PLEC DE PRESCRIPCIONS TÈCNIQUES PER A L'ADQUISICIÓ, SUPORT I MANTENIMENT D'EQUIPAMENT I SERVEIS DE CIBERSEGURETAT PER LA XARXA INFORMÀTICA DE LA FUNDACIÓ I2CAT

EXP. 2023072600

1. Presentació

1.1 Objecte del contracte

L'objecte d'aquest contracte és l'adquisició de nou equipament de comunicacions i serveis de ciberseguretat per a millorar la seguretat perimetral de la xarxa informàtica de la Fundació i2CAT (d'ara endavant, i2CAT), així com l'accés remot a les aplicacions i recursos accessibles a través d'ella. A més també s'inclou la prestació de serveis professionals de suport al desplegament i manteniment nivell 2 tant de l'equipament com dels serveis de ciberseguretat esmentats. Aquesta licitació està dividida en dos lots, els objectes dels quals es detallen a continuació.

Objecte del Lot 1: Adquisició, suport i manteniment d'equipament de comunicacions de la xarxa informàtica d'i2CAT. L'objecte d'aquest lot contempla l'adquisició d'equipament, llicències de programari, suport del fabricant i la prestació de serveis professionals d'integració per la instal·lació i manteniment de l'equipament de comunicacions de la xarxa informàtica d'i2CAT.

Objecte del Lot 2: Desplegament, operació i manteniment d'un servei SASE (Secure Access Service Edge) per a la xarxa informàtica d'i2CAT. L'objecte d'aquest lot contempla el desplegament, operació i manteniment d'un servei SASE que permet l'accés remot segur als recursos accessibles a través de la xarxa informàtica d'i2CAT, així com l'accés segur dels treballadors d'i2CAT a Internet i a serveis al núvol en modalitats Infrastructure as a Service (d'ara endavant IaaS) i Software as a Service (d'ara endavant SaaS).

1.2 Àmbit

L'àmbit del projecte és la xarxa informàtica d'i2CAT i els dispositius electrònics que els empleats d'i2CAT utilitzen per a accedir a l'esmentada xarxa i a altres xarxes de dades (com pot ser Internet). Més específicament:

Àmbit del Lot 1: Adquisició, suport i manteniment d'equipament de comunicacions de la xarxa informàtica d'i2CAT. L'àmbit d'aquest lot és la xarxa informàtica de la Fundació i2CAT, que està repartida en quatre emplaçaments. Els dos primers són les oficines centrals d'i2CAT a l'Edifici Nexus (d'ara endavant oficines Nexus), i el Centre de Processament de Dades de l'Edifici Omega (d'ara endavant CPD Omega), situats al Campus Nord de la Universitat Politècnica de Catalunya, a Barcelona. El tercer emplaçament és el laboratori de realitat virtual, augmentada i extesa (d'ara endavant XR Lab), ubicat a l'Edifici Neàpolis de Vilanova i la Geltrú. El darrer emplaçament es el laboratori de 5G Rural (d'ara endavant lab 5G Rural) ubicat a Móra la Nova. L'àmbit del projecte inclou:

- El desplegament de tallafocs amb capacitats de connectivitat Software Defined Wide Area Network (d'ara endavant, SD-WAN) als quatre emplaçaments mencionats anteriorment.
- La renovació de part dels equips d'accés cablejat a la xarxa de les oficines Nexus.
- La renovació dels equips d'accés inalàmbric a la xarxa de les oficines Nexus.

- L'aplicatiu per a poder gestionar els equips de forma centralitzada, incloent la gestió de la configuració, la monitorització d'esdeveniments i alarmes així com el seu posterior anàlisi.

Àmbit del Lot 2: Desplegament, operació i manteniment d'un servei SASE (Secure Access Service Edge) per a la xarxa informàtica d'i2CAT. L'àmbit d'aquest lot són els dispositius electrònics que els empleats d'i2CAT utilitzen per accedir a la xarxa informàtica d'i2CAT i a altres xarxes de dades (com pot ser Internet), així com els recursos de la xarxa informàtica d'i2CAT accessibles remotament per part dels empleats d'i2CAT i personal d'altres organitzacions amb les quals i2CAT col·labora. L'àmbit del projecte inclou:

- Un servei Zero Trust Network Access (d'ara endavant ZTNA) que permet l'accés remot segur als recursos disponibles a través de la xarxa informàtica d'i2CAT o infraestructura de proveïdors de serveis al núvol (Infrastructure as a Service, d'ara endavant IaaS).
- Un servei d'accés segur a Internet Secure Web Gateway (d'ara endavant SWG) per als empleats d'i2CAT, per tal de minimitzar la seva exposició a amenaces de ciberseguretat mentre naveguen per Internet i accedeixen a serveis allotjats al núvol (en formats IaaS i SaaS).

1.3 Abast

Abast del Lot 1: Adquisició, suport i manteniment d'equipament de comunicacions de la xarxa informàtica d'i2CAT. Forma part de l'abast del contracte:

- El subministrament de tot l'equipament i material necessaris.
- El subministrament de tots els aplicatius necessaris.
- 5 anys de garantia que inclou SLAs garantits.
- Suport a la instal·lació i configuració de l'equipament.
- Suport a la posada en marxa i validació de la instal·lació.
- Formació dels tècnics de suport i manteniment designats per i2CAT.
- 5 anys de suport de nivell 2 en l'operació i manteniment de l'equipament proporcionat.

Abast del Lot 2: Desplegament, operació i manteniment d'un servei SASE (Secure Access Service Edge) per a la xarxa informàtica d'i2CAT. Forma part de l'abast del contracte:

- 3 anys de subscripció a un servei de ZTNA per protegir l'accés remot a recursos d'i2CAT.
- 3 anys de subscripció a un servei SWG d'accés segur a Internet i serveis al Núvol en modalitats IaaS i SaaS per als treballadors d'i2CAT.
- Formació dels tècnics que utilitzaran els serveis anteriors, designats per i2CAT.
- 3 anys de suport.

1.4 Terminis

Terminis del Lot 1: Adquisició, suport i manteniment d'equipament de

comunicacions de la xarxa informàtica d'i2CAT.

Termini màxim d'instal·lació de l'equipament d'accés cablejat, inalàmbric i tallafocs a la xarxa informàtica d'i2CAT des de la data de signatura del contracte: 4 mesos.

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

Terminis del Lot 2: Desplegament, operació i manteniment d'un servei SASE (Secure Access Service Edge) per a la xarxa informàtica d'i2CAT.

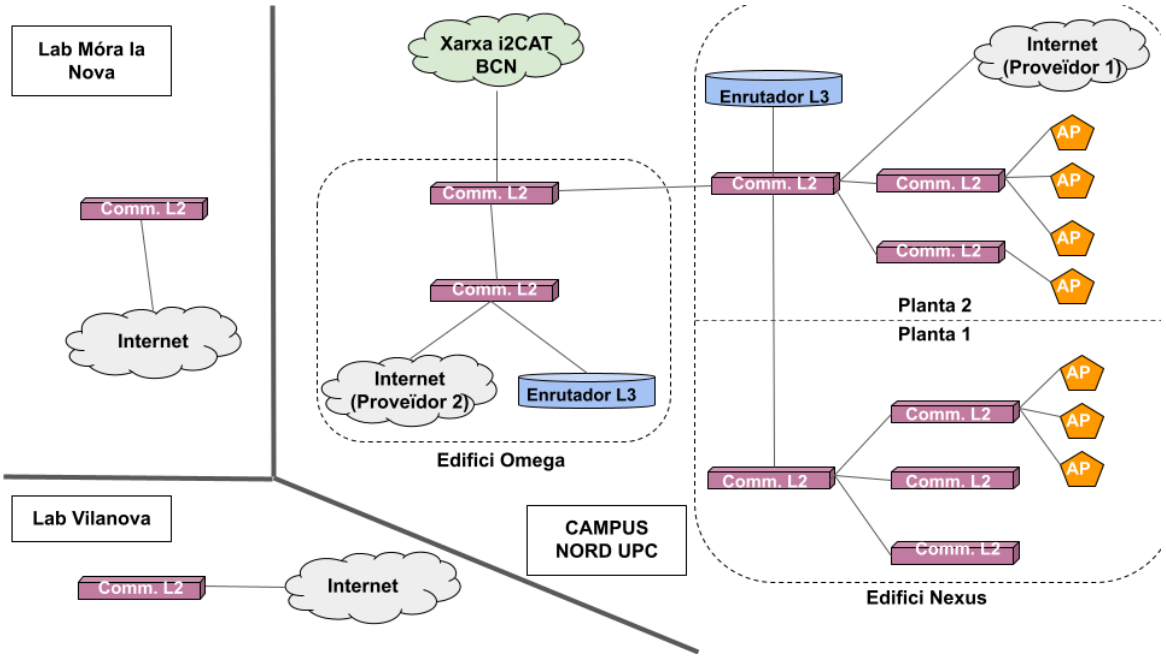
Termini màxim de configuració i posada en operació del servei SASE des de la data de signatura del contracte: 2 mesos.

