PLEC DE PRESCRIPCIONS TÈCNIQUES

(Codi de l'expedient: 2025-CREAF-AS-006-ES100001)

1. INTRODUCCIÓ: SITUACIÓ ACTUAL I NECESSITATS

El Centre de Recerca Ecològica i Aplicacions Forestals (CREAF) es troba físicament a l'edifici C de la Universitat Autònoma de Barcelona (UAB), i actualment està connectat a la xarxa d'Internet de la pròpia universitat.
Arran de l'atac informàtic de l'octubre del 2021, la UAB està reestructurant la seva xarxa per tal d'incrementar la seva seguretat. En aquest context, la UAB ha demanat a tots el centres que tenen la seva seu al campus de Bellaterra que han de dotar-se d'una connexió de xarxa pròpia i independent.
El nostre centre es connectarà al node Vallés ubicat al campus de la UAB, cosa que permetrà una integració eficient i segura amb la infraestructura de xarxa existent a la regió. Aquest contracte busca assegurar que la xarxa local compleixi els estàndards més alts de rendiment, fiabilitat i seguretat, facilitant així les activitats de recerca, acadèmiques i administratives de la nostra institució.
L'objectiu d'aquest document és establir els requeriments i les especificacions tècniques per a l'adquisició de tota l'electrònica de xarxa necessària per dotar al CREAF d'una xarxa local (LAN) que ens proporcioni connectivitat a Internet, dins l'Anella Científica, garantint així l'autonomia i la seguretat de les nostres comunicacions.

2. OBJECTE I DESCRIPCIÓ BÀSICA DE LA PRESTACIÓ

EL CREAF necessita substituir tota l'electrònica de xarxa actual, propietat de la UAB, i crear la seva pròpia xarxa de connexió a Internet. El contracte preveu la instal·lació de diferents equips d'electrònica de xarxa als espais de treball del CREAF, amb la tipologia i nombre d'equips descrits més endavant. Aquest equipament queda distribuït en 2 grans espais:

- Seu principal CREAF a la Facultat de Ciències de la UAB (inclou el mòdul CM7):
  - Tallafocs (enrutador amb Firewall): 2 unitats. Han tenir les característiques tècniques suficients per donar servei al total de connexions de la seu, amb un nombre aproximat de 350 usuaris i uns 50 servidors. Els 2 tallafocs han de poder treballar en alta disponibilitat (HA, High Availability).
  - Commutadors amb un mínim de 48 ports POE (Switchos): 8 unitats.
  - Punts Accés WI-FI (AP): 9 unitats.
  - Tot el cablejat (*) i mòduls transceptors SPF necessaris.
  - Sistemes d'Alimentació Ininterrompuda per protegir els 2 tallafocs.

- Seu coworking "Paranoia Hub" del Carrer Estació a Cerdanyola del Vallès:
  - Tallafocs (enrutador amb Firewall): 1 unitat. Ha tenir les característiques tècniques suficients per donar servei al total de connexions de la seu, amb un nombre aproximat de 50 usuaris.
  - Commutadors amb un mínim de 48 ports POE (Switchos): 1 unitat.
  - Punts Accés WI-FI (AP): 2 unitats.
  - Tot el cablejat (*) i mòduls transceptors SPF necessaris.
  - Sistemes d'Alimentació Ininterrompuda per protegir el tallafocs.

(*) Només cablejat de l'interior del rack.

Detall de la distribució dels equips als diferents espais:

SALA RACK PRINCIPAL – DESPATX C5/1082	
Tallafocs (enrutador amb Firewall)	2 unitats
Commutadors 48 ports POE (Switchos)	4 unitats
Punts Accés WI-FI (AP)	3 unitats
SALA RACK SECUNDÀRIA – DESPATX C5b/026	
Commutadors 48 ports POE (Switchos)	3 unitats
Punts Accés WI-FI (AP)	5 unitats
MÒDUL CM7	
Commutadors 48 ports POE (Switchos)	1 unitat
Punts Accés WI-FI (AP)	1 unitat
COWORKING CERDANYOLA DEL VALLÈS	
Tallafocs (enrutador amb Firewall)	1 unitat
Commutadors 48 ports POE (Switchos)	1 unitat
Punts Accés WI-FI (AP)	2 unitats

El contracte també contempla els serveis professionals necessaris per a la instal·lació i configuració de tots els equips, la formació dels membres del Servei IT del CREAF i un pla de seguiment i suport durant els mesos posteriors a la instal·lació.

3. REQUERIMENTS TÈCNICS DELS EQUIPS

La proposta ha d'estar basada en una plataforma de switching integrada, que compleixi amb les següents característiques bàsiques:

- Que permeti una gestió unificada de tots els dispositius inclosos (firewall, switchos i Access Point WIFI) des de la GUI del firewall.
- Els equips han de ser en format "Appliance físic" d'un únic fabricant, quedant exclosos màquines virtuals i servidors de propòsit general, i han de poder ser instal·lats en un rack estàndard de 19'.
- Incloure, durant la totalitat de la duració del contracte, així com les possibles pròrrogues, totes les llicències i subscripcions necessàries per activar, en el cas que sigui necessari, totes les funcionalitats associades als requeriments obligatoris que es llisten a continuació.

