PLEC DE CONDICIONS TÈCNIQUES PEL SUBMINISTRAMENT I INSTAL·LACIÓ DELS FIREWALLS PEL CENTRE D'ALT RENDIMENT

(EXPEDIENT NÚM. 2025/08)

Informat favorablement per l'Assessoria Jurídica del Departament d'Esports: 10.07.2025

Índex de continguts

Index

Informat favorablement per l'Assessoria Jurídica del Departament d'Esports: 10.07.2025

1 Presentació

Un talla focs o firewall és essencial per a qualsevol entitat, especialment quan hi ha menors que hi viuen, ja que protegeix la xarxa i les dades sensibles de l'organització contra amenaces cibernètiques. Els centres que acullen menors gestionen informació confidencial, com ara dades personals dels infants, informació mèdica i documents oficials, que poden ser objectiu d'atacs informàtics. Un firewall actua com una barrera de seguretat, filtrant el tràfic entrant i sortint de la xarxa, bloquejant l'accés no autoritzat i prevenint intrusions.

En un entorn amb menors, la seguretat de la xarxa és especialment crítica per garantir la protecció de la seva informació i evitar interrupcions en els serveis que reben. Un atac cibernètic podria causar danys importants, com la pèrdua de dades, la corrupció de sistemes o l'accés no autoritzat a informació sensible sobre els menors. A més, pot afectar la reputació del centre i provocar una pèrdua de confiança de les famílies i la comunitat.

Els firewalls també ajuden a complir amb les normatives i regulacions de protecció de dades, que sovint exigeixen mesures de seguretat específiques per a la gestió de la informació dels menors. Implementar un firewall permet al centre controlar l'accés a la seva xarxa, definir polítiques de seguretat i detectar activitats sospitoses, la qual cosa és fonamental per a la prevenció d'amenaces.

Actualment la xarxa de CAR disposa de 2 firewalls Palo Alto al Nus Central de Comunicacions ubicat a Sant Cugat del Vallès

Amb l'objectiu de mantenir la seguretat i redundància dels diferents serveis del CAR, cal mantenir al dia i actualitzar el sistema de tallafocs.

2 Àmbit de la contractació

L'objectiu d'aquest plec és la contractació de la instal·lació, configuració i posada en servei d'una nova parella de firewalls ubicats al Nus Central de Comunicacions que permeti implementar la redundància.

Per l'electrònica de seguretat es demana:
L'enginyeria de xarxa, el subministrament, la configuració i tota la instal·lació física de la nova parella de firewalls al Nus Central de Comunicacions substituint, en totes les seves funcions, la parella actual.

Entra dins l'abast d'aquesta licitació la optimització i migració de polítiques actuals, així com la resta de configuració dels equips, mantenint com a mínim totes les funcions actuals.

Integració d'aquests equipaments amb la xarxa actual. Això inclou la configuració d'equips de xarxa ja existents a CAR i les interfícies de xarxa i routing en els propis firewalls.

La integració dels equips ha de tenir en consideració els punts següents:

- Validació de noves versions dels equips.
- Actualització de versions de l'equipament existent si es requereix.
- Posada en servei.
- Proves de funcionament.
- Documentació d'acord amb els requeriments de CAR.

Garantia de 5 anys de tots els equips i per resolució d'incidències amb un temps de resposta de 8x5 NBD, a partir de la data d'acceptacions parcials per part de l'adjudicatari. Durant els 5 anys de garantia de l'adjudicatari, el suport del fabricant haurà d'estar inclòs per 5 anys.

El llicenciament haurà de ser Advanced Threat Prevention, Advanced WildFire, Advanced URL Filtering, Advanced DNS Security, Next-Generation CASB, IoT Security, GlobalProtect Gateway i Cortex XDR.

Queda inclòs en l'abast del projecte els transceiver o cables DAC dels firewalls i de l'electrònica de xarxa on s'hauran de connectar així com tots els fuetons necessaris.

