Consorci Sanitari
Alt Penedès-Garraf

PLEC DE PRESCRIPCIONS TÈCNIQUES QUE REGIRAN LA CONTRACTACIÓ DEL SUBMINISTRAMENT, INSTAL·LACIÓ I MANTENIMENT DELS SISTEMES DE SEGURETAT PERIMETRAL, REGISTRE D'AUDITORIA DE CONNEXIONS, ZTNA I DOBLE FACTOR D'AUTENTICACIÓ PER AL CONSORCI SANITARI DE L'ALT PENEDÈS I GARRAF.

Expedient CSAPG OB 2026/03

Índex

1 Introducció

El Consorci Sanitari de l'Alt Penedès i Garraf (d'ara endavant, CSAPG) necessita dur a terme una actualització integral de la seva infraestructura de seguretat perimetral per adequar-la als requeriments actuals de protecció, rendiment, disponibilitat i eficiència operativa.

L'objectiu d'aquest contracte és assolir una millora substancial de la seguretat de la informació mitjançant la renovació i ampliació dels tallafocs, la seva implantació en tots els centres amb connexions externes, l'augment de la capacitat per als registres d'auditoria, l'actualització del suport del sistema ZTNA, la renovació i ampliació del sistema MFA, així com la contractació dels serveis d'implantació i de suport operacional necessaris per garantir el correcte funcionament de tots els elements de la solució.

2 Situació actual

Actualment, el CSAPG disposa de tres centres de processament de dades (d'ara endavant CPD), un a cadascun dels hospitals que formen part de l'entitat. Cada CPD té una infraestructura de tallafocs Fortinet en clúster, que actuen com tallafocs perimetrals i d'algunes xarxes internes. Existeix un altre centre amb connexió a l'exterior que actualment no disposa de tallafocs perimetral.

El CSAPG disposa d'una eina de recol·lecció de logs i reporting FortiAnalyzer FAZVM64, on els tallafocs envien els logs actualment. Aquesta eina es mantindrà, però caldrà ampliar el llicenciament per cobrir les necessitats creixents de registre d'auditoria.

A més, es disposa d'una solució ZTNA i gestió de clients VPN de Fortinet (FortiClient EMS), desplegada en 150 clients, i d'una solució de doble factor d'autenticació (FortiAuthenticator), amb 700 tokens FortiToken mobile llicenciats.

2.1 Seus i centres d'activitat del CSAPG

Els diferents centres d'activitat del CSAPG són:

Centre	Adreça
Hospital Comarcal de l'Alt Penedès (**HCAP**) **Seu Social**	Carrer de l'Espirall, 61 08720 Vilafranca del Penedès
Hospital Residència Sant Camil (**HRSC**)	Ronda Sant Camil s/n 08810 Sant Pere de Ribes
Hospital Sant Antoni Abat (**HSAA**)	Carrer Sant Josep 21-23 08800 Vilanova i la Geltrú
Centre de Rehabilitació (**CRHB**)	Rambla Exposició 87 08800 Vilanova i la Geltrú
ABS Vilanova III CAPI Baix-a-Mar (**CAPI**)	Plaça Boleranys, 5 08800 Vilanova i la Geltrú

3 Objecte del contracte

L'objecte del present contracte és dur a terme una actuació integral orientada a la millora substancial de la seguretat de la informació del CSAPG, mitjançant les següents prestacions:

- La renovació de l'equipament tallafocs de seguretat perimetral existent i del suport del fabricant corresponent, incloent-hi l'ampliació de la capacitat de processament i la millora de l'amplada de banda dels enllaços.
- La implantació d'equipament tallafocs en tots els centres que disposen de connexions externes.
- La renovació del suport i l'ampliació de la capacitat d'emmagatzematge del registre d'auditoria de les connexions.
- La renovació del suport del sistema ZTNA (Zero Trust Network Access).
- La renovació del suport i l'ampliació del sistema d'autenticació de doble factor.
- La contractació dels serveis d'implantació dels elements que integren la solució.
- La contractació d'un servei de suport per a l'operació i administració de tots els components.

NOTA IMPORTANT:

En el present Plec de Prescripcions Tècniques es fa referència a alguns aspectes que el licitador haurà d'incloure en la seva proposta, però no s'indica en quin sobre ho haurà d'incorporar.

El contingut de cada sobre ve detallat al Quadre de Característiques de la licitació, sent **imprescindible no incorporar informació d'un sobre determinat dins d'un altre sobre.** Així, tota aquella informació relativa a característiques, imports i millores que en el quadre de característiques s'indiqui que s'han d'incorporar en el sobre C (sobre que conté l'oferta quina valoració depèn de fórmules automàtiques) no es podran incorporar en cap altre sobre.

En cas que el licitador incorpori aquesta informació dins del sobre A (documentació administrativa) o dins del sobre B (documentació avaluable mitjançant judici de valor) **serà exclòs del procediment de licitació**.

4 Exclusivitat de fabricant

Per raons econòmiques i operatives, el CSAPG vol mantenir el producte actual del sistema ZTNA, FortiClient EMS, el qual requereix que l'equipament de seguretat perimetral sigui del fabricant Fortinet.

L'organització ha realitzat una inversió significativa en aquesta solució i disposa de nombrosos clients VPN instal·lats en els ordinadors dels treballadors que accedeixen remotament. L'adopció d'una plataforma d'un altre fabricant comportaria la necessitat d'adquirir un nou producte, substituir el sistema existent, reinstal·lar i reconfigurar tots els clients VPN i adaptar els processos associats, amb el consegüent increment de costos en temps, recursos tècnics i formació.