3.1. Requeriments obligatoris dels equips de seguretat (firewall)

- La gestió dels equips ha de ser de fàcil ús i intuïtiva, 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. Quedaran excloses aquelles solucions que requereixin una plataforma de gestió externa per gestionar i administrar la solució.
- La solució ha d'incloure funcionalitats de control d'aplicacions, IPS, Antimalware amb Cloud Sandbox inclós, Webfilter, DNS Filter, Antispam, protecció antiDoS i Web Application

Firewall. Totes aquestes funcionalitats han d'incloure les llicències necessàries per tota la durada del contracte.

- Els equips han de disposar de la funcionalitat de Firewalls virtuals per tal de crear entorns completament diferencials.
- La solució de seguretat ha de permetre diferents modes de funcionament, amb la possibilitat de combinar els diferents Firewalls virtuals entre ells: mode transparent, routed i sniffer.
- S'haurà d'incloure a la proposta, dins dels mateixos equips, la funcionalitat d'Auditoria pròpia del Sistema, que com a resultat tingui un indicador o valor numèric de risc, així com puntuació negativa per cada paràmetre auditat no complert. Aquests paràmetres que s'han de comprovar son com a mínim: política de seguretat sense ús en els últims 90 dies, política de contrasenyes dèbils i comprovació del llicenciament/suport.
- La pròpia plataforma ha de tenir connectors automàtics amb l'objectiu d'integrar-se amb identitats terceres i poder recollir informació, adreçament IP, inventari d'objectes i etiquetes. Aquesta funcionalitat haurà d'estar suportada en els equips de seguretat (sense necessitat de consola addicional). En concret es requereixen les següents:
  - Cloud pública: Google Cloud, Azure, AWS, Oracle i AliCloud.
  - Cloud privada: VMware NSX i ESXi, Openstack, Kubernetes, Cisco ACI i Nuage.
  - Fonts d'identitat: Active directory, Microsoft Entra ID i Radius.
  - Fonts d'amenaces: Llistat d'IP, dominis, URLs i hash's de malware customitzats.
- La mateixa solució de seguretat ha de permetre la creació d'automatismes per tal de:
  - Davant la detecció d'un host compromès, els tallafocs enviïn (tots alhora): un email, una notificació tipus push a dispositius smartphone, poder banejar l'adreça IP, invocar funcions AWS Lambda, Google functions, Azure Functions i Webhook.
  - Davant el canvi de configuració del tallafocs, un failover, reboot, actualització de firmes, de forma programada i qualsevol event del tallafocs, aquest enviï (tots alhora): un email, una notificació tipus push a dispositius mòbils e invocar funcions AWS Lambda, Google functions, Azure Functions, AliCloud Function, comanda per CLI i Webhook.
- Capacitat de configuració de Proxy explícit per Interface, amb la funcionalitat de Proxy chaining en cas necessari, a més de capacitat de caching.

- **Hardware i rendiment:**
  - Processadors ASIC SPU amb acceleració per tràfic IPv4/IPv6, CAPWAP, VXLAN, GRE, IPSEC.
  - Protecció anti-DoS per hardware.
  - QoS amb traffic shaping i queuing.
  - Coprocessadors per inspecció de seguretat i tràfic criptogràfic.
  - Suport SNMP, sFlow i exportació de logs per SYSLOG, FTP, SCP, TFTP.

- **Networking:**
  - Protocols: RIP, OSPF, ISIS, BGP, WCCP, Multicast.
  - Dual Stack IPv4/IPv6, NAT (IPv4, NAT64, NAT66).
  - Serveis: DHCP, DNS, NTP, PPPoE, VLANs 802.1Q.
  - Agregació de ports amb LACP.
  - Balanceig de servidors L4 i SSL offloading.
  - SD-WAN amb fins a 256 connexions, 100 health-checks, polítiques intel·ligents.

- **Visibilitat:**
  - Topologies gràfiques físiques i lògiques.
  - Logs agrupats per origen, destí, aplicació, amenaça, etc.
  - Visualització drill-down des de la GUI, en temps real.

- **Seguretat:**
  - Polítiques de seguretat IPv4/IPv6 amb paràmetres detallats.
  - Inspecció de tràfic per nivells 4 i 7.
  - Funcions avançades: antivirus, webfilter, DNS filter, WAF, control d'aplicacions, IPS, DLP.

- Desxifrat SSL selectiu.
- Logging per nivells i captura de paquets.
- Regles DoS per nivells 3 i 4.
- Base de dades de reputació dinàmica contra botnets.

- **Control d'aplicacions:**
  - Identificació de ≥4400 aplicacions.
  - Classificació per categories/subcategories.
  - Identificació en túnels HTTPS.
  - Firmes personalitzades amb protecció IPS i antimalware.

- **IPS:**
  - Protecció de servidors i clients amb ≥11.000 signatures IPS agrupades per categoria, severitat, objectiu i protocol.
  - Captura de tràfic en cas d'atac.
  - Protecció basada en la identificació de patrons d'atacs basats en comportament.
  - Creació de firmes d'IPS personalitzades.

- **Antimalware:**
  - Detecció de malware basat en signatures signatures i mètodes avançats.
  - Sandboxing cloud (fitxers ≥100MB).
  - Eliminació de contingut dinàmic en documents.
  - Verificació per hashing i threat intelligence extern.