Termini de garantia i manteniment: 3 anys des de la data de posada en producció.

2. Descripció de la situació actual

2.1 Estructura actual de la xarxa informàtica d'i2CAT

La següent imatge mostra una versió simplificada de l'estructura actual de la xarxa informàtica d'i2CAT en els quatre emplaçaments rellevants per aquesta licitació: els laboratoris de Móra la Nova i Vilanova i la Geltrú, així com l'edifici Nexus i el CPD Omega al Campus Nord de la UPC.



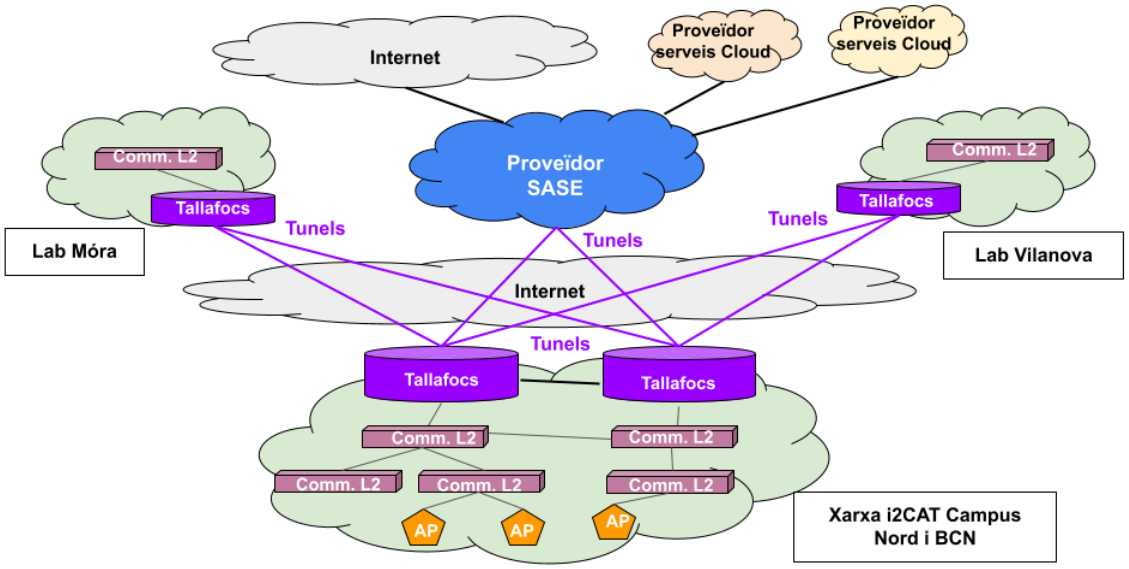
La xarxa informàtica d'i2CAT al campus Nord utilitza bàsicament tecnologies de nivell 2 (Ethernet amb VLANs) per a la connectivitat interna entre les estacions de treball individuals dels empleats d'i2CAT a les oficines de l'edifici Nexus i els diferents dispositius (servidors, equips de comunicacions ràdio, dispositius IoT, etc.) localitzats al laboratori de l'edifici Nexus, al CPD de l'edifici Omega i a altres emplaçaments de Barcelona i Castelldefels (connectats a través de la xarxa de fibra òptica d'i2CAT).

Dos proveïdors de serveis a Internet permeten als empleats d'i2CAT accedir a Internet així com a serveis Cloud en modalitats IaaS (Infrastructure as a Service) i SaaS (Software as a Service). El personal d'i2CAT en mode teletreball pot accedir a la xarxa interna d'i2CAT a través de una VPN (Virtual Private Network).

Actualment no es disposa de connectivitat de nivell 2 entre la xarxa del lab de Vilanova i la xarxa principal d'i2CAT, idèntica situació a la presentada pel laboratori de Móra la Nova. Per tant, per accedir remotament als recursos i serveis d'aquests laboratoris a través d'Internet també s'utilitza un servei de VPN.

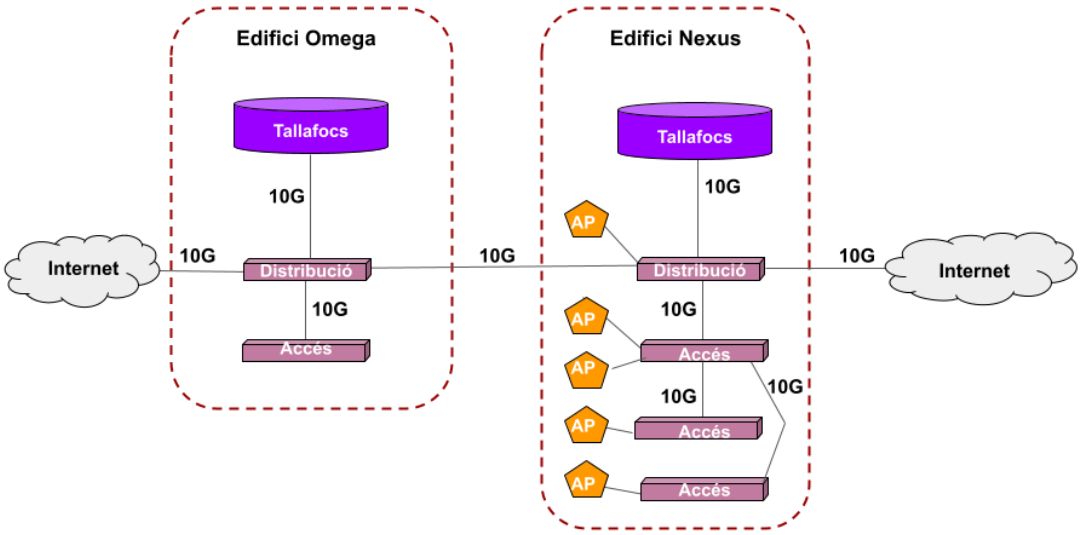
2.2 Modificacions previstes a la xarxa actual

La següent imatge mostra una versió simplificada dels canvis en l'arquitectura de la xarxa informàtica d'i2CAT en el marc de la licitació actual.



Es vol assolir una millor integració entre les xarxes dels diversos emplaçaments considerats en aquesta licitació (lab 5G rural, XR lab, oficines Nexus i CPD Omega), així com la millora del nivell de seguretat tant en accés segur a Internet i serveis Cloud com l'accés segur als recursos i serveis d'i2CAT des d'Internet o una altra xarxa externa. Per a aconseguir aquests objectius es preveuen els següents canvis.

- **Lot 1:** Desplegament d'una capa d'equips tallafocs que controlin l'accés a Internet en cada una de les seus. Aquests equips tallafocs també han de disposar de funcionalitat de SD-WAN (Software Defined Wide Area Network) per a poder crear una xarxa privada de nivell 2 d'àrea extesa a través de túnels sobre Internet.
- **Lot 1:** Renovació dels equips de commutació de nivell 2 de l'edifici Nexus, augmentant les seves prestacions amb funcionalitats de ciberseguretat integrables amb les dels tallafocs, i gestionar de forma conjunta.
- **Lot 1:** Renovació dels equips d'accés inalàmbrics de les oficines del Nexus, augmentant les seves prestacions amb funcionalitats de ciberseguretat que es puguin integrar amb les dels tallafocs i les equips de commutació de nivell 2, i gestionar-los de forma conjunta.
- **Lot 1:** Desplegament d'un sistema de gestió que permeti gestionar els elements anteriors (tallafocs, equips de commutació de nivell 2 i equips d'accés inalàmbrics) des d'una sola consola d'administració.
- **Lot 2:** Contractació d'un proveïdor SASE al núvol per tal d'oferir un accés segur als recursos i serveis presents a la xarxa d'i2CAT (funcionalitat ZTNA), així com un accés segur a Internet i als serveis de proveïdors Cloud per als treballadors, socis i clients d'i2CAT (funcionalitat SWG).



La imatge anterior proporciona una visió més acurada de l'arquitectura de desplegament prevista dels equips de comunicacions en els emplaçaments de l'edifici Omega i l'Edifici Nexus. Els commutadors de nivell 2 es diferencien entre commutadors de distribució (se'n volen adquirir dues unitats) i commutadors d'accés (se'n volen adquirir 5 unitats, no estan totes representades a la imatge).