3 Requisits tècnics

3.1 Especificacions tècniques del hardware del firewalls

La nova parella de firewalls proporcionarà la seguretat per els servidors que on s'instal·laran les aplicacions del telecomandament.

El maquinari de cada firewall ha de suportar com a mínim:

- 9.5 Gbps de rendiment de Next Generation Firewall (Entès com la combinació de les funcionalitats Firewall, Application Control i IPS).
- 6.2 Gbps de rendiment de Threat Prevention .
- 1,4 Milions de connexions concurrents.
- 5,6 Gbps de rendiment VPN IPsec mesurats amb transaccions HTTP de 64 KB i el registre activat
- Un mínim de 8 x 1G/10G SFP/SFP+
- Un mínim de 4 x 1G/2.5G/5G de BaseT de coure
- Font d'alimentació redundada.
- Port de consola en format RJ-45 o micro USB

3.2 Especificacions tècniques del software del firewalls

3.2.0 Gestió

- Consola d'administració unificada. Aquesta consola s'ha de proporcionar exclusivament a través d'un servei web. En cap cas pot ser un client basat en Java.

3.2.1 Pla accés/seguretat

- Identifica i categoritza totes les aplicacions, en tots els ports, tot el temps, amb inspecció completa de capa 7.
- Identifica les aplicacions que travessen la teva xarxa independentment del port, protocol, tècniques d'evasió o xifratge (SSL/TLS). A més, descobreix automàticament i controla noves aplicacions per seguir el ritme de l'explosió SaaS amb la subscripció de seguretat SaaS.
- Utilitza l'aplicació, no el port, com a base per a totes les teves decisions de política de seguretat: permetre, denegar, programar, inspeccionar i aplicar modelatge del tràfic.
- Ofereix la capacitat de crear etiquetes personalitzades per a aplicacions propietàries o sol·licitar el desenvolupament identificadors d'aplicació per a noves aplicacions.
- Identifica totes les dades de càrrega útil dins de l'aplicació (per exemple, fitxers i patrons de dades) per bloquejar fitxers maliciosos i frustrar intents d'exfiltració de dades.
- Genera informes d'ús d'aplicacions estàndard i personalitzats, inclosos informes de programari com a servei (SaaS) que proporcionen informació sobre tot el trànsit SaaS autoritzat i no autoritzat a la teva xarxa.

3.2.2 Protecció Malware Zero-day

- Anàlisi de fitxers en temps real per detectar amenaces desconegudes.
- Ús de tècniques de sandboxing avançades per identificar malware, exploits i amenaces zero-day.
- Identificació de malware que utilitza tècniques d'evasió complexes.
- Emmagatzematge global de la informació de les amenaces per millorar la detecció en futures anàlisis.
- Generació d'informes detallats sobre l'anàlisi de fitxers maliciosos.
- Integració amb les solucions de seguretat del fabricant per aplicar protecció automàtica a tota la xarxa.
- Actualitzacions constants de les signatures de malware per protegir contra noves amenaces.
- Capacitat per analitzar una àmplia varietat de fitxers, inclosos executables, documents i fitxers comprimits.
- Integració i comunicació amb l'endpoint.

3.2.3 Routing

- Policy-based forwarding
- OSPFv2/v3 amb reinici suau (graceful restart), BGP amb reinici suau, RIP, enrutament estàtic.
- Modes NAT (IPv4): IP estàtica, IP dinàmica, IP dinàmica i port (traducció d'adreça de port), NAT64, NPTv6, Funcions addicionals de NAT: reserva d'IP dinàmica, sobrea-ssignació ajustable d'IP dinàmica i port.

3.2.4 Altres funcionalitats requerides

- Regles basades en usuaris corporatius (integració amb directori actiu).
- Inspecció de paquets a nivell de capa 7 (Regles per aplicació).
- Regles tradicionals basades en capa 4.
- Virtual wire (mode transparent, filtrat L3 en mode L2)
- Enviament de logs a Wazuh.

