Ajuntament de Barcelona

Institut de Cultura

Palau de la Virreina
La Rambla, 99
08002 Barcelona
Telèfon 933 161 000
www.bcn.cat/barcelonacultura

PLEC DE PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE SUBMINISTRAMENT D'EQUIPAMENT DE LA SALA TÈCNICA, INSTAL•LACIÓ I GESTIÓ DE LLICÈNCIES I GARANTIES A L'INSTITUT DE CULTURA DE BARCELONA.

INDEX

1. PRESTACIONS OBJECTE DEL CONTRACTE

En el present apartat es mostren les característiques tècniques requerides per l'execució del present contracte.

Les prestacions del present contracte són:

- Subministrament d'equipament de la Sala Tècnica per substitució per obsolescència
- Instal·lació a les seus de l'Institut de Cultura de Barcelona
- Migració i posada en marxa dels equips a les instal·lacions de l'ICUB designades
- Gestió de les llicències i garanties dels equips detallats

2. ESPECIFICACIONS TÈCNIQUES

2.1 Subministrament - Especificacions Tècniques

L'equipament presentat pel contractista haurà de complir amb els requisits tècnics especificats a continuació, o en tot cas, oferir una configuració alternativa superior pera cada una de les tipologies. Aquests requisits tècnics també consideren la necessitat d'una òptima compatibilitat amb l'equipament actual per garantir una correcta migració de les dades i configuració, així com una integració adequada amb la resta d'equipaments que no són objecte de renovació d'aquest contracte.

La contractista haurà de garantir el subministrament de peces dels equips per a tot el període de garantia obert.

Els equips a subministrar hauran de ser nous. En cap cas s'acceptaran equips remanufacturats o recondicionats.

Els equips sol·licitats son els següents:

A. Emmagatzematge per a l'entorn de còpia de seguretat remot
B. Equips sol·licitats com a switches de perímetre
C. Equips sol·licitats com a tallafocs de perímetre

Les especificacions tècniques que han de complir són:

A. Equip sol·licitat com a emmagatzematge per a l'entorn de còpia de seguretat remot:

Se sol·licita un nou sistema per substituir l'actual equip que s'utilitza com a destinació de còpia de seguretat remot: NetApp model FAS2720A. Aquest equip està a les dependències del Disseny Hub Barcelona (D-HUB) i té actualment com a objectiu rebre rèpliques de les dades contingudes al CPD Principal del Palau de la Virreina. Aquesta replicació entre CPDs és nativa entre les cabines d'emmagatzematge d'origen i el FAS2720A de destinació, per tant permeten replicar dades entre cabines d'emmagatzematge sense l'obligació de disposar d'equips intermedis. El nou equip ha de permetre mantenir aquesta replicació per disseny, com detallarem més endavant.

Aquest nou sistema d'emmagatzematge demanat ha de disposar a més d'una sèrie de característiques tècniques que es detallen a continuació. En qualsevol cas, no s'ha de perdre cap de les funcionalitats actualment prestades per l'equip NetApp FAS2720A al D-HUB.

Les característiques i funcionalitats del nou equip que vindria a substituir el FAS2720A han de ser les següents, i es prenen com a requisits mínims obligatoris:

