Plec de Prescripcions Tècniques per al servei de renovació i manteniment de la infraestructura LAN i la gestió dels sistemes de seguretat perimetral de l'Ajuntament de Santa Coloma de Gramenet

1. Introducció

El present Plec de Prescripcions Tècniques (PPT) té per objecte establir els requeriments tècnics, funcionals i de qualitat que hauran de regir el contracte per al servei de renovació i manteniment de la infraestructura de la xarxa d'àrea local (LAN) i la gestió dels sistemes de seguretat perimetral de l'Ajuntament de Santa Coloma de Gramenet, en endavant, l'Ajuntament. Aquest document defineix el marc tècnic i funcional de la solució, garantint que tots els licitadors comprenguin amb precisió l'abast i les expectatives del servei sol·licitat.

La transformació digital de l'administració pública és un procés continu i estratègic que exigeix disposar d'una base tecnològica sòlida, fiable i segura. La infraestructura de xarxa actual de l'Ajuntament ha complert el seu cicle de vida útil i presenta reptes significatius en termes de rendiment, capacitat i seguretat. Per tal de garantir un servei públic de qualitat, segur i eficient, la qual cosa exigeix una infraestructura tecnològica que ofereixi un **alt rendiment**, una **seguretat robusta** i una **gestió simplificada i proactiva**. La modernització d'aquesta infraestructura esdevé, per tant, una necessitat ineludible per sostenir l'operativa diària i impulsar nous projectes digitals.

Els objectius generals d'aquest contracte s'enfoquen a assolir una modernització integral i coherent. En primer lloc, es busca la **renovació completa de la infraestructura LAN**, incloent l'evolució dels sistemes de Core cap a una arquitectura més resilient i escalable, així com la renovació i ampliació dels commutadors d'accés a les diferents seus municipals. En segon lloc, es pretén consolidar una **gestió experta i centralitzada dels sistemes de seguretat perimetral**, que inclou la plataforma de tallafocs, el sistema de gestió d'esdeveniments i informació de seguretat (SIEM) i la plataforma de publicació segura d'aplicacions (ADC). Finalment, el tercer objectiu fonamental és garantir l'**evolució tecnològica contínua** de la solució, assegurant que tant el maquinari com el programari es mantinguin actualitzats i protegits contra l'obsolescència durant tota la vigència del contracte.

Per assolir aquests objectius, s'ha optat per un **model de servei integral**. Aquesta contractació no es concep com un simple subministrament d'equips, sinó com la prestació d'un servei complet que abasta des del disseny i la planificació fins a la instal·lació, configuració, migració, manteniment i gestió proactiva de tota la infraestructura. Aquest model de "claus en mà" permet a l'Ajuntament delegar la complexitat tècnica en un proveïdor especialitzat, assegurant uns nivells de servei òptims i alliberant recursos interns per a tasques de major valor estratègic. L'adjudicatari

actuarà com a soci tecnològic, aportant el seu coneixement i experiència per garantir una solució moderna, segura i alineada amb les necessitats presents i futures de l'Ajuntament.

2. Objecte i Abast del Contracte

L'objecte del present Plec de Prescripcions Tècniques és la contractació d'un **servei integral per a la renovació, gestió, manteniment i explotació de la infraestructura de la xarxa d'àrea local (LAN) i dels sistemes de seguretat perimetral** de l'Ajuntament de Santa Coloma de Gramenet. Aquest servei s'ha de concebre com una solució "claus en mà" que asseguri la modernització tecnològica, l'optimització del rendiment, l'increment de la seguretat i la simplificació de la gestió, tot garantint l'operativitat i l'evolució contínua de les infraestructures TIC municipals durant tota la vigència del contracte.

El contracte inclou el subministrament de tot l'equipament (maquinari) i programari (llicències) necessari, la seva instal·lació, configuració, migració des dels sistemes actuals, així com els serveis recurrents d'operació, manteniment proactiu i correctiu, suport tècnic especialitzat i gestió integral de tots els elements que conformen l'abast del servei. L'adjudicatari actuarà com a interlocutor únic per a tots els serveis descrits, proporcionant una solució cohesionada i alineada amb les necessitats estratègiques de l'Ajuntament.

A continuació, es detalla l'abast específic del servei, dividit en les diferents àrees tecnològiques que el componen.

2.1. Sistemes LAN

L'abast del servei per a la infraestructura de xarxa d'àrea local (LAN) inclou totes les actuacions necessàries per a la seva completa renovació, optimització i gestió. Això comprèn:

1. **Evolució del Core LAN:** Aquesta actuació contempla la substitució completa dels actuals xassís de Core de xarxa, actualment obsolets, per una nova arquitectura basada en un model **Spine-Leaf**. Aquesta evolució haurà de proporcionar un augment significatiu en la capacitat de commutació, millorar la latència, oferir una major resiliència mitjançant la redundància inherent al disseny i facilitar l'escalabilitat futura. L'abast inclou el subministrament, instal·lació, configuració i migració de tots els commutadors de tipus "Spine" i "Leaf" que conformaran el nou nucli de la xarxa.
2. **Renovació i Ampliació dels Equips d'Accés:** El servei haurà de cobrir la renovació de tots aquells commutadors d'accés (planta) que es trobin obsolets o propers al final del seu cicle de vida, així com l'ampliació de la xarxa en aquelles seus on sigui necessari. Aquests equips hauran de proporcionar connectivitat Gigabit als llocs de treball i disposar de ports amb capacitat **Power over Ethernet (PoE/PoE+)** per alimentar dispositius com telèfons IP, punts d'accés Wi-Fi, càmeres de videovigilància, etc. El servei inclou el subministrament, la

instal·lació física a les diferents seus municipals, la configuració coordinada amb el Core i la migració dels serveis existents sense impacte per als usuaris.

3. **Actualització i Gestió Centralitzada:** L'abast inclou l'actualització de la plataforma de gestió de xarxa existent (actualment Extreme NetSight) a la seva versió més recent, que serà **ExtremeCloud IQ - Site Engine**, o una solució equivalent del fabricant que s'ofereixi. Aquesta plataforma haurà de permetre la gestió, monitorització i configuració centralitzada de tots els elements de la xarxa LAN (Core i accés). A més, s'haurà d'implementar i llicenciar un sistema de **Control d'Accés a la Xarxa (NAC)** per a un mínim de 2000 dispositius, integrat amb la plataforma de gestió, per reforçar la seguretat mitjançant el perfilat, l'autenticació i l'autorització de tots els dispositius que es connecten a la xarxa corporativa.

2.2. Sistemes de Seguretat

El contracte també té per objecte la prestació de serveis de gestió especialitzada sobre la infraestructura de seguretat perimetral i sistemes associats de l'Ajuntament. L'objectiu és garantir que aquests sistemes crítics estiguin correctament configurats, actualitzats i monitoritzats per protegir els actius d'informació de l'Ajuntament davant les amenaces externes i internes. L'abast d'aquesta àrea inclou:

1. **Gestió de la Seguretat Perimetral (Firewalls Check Point):** L'adjudicatari haurà de prestar un servei de gestió integral sobre la plataforma de tallafocs **Check Point Quantum Maestro** de l'Ajuntament. Aquest servei inclou la gestió del cicle de vida de les regles de tallafoc, la configuració i manteniment de polítiques de NAT, la gestió de les connexions VPN (tant d'accés remot per a usuaris com túnels L2L amb altres organismes), l'actualització periòdica del programari (versions i pegats de seguretat), la monitorització del rendiment i la salut del sistema, i la resposta davant d'incidències de seguretat.
2. **Gestió del Sistema SIEM (Security Information and Event Management):** El servei es prestarà en modalitat **SIEM as a Service**. L'adjudicatari serà responsable de la gestió completa de la plataforma, actualment basada en tecnologia **RSA Multitenant o una solució equivalent** que compleixi els requisits especificats. L'abast inclou la gestió de les fonts de logs, la configuració i manteniment dels recol·lectors, el desenvolupament i afinament de regles de correlació per a la detecció d'amenaces, la generació d'alertes, la creació d'informes de compliment i operatius, i el suport en la investigació d'incidents de seguretat.
3. **Gestió de la Plataforma de Publicació d'Aplicacions (ADC NetScaler):** El servei inclou el manteniment i la gestió de la plataforma **ADC (Application Delivery Controller) NetScaler MPX-8905**. L'adjudicatari s'encarregarà de garantir el correcte funcionament dels serveis publicats a través d'aquesta plataforma, realitzant tasques de gestió de balanceig de càrrega, polítiques de commutació de continguts (*content switching*), actualitzacions de la plataforma, monitorització de la disponibilitat de les aplicacions i resolució d'incidències relacionades amb la publicació de serveis.