- **Webfilter i DNS Filter:**
  - Categorització de pàgines web i dominis DNS per aplicar block, monitor i aplicació de quotes de temps o tràfic per categoria.
  - Base de dades de categories web i dominis DNS (llistats locals i servei cloud en temps real) per tal de tenir la categorització de les URLs el més actualitzat possible.
  - Mode "Safe search" per YouTube i Google.
  - Suport de rating per imatges per URL.
  - Suport per a la creació de llistes blanques/negres externes sense necessitat de llicencia.
  - DNS redirect cap a portals personalitzats.

- **VPN:**
  - Fins a 500 usuaris simultanis SSL VPN.
  - Suport IPSEC VPN (IPv4 i IPv6), PPTP VPN, L2TP VPN, SSL VPN i GRE sobre IPSEC, sense requeriments addicionals de maquinari o mòduls.
  - Modes SSL VPN: accés web i túnel.
  - Agregació i balanceig de túnels VPN.
  - Integració, del mateix fabricant, del doble factor d'autenticació via token mòbil, així com per SMS i correu electrònic, integrat en la mateixa plataforma de seguretat.

- **Logging i reporting:**
  - Monitorització en temps real del trànsit filtrat i històrica amb capacitat de fer informes de 6 mesos aproximadament (incloure llicenciament i suport necessari durant tota la durada del contracte).
  - Informes per adreces, ports, protocols, usuaris i/o grups d'usuaris (AD/LDAP):
    - Analitzar, correlacionar i fer informes de la informació de seguretat de manera centralitzada.
    - Panell de control amb vista general d'usuaris destacables, aplicacions, destinacions, llocs web, vulnerabilitats, etc.
    - Models d'informes preconfigurats, editables, modificables i exportables.
  - Gestió d'esdeveniments amb generació d'alertes automàtiques a administradors.
  - Visor de logs en temps real o històric, que permeti distingir-los entre trànsit, esdeveniments i seguretat. També per dispositiu, dominis d'administració o agregats.

- Capacitat de filtratge i granularitat d'anàlisi de logs.
- Possibilitat de generació d'alertes per nivells de seguretat, esdeveniments específics, accions o destinacions i nombre d'esdeveniments en un determinat temps.
- Capacitat de cercar alertes històriques.
- Notificació d'alertes per correu electrònic, SNMP o syslog.
- Logs descarregables en format TXT.

3.1.1. Seu principal del CREAF (Edifici C, UAB):

Per la seu principal del CREAF, a l'edifici C del Campus de la UAB a Bellaterra, es requereixen 2 routers amb firewall integrat, d'idèntiques característiques:

- Arquitectura d'alta disponibilitat (HA, High Availability) en mode actiu-actiu i actiu-passiu. Sobre l'HA:
  - La transferència de servei d'un equip a l'altre s'ha de poder fer sense talls, ni pèrdua de les connexions TCP, ni aturada de servei.
  - Les configuracions s'han de traspassar de manera automàtica entre els dos equips.
  - Capacitat de funcionament en mode actiu/actiu, sincronitzant sessions entre els dos nodes però mantenint adreçament IP diferenciat en les interfícies de cada node del clúster.
  - En el cas de necessitat de llicenciament o subscripcions per activar l'alta disponibilitat, caldrà que aquestes estiguin incloses en la proposta durant la duració completa del contracte, sense necessitat de llicencies o incloses al contracte en cas que siguin necessàries.

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

- Rendiment del tallafocs (Firewall throughput) ≥ 10 Gbps.
- Capacitat per gestionar fins 1.5 Milions sessions concurrents.
- Latència inferior a 3.23 µs (per paquets 64 byte UDP).
- Capacitat mínima de 5000 polítiques de firewall.
- Rendiment per tràfic SSL VPN mínim de 715 Mbpss 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: 5 Gbps per tràfic Enterprise MIX.
  - Rendiment NGFW (IPS i control d'aplicacions): 1 Gbps .
  - Rendiment amb Threat Protection (Firewall mes IPS, control d'aplicacions i motor antimalware actius): 900 Mbps per tràfic.

- Número de interfícies mínimes per equip:
  - 1 port de consola.
  - 1 port d'USB 3.0 per a la connexió de mòdem 5G i/o pendrive: 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.
  - 2 ports 10GE SFP+
  - 6 ports 1GE
  - 2 ports HA/Gestió dedicats
  - 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.

3.1.2. Espai coworking del Carrer Estació a Cerdanyola del Vallès:

Per l'espai coworking a Cerdanyola del Vallés es requereix 1 router amb firewall integrat, amb els següents requeriments tècnics com a mínim:

- Processador dedicat amb acceleració per maquinari (ASIC/SoC) per inspecció SSL/TLS.
- Rendiment del tallafocs (Firewall throughput): ≥ 5 Gbps.
- Rendiment per tràfic IPSEC VPN (512 bytes): Ample de banda màxim: 4.4 Gbps amb xifrat AES256-SHA256.
- NGFW (Inspecció d'aplicacions): ≥ 800 Mbps.
- Protecció contra amenaces (UTM): ≥ 600 Mbps.
- Memòria: Integrada per logs locals; opcional integració amb gestió en núvol.
- Interfícies de Connexió:
  - Ports Ethernet: mínim 5 ports GE RJ45.
  - Ports WAN dedicats (mínim 1, ideal 2).
  - Suport VLAN: Etiquetatge 802.1Q i subinterfícies.
  - Routing avançat: IPv4/IPv6, OSPF, BGP.