- **[Requisit 1] Alta disponibilitat**. Ha de disposar de doble controladora, amb redundància i intercanvi en calent i failover automàtic entre controladores. A més, l'equip no ha d'incloure cap punt de fallada intern (SPOF) per disseny (controladores, fonts d'alimentació, etc.)
- **[R2] Substitució d'elements en calent.** Fonts d'alimentació, ventiladors i controladores han de ser reemplaçables en calent i sense parada de servei, ni tan sols s'admeten micro-talls de servei en cas de fallada.
- **[R3] Actualitzacions sense interrupció.** L'equip no ha de requerir parada ni tall de servei en cas d'actualització del sistema (el seu firmware). Tampoc ha d'existir un tall de servei en cas de commutació entre controladores, sigui planificada o no aquesta commutació, ni en cas d'actualització de totes dues controladores.
- **[R4] Memòria integrada.** Ha d'incloure diferents tipus de memòria:
  - 128GB de memòria RAM amb un repartiment de 64GB per controladora, com a memòria del sistema.
  - 2TB de memòria NVMe amb un repartiment d'1TB per controladora per a memòria cau de discos. Aquesta memòria cau per tant ha d'actuar com un accelerador de les transaccions contra discos rotacionals i ha de ser dedicada a aquest fi. La memòria cau ha de ser automàtica.
- **[R5] Persistència de memòria.** Ha d'incloure mecanismes de protecció de les dades en trànsit als discos, fins i tot en cas de fallada total d'energia (persistent write log over Flash o similar).
- **[R6] Protocols d'accés**. L'equip ha d'incloure accés a tots els protocols de servei SAN i NAS següents sense cap tipus de gateway intermedi: FC, FCoE, iSCSI, NFS, pNFS i CIFS/SMB. Encara que només es sol·liciten interfícies Ethernet, però s'ha de suportar protocols FC.
- **[R7] Escalabilitat vertical (scale-in).** L'equip ha de ser capaç de créixer fins a 144 discos de diferents capacitats i tecnologies, dotant de flexibilitat a futur en cas de requerir augmentar la capacitat de l'equip i/o prestar nous serveis.
- **[R8] Escalabilitat horitzontal (scale-out).** Pel que fa a l'escalabilitat horitzontal, l'equip ha de suportar la seva ampliació mitjançant l'addició de noves controladores (fins i tot de diferents models) fins a un màxim de vint-i-quatre (24) controladores en servei NAS i dotze (12) controladores en servei SAN. Aquesta escalabilitat horitzontal ha d'estar suportada de forma integrada també amb l'equipament actual FAS2720A, de manera que existeixi la possibilitat de formar un clúster entre les dues controladores del FAS2720A i les dues controladores del nou equip.
- **[R9] Connectivitat.** L'equip ha d'incloure, entre les dues controladores:
  - 8 ports de servei 1/10 GbE
  - 2 ports 1GbE de gestió dedicats (2 ports per controladora)
  - 2 ports Serial RJ45 (2 ports per controladora)
  - Si existeix la necessitat d'utilitzar ports de clúster entre ambdues controladores, han de ser diferents dels ports de servei, és a dir, no han de consumir ports de servei.
- **[R10] Capacitat.** L'equip ha d'incloure **12 discos de 4TB i tecnologia NL-SAS 7.2 Krpm.** Ha de permetre l'ampliació fins a almenys 144 discos de diferents capacitats (incloent-hi els 12 discos interns), així com discos HDD i SSD en el mateix sistema, mitjançant l'addició de safates de disc. L'addició de safates de disc, així com la seva eliminació/substitució, ha de poder fer-se en calent i sense parada de servei per disseny. La capacitat màxima bruta del sistema de doble controladora ha de ser superior als 2 PB.

- **[R11] Mida en rack.** L'equip, incloent-hi els primers 12 discos i les dues controladores, ha d'ocupar un màxim de 2 RU en armari rack estàndard.

Aquest nou equip que es sol•licita ha de comptar a més amb les següents funcionalitats de programari integrades, és a dir, sense necessitat de programari de tercers ni de maquinari addicional. Totes les funcionalitats han de ser aplicables independentment del protocol de dades que s'utilitzi (NAS, SAN):