Hi haurà un commutador de distribució a cada edifici (Nexus, Omega), connectats entre si a través d'un enllaç de 10G. Cada commutador de distribució estarà connectat a un tallafocs, a un proveïdor d'accés a Internet i a un commutador d'accés a través d'enllaços de 10G. També podrà estar connectat a un o més servidors (Edifici Omega) o a un o més punts de connexió d'escriptori o Access Points (Edifici Nexus) a través d'enllaços de 1G.

Els commutadors d'accés estan connectats a servidors (Edifici Omega) o a Access Points, punts de connexió d'escriptori o equipament de laboratori a través d'enllaços 1G (Edifici Nexus). En el cas de l'Edifici Nexus, els commutadors d'Accés també poden estar connectats a altres commutadors d'accés a través d'enllaços 10G.

3. Dimensionament i especificacions dels equips i serveis

3.1 Lot 1: dimensionament i especificacions dels tallafocs

i2CAT vol adquirir quatre tallafocs, un per cada un dels emplaçaments mencionats al punt 1.2 d'aquest document: oficines Nexus, CPD Omega, XR lab i lab 5G rural. Els quatre equips han de complir amb els requeriment i característiques mínimes especificades a continuació, i ser entregats segons els terminis establerts al punt 1.4 d'aquest document.

A més, per garantir una total integració, compatibilitat i homogeneïtat amb la resta d'equips en el marc d'aquesta licitació, els tallafocs hauran de ser del mateix fabricant que els commutadors de nivell 2 i els equips d'accés inalàmbrics. D'aquesta manera es facilitarà l'administració i manteniment posteriors.

3.1.1 Característiques generals dels tallafocs

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

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

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

La solució ha d'incloure funcionalitats de control d'aplicacions, IPS, Antimalware, Webfilter, Antispam i Web Application Firewall. Totes aquestes funcionalitats han d'estar llicenciades per a la duració del contracte.

S'hauran de subministrar fonts d'alimentació redundants per als equips tallafocs de les oficines Nexus i del CPD Omega (no es necessari en el cas dels tallafocs del XR-lab i del lab 5G Rural).

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

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

3.1.2 Rendiment

Els equips tallafocs tindran hardware específic (de tipus ASIC) per tal d'assegurar el rendiment requerit.

Tallafocs d'Oficines Nexus i CPD Omega

El tallafocs disposarà de fins a 25 Gbps o més de rendiment de tallafocs per paquets de 1518 bytes en IPv4 i IPv6; i fins a 10 Gbps o més de rendiment de tallafocs per a paquets de 64 bytes. El tallafocs ha de ser capaç de gestionar com a mínim 3 milions de sessions concurrents; i 250.000 noves sessions per segon.

El tallafocs ha de tenir una latència màxima de 5 µs (per a paquets UDP de 64 bytes).

El rendiment per tràfic SSL VPN ha de ser de com a mínim 2 Gbps i per tràfic IPsec VPN (512 bytes) de 13 Gbps.

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

- Rendiment IPS: 5 Gbps amb un mix de tràfic realista (amb logging actiu).
- Rendiment NGFW (IPS i control d'aplicacions): 3.5 Gbps amb un mix de tràfic realista (amb logging actiu).
- Rendiment amb Threat Protection (IPS, control d'aplicacions i motor antimalware actius): 3 Gbps amb un mix de tràfic realista (amb logging actiu).
- Rendiment Inspecció SSL amb IPS: 4 Gbps mesurat amb diferents Ciphers.
- Rendiment per control d'aplicacions: 13 Gbps mesurat per HTTP 64K.

Tallafocs XR lab i lab 5G Rural

El tallafocs disposarà de fins a 10 Gbps o més de rendiment de tallafocs per paquets de 1518 bytes en IPv4 i IPv6; i fins a 5 Gbps o més de rendiment de tallafocs per a paquets de 64 bytes. El tallafocs ha de ser capaç de gestionar com a mínim 500.000 sessions concurrents; i 30.000 noves sessions per segon.

El tallafocs ha de tenir una latència màxima de 4 µs (per paquets UDP de 64 bytes).

El rendiment per tràfic SSL VPN ha de ser de com a mínim 900 Mbps i per tràfic IPsec VPN (512 bytes) de 6.5 Gbps.

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

- Rendiment IPS: 1.4 Gbps amb un mix de tràfic realista (amb logging actiu).
- Rendiment NGFW (IPS i control d'aplicacions): 1 Gbps amb un mix de tràfic realista (amb logging actiu).
- Rendiment amb Threat Protection (IPS, control d'aplicacions i motor antimalware actius): 700 Mbps un mix de tràfic realista (amb logging actiu).
- Rendiment Inspecció SSL amb IPS: 630 Mbps mesurat amb diferents Ciphers.
- Rendiment per control d'aplicacions: 1.8 Gbps mesurat per HTTP 64K.

3.1.3 Connectivitat i característiques físiques

Els tallafocs han de tenir *com a mínim (per equip):*

- 1 port de consola.
- 1 port d'USB. El port USB ha de permetre la instal·lació desassistida del firmware i aplicació de configuració en el booting de l'equip per realitzar tasques automàtiques d'instal·lació i canvis d'equipament.
- Instal·lació en rack de 19' (directament o a través d'una safata)' i no més de 1 RU.
- En el cas que l'equipament permeti ampliacions modulars d'interfícies, caldrà que tots els mòduls d'ampliació estiguin equipats amb interfícies com a mínim de les mateixes velocitats que es sol·liciten pels ports mínims obligatoris.
- En el cas que l'equip suporti ampliacions de memòria RAM i Disc Dur, caldrà que l'appliance estigui equipat amb el màxim de capacitats RAM i de Disc suportats.

Tallafocs d'Oficines Nexus i CPD Omega

- 4 x 10GE SFP+
- 8 x GE SFP
- 8 x GE RJ45
- Disc dur de 480 GB en format SSD.
- Consum màxim inferior a 150 W.

Tallafocs XR lab i lab 5G Rural

- 10 x GE RJ45
- Disc dur de 128 GB en format SSD.
- Consum màxim inferior a 20 W.

3.1.4 Gestió dels equips

La gestió ha de ser de fàcil ús i intuïtiva. Capacitat de gestió dels equips mitjançant accés via web (HTTPS) i terminal (SSH) per la total configuració de les polítiques de seguretat de la plataforma.

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

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

Suport de SNMP i sFlow.

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

3.1.5 Networking

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

Suport Dual Stack IPv4 e IPv6 simultàniament.

Network address translation NAT IPv4, NAT64 i NAT66.

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

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

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

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

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

- Balanceig intel·ligent de connexions físiques i lògiques, indiferentment del tipus de connexió WAN (MPLS, 3G/4G, FTTH, VPN, etc..).
- Verificació de la disponibilitat d'Internet per cadascuna de les línies, per protocols HTTP, ping i TWAMP.
- Verificació de paràmetres de qualitat en temps real: jitter, packet loss i latència per línia.
- Configuració de polítiques de SD-WAN intel·ligent basat en origen (usuaris AD i direcció IP), en el destí (direcció IP, aplicacions i/o serveis d'Internet/aplicacions) i en la línia amb millor qualitat d'aquell moment basat en valors de jitter, packet loss, latència, tràfic de pujada/baixada o ampla de banda, així com una combinació per pesos.
- En el cas de necessitat de llicenciament o subscripcions per activar aquestes funcionalitats, caldrà que aquestes estiguin incloses en la proposta durant la duració completa del contracte.

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

3.1.6 Alta disponibilitat

La funcionalitat d'alta disponibilitat *només es requereix pels tallafocs dels emplaçaments de les oficines Nexus i el CPD Omega*.

Aquesta funcionalitat ha d'estar disponible sense necessitat de llicència.

Suport HA tipus Actiu – Passiu, Actiu - Actiu i, opcionalment, mode mixt (en el cas de que l'equip suporti tallafocs virtuals). El mode mixt implica poder tenir tallafocs virtuals actius i passius de forma barrejada, és a dir, el màster de certs tallafocs virtuals sigui la primera unitat de tallafocs, mentre que la segona unitat de tallafocs és màster de la resta de tallafocs virtuals alhora.

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

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

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

3.1.7 Polítiques de seguretat

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

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

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

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

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

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

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

3.1.8 Control d'aplicacions

Capacitat per identificar un mínim de 1000 aplicacions actives actuals. La solució ha de classificar les aplicacions en diferents categories i subcategories, per poder aplicar regles d'acord amb aquestes categories / subcategories (control granular dins de l'aplicació).

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

Capacitat per identificar les aplicacions sota túnels HTTPS.