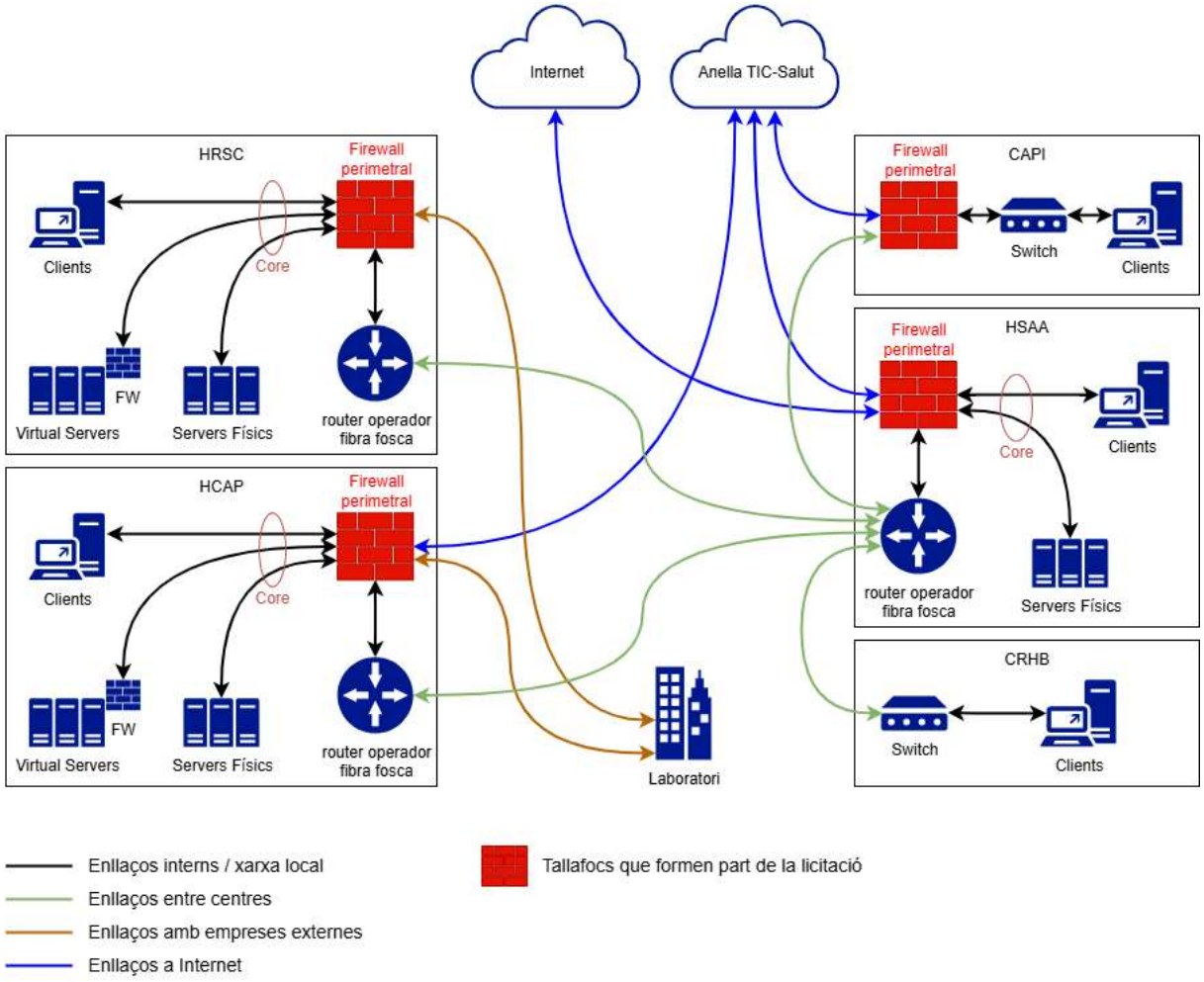
A més, el CSAPG també disposa d'un equip FortiAnalyzer en funcionament que també vol mantenir. Tot i que aquest sistema pot integrar-se amb solucions d'altres fabricants, només és possible obtenir-ne totes

les capacitats d'anàlisi avançada, correlació d'esdeveniments i monitoratge centralitzat amb tallafocs Fortinet.

Per aquests motius, els equips tallafocs requerits són del fabricant Fortinet.

5 Arquitectura de la solució

A nivell físic, la solució plantejada tindrà aquesta arquitectura:



Els nous equips tallafocs hauran de ser diferents, per ajustar-se als requeriments de cada centre. Concretament es contemplen 3 tipus d'equipament tallafoc diferent:

- Tipus A: equips de l'HSAA amb les connexió externes primàries a Internet i Anella TIC-Salut. Seran els equips amb major capacitat de processament i més ports de connexió.
- Tipus B: equips de l'HRSC i l'HCAP, amb capacitat de processament i connectivitat mitjanes. Es valorarà la millora d'aquests equips de manera que siguin iguals que els equips de l'HSAA.
- Tipus C: equips del CAPI, amb la menor capacitat de processament i connectivitat.

6 Requeriments tècnics

6.1 Requeriments generals per als equips tallafocs

Els equips tallafocs que caldrà incloure a la proposta han de complir amb els següents requeriments:

- En total es requereixen 8 equips tallafoc físics, dos per cadascun dels centres amb perímetre exterior. Cada parella es muntarà en clúster.
- Tots els equips han de ser nous i no poden tenir data de fi de cicle de vida (EOL) o suport (EOS), publicada a https://support.fortinet.com/support/#/lifecycle, inferior a 2032.
- Tots els equips, físics o virtuals, hauran de tenir suport de fabricant vigent mentre duri el contracte. Si un equip queda sense suport per part del fabricant de manera definitiva, l'adjudicatari es compromet a canviar-lo per un de característiques equivalents (pel que fa a rendiment, redundància, connectivitat i funcionalitat) sense cost per al CSAPG.
- Els equips tallafocs han de ser en format *appliance* físic del fabricant Fortinet, quedant exclosos màquines virtuals ni servidors de propòsit general. Han de poder ser instal·lats en un rack estàndard de 19" ocupant 1 RU com a màxim.
- Els dos equips físics de cada centre han de ser idèntics, redundats i en alta disponibilitat (HA). Han de permetre treballar en mode HA actiu-actiu i actiu-passiu.
- Els equips tindran doble font d'alimentació.
- Els equips tallafocs tindran hardware especialitzat de tipus ASIC per tal d'assegurar el rendiment requerit i garantir baixa latència.
- Els equips han d'incloure funcionalitats de control d'aplicacions, prevenció d'intrusions (IPS), protecció contra codi nociu, filtre web, filtres DNS, antispam, Data Loss Prevention (DLP), inspecció SSL/SSH, Web Application Firewall (WAF) i protecció antiDoS. Totes aquestes funcionalitats hauran d'estar llicenciades durant tota la vida del contracte.