- **[R12] Virtualització de l'emmagatzematge.** El nou equip ha de permetre crear instàncies lògiques d'emmagatzematge, és a dir, permetre disposar de diferents cabines de dades virtuals que s'executen en un mateix maquinari físic (les controladores). Cada una d'aquestes cabines virtuals ha de tenir la seva pròpia identitat de xarxa, integrar-se amb un AD diferent (si fos necessari) i ser a nivell lògic un sistema independent de la resta de cabines lògiques. Ha de permetre la creació d'almenys 512 cabines lògiques per cada parell de controladores.
- **[R13] Qualitat de servei.** El nou equip ha de permetre configurar diferents qualitats de servei (QoS) limitant el rendiment (en IOPS) així com l'ample de banda (en MBps) que està consumint un objecte: una LUN, un fitxer, un volum o una cabina de dades virtual completa. Ha de permetre la seva habilitació en temps real, així com modificar la configuració si fos necessari per poder adaptar-se a diferents requisits de les càrregues de treball al llarg del temps.
- **[R14] Protecció de discos.** Ha de disposar de nivells RAID de doble i triple paritat per a protecció del sistema, permetent un servei sense interrupció fins i tot en el cas d'una fallada de dos discos o fins i tot de tres discos (corresponents a doble paritat o triple paritat, respectivament). També ha de permetre discos de hot-spare amb recuperació automàtica en cas de fallada d'un disc de dades i/o de paritat.
- **[R15] Snapshot.** Ha de permetre realitzar fins a 255 snapshots per volum i sense penalitzar en el rendiment, suportant tant serveis NAS com SAN. El procés de creació d'un snapshot ha de ser instantani i independent de la mida de les dades (NAS, LUNs), ja que no s'ha de realitzar una còpia d'aquestes dades, sinó dels punters o representació lògica dels mateixos.
- **[R16] Recuperació de snapshots.** Ha de permetre recuperar informació des d'un snapshot a la pròpia cabina d'emmagatzematge sense haver de realitzar còpia de les dades des d'un equip extern, sense consumir temps i independentment de la mida de les dades a recuperar.
  S'ha de permetre accedir a més als usuaris als snapshots per recuperar un fitxer o una carpeta completa en cas de necessitat. L'accés ha de ser integrat amb l'explorador de fitxers de Windows. Aquest permís a usuaris ha de ser configurable a nivell de Directori Actiu, de manera que es pugui permetre als usuaris que es desitgi, per exemple, només a administradors.
- **[R17] Replicació.** L'equip ha de permetre replicar dades des de i cap a altres equips del mateix fabricant, així com contra el sistema existent NetApp FAS2720A. Aquesta replicació s'ha de realitzar utilitzant infraestructura de comunicacions IP, independentment que es tracti de models diferents d'equip (nou i l'existent FAS2720A).
  Aquesta replicació s'ha de realitzar per xarxa sense requerir elements intermedis, és a dir, aquesta rèplica ha de ser nativa i sense necessitat d'utilitzar programari de tercers (com per exemple un programari de còpia de seguretat), sense necessitat de servidors intermedis i per descomptat ha de ser compatible amb les funcionalitats d'eficiència incloses en el sistema (deduplicació) de manera que la rèplica no rehidrati les dades, sinó que les mantingui deduplicades entre ambdós sistemes, origen i destinació.

- **[R18] Tiering i replicació contra el núvol**. El nou equip ha de ser capaç de realitzar tiering (desbordament d'informació no utilitzada durant un període de temps) i replicació contra serveis de núvol públic.
  Aquesta funcionalitat és l'única que no s'ha d'ofertar, però ha de ser una característica que es pugui habilitar en el futur en l'equip proposat mitjançant l'adquisició únicament de llicències de programari i/o subscripcions. Ha de ser compatible almenys amb els serveis de disc en el núvol públic d'Amazon AWS, Microsoft Azure i Google Cloud.

- **[R19] Eficiència.** L'equip ha d'incloure les següents funcionalitats d'eliminació d'informació redundant, que han de ser compatibles entre si:
  - Deduplicació, que ha d'eliminar blocs redundants de disc per optimitzar l'espai d'emmagatzematge quedant-nos amb una única còpia de cada bloc de com a màxim 4K de mida.
  - Compressió, que ha de minimitzar la mida de cada objecte del sistema d'emmagatzematge, sent a més compatible amb la deduplicació.
- **[R20] Xifrat.** L'equip ha d'incloure la funcionalitat de xifrat, permetent el xifrat a nivell de volum per programari, integrat dins del seu propi programari embegut i sense necessitat d'elements externs (servidors, etc.). Aquesta funcionalitat ha de complir amb FIPS 140-2. Ha d'estar integrada amb les instruccions de xifrat dels processadors integrats en cada controladora per poder ser el més eficient possible en l'ús de recursos. Tampoc ha de requerir un gestor de claus extern per al seu funcionament.
- **[R21] Suport automàtic.** L'equip ha d'incloure alguna funcionalitat "call-home", és a dir, ha de poder enviar alertes de seguretat, així com informes programats al suport del fabricant i a les adreces de correu electrònic que es configurin de forma proactiva. Aquesta funcionalitat també ha d'avisar quan un element de l'equip falli (un disc, una font d'alimentació, una controladora, etc.) de forma automàtica per part de l'equip, facilitant les tasques de manteniment i suport en minimitzar el temps d'obertura d'una incidència.
- **[R22] Migració de dades.** Ha d'existir un mètode aprovat pel fabricant del nou equip, així com de l'existent (NetApp), per migrar les dades des de l'equip actualment instal•lat cap al nou equip que es proposi, de tal manera que:
  - Existeixi la possibilitat de migrar sense parada de servei de dades, ni tan sols micro-talls de servei contra la instal•lació existent, basada en una parella de controladores FAS2720.
  - Aquesta funcionalitat de migració sense parada ha de migrar tant les dades com la configuració de les cabines virtuals prèviament establertes en l'equip d'origen, de manera que sigui el menys disruptiva possible i es minimitzin les possibilitats d'error.

