F-FPOE	10
Fortinet	FortiSwitch 1048E	2
Fortinet	FAP431F (Access Point)	4
Fortinet	FAP231F (Access Point)	78
Fortinet	FAP231K (Access Point)	5

La renovació de les garanties de cada equip tindrà una durada de cinc (5) anys, iniciant-se en el moment de la data d'inici del contracte.

L'adjudicatari haurà de garantir que no hi hagi interrupció entre la cobertura actual i la renovada.

La renovació inclourà com a mínim:

- Servei FortiCare 24x7 o equivalent, amb cobertura completa de suport tècnic, actualitzacions de firmware i substitució avançada de maquinari (NBD o superior).
- Actualitzacions de seguretat FortiGuard per a totes les funcionalitats actives (IPS, antivirus, antimalware, control d'aplicacions, webfilter, DNS filter, antispam, etc.).
- Accés a noves versions de programari i "major releases" publicades durant el període de vigència.
- Assistència tècnica directa del fabricant o partner autoritzat, tant remota com in situ, segons els nivells de servei definits als Acords de Nivell de Servei (SLA).
- Garantia integral sobre tot l'equipament i accessoris inclosos, sense limitacions pel que fa a hores de servei o volum de trànsit.

L'adjudicatari haurà de lliurar a la Fundació, en un termini màxim de 30 dies naturals des de la formalització del contracte, la documentació acreditativa de la cobertura de garanties (certificats FortiCare i FortiGuard o equivalents), així com la relació nominal dels equips coberts, les seves sèries i dates d'activació i expiració.

La renovació de garanties forma part del manteniment adaptatiu descrit al punt 6.3.3 i queda sotmesa als mateixos Acords de Nivell de Servei (SLA), procediments d'escalat i mecanismes de control que la resta de manteniments.

5. Instal·lació de nou equipament

5.1 Descripció

Durant la fase inicial d'execució del contracte, l'adjudicatari serà responsable de la instal·lació, configuració, integració i posada en marxa del nou equipament de xarxa i seguretat previst en aquest plec, d'acord amb els punts 3.1 a 3.2 d'aquest plec que resumin a continuació:

- Punt 3.1 – Tallafocs:
  Instal·lació i configuració dels dos nous nodes de tallafocs del Recinte Modernista, configurats en alta disponibilitat (HA actiu-actiu o actiu-passiu), així com del tallafocs físic de la seu de Reus. Els tres equips s'hauran d'integrar dins de l'arquitectura de seguretat existent, mantenint la gestió centralitzada i la interoperabilitat amb la resta d'elements del sistema.
- Punt 3.2.1 – Centre de Control B:
  Instal·lació del commutador FortiSwitch FS-148F-POE, destinat a les funcions de concentrador de connectivitat entre els Centres de Control i els búnquers del Recinte Modernista, dins del model de gestió centralitzada definit al projecte.
- Punt 3.2.2 – Centre de Control A:
  Instal·lació de dos commutadors FortiSwitch FS-124G-FPOE, configurats en redundància i integrats amb la capa de core per a garantir la continuïtat del servei i la gestió centralitzada.
- Punt 3.2.3 – Pavelló del Carme:
  Instal·lació d'un commutador FortiSwitch FS-124G-FPOE, destinat a ampliar la capacitat d'accés i concentració de connexions del pavelló dins la mateixa arquitectura gestionada.

5.2 Criteris d'execució

L'adjudicatari haurà de complir les següents condicions per a la instal·lació i posada en servei dels equips:

- Integració i compatibilitat:
  Tot el nou equipament s'haurà d'integrar plenament dins de l'arquitectura de xarxa i seguretat existent, mantenint la compatibilitat funcional amb els sistemes de gestió actuals i amb el model de seguretat basat en Security Fabric.
- Planificació i desplegament:
  Abans de l'inici de les tasques, s'haurà de presentar un pla de desplegament detallat, que inclogui calendari, seqüència d'actuacions, recursos tècnics, riscos identificats i mesures de continuïtat de servei. El pla haurà de ser validat pel Departament de Sistemes de la Fundació.
- Execució sense interrupció de servei:
  Les operacions d'instal·lació es duran a terme garantint la màxima continuïtat operativa. En cas que sigui imprescindible una aturada planificada, aquesta haurà d'estar prèviament autoritzada i executada en franges de mínima afectació.
- Configuració i validació:
  L'adjudicatari realitzarà la configuració inicial, proves de funcionament, validació de rendiment i integració de seguretat, així com la documentació tècnica completa resultant (configuracions, topologies, adreçament, perfils de seguretat, etc.).
- Formació:
  Es proporcionarà formació tècnica específica als tècnics designats pel Recinte Modernista sobre la gestió, operació i manteniment del nou equipament instal·lat.
- Informe de validació:
  Cada actuació finalitzarà amb un informe tècnic de validació i acceptació, signat per ambdues parts, com a condició necessària per a la seva recepció i posada en servei formal.