- Funcionalitats de Seguretat:
  - Firewall de nova generació (NGFW).
  - Inspecció profunda de paquets (DPI).
  - Control d'aplicacions i usuaris.
  - IPS/IDS: Prevenció i detecció d'intrusions.
  - Antivirus/Antimalware: Signatures + heurística.
  - Filtrat web per categories i antispam.
  - Inspecció SSL/TLS (incloent TLS 1.3).
  - Protecció contra amenaces avançades: Sandboxing local o en núvol.
  - ZTNA (Zero Trust Network Access) integrat.

- Xarxa i SD-WAN natiu:
  - SLA per enllaç (latència, jitter, pèrdua).
  - Failover automàtic.

- VPN:
  - IPSec site-to-site.
  - SSL VPN per accés remot.

- Gestió i Compliment:
  - Consola web intuïtiva + CLI.
  - Gestió centralitzada (on-prem o núvol).
  - Zero Touch Provisioning (ZTP).
  - Exportació de logs a SIEM (syslog).
  - Compliment normatiu: RGPD, PCI-DSS.

3.2. Requeriments obligatoris dels commutadors (switchos).

La solució proposada ha de garantir una total integració i homogeneïtat amb els equips de seguretat, que permeti gestionar i aplicar polítiques directament des del Tallafocs i gestionar els commutadors també des de l'equip de seguretat. Tanmateix:

- Tots els commutadors oferts han de ser del mateix fabricant que els dispositius de seguretat. Quedaran excloses totes les solucions d'altres fabricants així com solucions alternatives que no facin servir la pròpia gestió webGUI del Tallafocs, com integracions via API i similars.
- Tots els equips han de ser d'última generació i no poden estar a la llista de End-of-Sale del fabricant.

- La solució proposada pels commutadors ha de tenir alta disponibilitat i tolerant a la fallada d'un element qualsevol dels que la composa sense que això suposi una degradació del servei ofert.
- Tot el maquinari ofert constituirà un mateix sistema que donarà servei de connectivitat als ordinadors del CREAF. Per maximitzar les prestacions de baixa latència, màxim rendiment i facilitar la gestió dels mateixos tot el hardware ofert haurà de ser del mateix fabricant. Tot el material, connectors i adaptadors necessaris inclosos, ha de ser nou i original del fabricant.

3.2.1. Característiques i funcionalitats del commutadors (switchos)

La solució proposada haurà de permetre connectivitat ethernet, així com disposar d'una connexió especifica per a configuració, manteniment i monitorització.
Cada equip ofert ha de disposar de com a mínim les següents característiques:

- 48 ports GE/RJ45.
- 4 ports 10GbE SFP+
- Alçada màxima 1U.
- Switching Capacity (Duplex) 176 Gbps
- Packets Per Second (Duplex) 260 Mpps
- Mac Address Storage 32 K
- Network Latency < 1µs
- VLANs Supported 4K
- Link Aggregation Group Size: de 8
- Total Link Aggregation Groups: 16
- Packet Buffers 2MB
- DRAM 512MB DDR3
- FLASH 64MB

Funcionalitats mínimes aplicables tant als commutadors de distribució i d'accés:

- Xarxa i.IPv4 i IPv6:
  - Unicast/Multicast
  - 802.1Q Vlan
  - LACP per la agregació de ports.

- Gestió i administració:
  - Possibilitat de tornar a una configuració anterior (Rollback).
  - Suport de SNMP.
  - Exportació de logs mitjançant FTP, SCP i/o TFTP
  - Log d'esdeveniments
  - DHCP Snooping
  - IP Source Guard
  - DAI Dynamic ARP Inspection
  - Qualitat de Servei (QoS): Per Queue Traffic Shaping i Per Port Traffic Shaping
  - Possibilitat de gestionar a través d'una consola centralitzada, amb accés mitjançant RADIUS
  - Monitorització de tràfic via SPAN i RemoteSPAN (Nivell 2)
  - Mínim de 1023 VLAN configurables
  - Capacitat de detecció automàtica dels dispositius connectats en cada port. Cada switch alimentarà de forma automàtica la base de dades de dispositius dels tallafocs mitjançant integració nativa del propi fabricant.
  - Automatismes per a que els tallafocs puguin posar en quarantena a dispositius infectats o maliciosos bloquejant de forma automàtica a nivell de port d'accés en el switch.

3.3. Requeriments obligatoris dels equips per la xarxa WI-FI

La solució WIFI proposada ha d'oferir un arquitectura única des d'on es pugui realitzar una gestió de tots els Punts d'Accés (AP) i anàlisis de la connectivitat WIFI, dispositius d'usuari, control de accés a la xarxa i seguretat NGFW aplicat a tot l'entorn LAN/WLAN sense necessitat d'afegir components addicionals. La proposta ha de ser sòlida des del punto de vista de la seguretat, connectivitat i experiència de l'usuari i el control d'accés. Es consideren como a requeriments mínims les següents característiques:

- Seguretat:
  - Identificació i control d'aplicacions mitjançant inspecció de nivell 7 per aplicar seguretat i control d'ample de banda:
  - Funcions d'UTM amb Antivirus, filtrat de continguts web, IPS, filtre de correu, sandbox integrat, DLP, control d'accés per DNS.
  - Seguretat Wireless mitjançant WIDS:
    - Unauthorized Device Detection
    - Rogue/Interfering AP Detection
    - Ad-hoc Network Detection and Containment
    - Wireless Bridge Detection
    - Misconfigured AP Detection
    - Weak WEP Detection
    - Multi Tenancy Protection
    - MAC OUI Checking
  - Supressió automàtic i contenció:
    - De Rogue AP connectades en LAN
    - De Rogue AP emetent SSID malintencionat.