B. Equips sol·licitats com a tallafocs de perímetre

Es sol·licita una nova parella de tallafocs per substituir l'actual entorn de tallafocs que es té al CPD del Palau de la Virreina: dos Cisco ASA 5516-X configurats en actiu-pasiu.

Aquesta nova parella de tallafocs que es sol·licita ha de disposar d'una sèrie de característiques tècniques que detallem a continuació, configurables mitjançant polítiques de capa 7. Els requisits mínims obligatoris són els següents:

- **[R1] Alta disponibilitat.** Ha de tractar-se d'una parella de dos equips bessons, configurables en modalitat Actiu-Actiu i Actiu-Pasiu.

- **[R2] Fonts d'alimentació duals**. Els equips han de disposar de doble font d'alimentació redundant integrada.
- **[R3] Disc dur.** Cada tallafocs ha d'incloure almenys 480GB de capacitat bruta en un disc SSD per guardar arxius de registre i quarantena, internament a cada tallafocs.
- **[R4] Connectivitat.** Cada equip de la parella ha de disposar almenys de la següent connectivitat:
    - Vint-i-dos (22) ports 1GbE:
        - Dotze (12) ports 1GbE RJ45
        - Un (1) port 1GbE RJ45 de gestió
        - Dos (2) ports 1GbE RJ45 dedicats d'alta disponibilitat
        - Un (1) port 1GbE RJ45 DMZ dedicat
        - Quatre (4) slots 1GbE compatibles amb SFP
        - Dos (2) ports 1GbE RJ45 WAN
    - Dos (2) slots 10GbE compatibles amb SFP+
    - Un (1) port de consola
- **[R5] Mida en rack.** Cada tallafocs ha d'ocupar un màxim d'1 RU en armari rack estàndard, per un total de 2 RU.
- **[R6] Rendiment general de l'equip.** Cada equip ha de presentar el següent rendiment mínim:
    - IPS: 2,6 Gbps
    - Next Generation Firewall: 1,6 Gbps
    - Protecció contra amenaces: 1 Gbps
    - Ipsec VPN (AES256-SHA256): 11,5 Gbps
    - Control d'aplicacions (HTTP): 2,2 Gbps
    - Nombre d'usuaris concurrents via VPN-SSL: 500 mínim
    - Nombre de polítiques configurables: 10.000
    - Tallafocs IPv4 (1518 / 512 / 64 byte, UDP): 20 / 18 / 10 Gbps
        - Latència del tallafocs (64 bytes, UDP): inferior a 5 µs
        - Paquets per segon com a tallafocs: 15 Mpps
- **[R7] Integració amb WiFi.** L'entorn ha de ser capaç d'actuar com a controladora WiFi i gestionar fins a 128 punts d'accés. No es sol·licita aquesta característica al subministrament, ni antenes WiFi, però ha de ser una possibilitat d'ús futur.
- **[R8] Virtualització del servei.** Els nous equips han de permetre crear instàncies lògiques de tallafocs, és a dir, permetre disposar de diferents entorns de tallafocs segmentats entre si que s'executen en el mateix maquinari. Cada una d'aquestes instàncies ha de poder permetre assignació d'interfícies pròpies (físiques o lògiques/VLAN), disposar de la seva pròpia col·lecció d'objectes, polítiques de filtratge, taules d'encaminament i configuracions de VPN. Aquesta funcionalitat per tant ha de possibilitar una segmentació total dins del tallafocs, permetent un mínim de 10 instàncies lògiques de tallafocs en cada dispositiu.