3.3 Requeriments tècnics per a un tallafoc segons l'Esquema Nacional de Seguretat (ENS)

En el marc de la licitació per a l'adquisició i desplegament d'un sistema de tallafocs, i amb l'objectiu de garantir el compliment de les disposicions del Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS), es detallen a continuació els requisits que ha de complir el dispositiu sol·licitat:

3.3.0 **Compliment normatiu**

- El tallafoc haurà d'estar homologat al Catàleg de Productes de Seguretat TIC del Centre Criptològic Nacional (CCN) en el marc de l'ENS en la categoria ALTA.

- Ha d'acreditar la seva conformitat amb les mesures de seguretat de les guies del CCN-STIC pertinents.

3.3.1 Control d'accés i segregació de xarxes

- Implementar polítiques estrictes de control d'accés basades en regles configurables i dinàmiques.
- Suport per a la segmentació de xarxes mitjançant VLANs, VPNs o altres tecnologies que assegurin la separació de fluxos d'informació (mp.com.4).
- Capacitat per a gestionar múltiples zones de seguretat amb polítiques diferenciades.

3.3.2 Protecció del perímetre (mp.com.1)

- Possibilitat de filtrar trànsit entrant i sortint, permetent només el trànsit autoritzat previ.
- Detecció i prevenció d'atacs externs, incloent-hi protecció contra intrusions (IPS/IDS).

3.3.3 Confidencialitat de les comunicacions (mp.com.2)

- Compatibilitat amb xarxes privades virtuals (VPN) que implementin protocols i algoritmes criptogràfics homologats pel CCN.
- Suport per a túnels IPsec i TLS per a nivells de seguretat mitjà i alt.

3.3.4 Integritat i autenticitat (mp.com.3)

- Validació de la identitat de l'origen i el destí de les comunicacions abans d'establir una connexió.
- Habilitats per detectar intents d'atacs actius i notificar incidents segons les polítiques definides.

3.3.5 Capacitat de gestió i auditoria

- Haurà d'incloure una interfície d'administració segura amb autenticació multifactor.
- Registre d'esdeveniments (logs) detallat, amb capacitat per exportar les dades en formats compatibles amb sistemes de gestió de seguretat (SIEM).
- Generació d'informes complerts que acreditin el compliment de l'ENS.

3.3.6 Altres requisits tècnics

- Escalabilitat per a adaptar-se a possibles ampliacions de la infraestructura de xarxa.
- Alta disponibilitat (HA) amb mecanismes de redundància per evitar interrupcions de servei.
- Capacitat d'actualització de programari per protegir-se contra noves amenaces.

3.3.7 Documentació requerida

- Certificat d'homologació emès pel CCN.
- Guia d'instal·lació, configuració i bones pràctiques conforme al nivell de seguretat requerit.
- Declaració del fabricant assegurant el suport tècnic i les actualitzacions durant un mínim de cinc anys.

3.4 Requeriments tècnics per a un antivirus o solució de protecció d'endpoint sincronitzat amb el tallafoc (compliment ENS)

Per garantir una protecció integral i alineada amb les disposicions del Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS), es detallen a continuació els requisits específics que ha de complir una solució antivirus o de protecció d'endpoint que estigui sincronitzada amb el tallafoc.

3.4.0 Compliment normatiu i homologació

- La solució ha d'estar homologada en el Catàleg de Productes de Seguretat TIC del Centre Criptològic Nacional (CCN) en el marc de l'ENS en la categoria MEDIA.
- Acreditació de la seva conformitat amb les guies CCN-STIC relacionades amb la protecció d'endpoint i integració amb tallafocs.

3.4.1 Protecció avançada contra amenaces

- **Detecció en temps real de programari maliciós** (malware), incloent-hi ransomware, troians i altres tipus d'amenaces avançades.
- Anàlisi heurístic i basat en signatures, amb suport per a mecanismes de detecció d'amenaces persistents avançades (APT).
- Capacitat de sandboxing per a l'anàlisi segura d'arxius sospitosos.