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

3.1.9 IPS

Capacitat per protegir tant servidors com clients amb un mínim de 10000 firmes d'IPS, agrupades per categoria, severitat, objectiu i protocol. Davant la identificació d'un atac per IPS, cal que el tallafocs capturi el tràfic en un arxiu pcap per tal d'evidenciar-ho i fer un estudi posterior.

Capacitat per identificar patrons d'atacs basats en comportament o rated-base, per tal de bloquejar intents d'atacs un cop superat un umbral d'ús en un temps determinat.

Capacitat de creació de firmes d'IPS per un reconeixement personalitzat.

3.1.10 Antimalware

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

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

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

3.1.11 Webfilter

Capacitat de categoritzar més de 250 milions de pàgines web en més de 60 categories web per tal d'aplicar accions de bloqueig, monitorització i aplicació de quotes de temps

o tràfic per categoria.

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

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

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

Suport de rating per imatges per URL.

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

3.1.12 VPN

Els tallafocs del CPD Omega i Oficines Nexus han de permetre fins a 500 usuaris simultanis VPN SSL, ja sigui amb agent o sense, però en qualsevol cas sense llicència addicional. En el cas dels tallafocs del XR lab i el lab 5G Rural, s'han de permetre fins a 200 usuaris simultanis VPN SSL, en les mateixes condicions.

El sistema proposat haurà de complir els estàndards de la indústria, sense el suport extern addicional de maquinari o mòduls: IPSEC VPN (IPv4 i IPv6), PPTP VPN, L2TP VPN, SSL VPN i GRE sobre IPSEC.

El sistema proposat haurà de suportar 2 modes de funcionament SSL VPN:

- Sense client - Accés web: per a clients remots que només necessiten un navegador i no requereix la instal·lació de cap agent, per tal d'accedir via web a: HTTP / HTTPS Servidor intermediari, FTP, Telnet, SMB / CIFS, SSH, VNC i RDP.
- Mode túnel: per a equips remots que executen una varietat d'aplicacions de client i servidor.

Suport d'agregació de túnels VPN i balanceig per paquet podent així afegir l'ample de banda dels accessos VPN IPsec entre seus.

Capacitat d'integració del mateix fabricant de doble factor d'autenticació via token mòbil, així com per SMS i correu electrònic, integrat en la mateixa plataforma de seguretat. Aquest token també s'ha de poder fer servir per l'accés a la GUI dels equips tallafocs.

Capacitat d'integració amb proveïdors d'identitat externs a través del protocol SAML, amb distinció per grups d'usuaris.

3.2 Lot 1: dimensionament i especificacions dels equips de commutació

i2CAT vol adquirir set commutadors per a la xarxa de nivell 2 dels edificis Nexus i Omega. Concretament, 2 commutadors de distribució, i cinc commutadors d'accés. Tot

el maquinari ofert constituirà un mateix sistema que donarà servei de connectivitat als usuaris de la xarxa informàtica d'i2CAT. Per maximitzar les prestacions de baixa latència, màxim rendiment i facilitar la gestió dels mateixos, tot el hardware ofertat haurà de ser del mateix fabricant. Tot el material, connectors i adaptadors necessaris inclosos, ha de ser nou i original del fabricant. Els equips ofertats no poden estar a la llista de End-of-Sale del fabricant.

3.2.1 Característiques generals dels commutadors

Es demana el compliment de les següents especificacions:

- Tots els equips i programaris seran de marca registrada.
- Tot el hardware i software ha de ser nou, sense utilització prèvia.
- Tot el hardware i software ha de ser vigent, trobar-se en període de comercialització del producte, sense que el fabricant n'hagi anunciat la discontinuïtat o la substitució per nous models.
- Tot el hardware i software ha de disposar d'un mínim de 5 anys de suport del fabricant un cop anunciat el fi de la comercialització del producte. Aquest suport ha d'incloure la reparació o substitució d'equips avariats, i el suport i resolució de dificultats amb el programari "firmware" dels equips i el programari de gestió.
- Tot el hardware i software s'ha de gestionar des d'una única plataforma de gestió, que implementi les necessitats de configuració de monitoratge descrits.
- En el lliurament de les implementacions realitzades caldrà presentar documentació exhaustiva del resultat final.
- Si en el període de vigència de l'acord es publiquessin noves normatives catalanes, estatals, o internacionals, el licitador s'obliga al seu compliment.
- Els equips tindran format i accessoris adequats pel muntatge en rack estàndard de 19" d'amplada i 600 mm o 1000 mm de fons, incloent espai necessari per connexions, cables i similars. Provisió dels accessoris necessaris pel muntatge en el rack.
- Els equips s'alimentaran amb fonts d'alimentació AC 220V i 50Hz.
- Cables alimentació
- Els commutadors hauran de ser del mateix fabricant que els tallafocs.
- No es permeten fonts d'alimentació externes als equips.
- Es requereix suport de tots els estàndards habituals de mercat.
- Cal incloure tot el llicenciament necessari per a totes les opcions demanades.
- Subministrament de tots els materials i accessoris necessaris per a la interconnexió dels commutadors amb els tallafocs i altres equips. Això inclou les òptiques, els cables de connexió de FO, els mòduls i cables específics, els cables d'alimentació, els cables d'stack, els cables de consola, ... i qualsevol altre element que resulti necessari.
- Les òptiques (transceivers) necessàries en els equips commutadors, (GBIC, SFP, SFP+, QSFP, QSFP+, ...) seran del mateix fabricant que el fabricant dels equips. No s'admeten òptiques compatibles ni reacondicionades ("refurbished").
- Tots els equips subministrats procediran del canal formal de distribució i manteniment que tingui el fabricant al país.

- El projecte inclou la implementació d'un model de gestió automatitzada via un paradigma Security Fabric i la implementació d'un model de seguretat proporcionat per la pròpia xarxa.
- El programari que es subministri en modalitat de subscripció es subministrarà de manera que s'inclogui un mínim de 5 anys de subscripció.
- En qualsevol lloc on s'anomeni una normativa estàndard cal entendre que també s'accepta com a vàlida una normativa posterior que actualitzi i millori la normativa indicada.

3.2.2 Rendiment

Els equips commutadors tindran hardware específic (de tipus ASIC) per tal d'assegurar el rendiment requerit.

Commutadors de distribució:

- Capacitat de commutació mínima: 170 Gbps
- Latencia màxima: 1 us
- DRAM: 1 GB DDR4
- Emmagatzematge d'adreces MAC: 32000
- Número de VLANs: 4000

Commutadors d'accés:

- Capacitat de commutació mínima: 120 Gbps (commutadors de 24 ports) / 170 Gbps (commutadors de 48 ports)
- Latencia màxima: 1 us
- DRAM: 512 MB DDR3
- Emmagatzematge d'adreces MAC: 32000
- Número de VLANs: 4000

3.2.3 Connectivitat i característiques físiques

Els commutadors han de tenir com a mínim (per equip):

- 1 port de consola.
- Instal·lació en rack de 19'' i no més de 1 RU.
- Capacitat d'ampliar ports de l'appliance de seguretat amb l'addició de commutadors externs, que es gestionin de forma única i del mateix fabricant.
- En el cas que l'equipament permeti ampliacions modulars d'interfaces, caldrà que tots els mòduls d'ampliació estiguin equipats amb interfícies com a mínim de les mateixes velocitats que es sol·liciten pels ports mínims obligatoris.
- En el cas que l'equip suporti ampliacions de memòria RAM, caldrà que l'appliance estigui equipat amb el màxim de capacitats RAM.

Commutadors de distribució

- 4 x 10GE SFP+
- 48 x GE RJ45
- Memòria FLASH de 256 MB

- Consum màxim inferior a 50 W

Commutadors d'accés de 24 ports

- 4 x 10GE SFP+
- 24 x GE RJ45, dels quals 12 son ports PoE
- Memòria FLASH de 64 MB
- Consum màxim inferior a 240 W

Commutadors d'accés de 48 ports

- 4 x 10GE SFP+
- 48 x GE RJ45, dels quals 24 son ports PoE
- Memòria FLASH de 64 MB
- Consum màxim inferior a 480 W

3.2.4 Gestió dels equips

La gestió ha de ser de fàcil ús i intuïtiva. Capacitat de gestió dels equips des dels equips tallafocs, però també mitjançant accés via web (HTTPS) i terminal (SSH) per la total configuració dels protocols i funcionalitats dels commutadors.

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

Suport de SNMP i sFlow.