2.3. Model de Servei

El present contracte s'articula sota un **model de serveis**, on l'Ajuntament no realitza una adquisició directa de maquinari, sinó que contracta una solució tecnològica integral que inclou l'ús de tots els elements de maquinari i programari necessaris per a la correcta prestació dels serveis descrits en aquest plec.

Aquest model implica que l'adjudicatari és el propietari dels equips durant la vigència del contracte i, com a tal, és responsable del seu correcte funcionament, manteniment, actualització i substitució en cas d'avaria o obsolescència, sense cap cost addicional per a l'Ajuntament. La quota mensual del servei ha de cobrir la totalitat de les prestacions i equipaments necessaris.

Com a condició essencial del contracte, s'estableix que **a la finalització del període contractual, la totalitat del maquinari subministrat i instal·lat per l'adjudicatari per a la prestació del servei de renovació de la LAN passarà a ser propietat de l'Ajuntament de Santa Coloma de Gramenet, sense cap cost addicional ni valor residual**. Aquesta transferència de propietat s'haurà de formalitzar degudament, lliurant tota la documentació pertinent. Aquest model permet a l'Ajuntament disposar d'una infraestructura tecnològica d'última generació mitjançant una despesa operativa (OPEX) durant la vida del contracte, i consolidar la inversió (CAPEX) en forma d'actius propis a la seva finalització.

3. Descripció de la Situació Actual

El present capítol té com a objectiu proporcionar una descripció detallada i transparent de l'estat actual de la infraestructura tecnològica de l'Ajuntament de Santa Coloma de Gramenet que és objecte d'aquest contracte. Aquesta anàlisi serveix com a punt de partida per als licitadors, permetent-los comprendre l'entorn existent, identificar els reptes tecnològics i dimensionar adequadament la proposta de servei de renovació, manteniment i gestió. La informació que es presenta a continuació abasta els sistemes de xarxa local (LAN), la infraestructura de seguretat perimetral i les plataformes de gestió i serveis associats, destacant-ne les característiques tècniques, les versions de programari, les configuracions rellevants i, especialment, els punts d'obsolescència o les àrees que requereixen una evolució tecnològica.

Infraestructura de Xarxa Local (LAN)

La xarxa local de l'Ajuntament es fonamenta principalment en equipament del fabricant **Extreme Networks**. L'arquitectura actual, tot i que ha estat funcional durant anys, presenta una combinació d'equipament de diferents generacions, la qual cosa implica reptes en termes de gestió, rendiment i seguretat. Aquesta heterogeneïtat i l'antiguitat d'alguns dels seus components clau justifiquen la necessitat d'una renovació integral.

Equipament del Core de la Xarxa

El nucli de la xarxa corporativa de l'Ajuntament, ubicat al Centre de Processament de Dades (CPD) central, està conformat per dos xassís modulars **Extreme S-Series S8**. Aquests equips, configurats per proporcionar redundància, actuen com a punt central de commutació per a tot el tràfic de la xarxa corporativa. La composició detallada d'aquests xassís inclou diversos mòduls que reflecteixen les necessitats de connectivitat al llarg del temps:

- **Xassís i Alimentació:** Dos xassís S-Series S8 amb tres fonts d'alimentació redundants cadascun.
- **Targetes de ports PoE:** Múltiples targetes `ST4106-0348-F6` (48 ports PoE) i `ST4106-0248` (48 ports PoE+), que proporcionen connectivitat i alimentació a dispositius finals com telèfons IP, càmeres o punts d'accés Wi-Fi.
- **Targetes de ports 10GbE:** Targetes `SK8009-1224-F8` (24 ports 10GbE de coure) i `SK8008-1224-F8` (24 ports 10GbE SFP+), que serveixen com a enllaços d'alta velocitat cap als commutadors de distribució o d'accés principals i per a la connexió de servidors.
- **Mòduls d'expansió i transceptors:** Diversos mòduls d'expansió de 12 ports SFP i 4 ports SFP+, juntament amb un gran nombre de transceptors `MGBIC-LC01` (1GbE) i `10GB-C10-SFPP` (10GbE).

Diagnòstic d'obsolescència: La sèrie S8 d'Extreme Networks és una plataforma que ja ha estat declarada **End-of-Life (EoL)** pel fabricant. Això implica riscos significatius per a l'operativa de l'Ajuntament, entre els quals destaquen:

1. **Fi del Suport Tècnic:** El fabricant ja no proporciona suport tècnic ni actualitzacions de microprogramari (firmware) per a aquests equips.
2. **Vulnerabilitats de Seguretat:** La manca d'actualitzacions de seguretat deixa la xarxa exposada a noves vulnerabilitats que no seran corregides, la qual cosa és inacceptable en el marc de l'Esquema Nacional de Seguretat (ENS).
3. **Manca de Recanvis:** La dificultat per trobar peces de recanvi (fonts d'alimentació, ventiladors, targetes de línia) en cas d'avaria pot provocar temps d'interrupció del servei perllongats i impredictibles.
4. **Limitacions de Rendiment:** Aquesta arquitectura, basada en un model tradicional, no està optimitzada per als patrons de tràfic est-oest predominants en entorns virtualitzats moderns, a diferència de les arquitectures **Spine-Leaf**.

A continuació es presenta el dimensionament d'equips Core LAN actual:

CORE BACKBONE		XASSÍS 1	XASSÍS 2
Xassís S8	S-SERIES S8 CHASSIS/FANTRAYS	1	1
Font d'alimentació	S-SERIES AC POWER SUPPLY S3/S4/S8	3	3
ST4106-0248	Tarja: S-IOM 48 PORT TS RJ45 POE AT W1 OPSLOT	4	4
SK8009-1224-F8	Tarja: S180 24PORT 10GB-T FABRIC	1	1
SK8008-1224-F8	Tarja: S180 24PORT SFPP FABRIC	1	1
Mòdul expansió	12 PORTS SFP TYPE1 OM	2	2
Mòdul expansió	4 PORTS SFP+ TYPE2 OM	2	2
10GB-C10-SFPP	-	2	2
MGBIC-LC01	-	48	48

Equipament d'Accés/Planta

La capa d'accés de la xarxa, distribuïda per les diferents seus municipals, està composta per una varietat de commutadors d'Extreme Networks. Aquesta diversitat de models i generacions complica la gestió homogènia de la xarxa. Els models principals en ús són:

- **Sèrie G (`08H20G4`):** Models com el `08H20G4-24P` i `08H20G4-48P`. Aquests equips són els més antics de la xarxa i es consideren **obsolets**. No disposen de capacitats avançades com el suport per a estàndards PoE més moderns (PoE+), ports multi-gigabit o funcionalitats de seguretat avançades. La seva renovació és una prioritat absoluta.
- **Sèrie 200 (`220`):** Models com el `220-24p-10GE2` i `220-48p-10GE4`. Aquests commutadors són més recents i ofereixen millors prestacions, com ara ports d'uplink de 10GbE i suport per a PoE+. Tot i que no són obsolets, no representen la darrera generació del fabricant i podrien tenir limitacions per a futures necessitats, com el suport de PoE++ (60-90W) per a dispositius d'alt consum.