- Connectivitat:
  - Solució amb AP d'alta densitat, amb capacitat d'agregar zones i fins a 512 clients connectats en un sol AP.
  - Solució d'alta disponibilitat (HA) sense temps de fallada i recuperació immediata.
  - Els AP han de tenir com a mínim 2 ports ethernet i suportar LACP.
  - Els AP han de disposar d'una freqüència dedicada, a part de les de 2.4 / 5 Ghz, per a la inspecció de la qualitat de l'entorn RF i l'elecció del millor canal en funció dels paràmetres RF com interferències no WIFI, densitat de dispositius…
  - Múltiples opcions de connectivitat incloses en el controlador Wireless sense necessitat d'afegir elements addicionals:
    - Autenticació estàndard WPA2/WPA3
    - Autenticació empresarial WPA2/WPA3 amb autenticació d'usuari mitjançant EAP
    - Autenticació d'usuari mitjançant portal captiu personalitzable.
    - Autenticació de dispositius mitjançant claus compartides dinàmiques, de manera que en un SSID es puguin distribuir diferents claus compartides a dispositius o grups de dispositius.

- Control d'accés:
  - El controlador Wireless haurà de disposar de funcionalitats de control d'accés dinàmic en funció del dispositiu connectat.
  - S'ha de poder realitzar el perfilat dels dispositius mitjançant signatures integrades o bé mitjançant integració cloud amb servei de base de dades de perfils.
  - Es podran aplicar diferents criteris d'accés a la xarxa WLAN en funció de:
    - Fabricant del hardware
    - Tipus de dispositiu
    - Sistema Operatiu
    - Versió de Sistema Operatiu
    - Família de dispositiu
    - Adreces o grup d'adreces MAC

- Els punts d'accés realitzaran les funciones de monitorització i captura de tràfic para poder realitzar el perfilat des del controlador Wireless
- Al aplicar-se una regla de control de accés el controlador podrà aplicar las següents funcions:
  - Assignació de VLAN.
  - Aplicar polítiques de seguretat NGFW específiques.
  - Aplicar polítiques de QoS i traffic Shaping .
  - Accés autentificat mitjançat portal captiu.

3.3.1. Característiques i funcionalitats dels punts d'accés Wireless.

Els punts d'accés Wireless ha d'incloure les següents característiques i funcionalitats sense necessitat d'incloure o afegir llicenciament, software o hardware addicional:

- **Networking:**
  - DHCP server integrat.
  - VLANs: Suport 802.1Q, mapeig de SSID a VLAN, assignació de pool de VLANs i VLANs dinàmiques.
  - Routing: Estàtic, policy routing, VRRP, VRF, RIP, OSPF i BGP.
  - Multicast: PIM mode, conversió de Multicast a unicast, limitació d'ample de banda de multicast i control de fluxos.
  - Tràfic de dades: centralitzat, distribuït, mixta i Split Tunnel.

- **Gestió:**
  - HTTPS via web.
  - SSH, Telnet i consola.
  - SNMP (V1, V2, V3).
  - REST API.
  - Gestió centralitzada (on-premise i SaaS).
  - Control d'accés per gestió local dels AP.
  - Gestió única des del mateix controlador per a la configuració i monitorització de commutadors, punts d'accés, SD-WAN, polítiques de seguretat, proxy i NAT.
  - Gestió centralitzada de múltiples controladores hardware o en màquina virtual mitjançant solució de gestió i anàlisis d'esdeveniments i logs per una major escalabilitat.

- **Monitorització:**
  - Access Point: Estat, uso, interferències.
  - Client: Signal strength, SNR, usuari, IP, tipo de dispositiu, sistema operatiu, consum d'ample de banda por aplicacions, serveis cloud, política de Firewall.
  - Rogue AP.
  - Informació general de l'estat, tendències, dashboards d'ús, estat d'AP, clients, errors de RF.

- **Resolució de problemes:**
  - Captura de paquets des dels punts d'accés, switch o controlador.
  - Diagnòstic de cablejat mitjançant "cable-test".
  - Diagnòstic d'estat d'entorn de RF mitjançant anàlisis d'espectres en bandes de 2,4 / 5 Ghz i detecció d'origen de interferències, ús de canal, espectrogrames mitjançant l'ús de ràdios dedicades als AP.
  - Enviament de tràfic sintètic per analitzar el rendiment WIFI i ample de banda des dels punts de accés sense interferir en el seu funcionament normal.
  - Detecció de la disponibilitat del servei DHCP en cada VLAN-SSID que estigui emetent l'AP.
  - Localització de punts d'accés mitjançant Bluetooth.

- **Suport remot:**
  - Suport remot a tots els AP.
  - Opció d'encriptació del tràfic mitjançant DTLS/IPSec.
  - Acceleració de tràfic encriptat en IPSec mitjançant ASIC específica.
  - Split-tunnel per seleccionar el tipus de tràfic gestionat en local o al controlador.
  - Suport NAT del tràfic local para evitar la configuració de VLANs en remot.