3.4.2 Integració amb el tallafoc

- Sincronització automàtica amb el tallafoc per compartir dades sobre esdeveniments de seguretat en temps real.
- Implementació de polítiques conjuntes per bloquejar amenaces detectades als endpoints en el trànsit de xarxa.
- Compatibilitat amb protocols de comunicació estàndard per a integració, com ara syslog, API REST o altres especificats pel fabricant del tallafoc.

3.4.3 Gestió i monitoratge centralitzat

- Consola unificada per a la gestió tant del tallafoc com de la protecció d'endpoint.
- Capacitat de desplegament i gestió remota de les solucions d'endpoint, incloent-hi la configuració i aplicació de polítiques.
- Generació d'informes d'activitat i incidents, compatibles amb solucions SIEM i alineats amb els requisits de l'ENS.

3.4.4 Protecció de la integritat i la confidencialitat

- Capacitat per a prevenir la manipulació de dades sensibles a través de l'aplicació de polítiques de seguretat.
- Mecanismes per al control i bloqueig d'execució de processos no autoritzats als endpoints.

3.4.5 Característiques avançades

- **Resposta automàtica davant d'incidents:** Possibilitat d'aïllar automàticament els endpoints compromesos per evitar la propagació de l'amenaça.
- **Suport per a sistemes operatius múltiples:** Compatibilitat amb entorns Windows, macOS i Linux, així com dispositius mòbils (Android i iOS).
- **Protecció offline:** Capacitat per mantenir els nivells de protecció en absència de connexió a la xarxa o al servidor central.

3.4.6 Registre i traçabilitat

- Registre complet de les accions i esdeveniments de seguretat, amb opcions per a auditories detallades.
- Traçabilitat de les amenaces detectades, amb identificació de l'origen i accions aplicades.

3.4.7 Altres requeriments operatius

- Mecanismes d'actualització automàtica i contínua de bases de dades de signatures i motor d'anàlisi.
- Garantia de compatibilitat amb polítiques de segmentació de xarxa implementades pel tallafoc.
- Alta disponibilitat i capacitat per operar en escenaris de gran escala amb mínim impacte en el rendiment dels endpoints.

3.4.8 Documentació requerida

- Certificació d'homologació CCN per a la solució antivirus o endpoint.
- Documentació tècnica que detalli la integració amb el tallafoc especificat.
- Guia de configuració conforme als requisits de seguretat del nivell alt de l'ENS.

Aquestes especificacions asseguren que la protecció d'endpoint no només compleixi amb els estàndards de seguretat establerts, sinó que treballi de manera coherent amb el tallafoc per oferir una defensa integral i adaptada a les necessitats de la infraestructura.

3.5 Justificació fabricant

Per a una entitat com el CAR, l'elecció dels firewalls de Palo Alto no només representa una decisió tècnica, sinó també una decisió estratègica que optimitza recursos, minimitza riscos legals i operatius i assegura un compliment normatiu rigorós. Aquesta

elecció afavoreix l'estabilitat, eficiència i sostenibilitat de la infraestructura tecnològica pública.

3.5.0 Optimització dels recursos humans existents

El personal encarregat de la gestió i configuració dels firewalls ja està format i té experiència amb els dispositius de Palo Alto. Això redueix la necessitat de formacions addicionals, minimitza la corba d'aprenentatge i garanteix una administració més eficient des del primer moment.

3.5.1 Reducció de costos operatius i de manteniment

L'ús continuat d'una marca ja coneguda evita inversions addicionals en formació, consultories externes i adaptació de processos interns. Això es tradueix en un estalvi econòmic directe i en una gestió més àgil i eficaç dels recursos públics.

3.5.2 Garantia de continuïtat operativa i seguretat jurídica

Mantindre's amb una tecnologia coneguda redueix el risc d'errors operatius i de problemes de seguretat que podrien derivar en responsabilitats legals. Aquesta estabilitat és fonamental per assegurar el compliment normatiu i la protecció de dades en una entitat pública.