6.2 Requeriments específics dels equips tallafocs

6.2.1 Tipus A

Els equips destinats a l'HSAA han de tenir com a mínim les característiques que es detallen a continuació.

Connectivitat

- 1 port de consola RJ45.
- 1 port de management *Out-of-Band* RJ45.
- 1 port HA (ports dedicats per establir el clúster HA).
- 1 port USB 3.0 per a la connexió de dispositiu d'emmagatzematge extraïble USB. El port USB ha de permetre la instal·lació desatesa del firmware i aplicació de configuració en el *boot* de l'equip.
- 8 ports 10GE SFP+.
- 20 ports 1GE (mínim 4 ports 1GE SFP, la resta RJ45).

Rendiment

- El tallafocs disposarà de com a mínim 39/39/26,5 Gbps d'amplada de banda de firewall per a paquets de 1518, 512 i 64 bytes UDP respectivament, en IPv4 i IPv6.
- El tallafocs ha de ser capaç de gestionar com a mínim 11 milions de sessions concurrents així com a mínim 400.000 noves sessions TCP per segon.
- El tallafocs ha de tenir una latència inferior a 5 µs (per paquets de 64 bytes UDP).
- Ha de tenir capacitat per com a mínim 10.000 polítiques de firewall.
- El rendiment per al tràfic SSL VPN ha de ser de com a mínim 3 Gbps i per tràfic IPSEC VPN (mesurat en paquets de 512 bytes) de 36 Gbps.
- A nivell 7, l'equip ha de proporcionar com a mínim el següent rendiment:
    - IPS: 9 Gbps.
    - NGFW: 7 Gbps.
    - Threat Protection: 6 Gbps.
    - Inspecció SSL amb IPS: 7 Gbps.
    - Control d'aplicacions: 27,8 Gbps (mesurat amb tràfic HTTP amb paquets de 64K).

6.2.2 Tipus B

Els equips destinats a l'HCAP i l'HRSC han de tenir **com a mínim** les característiques que es detallen a continuació.

Connectivitat

- 1 port de consola RJ45.
- 1 port de management *Out-of-Band* RJ45.
- 1 port HA (ports dedicats per establir el clúster HA).
- 1 port USB 3.0 per a la connexió de dispositiu d'emmagatzematge extraïble USB. El port USB ha de permetre la instal·lació desatesa del firmware i aplicació de configuració en el *boot* de l'equip.
- 4 ports 10GE SFP+ com a mínim.
- Com a mínim 20 ports 1GE (mínim 4 ports 1GE SFP, la resta RJ45).

Rendiment

- El tallafocs disposarà de com a mínim 39/39/25 Gbps d'amplada de banda de firewall per a paquets de 1518, 512 i 64 bytes UDP respectivament, en IPv4 i IPv6.
- El tallafocs ha de ser capaç de gestionar com a mínim 3 milions de sessions concurrents així com a mínim 140.000 noves sessions TCP per segon.
- El tallafocs ha de tenir una latència inferior a 5 µs (per paquets de 64 bytes UDP).
- Ha de tenir capacitat per com a mínim 10.000 polítiques de firewall.

- A nivell 7, l'equip ha de proporcionar com a mínim el següent rendiment:
    - IPS: 5,3 Gbps.
    - NGFW: 3,1 Gbps.
    - Threat Protection: 2,8 Gbps.
    - Inspecció SSL amb IPS: 3 Gbps.
    - Control d'aplicacions: 6,7 Gbps.

6.2.3 Tipus C

Els equips destinats al CAPI han de tenir com a mínim les característiques que es detallen a continuació.

Connectivitat

- 1 port de consola RJ45.
- 1 port USB 3.0 per a la connexió de dispositiu d'emmagatzematge extraïble USB. El port USB ha de permetre la instal·lació desatesa del firmware i aplicació de configuració en el *boot* de l'equip.
- 2 ports 10GE SFP+.
- 8 ports 1GE RJ45.

Rendiment

- El tallafocs disposarà de com a mínim 28/28/25 Gbps d'amplada de banda de firewall per a paquets de 1518, 512 i 64 bytes UDP respectivament, en IPv4 i IPv6.
- El tallafocs ha de ser capaç de gestionar com a mínim 3 milions de sessions concurrents així com a mínim 124.000 noves sessions TCP per segon.
- El tallafocs ha de tenir una latència inferior a 5 µs (per paquets de 64 bytes UDP).
- Ha de tenir capacitat per com a mínim 5.000 polítiques de firewall.
- A nivell 7, l'equip ha de proporcionar com a mínim el següent rendiment:
    - IPS: 4,5 Gbps.
    - NGFW: 2,5 Gbps.
    - Threat Protection: 2,2 Gbps.
    - Inspecció SSL amb IPS: 2,6 Gbps.
    - Control d'aplicacions: 6,7 Gbps.

6.3 Transceptors i cablejat

S'han d'incloure els següents transceptors i cables per a la interconnexió dels equips:

- 6 transceptors Fortinet FN-TRAN-SFP+LR de llarga distància SMF.

- 30 transceptors Fortinet FN-TRAN-SFP+SR de curta distància MMF.
- 20 transceptors HP J9150D o compatibles del fabricant FS.
- 28 cables de fibra del tipus i longitud adients per fer les connexions necessàries amb la xarxa intercentres i el Core de cada centre. La longitud i el tipus exacte de cada cable s'establirà durant la implantació.
- Cablejat adient per enllaçar els dos membres de cada clúster de tallafocs.