A més de disposar de característiques de tallafocs, segmentació de xarxa i de securització de SD-WAN, l'equipament ofert ha d'incloure les següents funcionalitats de programari, activades i per tant usables en els equips:

- **[R9] Protecció Antimalware.** Aquesta funcionalitat ha de protegir contra la transmissió de codi maliciós, referit normalment com a malware (troians, virus, cucs, exploits de porta del darrere, spyware, etc.). Per a això ha d'incloure perfils de seguretat antivirus de forma integrada contra una varietat d'amenaces, incloent-hi codis coneguts o desconeguts (malware) però també APTS (Advanced Persistent Threats).

S'ha de poder configurar que el tallafocs apliqui la protecció antivirus a les sessions HTTP, FTP, IMAP, POP3, SMTP, NNTP, HTTPS, IMAPS, POP3S, SMTPS, i FTPS. El motor d'escaneig antimalware ha d'utilitzar una base de dades de signatures de virus (signature database) en la qual es detallin els atributs únics de cada infecció. L'escàner d'antimalware ha de buscar en aquestes signatures i si localitza un patró a la xarxa, el tallafocs ha de determinar que el fitxer està infectat i prendre l'acció configurada en la seva política (per exemple, impedir la descàrrega, bloquejar la sessió, etc.). Les tècniques que ha d'utilitzar aquest motor d'antimalware han de ser: escaneig de virus, protecció grayware, escaneig heurístic, protecció de connexió a botnets conegudes i a llocs que incloguin phishing. L'actualització de la base de dades on es connecti el tallafocs per obtenir informació de noves amenaces ha de ser automàtica (descàrrega i instal·lació) i freqüent (diària). Aquesta base de dades l'ha de facilitar el fabricant dels equips de forma globalment distribuïda, garantint que el servei d'actualitzacions no es vegi interromput i que els tallafocs sempre tinguin accés a l'última definició d'amenaces.

- **[R10] Filtrat Web.** Aquesta funcionalitat ha de permetre protegir de URLs i continguts web no apropiats. Els filtres almenys han de filtrar en base a URLs, categories, continguts, scripts web i escaneig antimalware.
    - El filtrat URL haurà de bloquejar o permetre URLs específiques afegint-les a una llista de filtrat. Per afegir les URLs s'han de poder utilitzar patrons de text, comodins o expressions regulars. Ha de permetre configurar llistes blanques i llistes negres. A més de permetre i bloquejar, ha de poder configurar monitorització i crear excepcions (per exemple, en el cas d'accedir a una Intranet). En cas de bloquejar l'accés a un usuari, ha de permetre mostrar-li un missatge per a la seva informació.
    - El filtrat de continguts ha de bloquejar l'accés a webs que continguin patrons determinats de contingut. Aquests patrons s'han de poder configurar específicament mitjançant paraules, frases, comodins i expressions regulars. Aquest filtrat ha de detectar scripts i codis maliciosos, així com bloquejar contingut web insegur, com ara Java Applets, Cookies i ActiveX. S'han de poder escollir categories a filtrar en base a bases de dades del fabricant que ja hagi pre-categoritzat contingut web.
- **[R11] Control d'aplicacions.** Ha de determinar quines aplicacions poden operar a la xarxa en funció de polítiques, i restringir l'ús d'aquestes aplicacions segons es configuri en les polítiques de seguretat. Permetrà per tant que l'entorn de tallafocs detecti i prengui decisions sobre el trànsit de la xarxa en funció de l'aplicació que l'hagi generat. Ha de, a més, detectar les aplicacions, encara que aquest trànsit no utilitzi els ports i els protocols estàndard d'aquesta aplicació.
  Ha de disposar d'un catàleg d'aplicacions pre-identificades per part del fabricant, així com els serveis i protocols que aquestes utilitzin, de manera que sigui fàcil per al tallafocs detectar les aplicacions d'ús més comú i poder aplicar la política que es configuri. Aquest catàleg ha de disposar d'un coneixement d'almenys 2000 aplicacions d'antuvi, i ha de ser actualitzat pel fabricant sense necessitat d'intervenció de l'administrador del tallafocs. Per tant, ha de ser un servei en núvol actualitzat per part del fabricant dels tallafocs.
  Aquesta base de dades ha de facilitar informació útil sobre les aplicacions que permeti prendre decisions de configuració (almenys: permetre, denegar, monitoritzar i posar en quarantena) de manera senzilla. Per tant, ha de facilitar almenys la següent informació sobre cada aplicació:
    - Nom de l'aplicació