La topologia de la xarxa d'accés és principalment en estrella, amb els commutadors de planta connectant-se al nucli de la xarxa. La gestió de les VLANs es realitza de manera centralitzada, amb una particularitat destacable: la política de segmentació i part de la gestió de les VLANs es delega a la infraestructura de seguretat perimetral de Check Point, la qual cosa crea una dependència operativa que ha de ser gestionada amb cura durant la migració.

A continuació es presenta el dimensionament d'equips LAN actual, per tipus de centre, així com també les ampliacions requerides d'inici. L'abast final pot augmentar o disminuir en funció del replanteig final i no suposa cap compromís per part de l'Ajuntament.

Model	Criticitat de la seu	Unitats	Requeriments
08H20G4-24P	Alta	9	Renovació, manteniment i gestió
08H20G4-24P	Estàndard	14 (*)	Renovació, manteniment i gestió
08H20G4-48P	Alta	6	Renovació, manteniment i gestió
08H20G4-48P	Estàndard	2	Renovació, manteniment i gestió
220-24p-10GE2	Alta	4	Manteniment i gestió
220-48p-10GE4	Alta	5	Manteniment i gestió
220-48p-10GE4	Estàndard	4	Manteniment i gestió
Total Commutadors Accés		**44**	

(*) 1 d'aquests commutadors de 24 ports s'ha de substituir per un de 48 ports (seu EBAS3).

Infraestructura de Seguretat i Serveis Associats

La seguretat de la xarxa de l'Ajuntament es basa en un ecosistema de solucions de diversos fabricants, que treballen de manera conjunta per protegir el perímetre, les aplicacions i analitzar els esdeveniments de seguretat.

Gestió de la Seguretat Perimetral

El perímetre de la xarxa està protegit per una solució de tallafocs d'última generació del fabricant **Check Point**. La plataforma implementada és **Check Point Quantum Maestro**, una solució d'orquestració hiperescalable que ofereix un alt rendiment i resiliència. La configuració actual consta de:

- **Orquestradors:** Dos (2) orquestradors `MHO-140` que gestionen la distribució del tràfic i la sincronització dels passarel·les de seguretat.
- **Passarel·les de Seguretat (Security Gateways):** Un grup de seguretat format per sis (6) Security Gateways que processen el tràfic.
- **Versió de Programari:** La plataforma opera amb la versió **R81.10 (Take 110)**. La gestió es realitza mitjançant una consola de gestió virtualitzada en l'entorn de servidors de l'Ajuntament.

Aquesta infraestructura és moderna i potent. Tanmateix, el present contracte contempla la **gestió continuada** d'aquesta plataforma, la qual cosa implica l'administració de regles, polítiques de prevenció d'amenaces (IPS, Anti-Virus, etc.), la gestió de VPNs i l'actualització de versions, d'acord amb les millors pràctiques i les necessitats de l'Ajuntament.

Sistema d'Informació i Gestió d'Esdeveniments de Seguretat (SIEM)

L'Ajuntament disposa d'un sistema SIEM basat en la tecnologia **RSA Multitenant**, operat actualment en una modalitat de servei gestionat. Aquesta plataforma centralitza la recol·lecció i anàlisi de logs de múltiples fonts (tallafocs, servidors, sistemes de xarxa, etc.) per a la detecció d'amenaces i l'anàlisi forense. Les capacitats actuals del servei són:

- **Capacitat de Processament:** Fins a **700 esdeveniments per segon (EPS)**.
- **Volum d'Emmagatzematge:** Gestió d'aproximadament **50 GB de logs diaris**.

La plataforma actual compleix la seva funció, però el contracte ha de garantir la continuïtat d'un servei equivalent o superior, preferiblement en una modalitat **"as a Service"** que alliberi l'Ajuntament de la gestió de la infraestructura subjacent, mantenint o millorant les capacitats d'anàlisi, correlació i resposta.

Plataforma de Lliurament d'Aplicacions (ADC)

Per a la publicació segura i eficient d'aplicacions web, l'Ajuntament utilitza una plataforma de lliurament d'aplicacions (ADC) del fabricant Citrix (actualment part de Cloud Software Group). L'equipament físic instal·lat és un **NetScaler MPX-8905**. Aquest dispositiu realitza funcions crítiques com:

- Balanç de càrrega de servidors.
- Commutació de contingut.
- Descàrrega SSL (SSL offloading).
- Funcionalitats de tallafocs d'aplicacions web (WAF).

Aquest equip, amb número de sèrie `3P2Z1CZT02`, tot i que funcional, representa un element físic aïllat en la infraestructura. L'estratègia a llarg termini podria considerar la migració cap a solucions virtuals o basades en contenidors (com Citrix ADC VPX o CPX) per millorar la flexibilitat, l'escalabilitat i la integració en entorns de núvol híbrid. El servei objecte d'aquest contracte ha d'incloure la gestió, el manteniment i l'actualització d'aquesta plataforma.

Sistema de Gestió i Monitorització

La gestió i la visibilitat de la xarxa són fonamentals per a una operació eficient. Actualment, l'Ajuntament utilitza principalment dues eines.

Sistema de Gestió de Xarxa

La gestió de la infraestructura de xarxa d'Extreme Networks es realitza mitjançant la plataforma **Extreme NetSight**. Aquesta eina permet realitzar tasques d'inventari, configuració bàsica, i monitorització de l'estat dels commutadors. Tanmateix, NetSight és una plataforma que ha evolucionat i ha estat substituïda per **ExtremeCloud IQ - Site Engine**. La versió actualment en ús a l'Ajuntament és, per tant, **antiga i limitada** en comparació amb les solucions de gestió

modernes. No disposa de funcionalitats natives avançades de Control d'Accés a la Xarxa (NAC) ni de gestió automatitzada de seguretat, la qual cosa representa una carència important.

Sistema de Monitorització General

Addicionalment, l'Ajuntament utilitza el sistema de codi obert **Nagios** per a la monitorització de la disponibilitat de serveis, processos i recursos en una varietat d'equips. Tot i que Nagios és una eina potent i flexible, la seva gestió i manteniment poden ser complexos i requerir un esforç manual considerable. L'Ajuntament ja ha manifestat que està avaluant alternatives, la qual cosa indica una voluntat de modernitzar també aquest àmbit per disposar de sistemes més integrats i automatitzats.

4. Requeriments Generals del Servei

Aquest capítol estableix el marc de condicions transversals i principis rectors que han de governar la prestació del servei objecte d'aquest contracte. Aquests requeriments són d'obligat compliment per a l'adjudicatari i complementen les especificacions tècniques detallades en els capítols posteriors. La seva finalitat és definir la filosofia del servei, assegurar la qualitat i la continuïtat de la prestació, i garantir l'alineació de l'adjudicatari amb els objectius estratègics de l'Ajuntament de Santa Coloma de Gramenet en matèria de modernització tecnològica, seguretat i eficiència.

4.1. Model de "claus en mà" i de servei

El contracte es licita sota una modalitat de **servei integral "claus en mà"**. Aquest model implica que l'oferta econòmica presentada per l'adjudicatari haurà d'incloure tots els costos directes i indirectes necessaris per a la posada en marxa, l'explotació i el manteniment complet i funcional de tots els sistemes i serveis descrits en aquest plec, durant tota la vigència del contracte. L'objectiu és garantir que l'Ajuntament no hagi d'assumir cap despesa addicional o imprevista per aconseguir els resultats esperats.