3.5.3 Compatibilitat amb infraestructures ja existents

Els sistemes Palo Alto ja estan integrats amb la infraestructura tecnològica actual de l'empresa. Això garanteix una interoperabilitat sense complicacions, evitant riscos derivats de problemes d'integració amb altres tecnologies.

3.5.4 Fiabilitat i reputació reconeguda internacionalment

Palo Alto és una marca de referència a escala mundial en l'àmbit de la ciberseguretat. La seva reputació i solvència ofereixen una garantia addicional que els dispositius adquirits compleixen amb els estàndards més alts de qualitat, fet que redueix riscos legals i reputacionals per a l'organització.

3.5.5 Compliment normatiu i adequació a la regulació pública

Els productes de Palo Alto compleixen amb normatives internacionals de seguretat i privacitat, aspecte fonamental per a qualsevol administració pública. En particular, els dispositius Palo Alto compleixen amb el **Nivell Alt de l'Esquema Nacional de Seguretat (ENS)**, un requisit clau per garantir la protecció adequada dels sistemes d'informació en l'àmbit públic espanyol. Aquest compliment assegura que no es vulnerin lleis sobre protecció de dades o ciberseguretat, aspecte crític per a entitats públiques.

3.5.6 Estandardització i simplificació dels processos interns

L'ús d'una única tecnologia facilita la creació de protocols unificats, simplifica els processos de manteniment i garanteix un entorn de seguretat més robust. Aquesta uniformitat també facilita futures auditories i controls interns, aspectes essencials en el sector públic.

3.5.7 Reducció del risc operatiu

El canvi a una nova tecnologia comporta riscos associats a la migració de dades, adaptació del personal i compatibilitat amb altres sistemes. Optar per Palo Alto elimina aquests riscos, assegurant una continuïtat del servei essencial per al bon funcionament de l'empresa pública.

3.5.8 Assistència tècnica eficient i de qualitat

Palo Alto disposa d'una xarxa consolidada d'assistència tècnica, garantint respostes ràpides i efectives en cas d'incidències. Aquesta capacitat de resposta és fonamental per minimitzar interrupcions en els serveis públics, que podrien derivar en perjudicis per a la ciutadania.

3.5.9 Sostenibilitat de la inversió a llarg termini

La compra de tecnologia coneguda i consolidada assegura una inversió sostenible. Els dispositius Palo Alto tenen una llarga vida útil, amb actualitzacions regulars i suport garantit, evitant inversions recurrents a curt termini.

Per aquests motius s'hauran d'oferir els següents equips del fabricant Palo Alto:

Descripció	Quantitat	Observacions
PA-1420	2	El llicenciament de cada firewall ha de ser per 5 anys
Suport anual amb fabricant 8x5 NBD per 5 anys	2	-
Suport anual amb l'adjudicatari 8x5 NBD per 5 anys	2	Suport amb l'empresa adjudicatària per a la resolució d'incidències des de la posada en producció de l'equipament
Advanced Threat Prevention, Advanced WildFire, Advanced URL Filtering, Advanced DNS Security, Next-Generation CASB, IoT Security	2	El llicenciament ha de ser per 5 anys
GlobalProtect Gateway Licence	2	El llicenciament ha de ser per 5 anys
Cortex XDR for endpoint	50	El llicenciament ha de ser per 5 anys
Serveis gestionats	20	Serveis professionals amb l'empresa adjudicatària per a la implementació del projecte i la posterior gestió dels equips

Tots aquests equips hauran d'incloure els fuetons necessaris per fer les connexions entre ells i els equips actuals.

És obligació dels licitadors revisar els amidaments per tal que s'ajustin al projecte detall. S'acceptaran modificacions en els models dels equips oferts, sempre i quan es justifiqui que el motiu de la modificació és degut a EndOfSale o EndOfLife.

La taula d'amidaments ha d'incloure tots els codis del hardware o serveis contractats a fabricant.

Respecte a la garantia, és imprescindible llistar el codi dels suports contractats al fabricant per cada un dels elements de la xarxa i per garantir un temps de resposta de 8x5 NBD.