- L'adjudicatari haurà de lliurar al final de la instal·lació un informe de validació i posada en servei conforme al model aprovat pel Departament de Sistemes de la Fundació.

6. Servei de manteniment

6.1 Resum executiu del servei de manteniment

El servei licitat inclou:

- Contractació de les garanties necessàries amb els fabricants per garantir el correcte funcionament de l'equipament: reparacions, substitucions, suport a incidències, actualització del programari tant per corregir incidències o defectes de seguretat com per evolució de la instal·lació.
- Reparació o substitució in-situ de l'equipament avariat.
- Resolució d'incidències en el funcionament dels sistemes .
- Atenció a dubtes i consultes sobre els sistemes.
- Actualització del programari dels sistemes, tant per resoldre incidències o defectes de seguretat, com per motius evolutius.

Els sistemes als que es fa referència són l'equipament actual de la xarxa de dades de la Fundació que nos es renovarà (Annex 2), i el nou equipament a adquirir detallat en d'aquest plec (Annex 1).

El servei s'ha de proveir en horari 24x7 en tot allò que s'esdevingui necessari pel correcte funcionament de la xarxa de dades. Tot i això, l'elevada redundància de hardware hauria de fer molt improbables les actuacions en horari nocturn o de cap de setmana.

L'abast de la present contractació contempla la provisió i gestió d'aquests serveis per un període de 5 anys des de la data del contracte.

6.2 Descripció del servei de manteniment

Detall de les prestacions incloses en el contracte:

- Resolució d'incidències en el funcionament dels sistemes (2on i 3er nivell). Inclou avaries. Es requereix:
  - Atenció a incidències greus (o crítiques) enteses com les que impedeixin el correcte funcionament de les instal·lacions de la Fundació.
  - Atenció a la resta d'incidències
  - Capacitat de diagnòstic remot.
  - Capacitat de presència in-situ en cas de ser necessari.
  - Informació de l'estat de les incidències en curs.
  - Gestions amb els fabricants.

- Contractació, inclosa en el preu del projecte, amb els fabricants de les garanties necessàries per assegurar el correcte funcionament de tot l'equipament:
  - Reparacions o substitucions.
  - Suport a incidències.
  - Actualització del programari per corregir incidències o defectes de seguretat.
  - Actualitzacions de programari per motius evolutius compatibles amb el hardware actual.
  - El manteniment de programari ha d'incloure dret a noves versions "major releases".
  - La contractació al fabricant de garanties pot ser amb temps de resolució de l'avaria NBD, sempre que el licitador garanteixi amb els seus mitjans la resolució de les incidències amb nivell de resposta inferior a aquest termini.

- Atenció a dubtes i consultes sobre els sistemes.
- Actualització del programari dels sistemes (actualitzacions compatibles amb el hardware actual).
- Planificació conjunta amb el personal de la Fundació segons necessitats i avaluació de riscos.
- Es considera inclòs en el preu d'aquest contracte un mínim d'una actualització anual amb motiu de la posada al dia de la instal·lació; i tantes actualitzacions com siguin necessàries per motius de seguretat, estabilitat o garanties de funcionament de la instal·lació.

- Administració dels sistemes (2on i 3er nivell)

    - Tasques d'administració avançada per canvis no estàndard, (no habituals en el dia a dia de la Fundació).
    - A efectes estimatius, en l'experiència recent de la Fundació aquest servei es ve utilitzant en 2 ocasions anuals. Això no és un compromís de volum màxim, només és una estimació del que pot fer falta.

Coordinació i reporting del servei.

Totes aquestes condicions de prestacions són d'obligat compliment. La falta de compliment d'algun dels requeriments implicarà l'aplicació de les penalitzacions que corresponguin o, en el seu cas, la resolució del contracte.

6.3 Tipus de manteniments

L'empresa adjudicatària, un cop confirmada la contractació i a petició de la Fundació, haurà de presentar proves de la contractació, pel seu compte, de les garanties que aquest plec requereix contractar als fabricants.

L'incompliment d'aquesta condició es considerarà incompliment del servei.