7 Programari

El programari que cal incloure en la proposta, a nivell de llicenciament, subscripcions i suport de fabricant, es detalla en els següents apartats.

7.1 Registre d'auditoria de connexions - FortiAnalyzer

- Ampliació de la llicència del FortiAnalyzer fins als 25GB/diaris.
- Renovació del suport en modalitat FortiCare Premium Support durant tota la vigència del contracte. El suport ha de tenir en compte l'ampliació de l'emmagatzematge diari.

7.2 ZTNA - FortiClient EMS

- Renovació dels 6 paquets de 25 llicències en model subscripció existents de FortiClient EMS durant tota la vigència del contracte.

7.3 Doble factor d'autenticació - FortiAuthenticator

- Ampliació del llicenciament d'usuaris existent amb 2 paquets de 1000 usuaris addicionals.
- 2000 unitats de FortiToken Mobile amb llicència perpètua.
- Renovació del suport de la màquina virtual en modalitat FortiCare Premium Support durant tota la vigència del contracte. La renovació del suport ha de tenir en compte l'ampliació del nombre d'usuaris.

8 Requeriments referents a la seguretat de la informació

Els requeriments pel que fa a la seguretat de la informació són:

- De conformitat amb l'article 2 del Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (en endavant ENS o RD 311/2022), els proveïdors que participin en el procés de contractació hauran d'estar en condicions de poder evidenciar la conformitat amb l'ENS dels sistemes d'informació en què es fonamentin els serveis objecte del contracte o que proporcionin solucions informàtiques. Es requerirà que l'empresa proveïdora, o la proposada com a tal, presenti el Certificat de Conformitat amb l'ENS en categoria ALTA abans de l'adjudicació.

L'empresa proveïdora haurà de mantenir la conformitat vigent durant tot el cicle de vida del contracte. La pèrdua o retirada temporal de la conformitat s'haurà de comunicar de manera immediata i sense dilació indeguda a l'entitat contractant, que haurà de valorar l'impacte en el contracte d'aquesta situació. La renovació de la conformitat durant la vigència del contracte s'haurà de notificar immediatament, incloent-hi el procés d'adaptació del sistema d'informació al Reial decret 311/2022.

Amb caràcter excepcional, i atenent a les circumstàncies de la contractació, considerant la proporcionalitat i la lliure concurrència, en equilibri amb la seguretat i el compliment de l'ENS, es podrà acceptar una declaració del responsable de seguretat de l'entitat participant, en què es comprometi a sotmetre el sistema d'informació a l'adequació a l'ENS en la categoria declarada en un termini de 6 mesos.

- L'accés a possibles components ubicats al núvol o a plataformes de gestió centralitzada instal·lades On-Premise haurà de comptar amb mecanismes d'autenticació robustos, incloent múltiples factors d'autenticació (MFA). Aquest sistema s'ha de poder integrar amb la solució MFA disponible al CSAPG, que actuarà com proveïdor d'identitats (IdP) mitjançant el protocol RADIUS per als components en local o els protocols SAML o OAuth per als components ubicats al núvol.
- Pel que fa a l'accés remot a qualsevol dels elements que formen part de la solució (plataformes de gestió incloses, ja sigui centralitzada o individual de cada dispositiu), l'ús de protocols considerats insegurs o obsolets no està permès. La configuració dels dispositius haurà de ser ajustada de manera que els protocols configurats compleixin les recomanacions de la "*Guía de Seguridad de las TIC CCN-STIC 807 – Criptología de empleo en el Esquema Nacional de Seguridad*".
- Els elements físics i lògics que formen part de la solució proposada han d'estar coberts per un servei de manteniment durant la vigència del contracte que inclogui:
    - L'aplicació d'actualitzacions de manera programada, per mantenir dits elements actualitzats. La periodicitat d'aquests cicles d'actualització serà trimestral en el cas de sistemes operatius i components base, si existissin, i anual en el cas del programari propi de la solució proposada i del firmware dels dispositius.
    - L'aplicació d'actualitzacions i pegats per resoldre vulnerabilitats publicades pel fabricant dels dispositius o del programari, en el termini màxim de 30 dies des de la publicació de la vulnerabilitat, sense límit pel que fa a la quantitat i sense cost addicional per al CSAPG.
- Les configuracions de tots els components que formen part de la solució han d'estar protegides per polítiques de còpia de seguretat automatitzades.
- El programari ha de complir amb el principi de mínim privilegi, de manera que els usuaris únicament puguin accedir als recursos imprescindibles per realitzar la seva funció, amb els privilegis indispensables.
- L'accés a l'administració i gestió d'usuaris del programari i a l'administració dels dispositius estarà limitat i només els usuaris administradors amb els privilegis corresponents hi podran accedir.
- Tant els elements físics com lògics que formen part de la solució han de tenir capacitat d'auditoria, permetent la traçabilitat de les accions dels usuaris i dels administradors.

- Tots els programes i sistemes hauran de ser configurats de manera que es compleixi amb l'ENS, preferentment durant la implantació inicial. Es podran implantar determinades mesures de protecció posteriorment a la implantació, però s'haurà de plantejar el desplegament inicial de la plataforma de manera que totes les mesures requerides per l'ENS siguin aplicables de manera senzilla sense haver de reinstal·lar components o fer canvis importants en l'arquitectura, en especial aquells que requereixin aturada de serveis.
- Seran d'aplicació les guies CCN STIC corresponents al programari i maquinari adquirit. Els documents i guies aplicables es poden trobar a https://www.ccn-cert.cni.es/guias/indice-de-guias.html.