4 Procediment d'instal·lació

4.1 Instal·lació d'equips

Els equips s'instal·laran en l'armari de comunicacions situats al NCC. No es pot fer cap instal·lació ni entrada de material sense la prèvia autorització del CAR.

El CAR indicarà la ubicació exacta dels equips i s'hauran de col·locar en el bastidor de xarxa i connectar correctament. Els equips hauran d'estar perfectament identificats mitjançant etiquetes.

Els equips s'instal·laran en mode alta-disponibilitat actiu-passiu.

Els equips nous substitueixen els antics, per tant s'haurà de dissenyar un pla de substitució amb l'interrupció mínima possible i s'haurà de configurar de manera que tots els serveis i regles actuals estiguin en els equips nous.

Els fuetons de fibra i cables de coure també hauran d'estar correctament identificats amb la nomenclatura que definirà CAR.

Per enllaços de menys de 10m es poden fer servir cables DAC.

Si son compatibles, es poden fer servir els fuetons i cables actualment en us

L'adjudicatari haurà de portar tot material que sigui necessari per la instal·lació: material necessari per instal·lar els equips, fuetons de fibra entubats, fuetons de coure, espirals de protecció de cables, etc.. . L'adjudicatari també haurà de realitzar les modificacions que siguin necessaris en els armaris de comunicacions, com talls de rejibands, redistribució d'equips, retirada de safates, entre altres.

Tots aquests materials i tasques es concretaran en la fase de replanteig. S'hauran de fer els replantejos necessaris per tal que les condicions d'instal·lacions quedin ben definides.

4.2 Planificació de la instal·lació

Abans de la instal·lació s'haurà de fer una planificació complerta indicant l'afectació, la durada de la instal·lació i les proves que es realitzaran. Sense aquesta planificació no es podrà autoritzar cap canvi.

L'adjudicatari no acopiarà cap material sense l'autorització de CAR.

4.3 Control de qualitat de la instal·lació

CAR revisarà totes les instal·lacions físiques per assegurar-se que la qualitat de la instal·lació és correcta.

4.4 Planificació de les proves amb serveis

Un cop feta la instal·lació i configuració s'hauran de fer proves de funcionament. Les proves i la posada en servei serà efectuada per l'adjudicatari amb la supervisió de CAR i l'adjudicatari haurà de garantir el bon funcionament de la xarxa i resoldre incidències en cas que es produeixin, en aquest sentit,. les proves hauran de ser exhaustives, i en cap cas no podran consistir en meres comprovacions de funcionament.

Abans de realitzar les proves serà necessari planificar-les i proporcionar un document amb el protocol de proves.

CAR no autoritzarà la realització d'aquestes proves sense aprovar prèviament el protocol.

Informat favorablement per l'Assessoria Jurídica del Departament d'Esports: 10.07.2025

5 Amidaments

En aquesta licitació s'executarà el disseny i instal·lació dels nous firewalls per el Nus Central de Comunicacions que serviran com a capa de seguretat principals per la xarxa del CAR.

Informat favorablement per l'Assessoria Jurídica del Departament d'Esports: 10.07.2025

6 Serveis a Oferir

6.1 Optimització de les regles actuals

Aquest plec inclou la optimització de la configuració dels equips en producció actuals per migrar-les al nou equipament. Aquesta optimització s'haurà de realitzar amb CAR abans de fer la migració.

Aquestes regles inclouen com a mínim: regles de filtrat, regles de NAT, configuració de VPN, etc.

Així mateix s'hauran de configurar en els equips els traps SNMP més rellevants per a la operació i que seran recollits per la consola de monitorització de CAR.

6.2 Instal·lació

Tot l'equipament que es subministri s'haurà d'instal·lar seguint les bones practiques del fabricant i la normativa d'instal·lació explicada en aquest plec.

6.3 Configuració

Tot l'equipament que es subministri s'haurà de configurar segons els requeriments establerts per CAR.

6.4 Proves

Un cop instal·lats els equips s'haurà d'executar el protocol de proves per validar el correcte funcionament de l'equipament. El protocol de proves definitiu es definirà en la fase de disseny.