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

3.2.5 Networking L2

Suport dels següents protocols i funcionalitats:

- IEEE 802.1D MAC Bridging/STP
- IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
- IEEE 802.1Q VLAN Tagging
- IEEE 802.3ad Link Aggregation with LACP
- Unicast/Multicast traffic balance over trunking port
- IEEE 802.1AX Link Aggregation
- IEEE 802.3x Flow Control and Back-pressure
- IEEE 802.3 10Base-T
- IEEE 802.3u 100Base-TX
- IEEE 802.3z 1000Base-SX/LX
- IEEE 802.3ab 1000Base-T
- IEEE 802.3ae 10 Gigabit Ethernet
- IEEE 802.3az Energy Efficient Ethernet
- IEEE 802.3bz Multi Gigabit Ethernet
- IEEE 802.3 CSMA/CD Access Method and Physical Layer Specifications

- MAC, IP, Ethertype-based VLANs
- Per-port storm control
- Priority-based Flow Control (802.1Qbb)
- IEEE 802.1ad QinQ
- Buffers de paquets compartits dinàmicament

3.2.6 Networking L3

Suport de protocols i funcionalitats:

- Encaminament estàtic
- Encaminament dinàmic: OSPFv2, RIPv2, VRRP, BGP
- ECMP
- Bidirectional Forwarding Detection (BFD)
- DHCP Relay
- Servidor DHCP
- Unicast Reverse Path Forwarding - uRPF
- IPv6 route filtering

3.2.7 Seguretat i visibilitat

Suport de protocols i funcionalitats:

- Port Mirroring
- Admin Authentication Via RFC 2865 RADIUS
- IEEE 802.1X Authentication Port-based
- IEEE 802.1X Authentication MAC-based
- IEEE 802.1X Guest and Fallback VLAN
- IEEE 802.1X MAC Access Bypass (MAB)
- IEEE 802.1X Dynamic VLAN Assignment
- Radius CoA (Change of Authority)
- Radius Accounting
- MAC-IP Binding
- ACL
- IEEE 802.1ab Link Layer Discovery Protocol (LLDP)
- IEEE 802.1ab LLDP-MED
- IEEE 802.1ae MAC Security (MAC Sec)
- DHCP-Snooping
- IEEE 802.1X open auth
- IEEE 802.1X EAP pass-through
- ACL Multistage
- ACL Multiple Ingress
- ACL Schedule
- Per-port and per-VLAN MAC learning limit
- Assign VLANs via Radius attributes (RFC 4675)
- Wake on LAN

3.3 Lot 1: dimensionament i especificacions dels punts d'accés inalàmbrics

i2CAT vol adquirir set punts d'accés inalàmbrics per a donar connectivitat WiFi a les oficines d'i2CAT situades a l'edifici Nexus. Per maximitzar les prestacions de baixa latència, màxim rendiment i facilitar la gestió dels mateixos, tot el hardware ofertat haurà de ser del mateix fabricant. Tot el material, connectors i adaptadors necessaris inclosos, ha de ser nou i original del fabricant. Els equips ofertats no poden estar a la llista de End-of-Sale del fabricant.

3.3.1 Característiques generals dels punts d'accés inalàmbrics

Es demana el compliment de les següents especificacions:

- Tots els equips i programaris seran de marca registrada.
- Tot el hardware i software ha de ser nou, sense utilització prèvia.
- Tot el hardware i software ha de ser vigent, trobar-se en període de comercialització del producte, sense que el fabricant n'hagi anunciat la discontinuïtat o la substitució per nous models.
- Tot el hardware i software ha de disposar d'un mínim de 5 anys de suport del fabricant un cop anunciat el fi de la comercialització del producte. Aquest suport ha d'incloure la reparació o substitució d'equips avariats, i el suport i resolució de dificultats amb el programari "firmware" dels equips i el programari de gestió.
- Tot el hardware i software s'ha de gestionar des d'una única plataforma de gestió, que implementi les necessitats de configuració de monitoratge descrits.
- Els punts d'accés inalàmbrics hauran de ser del mateix fabricant que els tallafocs.
- Es requereix suport de tots els estàndards habituals de mercat.
- Cal incloure tot el llicenciament necessari per a totes les opcions demanades.
- Subministrament de tots els materials i accessoris necessaris per a la interconnexió dels commutadors amb els tallafocs i altres equips.
- Tots els equips subministrats procediran del canal formal de distribució i manteniment que tingui el fabricant al país.
- El projecte inclou la implementació d'un model de gestió automatitzada via un paradigma Security Fabric i la implementació d'un model de seguretat proporcionat per la pròpia xarxa.
- En qualsevol lloc on s'anomeni una normativa estàndard cal entendre que també s'accepta com a vàlida una normativa posterior que actualitzi i millori la normativa indicada.

3.3.2 Característiques radio dels punts d'accés inalàmbrics

Els punts d'accés inalàmbrics han de venir equipats amb 3 radios com a mínim.

- Característiques de la radio 1
  - Banda de freqüència: 2.4 GHz
  - Ample de banda per canal: 20/40 MHz
  - Modulacions: BPSK, QPSK, 64/256/1024 QAM
  - MIMO: 2 x 2 service
  - Màxima velocitat de dades: 574 Mbps
  - Màxim número de clients concurrents: 512
- Característiques de la radio 2
  - Banda de freqüència: 5.0 GHz

- Ample de banda per canal: 20/40/80/80+80 MHz
- Modulacions: BPSK, QPSK, 64/256/1024 QAM
- MIMO: 2 x 2 service
- Màxima velocitat de dades: 1201 Mbps
- Màxim número de clients concurrents: 512

- Característiques de la radio 3
  - Banda de freqüència: 2.4GHz, 5.0GHz i 6.0GHz
  - Ample de banda per canal: 20/40/80/160MHz
  - Modulacions: BPSK, QPSK, 64/256/1024 QAM
  - MIMO: 2 x 2 service i escanejat de freqüències
  - Màxima velocitat de dades: 2401 Mbps
  - Màxim número de clients concurrents: 512

3.3.3 Connectivitat i característiques físiques

Els punts d'accés inalàmbrics han de tenir com a mínim (per equip):

- 1 port de consola.
- 1 port USB.
- 1 port GE RJ45

3.3.4 Networking i seguretat

Els punts d'accés inalàmbrics han de suportar els següents protocols de l'IEEE: 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.11ax, 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az, 802.3bz.

També han de proporcionar les següents funcionalitats:

- Power over Ethernet (PoE)
- Suport per a diversos tipus de SSID: Local-Bridge, Mesh i Tunnel.
- OFDMA
- UL-MU-MIMO
- DL-MU-MIMO
- Enhanced Target Wake Time (TWT)
- Reús espacial (BSS Coloring)
- Capacitats de monitorització inalámbrica
  - Analitzador d'espectre
  - Analitzador de paquets

Finalment, els punts d'accés inalàmbrics han de tenir suport pels següents mètodes d'autenticació:

- WPA, WPA2, i WPA3 with 802.1x o clau prèviament compartida
- WEP
- Portal Web Captiu
- Llista de MACs bloquejades i permeses

3.4 Lot 1: Plataforma de gestió i d'anàlisi de registres dels equips de comunicacions

i2CAT vol adquirir una plataforma d'operació de xarxa que permeti centralitzar i automatitzar la gestió dels equips descrits en les seccions 3.1, 3.2 i 3.3 d'aquest document; així com millorar la capacitat d'anàlisi dels registres reportats pels mateixos.

3.4.1 Característiques generals de la plataforma de gestió

- *Gestió dels equips*. Gestió centralitzada a través d'una consola única dels equips tallafocs, commutadors de distribució, commutadors d'accés i punts d'accés inalàmbrics.
- *Visibilitat*. Quadres de comandament avançats per a facilitar les operacions i la seguretat a la xarxa.
- *Desplegament i manteniment*. Capacitat d'interactuar amb el sistema de gestió a través d'API o línea de comandes (Command Line Interface, CLI).
- *Automatització i integracions*. Capacitat d'automatitzar la resposta a esdeveniments determinats. Capacitat d'integració amb la eina de gestió de registres i altres eines.
- *Accés basat en rols*. Control d'accés basat en rols, que limiten la visibilitat i capacitat d'operació segons el tipus d'usuari.

3.4.2 Característiques generals de l'eina d'anàlisi de traces

- *Emmagatzematge de registres*. Emmagatzematge centralitzat dels registres de tots els equips de comunicacions descrits en aquest document.
- *Generació d'informes*. Eines de generació d'informes adaptables, que incloguin alguns informes de seguretat pre-configurats per diversos estàndards.
- *Correlació de dades*. Correlació de dades dels registres provinents de diversos equipaments per tal d'identificar anomalies i situacions de risc.
- *Capacitats de visualització*. Capacitats avançades de visualització dels equips de comunicacions que envien registres a l'eina, en temps real.
- *Accés basat en rols*. Control d'accés basat en rols, que limiten la visibilitat i capacitat d'operació segons el tipus d'usuari.