6.3.1 Manteniment correctiu

Inclou l'esmena o reparació d'incidències, problemes, avaries o / i disfuncions tant físiques com lògiques que impedeixin la completa disponibilitat dels sistemes amb plena capacitat d'operació. Per a aquesta tasca es tindrà en compte el següent:

- La reparació d'un equip o de qualsevol dels seus components no comportarà en cap cas disminució de prestacions ni de fiabilitat.
- L'empresa adjudicatària haurà de garantir la provisió de qualsevol classe de recanvis. Si resultés impossible, s'haurà de plantejar en la seva oferta solucions alternatives, com canvi d'equips, per al que es requerirà l'acceptació prèvia per part de la Fundació.
- En cas de fallada lògic o desconfiguració dels equips, l'empresa adjudicatària ha de garantir una ràpida resolució de la incidència.

6.3.2 Manteniment preventiu

Implica la supervisió dels sistemes per assegurar un correcte funcionament de les comunicacions de dades, un adequat aprofitament dels amples de banda i eliminació de retards, bucles i colls d'ampolla, així com la securització de la xarxa tant de cara a l'exterior com a usos indeguts des de l'interior.

El manteniment preventiu ha d'incloure la pràctica de tests de diagnòstics i proves de servei complet que identifiquin possibles errors ocults, per esmenar, si fos possible i evitar avaries i disfuncions tant físiques

dels equips com lògiques mitjançant la reparació, substitució dels elements afectats o reconfiguració lògica dels equips. aquests test hauran de realitzar-se anualment durant l'execució del contracte.

Les revisions que requereixin una aturada planificada, només podran realitzar-se prèvia conformitat o acord amb el Departament de Sistemes de la Fundació, podent ser necessari realitzar-les fora de l'horari laboral.

El manteniment preventiu s'acomodarà en tot el possible a les especificacions del fabricant de l'equip.

6.3.3 Manteniment adaptatiu

Com a part del manteniment adaptatiu, l'empresa adjudicatària haurà d'incloure la renovació de les garanties i subscripcions de suport tècnic per a tot l'equipament de xarxa actualment operatiu al Recinte Modernista i a la seu de Reus.

Aquesta renovació tindrà una vigència de cinc (5) anys i garantirà la cobertura FortiCare 24x7 (o equivalent), incloent:

- Substitució avançada de maquinari,
- Suport tècnic 24x7 i assistència remota,
- Actualitzacions de firmware i *major releases*,
- Actualitzacions de seguretat FortiGuard per a totes les funcionalitats actives (IPS, antimalware, webfilter, DNS filter, control d'aplicacions, etc.).

L'adjudicatari haurà d'acreditar documentalment la contractació efectiva d'aquestes garanties i serveis amb el fabricant o amb un partner oficial autoritzat, garantint la continuïtat del servei sense interrupcions durant tota la vigència del contracte.

6.4 Acords de nivell de servei

Els Acords de Nivell de Servei (SLA) són d'obligat compliment. En cas d'incompliment s'aplicaran de manera automàtica les penalitzacions pactades.

La Fundació es reserva el dret de realitzar auditories periòdiques dels paràmetres SLA presentats, ja sigui amb personal propi o amb l'ajuda de tercers. L'adjudicatari es compromet a col·laborar amb els mitjans necessaris.

El servei es prestarà amb els següents nivells mínims:

Àmbit	Paràmetre	Valor mínim demanat
Resolució incidències greus (o crítiques)		
	Horari de cobertura	24x7

	Temps d'atenció màxim	5 minuts
	Temps de resposta màxim	1 hora
	Temps de resolució màxim	8 hores
Resolució incidències no crítiques i Reparacions		
	Horari de cobertura	10x5
	Temps d'atenció màxim	1 hora
	Temps de resposta màxim	4 hores
	Temps de resolució màxim	Dia següent
Atenció de dubtes i consultes		
	Horari de cobertura	10x5
	Temps d'atenció màxim	4 hores
	Temps de resposta màxim	Dia següent
Administració de sistemes (2on nivell)		
	Horari de cobertura	10x5
	Temps d'atenció màxim	4 hores
	Temps de resolució màxim	Dia següent

6.5 Condicions de prestació del servei

6.5.1 Pla de desplegament

Els serveis objecte de la present licitació hauran d'estar operatius en un termini màxim d'un mes a comptar des de la formalització del contracte.