- **Supervivència a fallades:**
  - La connectivitat dels usuaris es mantindrà en cas de caiguda de WAN.
  - Els clients podran seguir autenticant-se por PSK, 802.1x o portal captiu extern.

- **Mesh & Bridging:**
  - Topologia: Red mallada multi-punt.
  - Suport de diverses instàncies mesh per controlador.
  - Mesh Hops: Número de salts Mesh configurable.
  - Detecció automàtica de nodes Mesh.
  - Bridging: Enllaços punt a punt i punt a multi-punt.
  - Gestió centralitzada mitjançant controlador o API.

- **Accés i Autenticació Wireless:**
  - Mètodes de autenticació:
    - IEEE 802.1x (EAP, Cisco-LEAP, PEAP, EAP-TLS,EAP-TTLS, EAP-SIM,EAP-AKA).
    - RFC 2716 PPP EAP-TLS.
    - RFC 2865 RADIUS authentication.
    - RFC 3579 RADIUS support for EAP.
    - RFC 3580 IEEE 802.1x RADIUS Guidelines.
    - RFC 3748 Extensible Authentication Protocol.
    - WEP64 – 64-bit Web Equivalent Privacy.
    - WEP128 – 128 bit WEP.
    - WPA (Wi-Fi Protected Access) Personal & Enterprise:
      - WPA2 (Personal & Enterprise) – 802.11i Standard.
      - Multi-PSK Key Support.
      - Filtrat d'adreces direccions MAC basat en grups d'adreces locals.
      - Autenticació MAC mitjançant RADIUS.
      - Autenticació basada en certificats para BYOD.
    - WPA3 SAE.
    - WPA3 SAE transition.
    - WPA3 Enterprise amb encriptació 128/192 bits y PMF forçat.
    - WPA3 Enterprise amb PMF opcional.
    - OWE (Oportunistic Wireless Encryption)
    - OSEN.
  - Servidors d'autenticació:
    - Bases de dades internes, RADIUS, LDAP, TACACS+.
    - Externs: Microsoft Active Directory, Microsoft IAS RADIUS server, Cisco ACS Server, Free RADIUS, Interlink RADIUS server, Steel Belted Radius.
  - Protocols de encriptació:
    - CCMP/AES
    - TKIP
    - TKIP+AES
    - DTLS or IPSec for CAPWAP
    - L2TP/IPSec (RFC 3193)
    - XAUTH/IPSec
  - VPN:
    - SSL
    - IPSec

- Portal captiu:
  - Autenticació contra el portal captiu extern i interno.
  - Portal personalitzable sense limitacions: modificar el codi HTML, incloure scripts, modificar idioma, etc.
  - Portal d'avís legal
  - Múltiples portals captius per SSID en funció de diferents paràmetres: dispositiu, autenticació, usuari o grup de usuari.
  - Integració amb portals captius externs.
  - Redirecció a web després de l'autenticació.
- Gestió d'usuaris convidats:
  - Usuari restringit per a la gestió d'usuaris convidats mitjançant portal.
  - Temps d'expiració i d'ús personalitzables.
  - Creació massiva d'usuaris de forma automàtica.

- **Gestió de RF i rendiment:**
  - Selecció de canal de emissió i potencia en funció dels paràmetres de RF recollits per l'antena dedicada o de servei dels AP.
  - Suport per 802.11n HT20 & HT40.
  - Suport per 802.11ac 80Mhz.
  - Band Steering: Equilibra les estacions entre les bandes de RF de 2.4GHz i 5GHz per a un rendiment òptim i reduir les interferències.
  - AP Load Balancing: Distribueix els clients uniformement entre els APs en els canals disponibles.
  - Self Healing: Ajusta automàticament els nivells de potència TX per ampliar la cobertura i compensar els APs fallits.
  - RF Planning:
    - Planificació predictiva de RF.
    - Mapes de calor dinàmics en temps real.
    - Site Survey (estudi del lloc).

- **Gestió d'APs maliciosos (Rogue APs):**
  - Escaneig d'APs maliciosos (Background and full-time scanning).
  - On-Wire correlation (Correlació en cable) per identificar APs maliciosos connectats a la xarxa local.
  - Supressió d'APs maliciosos:
    - Supressió automàtica i/o manual configurable.
    - "Over-the-air suppression" dels APs infractors i mesures per evitar que els clients intentin connectar-se a un AP maliciós identificat.
  - Wireless IDS: Detecta i registra múltiples mètodes d'intrusió RF.
  - Event Logging: Syslog de tots els esdeveniments d'APs maliciosos.
  - Auditing: Informes predefinits per al compliment de PCI-DSS.

- **BYOD i Mobilitat:**
  - Identitat del dispositiu:
    - Distingir entre actius corporatius i dispositius propietat dels empleats.
    - Identificar i classificar els tipus de dispositius, informació del fabricant, tipus de sistema operatiu i versions del sistema operatiu.
  - Visibilitat d'aplicacions:
    - Detecció d'aplicacions de Layer 7 amb suport per a més de 3.000 signatures.
    - Capacitat per detectar, prioritzar o suprimir aplicacions.
    - Suport per a Bonjour Gateway.
  - Qualitat de servei:
    - End-to-end QoS.
    - Preservar les etiquetes de QoS a través de la xarxa cablejada i sense fil.
    - CAC – Call Admission Control.
    - Perfils QoS.