3.5 Lot 2: dimensionament i especificacions dels serveis SASE

i2CAT vol contractar un servei SASE per a 250 usuaris que inclogui les funcionalitats de ZTNA i SWG. La contractació del servei tindrà una duració de 3 anys.

3.5.1 Característiques generals del servei SASE

Es demana el compliment de les següents especificacions:

- Latència màxima des de la xarxa informàtica d'i2CAT al PoP (Point of Presence) més proper del proveïdor SASE de 40 ms.

- En cas que el servei SASE deixi d'estar disponible a través del PoP més proper a i2CAT, el servei es prestarà automàticament des d'un altre PoP del proveïdor, encara que es degradi la qualitat del servei degut a possibles augments de la latència. Tan aviat com el PoP més proper es recuperi, el servei s'ha de tornar a prestar des d'aquest PoP.
- S'ha de poder conectar el tràfic de dades sortint i entrant de la xarxa d'i2CAT al PoP del proveïdor SASE a través de tunels IPsec.
- El processament i emmagatzematge de la informació recollida pel servei SASE ha de realitzar-se en centres de dades localitzats a Europa.
- El proveïdor ha d'oferir un entorn consistent per als diversos components que formen el servei SASE: ZTNA i SWG. Les funcionalitats han d'estar ben integrades i no funcionar com a components independents molt poc acoblats.
- La gestió del servei ha de permetre la configuració de polítiques de seguretat dels dos components així com la visualització de la informació sobre usuaris, recursos, amenaces, dades i aplicacions a través d'una finestreta única.
- Els usuaris han de poder accedir al servei SASE a través d'un únic client que integri totes les funcionalitats requerides per interactuar amb els components del servei (ZTNA, SWG). Aquest client ha de suportar els sistemes operatius Windows, Mac OS, iOS i Android.
- El client d'accés al servei SASE s'ha de poder distribuir als dispositius utilitzats pels empleats d'i2CAT (ordinadors portàtils, tablets i telèfons mòbils) a través de l'aplicatiu Microsoft Intune.
- Tot i que no formi part dels serveis contractats en la licitació actual, el proveïdor del servei també ha d'oferir en el seu portfoli serveis de SD-WAN (Software Defined Wide Area Network), Cloud Access Security Broker (CASB) i Data Loss Prevention (DLP), per si i2CAT decideix utilitzar-los en potencials futurs contractes.
- Logs (registres d'activitat). Emmagatzematge de registres d'activitats i esdeveniments relatius a l'ús i operació del servei durant 30 dies com a mínim. Possibilitat d'exportar de forma automàtica els registres d'activitat a sistemes d'emmagatzematge externs o a sistemes de gestió d'informació o esdeveniments de seguretat.

3.5.2 Característiques específiques del servei ZTNA

El servei de ZTNA ha de proporcionar un accés segur dels usuaris autenticats i autoritzats a aplicacions privades que s'executin en recursos allotjats a la xarxa informàtica d'i2CAT o en un Cloud públic.

Es demana el compliment de les següents especificacions:.

- Suport de Single Sign-On (SSO) a través del protocol SAML per a autenticar l'usuari utilitzant proveïdors d'identitat externs al proveïdor del servei SASE.
- Control d'accés contextual, basat en la identitat de l'usuari i en la postura de seguretat del dispositiu des d'on s'està connectant. Com a mínim, s'ha de donar la possibilitat de fer les següents comprovacions:
    - Execució d'aplicacions determinades al dispositiu.
    - Número de sèrie del dispositiu.
    - Encriptació dels discs durs del dispositiu.

- Presència d'arxius determinats al dispositiu.
- Execució d'un firewall al dispositiu.
- Execució d'un antivirus al dispositiu.
- Tipus i versió del sistema operatiu del dispositiu.

- Els administradors del sistema han de poder decidir quines aplicacions privades han d'estar disponibles als usuaris.
  - Com a mínim s'ha de poder accedir a les aplicacions privades utilitzant els protocols HTTP, HTTPS, SSH, RDP, FTP i Telnet.
  - S'han de poder associar polítiques de seguretat diferents a cada aplicació o grups d'aplicacions.
  - En cas de necessitar la instal.lació de programari "on-premise" per a gestionar l'accés a les aplicacions privades:
    - La operació i manteniment d'aquest programari ha de ser el més automatitzada possible.
    - El rendiment d'aquest programari no ha de perjudicar el rendiment nadiu de les aplicacions privades a les quals ofereix accés; ni en termes de capacitat de processament de tràfic (Mbps) ni en termes de capacitat d'acceptar noves connexions.
  - S'ha de poder configurar l'accés tant a aplicacions privades específiques com a sub-xarxes de la xarxa informàtica d'i2CAT.
- Accés a aplicacions o sub-xarxes específiques basat en polítiques de seguretat (complint el principi de mínim privilegi). Les polítiques de seguretat han de permetre:
  - La definició de múltiples regles per política.
  - La inclusió de paràmetres tant d'identitat de l'usuari com de la postura de seguretat del seu dispositiu com a variables de les regles per cada política.
  - L'aplicació de la política tant a usuaris individuals com a grups d'usuaris.
- Suport d'accés a usuaris sense client instal.lat en el seu dispositiu, a través del navegador.
  - Usuaris externs a i2CAT.
  - Usuaris interns a través de dispositius personals.
- Suport de "split-tunnel" per aplicació, per a poder decidir quin tràfic de cada aplicació del dispositiu connectat va a través del proveïdor SASE i quin no.
- El servei ha d'oferir una sèrie de dades sobre: i) el tràfic destinat a cada aplicació; ii) els usuaris que hi accedeixen així com iii) alertes quan hi hagi violacions de les polítiques de seguretat.

3.5.3 Característiques específiques del servei SWG

El servei de SWG ha de proporcionar capacitats per a prevenir el malware, detectar amenaces avançades, filtrar llocs web per categoría, i controlar l'accés a aplicacions i serveis d'Internet per qualsevol usuari, localització o equip.

Es demana el compliment de les següents especificacions:

- Filtratge DNS, amb les següents característiques:
  - Visibilitat del tràfic DNS produit pels usuaris de la xarxa informàtica d'i2CAT.

    - Polítiques flexibles per usuari, grups, destí, postura de seguretat, etc.
    - Identificació de nous dominis registrats i observats.
    - Protecció contra amenaces sobre el DNS, tals com DNS tunneling.
- Inspecció de tràfic TLS sense que aquesta impacti en l'experiència d'usuari.
- Identificació, classificació i bloqueig de llocs web maliciosos que suposin amenaces pels usuaris, com:
    - Llocs que allotgen malware o altres continguts maliciosos.
    - Llocs coneguts pel fet de que roben informació personal (phishing).
    - Llocs que generen spam.
    - Llocs que allotgen o distribueixen codi que mostra anuncis indesitjats o recopilen informació de l'usuari sense avisar (spyware).
    - Llocs que minen criptomonedes robant recursos computacionals de l'usuari.
    - Llocs que suplanten o imiten marques reals.
- La classificació de llocs maliciosos ha de ser automàtica i s'ha d'anar actualitzant en temps real.
- Classificació de llocs webs en diverses categories de continguts, que permetin definir polítiques d'accés acceptable.
    - Polítiques flexibles per usuari, grups, destí, postura de seguretat, etc.
- Capacitat de detecció i classificació de milers d'aplicacions SaaS i IaaS a les quals els usuaris de la Fundació i2CAT estiguin accedint.
- Capacitat de creació de polítiques de seguretat que apliquin a una o múltiples aplicacions SaaS / IaaS.

Tot i no ser un requeriment essencial, es valorarà positivament les següents característiques del servei SWG:

- Capacitat d'especificar polítiques d'accés a Internet basades en atributs d'identitat de l'usuari que s'hi vol connectar. Aquests atributs s'obtenen a través de SAML quan l'usuari s'autentica, i poden ser els següents: grups als que pertany l'usuari, nom de l'usuari, correu de l'usuari, atributs continguts en les assercions de SAML.

4. Serveis de manteniment i d'assistència al desplegament

4.1 Model funcional

4.1.1 Abast i objectius

L'abast de la present contractació contempla la provisió i gestió dels serveis de manteniment per un període de 5 anys en el lot 1, i de 3 anys en el lot 2. El servei s'ha de proveir en horari 24x7 en tot allò que s'esdevingui necessari pel funcionament de la xarxa informàtica d'i2CAT. Tot i això, l'experiència històrica en el funcionament de la xarxa informàtica d'i2CAT i el tipus d'activitat del centre - recerca i innovació - hauria de fer molt improbables les actuacions en horari nocturn o de cap de setmana.