Això inclou, a títol enunciatiu i no limitatiu, tots els costos associats a:

- El subministrament de la totalitat del maquinari i programari necessaris (commutadors, llicències, etc.).
- La instal·lació física, el muntatge en rack, el cablejat i la connexió de tots els equips.
- L'execució de treballs menors d'obra civil o adequacions necessàries per a la correcta instal·lació, com ara petites canalitzacions o ajustos en els armaris de comunicacions.
- L'adequació de les connexions elèctriques necessàries per als nous equipaments.
- La gestió de projecte, la planificació detallada, la coordinació de recursos i el seguiment de la implantació.

- L'elaboració de tota la documentació tècnica requerida (disseny, configuració, plans de migració, documentació "as-built").
- Totes les tasques de migració de la infraestructura actual a la nova solució, assegurant la mínima interrupció del servei.
- La realització de proves i tests per validar la correcta implantació i funcionament de la solució.
- La formació i transferència de coneixement al personal tècnic de l'Ajuntament.

És fonamental destacar que el present contracte és de **serveis**. L'Ajuntament contracta un servei global de renovació, gestió i manteniment de la seva infraestructura, i no una adquisició de béns. El maquinari subministrat és un component indispensable per a la prestació d'aquest servei. No obstant això, s'estableix que, a la finalització del període contractual, la **totalitat del maquinari subministrat i instal·lat passarà a ser propietat de l'Ajuntament**, sense cap cost addicional per a aquest i en ple estat de funcionament.

4.2. Pla d'Evolució Tecnològica i Garantia de No-Obsolescència

L'adjudicatari haurà de presentar i mantenir durant tota la vigència del contracte un **Pla d'Evolució Tecnològica**. L'objectiu d'aquest pla és garantir que la infraestructura tecnològica de xarxa i seguretat de l'Ajuntament no quedi obsoleta des del punt de vista funcional, tecnològic o de suport del fabricant. L'adjudicatari ha d'actuar com un veritable soci tecnològic, assegurant que la solució es mantingui actualitzada, segura i alineada amb les millors pràctiques del sector.

Aquest pla haurà d'incloure, com a mínim, els següents aspectes:

- **Garantia de No-Obsolescència del Maquinari:** L'adjudicatari es compromet a substituir, sense cap cost per a l'Ajuntament, qualsevol equip de maquinari que durant la vigència del contracte sigui declarat "Fi de Venda" (End-of-Sale) o, especialment, "Fi de Suport" (End-of-Support / End-of-Life) pel fabricant. La substitució s'haurà de fer per un equip de característiques tècniques i rendiment iguals o superiors, garantint la plena compatibilitat amb la resta de la infraestructura.
- **Política d'Actualització de Programari i Microprogramari (Firmware):** El pla ha de definir una política proactiva d'actualitzacions. L'adjudicatari serà responsable de planificar, provar i executar les actualitzacions periòdiques de tot el programari i microprogramari dels equips, incloent-hi sistemes operatius, gestores, controladors i llicències. Es prioritzaran especialment els pegats de seguretat crítics, que s'hauran d'aplicar dins dels terminis establerts als Acords de Nivell de Servei (ANS).
- **Vigilància Tecnològica:** L'adjudicatari haurà de realitzar una vigilància tecnològica contínua sobre les solucions implementades i el mercat en general. Haurà d'informar proactivament l'Ajuntament sobre noves tecnologies, millores funcionals, optimitzacions de rendiment o noves capacitats de seguretat que puguin ser d'interès.

- **Reunions de Seguiment Tecnològic:** Com a mínim amb periodicitat anual, l'adjudicatari convocarà una reunió amb els responsables tècnics de l'Ajuntament per presentar formalment l'estat del Pla d'Evolució Tecnològica, les novetats del sector i propostes de millora per al període següent.

4.3. Seguretat, Confidencialitat i Protecció de Dades

L'adjudicatari estarà obligat al compliment estricte de tota la legislació vigent en matèria de seguretat de la informació i protecció de dades de caràcter personal. La infraestructura i els serveis objecte d'aquest contracte són crítics per a l'operativa de l'Ajuntament i gestionen informació sensible, per la qual cosa la seguretat és un pilar fonamental.

En concret, l'adjudicatari haurà de garantir el compliment, com a mínim, de les següents normatives i principis:

- **Esquema Nacional de Seguretat (ENS):** La solució proposada i els procediments de gestió i manteniment hauran de complir amb els requisits establerts al Reial Decret 311/2022, pel qual es regula l'Esquema Nacional de Seguretat. L'adjudicatari haurà d'implementar les mesures de seguretat corresponents a la categoria del sistema, que serà determinada per l'Ajuntament, i proporcionar tota l'evidència necessària per a les auditories de compliment.
- **Reglament General de Protecció de Dades (RGPD):** L'adjudicatari haurà de complir amb el Reglament (UE) 2016/679 del Parlament Europeu i del Consell. A efectes d'aquest contracte, l'Ajuntament de Santa Coloma de Gramenet té la consideració de **Responsable del Tractament**, i l'empresa adjudicatària tindrà la consideració d'**Encarregat del Tractament**. L'accés a dades personals per part de l'adjudicatari es limitarà a allò estrictament indispensable per a la prestació del servei.
- **Llei Orgànica de Protecció de Dades (LOPDGDD):** S'haurà de complir igualment amb la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.

Com a Encarregat del Tractament, l'adjudicatari assumeix les següents obligacions:

- Garantir la **confidencialitat, integritat, disponibilitat i resiliència** permanents dels sistemes i serveis.
- Tractar les dades únicament segons les instruccions documentades de l'Ajuntament.
- Assegurar que tot el personal autoritzat per tractar dades personals s'hagi compromès a respectar la confidencialitat de manera explícita i per escrit.
- Notificar a l'Ajuntament, sense dilació indeguda, qualsevol violació de la seguretat de les dades.
- Donar suport a l'Ajuntament en la realització d'Avaluacions d'Impacte relatives a la Protecció de Dades (AIPD) si fos necessari.

- Un cop finalitzi la prestació del servei, i segons l'elecció de l'Ajuntament, suprimir o retornar totes les dades personals, i suprimir les còpies existents.
- Posar a disposició de l'Ajuntament tota la informació necessària per demostrar el compliment de les seves obligacions i permetre i contribuir a la realització d'auditories.

5. Requeriments Tècnics de la Infraestructura LAN

Aquest capítol estableix les especificacions tècniques mínimes que ha de complir la nova infraestructura de xarxa d'àrea local (LAN) de l'Ajuntament de Santa Coloma de Gramenet. La solució proposada haurà de ser integral, cobrint des de l'arquitectura de xarxa fins a l'equipament de Core, distribució i accés, i els protocols i configuracions necessàries per garantir un servei d'alt rendiment, segur, resilient i escalable. La proposta ha de garantir la modernització dels sistemes actuals, la majoria dels quals es troben en estat d'obsolescència o propers a aquest, i ha de proporcionar una base sòlida per a la implementació de serveis digitals avançats. L'adjudicatari haurà de dissenyar i implementar una solució que s'alineï amb les millors pràctiques del sector i que sigui capaç de suportar les necessitats operatives de l'Ajuntament durant tota la vigència del contracte.

5.1. Arquitectura de xarxa

La nova infraestructura LAN s'haurà de basar obligatòriament en una arquitectura de xarxa de dues capes coneguda com a **Spine-Leaf (troncal-fulla)**. Aquest model substitueix l'arquitectura tradicional de tres capes (Core, distribució, accés) per oferir una topologia més eficient, previsible i escalable, especialment adequada per a les càrregues de treball actuals i futures. L'objectiu és construir una xarxa sense bloquejos (*non-blocking*), de baixa latència i amb una amplada de banda uniforme entre qualsevol punt de la xarxa.