  - Categoria (Business, Botnet, Collaboration, Audio/Video, etc.)
  - Tecnologia (Browser, Client to Server, P2P, etc.)
  - Popularitat, mitjançant una puntuació comparable amb la resta de les aplicacions
  - Risc que suposa (si es tracta d'un malware, si pertany a una xarxa botnet, si consumeix un ample de banda alt, etc.)
- **[R12] Prevenció d'intrusions (IPS).** El nou entorn de tallafocs ha de, a més, protegir la xarxa d'activitats o comportaments que concorden amb tècniques d'intrusió a la xarxa. El tallafocs per tant ha de ser capaç de detectar aquestes tècniques i prevenir el seu èxit (bloquejar la intrusió).
  La detecció s'ha de realitzar tant mitjançant signatures com mitjançant anomalies. Aquesta funcionalitat IPS ha d'incloure per tant descodificadors de protocol que analitzin el trànsit per protocol, podent comparar amb les signatures d'aquest protocol concret i facilitant l'eficiència en l'ús de recursos de la màquina. L'aplicació de protecció IPS s'ha de poder configurar de diverses formes:
  - Mitjançant identificació basada en patrons (Pattern-Based), seleccionant els atributs associats amb el tipus d'atac: aplicació afectada per l'atac, sistema operatiu, protocol (utilitzat com a vector d'atac), Severitat (nivell d'amenaça) i objectiu (target).
  - Mitjançant identificació basada en puntuació (Rate-Based). A la base de dades de signatures IPS, han d'existir unes signatures per defecte amb l'acció associada.
  - Configurades a mà, mitjançant especificació manual que puguin requerir els administradors.

  Les accions que s'han de poder configurar quan es detecta una concordança amb una signatura IPS, és a dir, un intent d'intrusió a la xarxa, han de ser:
  - Permetre (permet el trànsit)
  - Monitoritzar (permet el trànsit i registra l'activitat d'aquest)
  - Bloquejar (descarta el trànsit)
  - Reiniciar (tanca la sessió que va originar el trànsit)
  - Quarantena (rebutja el trànsit d'aquesta IP origen durant un temps. Aquest temps ha de ser configurable)

  Aquest servei s'ha de poder mantenir actualitzat (noves signatures IPS, etc.) mitjançant un servei d'actualització automàtic i desatès prestat pel fabricant.

C. Equips sol·licitats com a switches de perímetre

Es sol·licita una nova parella de *switches* per substituir l'actual entorn de *switches* que es té al CPD del Palau de la Virreina: dos Cisco WS-C2960 24-TS-S.

Els equips nous que s'ofereixin han de complir els següents requisits:

- **[R1].** Cada equip ha d'oferir 24 ports Ethernet RJ-45 que suportin velocitats 10/100/1000 i 4 ports 1G SFP.
- **[R2].** Tots els ports RJ-45 han de suportar PoE+, sent l'equip capaç de lliurar una potència per a PoE de 370W.
- **[R3].** Els equips han de suportar afegir en el futur un mòdul de stack dedicat. La possibilitat de fer stack entre els dos *switches* ha de ser amb un port dedicat en els equips, no mitjançant la utilització dels ports d'uplink o downlink per a la realització de l'stack.
- **[R4].** L'equip ha d'incloure una font d'alimentació AC de 600 W.

- **[R5].** L'equip ha d'incloure la possibilitat d'afegir una font d'alimentació secundària.
- **[R6].** Han de disposar d'una capacitat de stack de fins a 80 Gbps, amb almenys 8 membres per cada stack.
- **[R7].** Nombre total d'adreces MAC d'almenys 16000.
- **[R8].** Nombre total de rutes IPv4 d'almenys 11000.
- **[R9].** Memòria DRAM de 2 GB.
- **[R10].** Memòria flash de 4 GB.
- **[R11].** Capacitat de commutació de fins a 136 Gbps.
- **[R12].** Capacitat de taxa de reenviament de paquets de fins a 101 Mpps.
- **[R13].** Suport de protocols de nivell 3: RIP, OSPF, stub, EIGRP.
- **[R14].** Suport d'automatització a través de NETCONF, RESTCONF, YANG, PnP Agent.
- **[R15].** Temps mitjà entre fallades (MTBF) de mínim 392210 hores.
- **[R16].** MACSec-128.
- **[R17].** Suport de Full Flexible NetFlow.