L'abast de la present contractació contempla la provisió i gestió dels serveis de manteniment per un període de 5 anys en el lot 1, i de 3 anys en el lot 2. A continuació es descriuen els principals aspectes del servei de manteniment licitat pels dos lots.

Lot 1: Adquisició, suport i manteniment d'equipament de comunicacions de la xarxa informàtica d'i2CAT. El servei de manteniment inclou:

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

El servei de suport al desplegament inclou:

- Assistència al disseny de l'arquitectura seguida en el desplegament dels equipaments.
- Formació inicial del personal que ha d'operar els equipaments.
- Atenció a dubtes i consultes sobre el desplegament, posada en marxa i operació de l'equipament.

Els sistemes als que es fa referència són:

- Equipament de tallafocs (punt 3.1 d'aquest document).
- Equipament de commutació (punt 3.2 d'aquest document).
- Equipament dels punts d'accés inalàmbrics (punt 3.3 d'aquest document).
- Els sistemes de gestió i anàlisi de traces (punt 3.4 d'aquest document).

Lot 2: Desplegament, operació i manteniment d'un servei SASE (Secure Access Service Edge) per a la xarxa informàtica d'i2CAT. El servei de manteniment inclou:

- Contractació de les garanties necessàries amb els proveïdors del servei per garantir el correcte funcionament del mateix: suport a incidències, actualització

del programari tant per corregir incidències o defectes de seguretat com per evolució del servei.
- Resolució d'incidències en el funcionament del servei.
- Atenció a dubtes i consultes sobre el funcionament del servei.

El servei de suport al desplegament inclou:

- Formació inicial del personal que ha d'operar els equipaments.
- Atenció a dubtes i consultes sobre el desplegament, posada en marxa i operació del servei.

Els servei als que es fa referència és:

- Servei de SASE (punt 3.5 d'aquest document).

4.1.2 Descripció del servei

A continuació es detallen les prestacions incloses en el contracte, per cada lot.

Lot 1: Adquisició, suport i manteniment d'equipament de comunicacions de la xarxa informàtica d'i2CAT. Detall de les prestacions incloses en el contracte:

- Resolució d'incidències en el funcionament dels sistemes (2on i 3er nivell). Inclou avaries. Es requereix:
  - Atenció a incidències greus (o crítiques) enteses com les que impedeixin el correcte funcionament de la xarxa informàtica d'i2CAT o del treball d'una majoria dels usuaris.
  - Atenció a la resta d'incidències
  - Capacitat de diagnòstic remot.
  - Capacitat de presència in-situ en cas de ser necessari.
  - Informació de l'estat de les incidències en curs.
  - Gestions amb els fabricants.
- Contractació, inclosa en el preu del projecte, amb els fabricants de les garanties necessàries per assegurar el correcte funcionament de tot l'equipament:
  - Reparacions o substitucions.
  - Suport a incidències.
  - Actualització del programari per corregir incidències o defectes de seguretat.
  - Actualitzacions de programari per motius evolutius compatibles amb el hardware actual.
  - El manteniment de programari ha d'incloure dret a noves versions "major releases".
  - La contractació al fabricant de garanties pot ser amb temps de resolució de l'avaria NBD, sempre que el licitador garanteixi amb els seus mitjans la resolució de les incidències amb nivell de resposta inferior a aquest termini.
- Atenció a dubtes i consultes sobre els sistemes.
- Actualització del programari dels sistemes (actualitzacions compatibles amb el hardware actual). S'ha de garantir l'accés a actualitzacions de programari dels sistemes fins al final del temps de vida útil de l'equip.

- Planificació conjunta amb i2CAT segons necessitats i avaluació de riscos.
- Es considera inclòs en el preu d'aquest contracte un mínim d'una actualització anual amb motiu de la posada al dia del desplegament a i2CAT; i tantes actualitzacions com siguin necessàries per motius de seguretat, estabilitat o garanties de funcionament de la xarxa informàtica d'i2CAT.
- Administració dels sistemes (2on i 3er nivell)
    - Tasques d'administració avançada per canvis no estàndard, (no habituals en el dia a dia de la xarxa informàtica d'i2CAT).
    - A efectes estimatius, la previsió de consum d'aquest servei és de dues ocasions anuals. Això no és un compromís de volum màxim, només és una estimació del que pot fer falta.
- Suport inicial al desplegament dels sistemes
    - Suport al disseny i validació de l'arquitectura de desplegament.
    - Suport a dubtes sobre configuració i operació dels equips.
    - Formació inicial del personal que operarà els equips.
- Coordinació i reporting del servei.

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

Lot 2: Desplegament, operació i manteniment d'un servei SASE (Secure Access Service Edge) per a la xarxa informàtica d'i2CAT. Detall de les prestacions incloses en el contracte.

- Resolució d'incidències en el funcionament del servei (2on i 3er nivell). Es requereix:
    - Atenció a incidències greus (o crítiques) enteses com les que impedeixin el correcte funcionament de la xarxa informàtica d'i2CAT o del treball d'una majoria dels usuaris.
    - Atenció a la resta d'incidències
    - Capacitat de diagnòstic remot.
    - Capacitat de presència in-situ en cas de ser necessari.
    - Informació de l'estat de les incidències en curs.
    - Gestions amb els proveïdors del servei.
- Contractació, inclosa en el preu del projecte, amb els proveïdors del servei de les garanties necessàries per assegurar el correcte funcionament del servei SASE:
    - Suport a incidències.
    - Actualització del programari que implementa el servei per corregir incidències o defectes de seguretat.
- Atenció a dubtes i consultes sobre el servei.
- Planificació conjunta amb i2CAT segons necessitats i avaluació de riscos.
- Administració dels sistemes (2on i 3er nivell)
    - Tasques d'administració avançada per canvis no estàndard (no habituals en el dia a dia de la xarxa informàtica d'i2CAT).
    - Resolució de dubtes sobre funcionalitats i configuracions del servei.
- Suport inicial al desplegament del servei SASE
    - Suport al disseny i validació de l'arquitectura de desplegament del

servei.
    - Suport a dubtes sobre configuració i operació del servei.
    - Formació inicial del personal que operarà el servei.
- Coordinació i reporting del servei.

4.1.3 Manteniment

L'empresa adjudicatària, un cop confirmada la contractació i a petició d'i2CAT, haurà de presentar proves de la contractació, pel seu compte, de les garanties que aquest plec requereix contractar als fabricants. L'incompliment d'aquesta condició es considerarà incompliment del servei.

A continuació es detallen les prestacions incloses en el contracte, per cada lot.

Lot 1: Adquisició, suport i manteniment d'equipament de comunicacions de la xarxa informàtica d'i2CAT.

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

- La reparació d'un equip o de qualsevol dels seus components no comportarà en cap cas disminució de prestacions ni de fiabilitat.
- L'empresa adjudicatària haurà de garantir la provisió de qualsevol classe de recanvis. Si resultés impossible, s'haurà de plantejar en la seva oferta solucions alternatives, com canvi d'equips, per al que es requerirà l'acceptació prèvia per part d'i2CAT.
- En cas de fallada lògic o desconfiguració dels equips, l'empresa adjudicatària ha de garantir una ràpida resolució de la incidència.

4.2 Model organitzatiu

Les empreses concursants hauran de presentar les seves propostes de model organitzatiu per al desenvolupament del servei, garantint la coherència i compatibilitat amb el model organitzatiu de la Fundació i2CAT.

4.2.1 Recursos humans

L'empresa adjudicatària haurà de garantir no ocupar llocs en aquest servei amb personal d'Empreses de Treball Temporal (fora de campanyes puntuals que no superin els tres mesos continuats i amb tasques i formació molt específiques).

L'empresa adjudicatària serà responsable de substituir al personal del servei per malaltia, vacances, permisos o qualsevol altra circumstància sense que això afecti al compliment dels objectius d'atenció i funcionament establerts.

Qualsevol incompliment d'aquestes condicions pot estar subjecta a penalitzacions en la facturació del servei.

4.2.2 Perfils i rols de servei

Perfils i rols que l'empresa adjudicatària ha de disposar per poder prestar els serveis. Estan definits com a:

P1L1: Enginyer/a de xarxes (lot 1).

P1L2: Enginyer/a de ciberseguretat (lot 2).

P2: Responsable Tècnic/a del servei (comú als dos lots).