6.5 Serveis gestionats

Mínim 20 hores anuals de serveis gestionats (configuracions, actualitzacions, etc.) acumulables si no es gasten.

6.6 Garantia i manteniment

Per l'equipament es requerirà 5 anys de garantia amb modalitat 8x5 NBD amb l'empresa adjudicatària i 5 anys de suport 8x5 NBD amb fabricant. L'empresa adjudicatària haurà de disposar el Help Desk propi, atenent en català.

6.7 Serveis de manteniment correctiu.

Serveis de manteniment correctiu durant la duració del contracte amb l'objectiu de restablir el funcionament del servei de qualsevol element inclòs en aquest contracte en cas de fallada. L'empresa adjudicatària haurà de disposar dels recursos necessaris per garantir aquest servei.

El manteniment correctiu serà efectuat en la seva totalitat pel personal de la empresa adjudicatària.

Per realitzar el manteniment correctiu es podrà realitzar un diagnòstic remot. Per fer-ho CAR habilitarà una connexió VPN per intercanviar informació i tenir accés restringit a l'equipament objecte del contracte. En el cas del manteniment correctiu es pretén que mitjançant l'accés remot es pugui diagnosticar amb més precisió la possible causa de la incidència. En cap cas, aquest servei eximirà de realitzar el manteniment correctiu in situ. Aquest servei només pretén facilitar i agilitzar les tasques de diagnòstic del manteniment correctiu.

L'empresa adjudicatària haurà d'establir amb els fabricants dels equips els contractes de suport adients per assegurar el suport tècnic de l'equipament objecte del manteniment.

6.8 Actualització de versions de programari.

Durant el projecte s'haurà d'incloure l'actualització de tots els elements instal·lats en aquest projecte.

Així mateix, durant el període de manteniment s'ha d'incloure la possibilitat d'actualització, sense cost, de totes les versions de software dels equips inclosos en aquest contracte durant la seva duració.

6.9 Help Desk

(assistència telefònica, correu electrònic, videoconferència).

L'empresa adjudicatària disposarà d'un servei de help-desk propi amb modalitat 8x5 NBD accessible telefònicament i amb correu electrònic com a mínim, que atendrà en català.

Aquest help-desk es podrà fer servir per les següents tasques:

- Notificació d'incidències i avaries.
- Suport a les funcionalitats existents o millores d'aquestes.
- Dubtes de la operativa diària dels equips inclosos a aquest contracte.

La notificació d'una incidència d'un sistema serà notificada generalment a través del Departament d'Informàtica del CAR, aquest proporcionarà un número d'incidència que es el que ha d'utilitzat l'empresa mantenidora per la notificació de les actuacions. Les intervencions realitzades per solucionar els problemes es documentaran d'acord amb el format proposat per l'adjudicatari i acceptat per CAR.

Personal de CAR establirà la severitat del problema i col·laborarà, juntament amb el personal de l'empresa adjudicatària, en la identificació i aïllament del problema i en les

seves accions correctives. S'haurà d'incloure una descripció de l'evolució de la incidència així com tot l'intercanvi d'informació (fitxers d'error, logs..) que es produeixin durant la resolució de la mateixa.

L'empresa adjudicatària serà la responsable del registre, manteniment i actualització del diari d'incidències durant el període de manteniment.

CAR podrà consultar en tot moment l'estat de la incidència, pel que l'empresa adjudicatària haurà de proposar un sistema de consulta "on line" de la informació.

Tota l'atenció a l'usuari, tant telefònica com escrita, haurà de ser en català.

6.10 Informes d'incidències i/o actuacions.

L'empresa adjudicatària haurà de portar a terme un seguiment de la qualitat del servei i presentarà al CAR un informe de forma periòdica del seguiment de les incidències i la resta d'actuacions realitzades.

En el cas d'una incidència s'haurà de proporcionar, com a mínim, la següent informació: Codi Identificador proporcionat pel departament d'operació de la incidència.