La topologia física es caracteritzarà per la interconnexió completa de la capa Leaf amb la capa Spine. Cada commutador Leaf s'haurà de connectar a tots i cadascun dels commutadors Spine. No s'admetrà cap connexió directa entre commutadors de la mateixa capa (Leaf-Leaf o Spine-Spine). Aquesta estructura garanteix que el trànsit entre dos dispositius connectats a diferents commutadors Leaf només hagi de passar per tres salts (Leaf-Spine-Leaf), assegurant una latència constant i predictible.

Per a la implementació de l'arquitectura lògica, s'haurà d'utilitzar una **xarxa de superposició (overlay)** sobre una **xarxa de base (underlay)**. La xarxa de base serà una infraestructura de capa 3, on tots els enllaços entre els equips Spine i Leaf s'establiran com a enllaços enrutats. El protocol d'enrutament preferit per a la xarxa de base serà **BGP (Border Gateway Protocol)**, per la seva escalabilitat, flexibilitat i àmplia adopció en arquitectures de centres de dades moderns.

Sobre aquesta xarxa de base, es construirà una xarxa de superposició utilitzant **VXLAN (Virtual Extensible LAN)** com a tecnologia d'encapsulació i **EVPN (Ethernet VPN)** com a pla de control. La combinació **EVPN-VXLAN** permetrà estendre dominis de capa 2 sobre la infraestructura de capa 3, facilitant la mobilitat de dispositius i màquines virtuals a través de tota la xarxa sense les limitacions dels protocols de Spanning Tree. A més, aquesta arquitectura és la base per a la implementació de polítiques de **microsegmentació**, permetent aïllar trànsit i aplicar polítiques de seguretat granulars entre dispositius o aplicacions, fins i tot si es troben dins de la mateixa VLAN o subxarxa.

Aquesta arquitectura haurà de ser dissenyada per a una alta disponibilitat. L'ús de múltiples commutadors Spine i l'ús de protocols d'enrutament com BGP amb ECMP (Equal-Cost Multi-Path) permetrà el balanceig de càrrega actiu-actiu a través de tots els enllaços disponibles i una convergència gairebé instantània en cas de fallada d'un enllaç o d'un equip Spine, minimitzant l'impacte sobre el servei.

5.2. Equipament de Core (Spine i Leaf)

L'equipament de Core conforma el nucli de la xarxa i és crític per al seu rendiment i disponibilitat. Donada l'arquitectura Spine-Leaf, aquest equipament es divideix en commutadors Spine i commutadors Leaf. Tots els equips proposats hauran de ser nous, del mateix fabricant per garantir una gestió homogènia, i han de disposar de les llicències de programari necessàries (en la seva modalitat més avançada) per a totes les funcionalitats requerides durant tota la vigència del contracte.

Requeriments mínims per als commutadors de capa Spine:

Els commutadors Spine actuen com a troncal d'alta velocitat de la xarxa. La seva funció principal és reenviar trànsit entre els commutadors Leaf el més ràpidament possible.

- **Capacitat de commutació i rendiment:** Hauran de ser equips de xassís modular o de format fix d'alt rendiment, amb una capacitat de commutació non-blocking no inferior a **4 Tbps** i una taxa de reenviament de paquets superior a **1000 Mpps**, per garantir un funcionament sense colls d'ampolla.
- **Densitat i tipus de ports:** Hauran de disposar d'un mínim de **48 ports SFP28** amb capacitat per a velocitats de 1/10/25 Gbps i un mínim de **8 ports QSFP28** amb capacitat per a velocitats de 40/100 Gbps. Aquesta configuració permetrà la connexió dels commutadors Leaf a 25 Gbps i la possible interconnexió entre Spines o amb altres sistemes a 100 Gbps.
- **Redundància:** L'alta disponibilitat és obligatòria. Els equips han d'incorporar, com a mínim, **dues fonts d'alimentació redundants i hot-swappable** (intercanviables en calent) i mòduls de ventilació redundants i hot-swappable, per garantir la continuïtat del servei davant la fallada d'un component.

- **Suport de protocols:** Suport complet de protocols de capa 2 i capa 3. Imprescindible el suport de **BGP** (amb extensions per a EVPN), OSPF, i protocols de qualitat de servei (QoS) avançats (IEEE 802.1p, DSCP). Han de suportar plenament l'encapsulació **VXLAN** a nivell de maquinari (VTEP) i el pla de control **EVPN**.
- **Gestió:** Hauran de suportar la gestió via CLI (interfície de línia de comandes), SNMPv3, i ser totalment gestionables des de la plataforma centralitzada de gestió basada en el núvol proposada.

Requeriments mínims per als commutadors de capa Leaf:

Els commutadors Leaf actuen com a punt de connexió per als servidors, sistemes d'emmagatzematge, i com a punt d'agregació per als commutadors d'accés.

- **Capacitat de commutació i rendiment:** Hauran de ser equips de format fix d'alt rendiment, amb una capacitat de commutació non-blocking no inferior a **1 Tbps**.
- **Ports d'accés (downlinks):** Es requereixen models amb diferents opcions de connectivitat per als servidors i altres sistemes. S'hauran de proveir equips amb **24 ports 1/10GBASE-T (coure)** amb suport PoE++ (802.3bt) i equips amb **24 ports 1/10G SFP+ (fibra òptica)**.
- **Ports d'enllaç (uplinks):** Tots els commutadors Leaf hauran de disposar, com a mínim, de **6 ports SFP28 de 25 Gbps** per a la connexió redundant amb la capa Spine.
- **Redundància i apilament:** Els equips hauran de suportar fonts d'alimentació redundants i hot-swappable. A més, hauran de suportar tecnologies de **xassís virtual o apilament (stacking)** que permetin a dos o més equips físics operar com un únic commutador lògic, facilitant la gestió i permetent la configuració d'enllaços agregats multixassís (MLAG/LACP) per a una connexió redundant dels servidors o commutadors d'accés.
- **Suport de protocols:** Igual que els Spine, han de suportar plenament BGP, OSPF, VXLAN (com a VTEP de maquinari) i EVPN, així com protocols de seguretat a nivell d'accés com 802.1X.

En el moment de licitar s'haurà d'incloure l'evolució de l'equipament de Core LAN de l'Ajuntament, ja que aquest és obsolet. **El nou equipament ha de disposar del mateix dimensionament de ports de Cu (coure) actuals, , com a mínim, i incrementar en un 10% el nombre de ports de Fo (fibra).**

A mode orientatiu, una possible implementació del Core mitjançant una arquitectura del tipus Spine-Leaf, seria la següent:

Tipus de commutador de CORE		Unitats
Capa Spine	Switch de 48 ports 10/25Gb FO	2
Capa Leaf	Switch de 24 ports 10Gb Cu	2
	Switch de 24 ports 10Gb SFP+	2
Usuaris addicionals	Switch de 48 ports 1Gb Cu	8

Altres elements		Unitats
Capa Spine	25G Passive DAC SFP28	6
	100G Passive DAC QSFP28	2
	Cables /fuetons	els necessaris
Capa Leaf	Cables /fuetons	els necessaris
Usuaris addicionals	10 Gigabit Ethernet SFP+ passive cable assembly	16
	Cables /fuetons	els necessaris

L'adjudicatari haurà d'incloure tot el cablejat necessari per a interconnectar els nous equips entre ells i per a connectar la resta d'elements de xarxa que es troben en producció actualment a la màxima velocitat i rendiment que aquests permetin.