3. SERVEIS PROFESSIONALS - ESPECIFICACIONS

3.1 EQUIP PROFESSIONAL

Els licitadors o candidats han de comprometre's a dedicar a l'execució del contracte com a mínim, els mitjans personals i/o materials següents:

- Dues posicions tècniques amb una experiència mínima de 3 anys en tasques relacionades amb l'objecte del contracte en una organització de mida similar a l'Institut de Cultura de Barcelona atès que es considera el mínim requerit per assegurar la qualitat de la prestació d' aquest servei clau pels objectius de l'Institut de Cultura Barcelona.

- Una posició de gestió i coordinació del contracte amb titulació acadèmica en Llicenciatura en Informàtica que haurà d'acreditar una experiència mínima de 3 anys en funcions relacionades amb l'objecte del contracte en tasques de coordinació i gestió en una organització de mida similar a l'Institut de Cultura de Barcelona atès que la complexitat del servei requereixen un perfil amb prou experiència per coordinar i gestionar el servei.

3.2 SERVEIS PROFESSIONALS

Els serveis professionals requerits son els que es detalla a continuació.

Instal·lació, migració de dades i configuració dels nous equips

Al CPD del Disseny HUB (D-HUB), és necessari instal·lar el nou equipament, així com migrar les dades i configuració contingudes en el FAS2720A actualment instal·lat. S'han de realitzar per tant les següents tasques:

- Instal·lació física del nou equip, incloent-hi cablejat elèctric i de xarxa que sigui necessari, en col·laboració amb el personal d'IT de l'ICUB però també del D-HUB on s'allotjarà el nou equipament.
- Actualització del microcodi de l'equip a l'última versió.

- Migració de dades i configuració des de l'equip actual, sense pèrdua de servei (ni tan sols un micro-tall de servei) al nou equip, de manera que es continuïn prestant els serveis d'emmagatzematge a la xarxa que s'estaven utilitzant fins al moment, incloent-hi rèpliques des del CPD del Palau de la Virreina entre cabines d'emmagatzematge.
- Migrades les dades i la configuració al nou equip, s'ha de realitzar una documentació de la instal·lació (estat en què queda el nou equip i canals de suport) així com una formació d'1 jornada al personal que gestioni finalment aquest nou dispositiu, per assegurar que aquest personal és capaç de realitzar totes les tasques típiques del dia a dia en el nou equipament.

Al CPD del Palau de la Virreina, és necessari instal·lar el nou equipament, així com migrar les configuracions contingudes en els equips Cisco C2960 i tallafocs Cisco ASA 5516 actualment instal·lats. S'han de realitzar per tant les següents tasques:

- Instal·lació física del nou equipament, incloent-hi cablejat elèctric i de xarxa que sigui necessari en col·laboració amb el personal d'IT de l'ICUB.
- Actualització del microcodi dels equips a l'última versió.
- Migració de dades i configuració (VLANs, etc.) des dels *switches* actuals als nous, de manera que la xarxa mantingui tots els serveis actuals una vegada es presti el servei des dels nous com
- mutadors.
- Migració de dades i configuracions (objectes, regles, polítiques, etc.) des dels tallafocs actuals als nous, de manera que la xarxa mantingui tots els serveis actuals de seguretat perimetral i alta disponibilitat (redundància, etc.).
- Respecte de les funcionalitats de seguretat de què disposin els nous tallafocs però no els existents, serà necessari que es realitzi una presentació al personal que gestionarà els mateixos, de manera que:
    - El personal que finalment administri els tallafocs tingui clar el valor que aportarà aquesta funcionalitat a l'ICUB i com treure-li el màxim partit.
    - Es pugui establir quina política sobre aquesta funcionalitat es configurarà i per tant s'aplicarà a la xarxa.
    - El licitador tingui clar quina configuració ha de realitzar dins del conjunt de regles d'aquestes funcionalitats en els nous tallafocs.
- Migrats els serveis de xarxa i seguretat als nous equips, s'ha de realitzar una documentació de la instal·lació del tallafocs (estat en què queden els equips i canals de suport) i una formació d'1 jornada al personal que gestioni els mateixos, per assegurar que aquest personal és capaç de realitzar totes les tasques típiques del dia a dia en el nou equipament.