- Prioritat (greu, principal, secundaria).
- Dia i hora d'apertura.
- Dia i hora de tancament.
- Descripció de la incidència.
- Persona que comunica la incidència per part de CAR.
- Persona que atén la incidència per part de l'empresa adjudicatària.
- Elements substituïts i/o accions realitzades.

Es generarà un informe que haurà d'incloure:

- Nº total d'incidències ateses
- Nº incidències corresponents a cada sistema
- Temps de resolució empleat per incidència
- Altres activitats realitzades

Informat favorablement per l'Assessoria Jurídica del Departament d'Esports: 10.07.2025

7 Termini d'execució

El contracte tindrà una durada de 5 anys, sense possibilitat de pròrroga, que començarà a comptar a partir de la signatura del contracte.

En funció de les prestacions objecte del contracte, l'execució del subministrament i servei tindrà dos períodes:

- Un primer de subministrament de màxim 3 mesos de durada:
  - 1 mes de subministrament, configuració i instal·lació.
  - 2 mesos per integració amb el SIEM i sistema de monitorització.
- Un segon període de funcionament, des de la posada en marxa fins a un màxim de 4 anys i 9 mesos. Durant aquest període es mantindran al dia totes les llicències, funcionalitats i manteniment dels equips.

L'acta de recepció de la part del subministrament, configuració i instal·lació no es signarà fins que el sistema de tallafocs no estigui en funcionament, integrat en el SIEM i realitzades les proves.

8 Documentació a entregar

A la finalització de la instal·lació de l'equipament de xarxa s'haurà de lliurar la següent documentació:

- Documentació "AS BUILT". Ha d'incloure descripció de la ubicació i configuració de tots els equips així com un mapa global de tota la xarxa. També inclourà la definició dels serveis de la xarxa i l'adreçament IP definit.
- Diagrames de xarxa. Per tal de tenir la xarxa ben documentada serà necessari entregar, a més del mapa global de la xarxa, els següents diagrames:
  - Diagrama Físic: mostra tots els switchs, routers, connexions, etc. (ha d'incloure enllaços, grups, velocitats, ports, slots, tipus de xassís, software, MAC Address, ports bloquejats, enllaços principals, enllaços de backup...).
  - Diagrama Lògic: mostra les funcionalitats a nivell 3 (routers, VLANs i segments Ethernet). Adreces IP, subxarxes, capes d'accés, distribució i nucli i tota la informació de routing.
- La documentació es complementarà amb catàlegs de tot l'equipament instal·lat amb les seves característiques tècniques incloent codis i referències.
- Inventari detallat per introduir al sistema de gestió del CAR (Netbox) tot el material instal·lat amb la següent informació: equipament (nom, model, versió HW), número de sèrie, adreça IP, versió software, ports fonts d'alimentació, enllaços, etc.
- Procediments bàsics d'operació.

Seran propietat de CAR tots els documents elaborats para la instal·lació del present contracte.
Tota la documentació estarà escrita en català.

8.1 Informes de seguiment

Per tal de tenir un control exhaustiu de tota la instal·lació que s'està realitzant serà necessari la següent informació:

- Abans de començar la instal·lació serà necessari una planificació detallada de tota la instal·lació.
- Actes de seguiment periòdiques amb tot el que s'ha instal·lat durant aquest període. En aquestes actes s'ha de contemplar evolució de la instal·lació, incidències possibles que hi hagi pogut haver, fotos dels punts crítics d'instal·lació, així com tota aquella informació que el Contractista consideri oportuna. La periodicitat pot variar si CAR ho creu necessari i segons l'avanç del projecte.

A part d'aquesta documentació seran necessàries reunions periòdiques per fer el seguiment de l'avanç del projecte i analitzar problemes o futures actuacions. Aquestes reunions podran ser semestrals o o anuals segons cregui CAR. En aquestes reunions s'haurà de lliurar tota documentació dels mesos anteriors i la planificació al dia de la instal·lació indicant punts crítics per possibles de retards si s'escau.