5.3. Equipament d'Accés/Planta

L'equipament d'accés és el que proporciona connectivitat directa als dispositius finals dels usuaris (ordinadors, telèfons IP, punts d'accés Wi-Fi, càmeres IP, impressores, etc.) a les diferents seus i plantes de l'Ajuntament. Aquests equips són fonamentals per garantir la qualitat i la seguretat del servei a l'usuari final. Tots els equips d'accés han de ser del mateix fabricant que els equips de Core, per assegurar una gestió unificada i una compatibilitat total.

Requeriments mínims per als commutadors d'Accés/Planta:

- **Densitat i tipus de ports:** Es requereixen principalment models de **24 i 48 ports 10/100/1000BASE-T (coure)**. Tots els ports de coure han de ser capaços de negociar automàticament la velocitat i el mode dúplex.
- **Alimentació per Ethernet (PoE):** Tots els commutadors d'accés han de suportar l'estàndard **IEEE 802.3at (PoE+)**, oferint fins a 30W per port. Es valorarà positivament el suport de l'estàndard **IEEE 802.3bt (PoE++)** per a necessitats futures. El pressupost de potència (power budget) total del commutador ha de ser suficient per alimentar tots els ports simultàniament

a la seva màxima capacitat PoE+. La solució ha de permetre una gestió dinàmica de la potència i la priorització de ports.

- **Ports d'enllaç (uplinks):** Cada commutador ha de disposar d'un mínim de **4 ports SFP+ de 10 Gbps**. Aquests ports s'utilitzaran per a la connexió redundant amb els commutadors de la capa Leaf o de distribució.
- **Apilament (Stacking):** La funcionalitat d'apilament físic o de xassís virtual és obligatòria. Ha de permetre apilar un mínim de 8 commutadors perquè operin i es gestionin com una única entitat lògica, amb una única adreça IP de gestió. L'ample de banda de l'enllaç d'apilament ha de ser suficient per no crear colls d'ampolla. Aquesta tecnologia simplifica l'administració i millora la resiliència, permetent la creació d'enllaços agregats (LACP) distribuïts entre diferents membres de la pila.
- **Rendiment:** Els equips han de ser non-blocking, garantint que la capacitat de la matriu de commutació sigui suficient per gestionar el trànsit de tots els ports a la seva màxima velocitat simultàniament.
- **Funcionalitats de seguretat de capa 2:** Han de suportar un conjunt complet de funcionalitats de seguretat per protegir la xarxa a la capa d'accés. Això inclou, com a mínim: **autenticació d'accés basada en ports (IEEE 802.1X)**, autenticació basada en MAC, **DHCP Snooping**, **Dynamic ARP Inspection (DAI)**, IP Source Guard i llistes de control d'accés (ACLs) basades en capa 2, 3 i 4.
- **Gestió:** Han de ser totalment gestionables des de la plataforma de gestió centralitzada al núvol, permetent el desplegament "zero-touch" (Zero Touch Provisioning), la configuració massiva, la monitorització i l'actualització de microprogramari de forma centralitzada.

5.4. Requeriments de Configuració

Una correcta configuració de la xarxa és tan important com la qualitat de l'equipament. L'adjudicatari serà responsable de dissenyar i implementar una configuració que optimitzi el rendiment, la seguretat i la gestió de la xarxa, seguint les millors pràctiques i les polítiques de l'Ajuntament.

Política de VLANs i Segmentació de la Xarxa:

L'adjudicatari, en col·laboració amb l'equip tècnic de l'Ajuntament, definirà una política de VLANs i subxarxes que segmenti la xarxa de manera lògica i segura. Es crearan, com a mínim, VLANs separades per a diferents tipus de trànsit i serveis, com ara:

- **VLAN de Dades d'Usuaris:** Per al trànsit dels llocs de treball corporatius.
- **VLAN de Veu sobre IP (Telefonia IP):** Per al trànsit dels telèfons IP, marcada amb prioritat de QoS.
- **VLAN de Gestió:** Per a l'accés a la gestió dels propis equips de xarxa. Aquesta VLAN haurà d'estar altament securitzada.

- **VLAN de Servidors:** Per als servidors del CPD.
- **VLAN Wi-Fi Corporativa:** Per als usuaris que es connecten a la xarxa sense fils corporativa.
- **VLAN Wi-Fi de Convidats:** Per a l'accés a Internet dels visitants, totalment aïllada de la xarxa interna.
- **VLAN d'Internet de les Coses (IoT) / Dispositius Especials:** Per a dispositius com sensors, sistemes de climatització, control d'accessos, etc.
- **VLAN de Videovigilància:** Per al trànsit de les càmeres de seguretat IP.

L'arquitectura EVPN-VXLAN s'utilitzarà per implementar aquestes VLANs com a segments de xarxa virtual (VNIs) i per aplicar polítiques de microsegmentació que restringeixin la comunicació entre dispositius dins d'una mateixa VLAN, seguint un model de seguretat de **confiança zero (Zero Trust)**.

Securització de la Xarxa:

La seguretat ha de ser un element central en el disseny i la configuració. S'implementaran les següents mesures com a mínim:

- **Control d'Accés a la Xarxa (NAC):** S'implementarà una solució NAC (com es detalla al capítol 7) que forci l'autenticació de tots els dispositius que es connecten a la xarxa, mitjançant 802.1X. Als ports on no sigui possible utilitzar 802.1X, s'utilitzarà l'autenticació per MAC.
- **Seguretat de Ports:** En els commutadors d'accés, es configurarà la seguretat de ports per limitar el nombre de dispositius que es poden connectar a un port i per definir accions en cas de violació (p. ex., apagar el port).
- **Protecció contra Atacs de Capa 2:** S'activaran i configuraran mecanismes com DHCP Snooping, Dynamic ARP Inspection (DAI) i IP Source Guard per prevenir atacs com la suplantació de servidors DHCP o atacs de "man-in-the-middle" mitjançant ARP spoofing.
- **Llistes de Control d'Accés (ACLs):** S'utilitzaran ACLs per filtrar el trànsit entre VLANs (en els gateways de capa 3) i per protegir l'accés a la infraestructura de xarxa i als serveis crítics.
- **Gestió Segura:** Tot l'accés per a la gestió dels equips es realitzarà mitjançant protocols segurs (SSHv2, HTTPS, SNMPv3). S'inhabilitaran tots els protocols de gestió insegurs (Telnet, HTTP, SNMPv1/v2c).

Protocols de Convergència i Redundància:

La configuració ha de garantir una alta disponibilitat i una ràpida recuperació davant de fallades.

- **Gateway Redundant:** S'utilitzarà un protocol de redundància de primer salt (FHRP) com **VRRP (Virtual Router Redundancy Protocol)** per proporcionar una passarel·la per defecte redundant als dispositius finals de cada VLAN.

- **Agregació d'Enllaços:** S'utilitzarà el protocol **LACP (Link Aggregation Control Protocol)** de manera extensiva per agregar múltiples enllaços físics en un únic enllaç lògic, augmentant l'ample de banda i proporcionant redundància. Això s'aplicarà en les connexions entre commutadors d'accés i distribució/Leaf, i entre servidors i la xarxa.
- **Protocols d'Enrutament:** Com ja s'ha esmentat, s'utilitzarà BGP amb ECMP a la xarxa Spine-Leaf per garantir un balanceig de càrrega i una convergència eficients. En zones de la xarxa on sigui necessari, es podrà utilitzar OSPF. La configuració dels temporitzadors dels protocols s'ajustarà per aconseguir temps de convergència inferiors al segon.

6. Requeriments Tècnics dels Sistemes de Seguretat

Aquesta secció descriu els requisits tècnics per a la gestió, manteniment i explotació dels diferents sistemes que componen l'arquitectura de seguretat de l'Ajuntament de Santa Coloma de Gramenet. L'objecte del contracte inclou la prestació d'un servei integral que garanteixi la confidencialitat, integritat i disponibilitat de la informació i els serveis municipals, mitjançant una administració proactiva i experta de les plataformes de seguretat perimetral, gestió d'esdeveniments de seguretat (SIEM) i publicació segura d'aplicacions (ADC).