6.5.2 Model de relació

Per part de l'adjudicatari es nomenarà un "Responsable Tècnic del Servei", encarregat de:

- Gestionar la prestació del servei per complir els objectius i nivells de servei acordats i establerts en els SLAs.
- Realitzar la coordinació dels serveis associats en aquest contracte amb el Responsable designat per la Fundació.
- Actuar com a referent del Contractista per facilitar la comunicació amb les diferents àrees involucrades en la prestació del servei.
- Assegurar la gestió eficient dels problemes, assegurant que es segueixen els procediments d'escalat acordats.
- Gestionar ampliacions o revisions en els serveis, dintre de l'abast del contracte.
- Informar del servei proporcionat en base a estadístiques exactes i actualitzades.
- Establir i assegurar el compliment dels nivells de qualitat acordats i mantenir una actitud proactiva per tal de suggerir iniciatives que incideixin en la millora continuada del servei.
- Establir un procediment de revisió regular del servei que asseguri que tots els assumptes del servei es tracten de forma eficient i dintre del temps requerit.
- Gestionar els assumptes propis del servei.
- Coordinar als departaments interns del contractista afectats.
- Coordinar als diferents fabricants afectats.
- Assegurar la gestió eficient de la provisió dia a dia del servei contractat per la Fundació.

Per part de la Fundació es nomenarà un "Responsable de Gestió del Servei", encarregat de:

- Assegurar que l'adjudicatari compleix les seves obligacions contractuals.
- Assegurar el compliment dels nivells de servei pactats.
- Assegurar la disponibilitat i el seguiment dels procediments de seguiment de resultats i gestió del contracte.
- Donar suport davant la Fundació en l'especificació de qualsevol requeriment de servei addicional i possibles canvis d'abast.
- Mantenir una preocupació proactiva pels objectius, millores tècniques i estratègiques del contracte.
- Negociar possibles renovacions o pròrrogues del contracte.
- Resoldre de forma satisfactòria qualsevol assumpte de facturació o comptabilitat que pogués sorgir.

6.5.3 Horaris i terminis

Els horaris de cobertura son els indicats al quadre de SLA per cada tipologia de activitat del servei.

6.5.4 Pla de seguiment

Els responsables de servei de la Fundació i del contractista mantindran els contactes necessaris per assegurar la coordinació d'actuacions, la millora de servei i la atenció immediata de incidències del procés de servei.

Mensualment, el contractista remetrà al Gestor del Servei de la Fundació un reporting mensual del nombre d'incidències, temps mig de resolució i compliments d'SLA.

Trimestralment o a petició d'una de les parts es faran reunions de seguiment, presencials o virtuals, per analitzar situació, tendències i propostes de millora.

6.5.5 Devolució del servei

L'adjudicatari es compromet un cop acabi la prestació del servei a facilitar la transició a nous proveïdors, facilitant tota la informació necessària, realitzant les tasques necessàries en els terminis necessaris, mantenint els nivells de servei fins al darrer moment de la prestació del servei, i sense dificultar de cap manera el procés de canvi.

Així mateix la Fundació es reserva el dret a, un cop finalitzat el termini del servei, a exigir la retirada dels equips i/o cablejats utilitzats en la prestació del servei sense considerar cap contraprestació, dret adquirit, reclamació o indemnització.

7. Certificacions

A l'objecte d'assegurar la conformitat de l'empresa adjudicatària amb determinades normes de qualitat directament relacionades amb el servei demandat, i garantir la capacitat tècnica de la mateixa en relació amb la infraestructura actual instal·lada a la Fundació i la proposta en la seva oferta, l'empresa licitadora ha de disposar i acreditar les següents certificacions:

7.1 Sistemes de gestió

El licitador ha d'estar en possessió de alguna de la següent certificació:

- ENS
- UNE-EN ISO 9001
- Certificació ISO-20.000 (Gestió de serveis) (o equivalent)
- Certificació ISO-27.000 (Seguretat de la informació) (o equivalent)

7.2 Partnership amb fabricants

El licitador ha d'estar en possessió de la certificació Fortinet Expert Partner.

7.3 Nombre de tècnics amb certificacions

El licitador ha de disposar de tècnics amb la certificació Fortinet NSE 7 (Network Security Architect o superior).

8. Annexes

8.1 Annex 1. Inventari equipament a adquirir

Marca	Model	Unitats
Fortinet	Fortigate 401F	2
Fortinet	Fortigate 121G	1
Fortinet	FS-124G	2
Fortinet	FS-148F-POE)	1

8.2 Annex 2. Inventari equipament a renovar garanties

Marca	Model	Unitats
Fortinet	FortiSwitch 548D-FPOE	2
Fortinet	FortiSwitch 448E-FPOE	31
Fortinet	FortiSwitch 424E-FPOE	20
Fortinet	FortiSwitch 108F-FPOE	10
Fortinet	FortiSwitch 1048E	2
Fortinet	FAP431F (Access Point)	4
Fortinet	FAP231F (Access Point)	78
Fortinet	FAP231K (Access Point)	5