    - Prioritització del tràfic crític per al negoci a través de WLAN.
    - Gestionar i aplicar polítiques de tallafocs i modelatge de trànsit basades en la identitat del dispositiu i de l'usuari.
  - Mobility Support:
    - Fast Roaming - 2-3ms between APs on the same router.
    - 802.11i fast-roam back.
    - 802.11i fast-associate in advance.
    - PMK caching.
    - 802.11 k/v/r.
    - OKC.
  - Detecció de presència i analítiques de presència.

- **Suport IPv6:**
  - Suport per clients IPv6.
  - Gestió sobre IPv6.
  - Tràfic: protocols de Routing, firewall i suport UTM.

- **Certificacions:**
  - Wi-Fi Alliance certified: 802.11a/b/g/n/d/h, WPA™ Personal, WPA™ Enterprise, WPA2™ Personal, WPA2™ Enterprise, WMM™, WMM™ Power Save.
  - Firewall: ICSA firewall enterprise certification, ICSA IPv6 certified Firewall, USGv6 certified Firewall
  - IEEE Standard Compliance; 802.11a, 802.11b, 802.11g, 802.11n (2x2 MIMO), 802.11n (3x3 MIMO), 802.11n with Automatic Power Save Delivery (UAPSD), 802.11n with HT40 support, 802.11ac, 802.11e & WME/WMM Multimedia Extensions, Block ACK, NoAck, 4 priority queues, 802.11h, 802.11j, 802.11 k/v/r, 802.11 az, 802.11i (TKIP/AES), 802.1x.
  - Multi-tenancy: Enabling Virtual Domains, Viewing the VDOM list, Global and per-VDOM Settings, Resource Settings, Virtual Domain Licensing, Logging in to VDOMs.

4. Eines de gestió i anàlisis

La proposta ha d'incloure una eina de gestió i anàlisi de registres de seguretat desenvolupada, que centralitzi els registres de tots els dispositius de seguretat dins d'una mateixa plataforma, i que permeti al Servei d'IT del CREAF tenir una visibilitat completa de la xarxa, facilitant la detecció i resposta a incidents de seguretat de manera automatitzada. La proposta ha d'incloure totes les llicències necessàries per a totes les funcionalitats sol·licitades en aquest document i ha d'abastar tota la duració del contracte.

Aquesta eina ha tenir les següents característiques:

- Visibilitat unificada i registre centralitzat: Consolida les dades de registre de múltiples fonts en una sola plataforma, simplificant la gestió i anàlisi. Ofereix una visió consolidada de la seguretat de la xarxa, eliminant colls d'ampolla operatius i reforçant les defenses amb informació històrica i en temps real.
- Detecció i anàlisi de amenaces i gestió proactiva: Utilitza anàlisis avançades i aprenentatge automàtic per identificar patrons i anomalies en el tràfic de xarxa. Permet als equips de seguretat anticipar-se i fer front a les amenaces de manera preventiva.
- Automatització de la resposta a incidents i anàlisis forense: Redueix la complexitat i els costos mitjançant l'automatització de la detecció i resposta a incidents. Proporciona anàlisis detallades per comprendre l'abast i impacte de les violacions de seguretat.
- Compliment normatiu: Simplifica el compliment de regulacions com PCI DSS, HIPAA, NIS2, ENS i GDPR mitjançant informes preconfigurats, facilitant la demostració de compliment durant les auditories i ajudant a identificar vulnerabilitats i configuracions no conformes.

5. Serveis professionals, garanties i suport

A part de l'equipament descrit anteriorment, el contracte ha d'incloure totes les tasques relatives a la instal·lació, configuració, proves de funcionament, documentació tècnica i formació i bossa d'hores de suport que es descriuen en els següents apartats. També la garantia de la contractista estesa a tota la duració del contracte.

5.1. Tasques relatives a la instal·lació i configuració dels equips.

- Instal·lació i configuració dels firewall:
  - Segmentació de la xarxa en VLAN en el cas que fos necessari.
  - Configuració de la xarxa VPN amb Microsoft Entra ID amb sistema d'autenticació MFA.
  - Configuració de IPS.
  - Configuració de polítiques d'accés LAN/WAN.
  - Configuració de SD-WAN.
  - Configuració de HA dels dos equips firewall.
  - Proves de Failover.

- Instal·lació i configuració dels switches:
  - Substitució d'electrònica antiga.
  - Configuració de VLAN's.
  - Configuració dels enllaços entre switches.
  - Etiquetat del cablejat troncal.

- Instal·lació i configuració dels punts d'accés WIFI (AP):
  - Configuració de VLAN's.
  - Substitució de l'electrònica antiga.
  - Creació de mapa de cobertura WIFI.

5.2. Documentació del projecte.

La proposta ha d'incloure una documentació completa i detallada que permeti la comprensió, implementació i manteniment de la nova infraestructura de xarxa. Aquesta documentació ha d'incloure com a mínim:

- Descripció del projecte.
- Especificacions tècniques detallades dels components de la xarxa (routers, switches, firewalls, etc.).
- Aspectes de configuració i paràmetres tècnics.
- Procediments de la seguretat de la xarxa.
- Configuració de mesures de seguretat (VPN, ACL, etc.).
- Guies per a l'ús i gestió dels dispositius de xarxa.
- Metodologies per a la verificació i validació de la instal·lació.