L'adjudicatari haurà de proporcionar un equip de tècnics especialitzats amb certificacions i experiència demostrable en les tecnologies especificades, capaços de gestionar el cicle de vida complet de la seguretat: des de la planificació i disseny de polítiques fins a la resposta a incidents, passant per la monitorització contínua i l'optimització de les configuracions. El servei s'ha de prestar seguint les millors pràctiques del sector i en estricte compliment del marc normatiu aplicable, especialment l'Esquema Nacional de Seguretat (ENS).

6.1. Gestió de la Seguretat Perimetral

L'adjudicatari serà responsable de la gestió integral de la infraestructura de seguretat perimetral de l'Ajuntament, basada en la plataforma **Check Point Quantum Maestro**. Aquesta plataforma, que actualment compta amb dos orquestradors MHO-140 i sis passarel·les de seguretat (*Security Gateways*) en versió R81.10 o superior, constitueix la primera línia de defensa de la xarxa corporativa. El servei de gestió ha d'assegurar que la plataforma operi amb la màxima eficàcia, eficiència i seguretat, adaptant-se constantment a l'evolució de les amenaces i a les necessitats de l'organització.

Les tasques mínimes a incloure en aquest servei són:

- **Gestió de Polítiques i Regles de Tallafocs:** L'adjudicatari realitzarà l'administració completa del conjunt de regles de tallafocs (*rulebase*). Aquesta tasca inclou la creació, modificació i eliminació de regles a petició de l'Ajuntament, seguint un procediment de gestió del canvi formal. Cada regla ha d'estar degudament documentada, especificant el seu propòsit,

sol·licitant i data de creació/modificació. A més, es durà a terme una **revisió periòdica (com a mínim semestral) de tot el conjunt de regles** amb l'objectiu d'identificar i eliminar regles redundants, obsoletes o excessivament permissives (*any/any*). Es presentaran informes amb propostes de neteja i optimització per millorar el rendiment i la seguretat.

- **Administració de la Traducció d'Adreces de Xarxa (NAT):** Es gestionaran totes les polítiques de NAT, tant d'origen (SNAT) com de destinació (DNAT), necessàries per a la publicació de serveis o per a la correcta sortida a Internet dels sistemes interns. Igual que amb les regles de tallafocs, qualsevol canvi serà gestionat mitjançant el procediment establert i documentat adequadament.
- **Gestió de Xarxes Privades Virtuals (VPN):** L'adjudicatari serà responsable de la configuració i el manteniment de totes les connexions VPN. Això inclou:
  - **VPNs d'Accés Remot:** Gestió dels perfils d'usuaris, polítiques d'accés i configuració dels clients VPN (per exemple, Check Point Mobile) per garantir un accés segur als recursos de la xarxa corporativa per part dels empleats en mobilitat.
  - **VPNs Lloc a Lloc (Site-to-Site):** Creació i manteniment de túnels IPsec amb terceres entitats o seus remotes, assegurant la interoperabilitat i la robustesa de les connexions. Es monitoritzarà l'estat dels túnels i s'actuarà proactivament en cas de caiguda.
- **Gestió de les Funcionalitats UTM (Unified Threat Management):** El servei inclou l'administració activa i l'afinament (*fine-tuning*) de les diferents fulles de seguretat (*blades*) de Check Point. Això comprèn, entre d'altres:
  - **IPS (Intrusion Prevention System):** Manteniment de la base de dades de signatures i adaptació del perfil de protecció per bloquejar atacs coneguts, minimitzant els falsos positius.
  - **Antivirus i Anti-Malware:** Assegurar que el motor d'inspecció de fitxers està actualitzat i configurat per analitzar el tràfic web (HTTP/HTTPS), correu electrònic (SMTP) i transferència de fitxers (FTP).
  - **Filtratge d'Aplicacions i URLs:** Gestió de les polítiques de control d'accés a aplicacions i categories de llocs web, d'acord amb les directrius de l'Ajuntament.
  - **Sandboxing (Threat Emulation):** Gestió de l'entorn d'emulació per a l'anàlisi de fitxers desconeguts i la detecció d'amenaces de dia zero (*zero-day*).
- **Manteniment i Actualització de la Plataforma:** L'adjudicatari serà responsable de mantenir tota la plataforma Quantum Maestro actualitzada a les versions de programari (firmware, sistema operatiu i aplicacions) recomanades pel fabricant. Això inclou la planificació i execució controlada de les actualitzacions, prèvia aprovació de l'Ajuntament i fora de l'horari productiu per minimitzar l'impacte en el servei. Aquesta gestió cobreix tant els orquestradors com les passarel·les de seguretat.
- **Monitorització i Resolució d'Incidències:** S'haurà de realitzar una monitorització proactiva 24x7 de la salut i el rendiment de la plataforma. S'analitzarà l'ús de CPU, memòria, estat de les sessions i disponibilitat dels enllaços. En cas de detectar-se una anomalia o un incident de

seguretat, l'adjudicatari haurà d'iniciar el procés de resolució dins dels terminis establerts als Acords de Nivell de Servei (ANS).

- **Informes i Documentació:** Es generaran informes mensuals que detallin l'activitat de la plataforma: resum d'atacs bloquejats, tràfic inspeccionat, estat de les VPNs, canvis realitzats i recomanacions de millora. Tota la configuració de la plataforma haurà d'estar completament documentada i actualitzada en tot moment.

6.2. Gestió del Sistema SIEM

El contracte inclou la prestació d'un servei gestionat de **SIEM as a Service**, que ha de garantir la recopilació, correlació i anàlisi centralitzada dels registres (*logs*) de seguretat generats per les diferents infraestructures tecnològiques de l'Ajuntament. La solució actual està basada en tecnologia **RSA Multitenant**, però l'adjudicatari podrà proposar una plataforma tecnològica equivalent, sempre que es compleixin o superin les funcionalitats i capacitats actuals, i es garanteixi una migració transparent i sense pèrdua de dades històriques. L'objectiu és proporcionar a l'Ajuntament una visibilitat completa sobre la seva postura de seguretat, detectar amenaces de forma primerenca i facilitar les anàlisis forenses.

El servei ha de garantir una capacitat de processament mínima de **1500 esdeveniments per segon (EPS)** i un volum d'emmagatzematge de **75 GB diaris**, amb capacitat d'escalat segons les necessitats futures. Els requeriments mínims del servei són:

- **Gestió de Fonts de Dades (*Log Sources*) i Recol·lectors:** L'adjudicatari serà responsable de la gestió integral de les fonts de dades. Això inclou:
  - La **integració de noves fonts de dades** a la plataforma SIEM, incloent-hi tallafocs, commutadors, servidors (Windows, Linux), controladors de domini, aplicacions corporatives i sistemes al núvol (Cloud).
  - La instal·lació, configuració i manteniment dels **recol·lectors de logs** necessaris, assegurant la seva correcta comunicació amb la plataforma central. Si és necessari un canvi de recol·lector, l'adjudicatari s'encarregarà de la seva configuració.
  - El desenvolupament i/o adaptació de *parsers* per a aquelles fonts de dades que no tinguin un connector estàndard, garantint que tots els logs siguin normalitzats i enriquits correctament.
- **Gestió de Regles de Correlació i Casos d'Ús:** Aquesta és una de les tasques clau del servei. L'adjudicatari haurà de:
  - Mantenir i **afinar contínuament les regles de correlació existents** per reduir la generació de falsos positius i millorar la precisió de les alertes.
  - Desenvolupar i implementar **nous casos d'ús i regles de correlació** en resposta a noves amenaces, la incorporació de noves fonts de dades o requeriments específics de l'Ajuntament. Es valorarà positivament l'alineació d'aquests casos d'ús amb marcs de referència com **MITRE ATT&CK**.