9 Execució

9.1 Planificació

Les empreses licitadores podran visitar els centres del CSAPG per a comprovar aspectes concrets de les instal·lacions actuals i emplaçaments del futur equipament. L'objecte d'aquesta visites és conèixer l'estat actual de la infraestructura i planificar l'execució del projecte. Aquestes visites són opcionals i han de ser sol·licitades amb una antelació d'una setmana i tindran una durada màxima de 1 hora.

El CSAPG assignarà un Responsable de Projecte i un tècnic de sistemes per donar suport i supervisar les tasques que durà a terme el licitador. Ambdues figures poden estar representades per la mateixa persona. L'empresa licitadora establirà un únic interlocutor responsable del servei de manteniment que s'encarregarà de la resolució de les situacions no contemplades en aquest plec, conjuntament amb personal del CSAPG.

El tècnic o tècnics designats pel licitador estaran assignats exclusivament a realitzar, de forma transparent per al CSAPG, tot el procés d'instal·lació, migració i posada en producció de la solució. Aquests tècnics hauran d'estar en possessió de les certificacions adients en les tecnologies amb les que treballaran.

9.2 Desplegament, migració i instal·lació

A la seva oferta, el licitador presentarà un Pla de Migració on detallarà els passos a seguir per migrar tota la configuració de l'entorn actual al nou entorn. El Pla de Migració serà objecte de revisió exhaustiva per part del personal responsable del projecte del CSAPG i serà necessari el seu vist i plau abans d'iniciar-ne l'execució.

Aquest Pla de Migració cal que inclogui un cronograma detallat que especifiqui les fases en què es durà a terme l'objecte del contracte.

El licitador ha de garantir que el canvi a la nova infraestructura serà sense talls i transparent. En cas que sigui necessària l'aturada de serveis, l'empresa adjudicatària i el CSAPG acordaran el temps màxim i el procediment de canvi.

El CSAPG tindrà l'última decisió en quant als horaris per realitzar la migració, tenint en compte que aquests podran ser en qualsevol hora per tal de minimitzar l'impacte en l'organització.

L'adjudicatari s'encarregarà de desempaquetar tots els components i instal·lar-los físicament amb els seus propis mitjans. Realitzarà les connexions adients per a la coexistència entre la plataforma actual i l'ofertada, sense interrupció de servei.

Tots els elements de connexió hauran de ser etiquetats segons les indicacions del CSAPG per a que siguin fàcilment identificables visualment.

En la reunió final de projecte es lliurarà la documentació recollida que com a mínim inclourà:

- Decisions preses en la fase d'anàlisi i disseny.
- Planificació final extreta de la fase d'anàlisi i disseny.
- Documentació de la intervenció de canvi d'equips.
- Documentació de la situació final de la nova infraestructura, incloent:
    - Diagrames a nivell físic i lògic de tots els elements implantats.
    - Llistat dels elements físics implantats amb les dades rellevants sobre model, número de sèrie, adreces de gestió, usuaris i contrasenyes, etc.
- Informació sobre el suport tècnic prestat directament per l'adjudicatari, com dades de contacte, particularitats horàries, etc.

9.3 Formació

A la finalització del desplegament, es farà una sessió formativa per a que el personal de l'Àrea de Sistemes del Departament d'Informàtica del CSAPG pugui administrar i operar la nova infraestructura de forma autònoma. En concret, la formació cobrirà almenys aquests aspectes:

- Noves funcionalitats i canvis realitzats respecte a la plataforma anterior.
- Resolució de dubtes.

L'adjudicatari podrà proposar punts i sessions formatives addicionals si ho creu convenient.

Independentment de la formació esmentada, durant les tasques d'implantació del projecte el personal del CSAPG estarà disponible per avançar en el traspàs del coneixement referent a la nova infraestructura.

10 Manteniment i suport tècnic

10.1 Manteniment i suport de fabricant

Tots els elements de la solució proposada hauran de tenir suport i manteniment per part del fabricant durant tota la vigència del contracte en modalitat 24x7x365, amb temps de resposta d'una hora per a incidències crítiques i NBD (*Next Business-Day*) per a la resta d'incidències.

10.2 Manteniment i suport de l'adjudicatari

Durant tota la vigència del contracte, es posarà a disposició del CSAPG un servei de suport tècnic que serà directament proporcionat per l'empresa adjudicatària i inclourà tots els elements de la plataforma implantada en les condicions que es preveuen en el present apartat.

10.2.1 Classificació d'incidències i peticions

Les incidències i peticions es classificaran segons la seva afectació al servei:

- N1 (crítica):
  - Fallada o indisponiblitat total de qualsevols dels clústers de tallafocs.
  - Actualitzacions urgents quan es publiquin vulnerabilitats amb CVE igual o superior a 9.0, que afectin a qualsevol dels elements que formen part de la solució.
- N2 (greu):
  - Fallada d'un membre de qualsevol dels clústers de tallafocs, sense aturada del servei.
  - Degradació del rendiment de qualsevol dels clústers de tallafocs.
  - Fallada amb indisponiblitat del sistema de registre d'auditoria de connexions.
  - Fallada amb indisponiblitat del sistema de doble factor d'autenticació.
  - Fallada amb indisponiblitat del sistema ZTNA.
  - Actualitzacions importants quan es publiquin vulnerabilitats amb CVE igual o superior a 7.0 i inferior a 9.0, que afectin a qualsevol dels elements que formen part de la solució.
- N3 (lleu):
  - Altres degradacions de qualsevol dels elements amb afectació al servei limitada.
  - Peticions i consultes.

S'assignarà un nivell acordat entre l'adjudicatari i el CSAPG a altres incidències o intervencions programades no previstes i en successives ocasions es seguirà el criteri establert.

Les actualitzacions periòdiques quedaran fora d'aquet sistema de nivells i seran planificades entre el responsable del servei per part de l'adjudicatari i el CSAPG.

10.2.2 Horaris

Els horaris que es tindran en compte per a les incidències i peticions són els següents:

- Horari 24x7: tots els dies de l'any a qualsevol hora.
- Horari estàndard: de dilluns a divendres, no festius, entre 8:00 i 17:00.