La documentació escrita, els manuals, les guies i informes s'ha d'entregar en format digital i/o paper.

5.3. Seguiment i suport.

La proposta ha d'incloure una pla de seguiment i suport del contracte per garantir el bon funcionament de la xarxa i els equipaments instal·lats. Aquest pla ha d'incloure com a mínim:

- Calendari d'execució del contracte.
- Calendari de reunions de control y seguiment de l'execució.

- Pla de formació al personal d'IT.
- Bossa d'hores de suport (mínim 20 hores) per a la resolució de incidències i consultes un cop finalitzat el projecte.

5.4. Formació al personal del Servei IT de la infraestructura instal·lada.

La proposta ha d'incloure un pla de formació per tots els integrants del Servei IT del CREAF. Aquest pla de formació ha de garantir que el personal del servei IT tingui els coneixements i habilitats necessàries per gestionar, mantenir i optimitzar la nova infraestructura de xarxa instal·lada.

El pla de formació ha de permetre als tècnics del Servei IT del CREAF conèixer tots els components de la xarxa i les seves funcionalitats, procediments de configuració inicial i gestió de dispositius, polítiques de seguretat i configuració de mesures de seguretat, diagnòstic i solució de problemes comuns, eines i tècniques per a la gestió de problemes i procediments per a actualitzacions i manteniment.

5.5. Garantia i suport de la contractista.

La garantia i suport per part de la contractista ha de cobrir tota la duració del contracte i ha d'incloure tots els equips i el software i firmware inclosos en els mateixos.

El suport ha de ser en modalitat 24x7x365 amb temps de resposta màxim de 1 hora per als dispositius crítics com els tallafocs, i NBD (Next Business Day) per als dispositius no crítics.

La contractista ha de donar suport via telefònica i web a través d'una aplicació de gestió d'incidències.

La contractista ha de proporcionar les actualitzacions de firmware i software per a tots els equips durant tota la duració del contracte.

5.6. Certificacions requerides.

Donada la naturalesa del contracte, es requereix que les empreses que es presentin a aquesta licitació disposin obligatòriament de les següents certificacions: ISO 27001 (Sistema de Gestió de Seguretat de la Informació) i l'Esquema Nacional de Seguretat (ENS).

Es valorarà positivament als criteris de puntuació que la licitadora disposi de les següents certificacions: ISO 14001 (Sistema de Gestió Ambiental) i ISO 9001 (Sistema de Gestió de qualitat).

5.7. Gestió ambiental.

L'empresa adjudicatària serà responsable de la gestió correcta de tots els residus que generi durant l'execució del contracte, incloent-hi però no limitant-se a equips electrònics obsolets, embalatges, materials d'instal·lació i qualsevol altre residu derivat de la prestació del servei.

Aquesta gestió haurà de complir amb la normativa vigent en matèria de residus, incloent-hi la Llei 7/2022, de 8 d'abril, de residus i sòls contaminats per a una economia circular, així com el Reial decret 110/2015 sobre residus d'aparells elèctrics i electrònics (RAEE).

L'empresa contactista haurà de:

- Recollir, classificar i transportar els residus a gestors autoritzats.
- Acreditar documentalment la gestió correcta dels residus mitjançant certificats de lliurament a gestor autoritzat.

- Minimitzar l'impacte ambiental mitjançant pràctiques sostenibles, com ara la reutilització de components quan sigui possible.
- Complir la normativa local en matèria de medi ambient i residus.

6. CONTINGUT DE L'OFERTA TÈCNICA

La documentació tècnica a presentar serà la següent:

- Memòria tècnica (pla de treball) de com es duran a terme les diferents tasques objecte del contracte (execució, seguiment i suport): es valorarà i puntuarà com a criteri qualitatiu, d'acord amb l'apartat H del quadre de característiques del PCAP.
  Per al suport es contempla una bossa mínima de 20 hores, d'acord amb l'apartat 5.3 d'aquest plec.
- Detall dels subministrament (materials) que s'han de proporcionar amb llur característiques, d'acord amb aquest plec.
- Descripció detallada de l'eina de gestió i anàlisi indicada a l'apartat 4 d'aquest plec. La seva qualitat respecte del mínim demanat en aquest plec i de les proposades per les altres licitadores es valorarà i puntuarà com a criteri qualitatiu, d'acord amb l'apartat H del quadre de característiques del PCAP.
- Garanties de totes les prestacions contemplades en aquest plec,
- Pla de gestió dels residus, d'acord amb l'apartat 5.7 d'aquest plec.
- Pla de formació per al personal del servei d'IT del CREAF (4 persones), que es valorarà i puntuarà com a criteri qualitatiu, d'acord amb l'apartat H del quadre de característiques del PCAP.
- Acreditació de les certificacions obligatòries i si s'escau, de les addicionals a les requerides obligatòriament (particularment ISO 14001 -Sistema de Gestió Ambiental- i ISO 9001 -Sistema de Gestió de qualitat-), d'acord amb l'apartat 5.6 d'aquest plec. L'acreditació de les certificacions no obligatòries es valorarà i puntuarà com a criteri qualitatiu, d'acord amb l'apartat H del quadre de característiques del PCAP.
- La millora de la proposta tècnica (per exemple, en la qualitat dels equips), respecte del que es demana en aquest plec, es valorarà i puntuarà com a criteri qualitatiu, d'acord amb l'apartat H del quadre de característiques del PCAP.