3.3 CERTIFICACIONS

Les certificacions ens permeten garantir que l'empresa compleix amb els estàndards de qualitat, seguretat i gestió ambiental requerits per l'administració pública en general i en particular amb l'objecte del contracte.

L'empresa haurà de disposar de les següents certificacions:

Certificació
ENS Mig (Esquema Nacional de Seguretat.)
ISO 27001: Sistema de gestió de la seguretat de la informació.

4. CONDICIONS GENERALS D'EXECUCIÓ

Llicències i garanties
Els equipaments oferts han d'incloure les llicències necessàries pel seu òptim funcionament amb un període mínim de 4 anys.
Tots els equips hauran de comptar amb una garantia de 4 anys en el lloc on estigui situat l'equip, i haurà d'incloure tots els costos relacionats amb la reparació: personal, desplaçament, components i qualsevol altra despesa no prevista.

Servei de suport reactiu
S'ha d'incloure el servei de suport reactiu durant els 4 anys de la vigència de la garantia amb un suport 8x5xNBD. Les garanties han d'incloure com a mínim la reparació i/o substitució de peces o components o equips que conformen el maquinari subministrat. Durant aquest termini, l'adjudicatari es compromet a reemplaçar o reparar tots aquells elements (mecànics, elèctrics i/o electrònics) de tots i cadascun dels equips, elements i unitats subministrades que presentin irregularitats en el seu funcionament, operació o execució imputables a defectes de fabricació o funcionament, en un termini màxim de 48 hores.
Serà responsabilitat de l'adjudicatari donar d'alta la garantia del fabricant de cada equip, en nom de l'òrgan de contractació. Aquesta alta s'haurà de fer efectiva en la data de recepció del subministrament.

Temps de resposta màxim del servei d'assistència tècnica:
El temps de resposta màxim des de la petició de l'ICUB fins a la recepció de la resposta serà de 8 hores laborables. El temps de resposta podrà ser millorat per l'oferta de les empreses.

Lliurament, instal·lació i posada en marxa
L'oferta ha d'incloure el serveis de lliurament a domicili que l'ICUB indiqui, que poden ser dues localitzacions diferents. Sempre a la ciutat de Barcelona. (El servei d'instal·lació està detallat a la Clàusula 3.2 d'aquest plec.)
L'adjudicatari ha d'estar en disposició de lliurar els equips, en un termini màxim de 45 dies naturals, a comptar des del dia següent a la data de formalització del contracte. Els equips han d'estar instal·lats i posats en marxa en el termini màxim de 30 dies naturals a comptar des del seu lliurament.
L'adjudicatari és farà càrrec de la retirada i correcta gestió de reciclatge del material d'embalatge de l'equipament subministrat i de la retirada dels equips vells. Els equips en bon estat es donaran gratuïtament a organitzacions sense ànim de lucre. En cas que l'equip no es pugui reutilitzar s'haurà de destinar a desballestament garantint en tot moment les normes de sostenibilitat ambiental. Aquest desballestament caldrà certificar-lo adequadament a requeriment de l'ICUB, mitjançant el lliurament de la documentació corresponent (fulls d'acceptació de gestors autoritzats o equivalent). Un cop s'hagi retirat l'equip, l'adjudicatari haurà de presentar l'informe de gestió corresponent, al qual adjuntarà els documents acreditatius de la gestió realitzada amb els equips vells (acords amb les ONG, fulls d'acceptació de gestors autoritzats...).
La retirada de l'equipament que hagi de realitzar l'adjudicatari s'executarà el mateix dia del lliurament, o excepcionalment el dia següent. El període de temps màxim per retirar l'equipament sortint serà de 5 dies laborables, a comptar des de la data del lliurament del nou equip.