P1L1. Enginyer/a de xarxes (lot 1). Persona/es suficient/s per arribar als acords de nivell de servei exigits, que s'encarreguen d'executar les tasques del Lot 1 descrites en la secció 4.1.2 d'aquest document. En cas necessari, escalen o deriven al/la responsable tècnic/a del servei.

Les seves tasques i responsabilitats son:

- La resolució d'incidències en el funcionament dels sistemes (2on i 3er nivell). Inclou avaries.
- Atenció a dubtes i consultes sobre els sistemes.
- Actualització del programari dels sistemes.
- Planificació conjunta amb i2CAT segons necessitats i avaluació de riscos.
- Administració dels sistemes (2on i 3er nivell).
- Suport inicial al desplegament dels sistemes.

P1L2. Enginyer/a de ciberseguretat (lot 2). Persona/es suficient/s per arribar als acords de nivell de servei exigits, que s'encarreguen d'executar les tasques del Lot 2 descrites en la secció 4.1.2 d'aquest document. En cas necessari, escalen o deriven al/la responsable tècnic/a del servei.

Les seves tasques i responsabilitats son:

- Resolució d'incidències en el funcionament del servei (2on i 3er nivell).
- Atenció a dubtes i consultes sobre el servei.
- Planificació conjunta amb i2CAT segons necessitats i avaluació de riscos.
- Administració dels sistemes (2on i 3er nivell).
- Suport inicial al desplegament del servei SASE.

P2. Responsable tècnic/a del servei. Persona amb experiència en tasques de gestió i coordinació de serveis. S'encarrega de la relació amb el fabricant d'equipaments (lot 1) o proveïdor de serveis SASE (lot 2), d'aquest document i de la gestió del servei de manteniment proporcionat a i2CAT.

Les seves tasques i responsabilitats son:

- Contractació, inclosa en el preu del projecte, amb els fabricants de les garanties necessàries per assegurar el correcte funcionament de tot l'equipament (Lot 1).
- Contractació, inclosa en el preu del projecte, amb els proveïdors del servei de les garanties necessàries per assegurar el correcte funcionament del servei

SASE (Lot 2).

- Gestió de la prestació del servei per complir els objectius i nivells de servei acordats i establerts en els SLAs.
- Realització de la coordinació dels serveis associats en aquest contracte amb el Responsable designat per i2CAT.
- Actuació com a referent del Contractista per facilitar la comunicació amb les diferents àrees involucrades en la prestació del servei.
- Assegurament de la gestió eficient dels problemes, assegurant que es segueixen els procediments d'escalat acordats.
- Gestió d'ampliacions o revisions en els serveis, dintre de l'abast del contracte.
- Informació del servei proporcionat en base a estadístiques exactes i actualitzades.
- Establiment i assegurament del compliment dels nivells de qualitat acordats i manteniment d'una actitud proactiva per tal de suggerir iniciatives que incideixin en la millora continuada del servei.
- Establiment d'un procediment de revisió regular del servei que asseguri que tots els assumptes del servei es tracten de forma eficient i dintre del temps requerit.
- Gestió dels assumptes propis del servei.
- Coordinació dels departaments interns del contractista afectats.
- Coordinació dels diferents fabricants o proveïdors de serveis afectats.

4.2.3 Vacances

Amb independència de quan es facin les vacances, caldrà garantir que l'equip restant estarà correctament dimensionat per tractar la demanda del període en qüestió.

Les vacances es comunicaran a la Fundació i2CAT, com a mínim, 30 dies abans que es produeixin per tal de coordinar-les amb els recursos interns i garantir que es compleixen els requisits dels serveis.

4.3 Condicions de prestació de servei

4.3.1 Pla de desplegament

Els serveis objecte de la present licitació hauran d'estar operatius en un termini màxim d' 1 mes a comptar des de la formalització del contracte. Un cop iniciada la prestació del servei, el pla de desplegament ha de permetre complir amb els terminis especificats en la secció 1.4 d'aquest document.

4.3.2 Model de relació

El model de relació és el mateix pels dos lots. Per part del contractista es nomenarà un "Responsable Tècnic/a del Servei", amb les responsabilitats detallades en la secció 4.2.2 d'aquest document.i

Per part d'i2CAT es nomenarà un "Responsable de Gestió del Servei", encarregat de:

- Assegurar que el Contractista compleix les seves obligacions contractuals.

- Assegurar el compliment dels nivells de servei pactats.
- Assegurar la disponibilitat i el seguiment dels procediments de seguiment de resultats i gestió del contracte.
- Donar suport davant i2CAT en l'especificació de qualsevol requeriment de servei addicional i possibles canvis d'abast.
- Mantenir una preocupació proactiva pels objectius, millores tècniques i estratègiques del contracte.
- Negociar possibles renovacions o ampliacions del contracte.
- Resoldre de forma satisfactòria qualsevol assumpte de facturació o comptabilitat que pogués sorgir.

4.3.3 Acord de Nivell de Servei

Els Acords de Nivell de Servei (SLA) són d'obligat compliment. En cas d'incompliment s'aplicaran de manera automàtica les penalitzacions pactades. i2CAT es reserva el dret de realitzar auditories periòdiques dels paràmetres SLA presentats, ja sigui amb personal propi o amb l'ajuda de tercers. L'adjudicatari es compromet a col·laborar amb els mitjans necessaris.

El servei es prestarà amb els següents nivells mínims:

- Resolució incidències greus o crítiques
  - Horari de cobertura: 24x7
  - Temps d'atenció màxim: 5 minuts
  - Temps de resposta màxim: 1 hora
  - Temps de resolució màxim: 8 hores
- Resolució incidències no crítiques i reparacions
  - Horari de cobertura: 10x5
  - Temps d'atenció màxim: 1 hora
  - Temps de resposta màxim: 4 hores
  - Temps de resolució màxim: Dia següent
- Atenció de dubtes i consultes
  - Horari de cobertura: 10x5
  - Temps d'atenció màxim: 4 hores
  - Temps de resolució màxim: Dia següent
- Atenció de sistemes (2on nivell)
  - Horari de cobertura: 10x5
  - Temps d'atenció màxim: 4 hores
  - Temps de resolució màxim: Dia següent

4.3.4 Horaris i terminis

Els horaris de cobertura son els indicats al quadre de SLA per cada tipologia d'activitat del servei (secció 4.4 d'aquest document).

4.3.5 Pla de seguiment

Els responsables de la xarxa informàtica d'i2CAT i el contractista de cada lot mantindran els contactes necessaris per assegurar la coordinació d'actuacions, la

millora de servei i l'atenció immediata de incidències del procés de servei.

El contractista de cada lot remetrà al Gestor del Servei d'i2CAT un reporting mensual del nombre d'incidències, temps mig de resolució i compliments d'SLA.

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

4.3.6 Devolució del servei

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

Així mateix en el cas del lot 1 i2CAT es reserva el dret a, un cop finalitzat el termini del servei, a exigir la retirada dels equips i/o cablejats utilitzats en la prestació del servei sense considerar cap contraprestació, dret adquirit, reclamació o indemnització.

5. Prevenció de riscos laborals

Tant l'empresa o empreses adjudicatàries com les empreses subcontractades o treballadors autònoms contractats per aquestes compliran en el desenvolupament de les seves funcions amb els requeriments legals que marca la Llei 31/1995 de Prevenció de riscos laborals i amb el R.D 171/2004, de coordinació d'activitats empresarials, en cada cas.

La empresa o empreses adjudicatàries informaran amb suficient antelació a l'àrea de People & Talent d'i2CAT (recursoshumans@i2cat.net) cada vegada que subcontractin treballs que es realitzaran a i2CAT, amb una altra empresa o treballador autònom, indicant la forma de coordinació preventiva establerta entre ells.

La empresa o empreses adjudicatàries complien també amb el procediment de coordinació d'activitats empresarials vigent a i2CAT en tot allò que li sigui aplicable.

En cas de que un treballador de la empresa o empreses adjudicatàries pateixi un accident de treball mentre desenvolupa els serveis contractats per i2CAT, la empresa o empreses adjudicatàries informaran així mateix a l'àrea de People & Talent d'i2CAT amb la major brevetat possible.

6. Mesures de protecció ambiental

A més de les accions de reutilització, reciclatge o eliminació adequades associades a la retirada dels embalatges, la empresa o empreses adjudicatàries es comprometen a respectar la normativa vigent al respecte, ja sigui de caràcter estatal, autonòmic o local en la recollida i reciclatge de qualsevol residu i component que puguin resultar de les actuacions del servei prestat a i2CAT.

Barcelona, 27 de juliol de 2023

l'Òrgan de contractació

Sr. Josep Paradells Aspas
Director

Sr. Joan Manel Martín Almansa
Director executiu