10.2.3 Serveis de suport tècnic

Els serveis de suport tècnic requerits són els següents:

- Primer nivell de gestió i resolució de consultes i d'incidències de tots els elements que formen part de la solució implantada, en les següents condicions horàries:
  - Incidències i peticions N1: suport en horari 24x7 davant d'incidències crítiques, intervencions programades i actualitzacions. En el cas de les actualitzacions programades i urgents, el CSAPG establirà les finestres horàries per portar-les a terme, que podran ser en horari laborable o fora d'hores segons convingui.
  - Incidències N2 i incidències, peticions i consultes N3: suport en horari estàndard.

- Interlocució amb el fabricant davant de consultes i d'incidències que s'hagin d'escalar al suport tècnic oficial.

L'empresa adjudicatària haurà de tenir en compte a la seva oferta els següents requeriments del servei de manteniment i suport:

- S'inclouran com a mínim 60 hores de suport anual en format bossa d'hores.
- El suport fora de l'horari estàndard podrà consumir hores de la mateixa bossa aplicant un multiplicador a les hores consumides de com a màxim 1,5 (una hora de treballs fora d'horari estàndard consumiria una hora i trenta minuts de la bossa).
- El servei inclourà els possibles desplaçaments del personal tècnic en cas d'intervencions presencials i el transport de les peces de recanvi i equips que requereixin reparació fora de les dependències del CSAPG.

10.2.4 Seguiment del servei

Pel que fa al seguiment del servei de suport per part de l'adjudicatari, caldrà tenir en compte aquests requeriments:

- L'adjudicatari designarà un responsable del servei que serà l'interlocutor amb el CSAPG per a tots els temes referents al seguiment del servei, incloent el seguiment dels SLA i l'aplicació de les possibles penalitzacions.
- Mensualment, s'informarà de l'estat de la bossa d'hores per correu electrònic, indicant les hores consumides en el mes anterior i el romanent d'hores del període anual en curs. En el cas que s'exhaureixin les hores abans de la finalització del període anual en curs, el CSAPG tramitarà una ampliació de les hores que s'estimin necessàries.
- Trimestralment s'enviarà un informe de seguiment que inclourà:
    - Taula amb totes les intervencions realitzades en el període, amb, com a mínim, les següents dades:
        - Identificador.
        - Data i hora d'obertura.
        - Data i hora de resposta.
        - Data i hora de resolució.
        - Estat (oberta, resolta, etc.).
        - Nivell (N1, N2, N3, N/A).
        - Descripció breu.
        - Quantitat d'hores consumides. Les intervencions fora de l'horari estàndard s'indicaran aplicant el multiplicador corresponent.
        - Horari de la intervenció (estàndard/24x7).
        - Temps de resposta en hores.

- Temps de resolució en hores.
- Compliment de SLA (sí/no).
- Justificació de l'adjudicatari en els casos on se superin els llindars establerts.

- Percentatge de compliment de SLA.
- Versions de tots els elements implantats i darrera versió disponible de la branca de *firmware* o programari en ús, juntament amb una valoració sobre la conveniència d'aplicar o no la darrera versió disponible.

10.2.5 Acords de nivell de servei

En el present apartat es defineixen els acords de nivell de servei exigits (d'ara endavant SLA):

Nivell	Temps màxim de resposta[1]	Temps màxim de resolució[2]
N1	2 hores	24 hores
N2[3]	8 hores	48 hores
N3[3]	48 hores	96 hores

Per al càlcul del temps de resolució no es tindrà en compte el temps degut a la impossibilitat de resolució de les incidències o peticions quan:

- Els motius siguin imputables al CSAPG, com la impossibilitat d'accés a les instal·lacions.
- Existeixi algun impediment per part del CSAPG que no permeti portar a terme les actuacions necessàries per a la resolució de la incidència.

11 Penalitzacions

S'estableixen les següents penalitzacions en cas d'incompliment dels requisits del present plec i dels SLA.

11.1 Penalització per incompliment del termini d'execució

En cas de no complir-se el termini d'execució, la penalització serà la següent:

$$Import\ de\ la\ penalització = Dies\ de\ retard \times 50€$$

[1] Temps de resposta: el temps transcorregut entre l'avís d'una incidència o petició per part del CSAPG, o la detecció per part de l'adjudicatari, i l'inici del seu tractament.

[2] Temps de resolució: el temps transcorregut entre l'avís d'una incidència o petició per part del CSAPG, o la detecció per part de l'adjudicatari, i la seva resolució.

[3] En incidències i peticions de N2 i N3, els dies festius i els caps de setmana no computaran per al càlcul dels temps de resposta ni de resolució.

11.1.1 Metodologia de càlcul i aplicació

- Per al còmput de dies de retard només es comptaran dies feiners, entenent com a dia feiner qualsevol dia laborable no festiu segons el calendari del CSAPG.
- El retard començarà a comptar el primer dia feiner posterior a la data límit de lliurament prevista.
- La penalització s'aplicarà en la factura del contracte que inclogui el pagament dels serveis d'implantació i no superarà el 20% de l'import d'aquesta partida. Si per qualsevol motiu no és possible incloure la penalització en la factura prevista, es descomptarà de la següent factura que emeti l'adjudicatari.

11.1.2 Exclusions

No s'aplicarà cap penalització quan:

- La responsabilitat del retard sigui imputable al CSAPG.
- Existeixi algun impediment o manca d'informació per part del CSAPG que no permeti portar a terme el lliurament.
- Es produeixin causes de força major o circumstàncies alienes a l'adjudicatari degudament justificades.
- El CSAPG acordi formalment una ampliació de termini.

11.2 Penalització per incompliment dels SLA

En cas d'incompliment dels temps de resolució d'incidències i peticions s'aplicarà la següent penalització:

Percentatge d'incompliment	Penalització per cada incompliment segons afectació
< 20%	Sense penalització
≥ 20% i <50%	N1: 50€ N2: 25€ N3: 10€
≥ 50%	N1: 100€ N2: 50€ N3: 20€

11.2.1 Metodologia de càlcul i aplicació

- El percentatge d'incompliment s'obtindrà amb la següent fórmula:

$$\%\ incompliment = \frac{Incidències\ i\ peticions\ del\ periode\ fora\ de\ SLA}{Total\ d'incidències\ i\ peticions\ del\ periode} \times 100$$

- Es comptarà com 1 incompliment de l'SLA quan se superi el temps màxim de resposta i/o el temps màxim de resolució en una incidència o petició.

- El període de càlcul serà trimestral.
- Les penalitzacions es regularitzaran en la factura de la següent quota anual de suport, amb un límit del 20% d'aquesta quota anual.

11.2.2 Exclusions

No s'aplicaran penalitzacions quan:

- L'incompliment es degui a manca de resposta, validació o acció per part del CSAPG.
- Siguin necessàries actuacions que requereixin tercers fora del control de l'adjudicatari.
- Es produeixin causes de força major o circumstàncies alienes a l'adjudicatari degudament justificades.

11.3 Procediment d'aplicació de penalitzacions

- Les penalitzacions es regularitzaran en la factura de la següent quota anual de suport.
- El CSAPG podrà demanar la revisió dels càlculs dels percentatges de compliment dels SLAs inclosos en els informes de seguiment detallats a l'apartat 10.2.4 en un termini màxim de 15 dies des de la recepció de l'informe.

12 Termini d'execució

Un cop realitzada l'adjudicació, l'empresa adjudicatària es compromet a lliurar, instal·lar i configurar tots els elements que formen part de la seva proposta en un període màxim de vuit setmanes a partir de la data de signatura del contracte.

13 Retirada de l'equipament a la finalització del contracte

Si així ho requereix el CSAPG, l'adjudicatari haurà de retirar l'equipament a la finalització del contracte, pel seu compte i càrrec, i s'haurà de coordinar amb l'adjudicatari del nou contracte referent a la infraestructura de seguretat perimetral substituta de la licitada en el present concurs per assegurar la disponibilitat en tot moment del sistema de seguretat perimetral del CSAPG.

En el cas que la nova infraestructura substituta es trobi en fase de licitació quan finalitzi el contracte objecte d'aquesta licitació, es podrà prorrogar el mateix fins que la nova infraestructura estigui en producció, en les condicions previstes a l'article 29 de la LCSP.

14 Solvència tècnica - Certificacions requerides

Les empreses licitadores han de formar part dels següents programes de Fortinet:

- Fortinet Expert Partner o equivalent.

Pel que fa al personal tècnic que participarà en el disseny, implantació i operació de la solució, s'exigeixen les següents certificacions de fabricant:

- La planificació, el disseny i el desplegament hauran de ser revisats i validats per tècnics amb la següent certificació:
  - Fortinet certified Solution Specialist – Secure Networking.
- Pel que fa al servei de manteniment i suport, es requereix que dins de l'equip que s'encarregarà d'aquest servei existeixin tècnics amb les següents certificacions:
  - Fortinet certified Professional – Secure Networking.
  - Fortinet certified Solution Specialist – Secure Networking.

15 Documentació a presentar

SOBRE A

- Documentació administrativa o DEUC.

SOBRE B

- Oferta tècnica d'acord al plec de prescripcions tècniques.
- Certificat de compliment de requeriments tècnics signat (Annex 1 del plec de prescripcions tècniques).
- Llistat del llicenciament de programari Fortinet inclòs, segons requeriments de l'apartat 7 del plec de prescripcions tècniques (no incloure el suport o altres llicenciaments relacionats amb els tallafocs).
- Certificat de compliment de l'ENS per part de l'empresa licitadora, o, en el seu defecte, declaració del responsable de seguretat de l'entitat participant en què es comprometi a sotmetre el sistema d'informació a l'adequació a l'ENS en la categoria declarada en un termini de 6 mesos.
- Pla d'execució, segons es detalla a l'apartat 9 del plec de prescripcions tècniques i d'acord amb les especificacions del criteri de valoració subjectiu que en fa referència.
- Pla del servei de suport, segons es detalla a l'apartat 10 del plec de prescripcions tècniques i d'acord amb les especificacions del criteri de valoració subjectiu que en fa referència.

SOBRE C

- Import oferta econòmica, d'acord al document "05b CSAPG 2026_03 PCAP_Annex 2_Seguretat perimetral_Sobre C".
- A més, un llistat de tots els elements físics que composen la solució indicant la quantitat de cada element i el seu preu unitari.

Annex I – Certificat de característiques tècniques mínimes

Mitjançant el present certificat, el licitador acredita que els equips que proposa compleixen, **com a mínim**, amb els requeriments tècnics especificats a l'apartat 6 del plec de prescripcions tècniques resumits a la següent taula, sense detallar el model concret dels equips per no desvetllar detalls que es valoraran a l'obertura del sobre C.

Requeriments generals	
001	En total es requereixen 8 equips tallafoc físics, dos per cadascun dels centres amb perímetre exterior. Cada parella es muntarà en clúster.
002	Tots els equips han de ser nous i no poden tenir data de fi de cicle de vida (EOL) o suport (EOS), publicada a https://support.fortinet.com/support/#/lifecycle, inferior a 2032.
003	Tots els equips, físics o virtuals, hauran de tenir suport de fabricant vigent mentre duri el contracte. Si un equip queda sense suport per part del fabricant definitivament, l'adjudicatari es compromet a canviar-lo per un de característiques equivalents (pel que fa a rendiment, redundància, connectivitat i funcionalitat) sense cost per al CSAPG.
004	Els equips tallafocs han de ser en format *appliance* físic del fabricant Fortinet, quedant exclosos màquines virtuals ni servidors de propòsit general. Han de poder ser instal·lats en un rack estàndard de 19" ocupant 1 RU com a màxim.
005	Els dos equips físics de cada centre han de ser idèntics, redundats i en alta disponibilitat (HA). Han de permetre treballar en mode HA actiu-actiu i actiu-passiu.
006	Els equips tindran doble font d'alimentació.
007	Els equips tallafocs tindran hardware especialitzat de tipus ASIC per tal d'assegurar el rendiment requerit i garantir baixa latència.
008	Els equips han d'incloure funcionalitats de control d'aplicacions, prevenció d'intrusions (IPS), protecció contra codi nociu, filtre web, filtres DNS, antispam, Data Loss Prevention (DLP), inspecció SSL/SSH, Web Application Firewall (WAF) i protecció antiDoS. Totes aquestes funcionalitats hauran d'estar llicenciades durant tota la vida del contracte.
Requeriments específics dels tallafocs Tipus A	
A01	1 port de consola RJ45.
A02	1 port de management Out-of-Band RJ45.
A03	1 port HA (ports dedicats per establir el clúster HA).
A04	1 port USB 3.0 per a la connexió de dispositiu d'emmagatzematge extraïble USB. El port USB ha de permetre la instal·lació desatesa del firmware i aplicació de configuració en el boot de l'equip.
A05	8 ports 10GE SFP+.
A06	20 ports 1GE (mínim 4 ports 1GE SFP, la resta RJ45).
A07	El tallafocs disposarà de com a mínim 39/39/26,5 Gbps d'amplada de banda de firewall per a paquets de 1518, 512 i 64 bytes UDP respectivament, en IPv4 i IPv6.

A08	El tallafocs ha de ser capaç de gestionar com a mínim 11 milions de sessions concurrents així com a mínim 400.000 noves sessions TCP per segon.
A09	El tallafocs ha de tenir una latència inferior a 5 µs (per paquets de 64 bytes UDP).
A10	Ha de tenir capacitat per com a mínim 10.000 polítiques de firewall.
A11	El rendiment per al tràfic SSL VPN ha de ser de com a mínim 3 Gbps i per tràfic IPSEC VPN (mesurat en paquets de 512 bytes) de 36 Gbps.
A12	A nivell 7, l'equip ha de proporcionar com a mínim el següent rendiment: a) IPS: 9 Gbps. b) NGFW: 7 Gbps. c) Threat Protection: 6 Gbps. d) Inspecció SSL amb IPS: 7 Gbps. e) Control d'aplicacions: 27,8 Gbps (mesurat amb tràfic HTTP amb paquets de 64K).
Requeriments **mínims** específics dels tallafocs Tipus B	
B01	1 port de consola RJ45.
B02	1 port de management Out-of-Band RJ45.
B03	1 port HA (ports dedicats per establir el clúster HA).
B04	1 port USB 3.0 per a la connexió de dispositiu d'emmagatzematge extraïble USB. El port USB ha de permetre la instal·lació desatesa del firmware i aplicació de configuració en el boot de l'equip.
B05	4 ports 10GE SFP+ com a mínim.
B06	Com a mínim 20 ports 1GE (mínim 4 ports 1GE SFP, la resta RJ45).
B07	El tallafocs disposarà de com a mínim 39/39/25 Gbps d'amplada de banda de firewall per a paquets de 1518, 512 i 64 bytes UDP respectivament, en IPv4 i IPv6.
B08	El tallafocs ha de ser capaç de gestionar com a mínim 3 milions de sessions concurrents així com a mínim 140.000 noves sessions TCP per segon.
B09	El tallafocs ha de tenir una latència inferior a 5 µs (per paquets de 64 bytes UDP).
B10	Ha de tenir capacitat per com a mínim 10.000 polítiques de firewall.
B11	A nivell 7, l'equip ha de proporcionar com a mínim el següent rendiment: a) IPS: 5,3 Gbps. b) NGFW: 3,1 Gbps. c) Threat Protection: 2,8 Gbps. d) Inspecció SSL amb IPS: 3 Gbps. e) Control d'aplicacions: 6,7 Gbps.
Requeriments específics dels tallafocs Tipus C	
C01	1 port de consola RJ45.

C02	1 port USB 3.0 per a la connexió de dispositiu d'emmagatzematge extraïble USB. El port USB ha de permetre la instal·lació desatesa del firmware i aplicació de configuració en el boot de l'equip.
C03	2 ports 10GE SFP+.
C04	8 ports 1GE RJ45.
C05	El tallafocs disposarà de com a mínim 28/28/25 Gbps d'amplada de banda de firewall per a paquets de 1518, 512 i 64 bytes UDP respectivament, en IPv4 i IPv6.
C06	El tallafocs ha de ser capaç de gestionar com a mínim 3 milions de sessions concurrents així com a mínim 124.000 noves sessions TCP per segon.
C07	El tallafocs ha de tenir una latència inferior a 5 µs (per paquets de 64 bytes UDP).
C08	Ha de tenir capacitat per com a mínim 5.000 polítiques de firewall.
C09	A nivell 7, l'equip ha de proporcionar com a mínim el següent rendiment: a) IPS: 4,5 Gbps. b) NGFW: 2,5 Gbps. c) Threat Protection: 2,2 Gbps. d) Inspecció SSL amb IPS: 2,6 Gbps. e) Control d'aplicacions: 6,7 Gbps.
Requeriments de transceptors i cablejat	
D01	6 transceptors Fortinet FN-TRAN-SFP+LR de llarga distància SMF.
D02	30 transceptors Fortinet FN-TRAN-SFP+SR de curta distància MMF.
D03	20 transceptors HPE J9150D o compatibles del fabricant FS.
D04	28 cables de fibra del tipus i longitud adients per fer les connexions necessàries amb la xarxa intercentres i el Core de cada centre.
D05	Cablejat adient per enllaçar els dos membres de cada clúster de tallafocs.

I perquè així consti, signa el present annex en mostra del seu compliment,

(data, signatura i segell de l'empresa)