- Gestionar les llistes de referència (*reference sets*) i la lògica de dependències del sistema per assegurar un funcionament coherent.

- **Manteniment i Operació de la Plataforma SIEM:** L'adjudicatari garantirà la salut i el rendiment de la infraestructura SIEM, realitzant tasques de:
  - Planificació i execució d'actualitzacions de programari i pegats de seguretat de tots els components de la plataforma.
  - Monitorització del rendiment del sistema, incloent-hi la ràtio d'EPS, la latència en la ingesta i el processament, i l'ús de recursos.
  - Gestió de les polítiques de retenció de dades, configurant els diferents nivells d'emmagatzematge per complir amb els requisits normatius i operatius.
- **Elaboració d'Informes i Quadres de Comandament:** El servei inclourà la creació i manteniment d'informes i quadres de comandament (*dashboards*) personalitzats per a l'Ajuntament, que proporcionin visibilitat sobre l'estat de la seguretat. Això comprèn:
  - **Quadres de comandament operatius** per al personal tècnic, amb una visió en temps real dels esdeveniments de seguretat més rellevants.
  - **Informes executius mensuals** que resumeixin la postura de seguretat, les principals tendències i els incidents destacats.
  - Generació d'informes a demanda per a auditories o investigacions d'incidents específics.

6.3. Gestió de la Plataforma ADC

L'adjudicatari serà responsable de la gestió i el manteniment de la plataforma de lliurament d'aplicacions (ADC), basada en l'equipament **NetScaler MPX-8905** o un model superior o equivalent. Aquesta plataforma és crítica per garantir la disponibilitat, el rendiment i la seguretat de les aplicacions i serveis web publicats per l'Ajuntament. El servei ha de cobrir tota la pila funcional de l'ADC, des del balanceig de càrrega fins a la seguretat de les aplicacions.

Les principals tasques de gestió associades a aquesta plataforma són:

- **Gestió de Servidors Virtuals (*Virtual Servers*) i Serveis:** Administració dels servidors virtuals que actuen com a punt d'entrada per a les aplicacions. Això inclou la creació, modificació i eliminació de servidors virtuals, l'associació de grups de serveis (*service groups*) que contenen els servidors reals, i la configuració dels monitors de salut per verificar l'estat dels servidors back-end.
- **Balanceig de Càrrega (*Load Balancing*):** Configuració i afinament dels algorismes de balanceig de càrrega (ex. *Least Connection*, *Round Robin*) per distribuir el tràfic de manera eficient entre els servidors d'aplicacions. S'implementaran mètodes de persistència (ex. basats en cookies o en l'adreça IP d'origen) per garantir que les sessions dels usuaris es mantinguin en el mateix servidor quan sigui necessari.

- **Descàrrega SSL/TLS (*SSL Offloading*):** Gestió del cicle de vida dels certificats digitals SSL/TLS instal·lats a la plataforma. L'adjudicatari s'encarregarà de la creació de les sol·licituds de signatura de certificats (CSR), la seva instal·lació, la renovació abans que expirin i la configuració dels perfils SSL/TLS per garantir l'ús de xifrats robustos i protocols segurs, seguint les millors pràctiques (ex. deshabilitació de SSLv3/TLS 1.0/1.1).
- **Tallafocs d'Aplicacions Web (WAF - *Web Application Firewall*):** L'adjudicatari gestionarà la funcionalitat WAF de la plataforma per protegir les aplicacions web contra atacs comuns com ara SQL Injection, Cross-Site Scripting (XSS) i altres amenaces recollides a l'**OWASP Top 10**. Això inclou la configuració dels perfils de seguretat, l'actualització de les signatures de protecció i l'anàlisi dels logs de WAF per identificar patrons d'atac i afinar les polítiques.
- **Gestió de Polítiques Avançades (*Responder, Rewrite, Content Switching*):** Implementació de polítiques per a la manipulació del tràfic. Això pot incloure la reescriptura d'URL, la inserció o modificació de capçaleres HTTP, o la redirecció d'usuaris a diferents grups de servidors en funció de les característiques de la seva petició (ex. *Content Switching* basat en l'URL o el tipus de dispositiu).
- **Manteniment i Actualització del Firmware:** L'adjudicatari serà responsable de mantenir el firmware del NetScaler actualitzat a una versió estable i segura recomanada pel fabricant. Les actualitzacions es planificaran i executaran de manera controlada, minimitzant l'impacte sobre la disponibilitat de les aplicacions.
- **Monitorització i Informes:** Monitorització contínua del rendiment i la salut de la plataforma, analitzant mètriques com el nombre de peticions per segon, l'ús de la CPU/memòria i el rendiment de les aplicacions. Es generaran informes periòdics sobre l'estat del servei i es proporcionarà accés a la documentació actualitzada de la configuració.

7. Sistema de Gestió, Monitorització i Control d'Accés

La gestió eficient, la visibilitat completa i la securització proactiva de la infraestructura de xarxa són pilars fonamentals per garantir la continuïtat i la integritat dels serveis que l'Ajuntament de Santa Coloma de Gramenet presta als seus ciutadans i al seu personal intern. Una plataforma de gestió centralitzada no només simplifica les tasques operatives i redueix el temps de resolució d'incidències, sinó que també proporciona les eines necessàries per aplicar polítiques de seguretat coherents i automatitzades a tota la xarxa. En aquest context, aquest apartat defineix els requisits tècnics per a la provisió d'una solució integral que comprèn dos components clau: l'actualització i l'evolució de la plataforma de gestió de xarxa existent i la implementació d'un sistema avançat de Control d'Accés a la Xarxa (NAC).

L'objectiu principal és dotar el personal tècnic de l'Ajuntament d'una monoconsola potent des de la qual puguin configurar, monitoritzar, analitzar i securitzar tots els elements de la infraestructura

LAN, des dels commutadors del nucli fins als dispositius finals que s'hi connecten. La solució haurà de ser escalable, robusta i estar perfectament integrada, assegurant una transició fluida des de la situació actual i proporcionant una base sòlida per al creixement futur.

L'adjudicatari haurà de proporcionar una solució "claus en mà", incloent-hi tot el maquinari, el programari, les llicències, els serveis professionals d'instal·lació, configuració, migració i formació necessaris per complir amb els requisits descrits en aquest apartat. Totes les llicències subministrades hauran de cobrir, com a mínim, la totalitat de la durada del contracte.

Actualització de la Plataforma de Gestió Centralitzada

Actualment, l'Ajuntament utilitza la plataforma Extreme NetSight per a la gestió de la seva infraestructura de xarxa. Atesa l'evolució tecnològica i l'obsolescència d'aquesta versió, és un requisit indispensable del present contracte l'actualització i migració a la darrera versió estable de la plataforma de gestió equivalent del mateix fabricant, actualment denominada **ExtremeCloud IQ – Site Engine (XIQ-SE)**. La solució proposada haurà de ser instal·lada en format de màquina virtual (appliance virtual) sobre la infraestructura de virtualització de l'Ajuntament, i haurà de ser dimensionada per gestionar la totalitat dels equips existents i els nous equips subministrats, amb un marge de creixement d'almenys un 30%.

La plataforma haurà de proporcionar, com a mínim, les següents funcionalitats:

- **Gestió Unificada i Centralitzada:** La plataforma ha de permetre la gestió integral de tots els dispositius de xarxa cablejada (commutadors de nucli, de distribució i d'accés) des d'una única interfície gràfica web. Ha de proporcionar una visibilitat completa de l'estat operatiu, la configuració i el rendiment de cada element de la xarxa.
- **Inventari i Topologia de Xarxa:** El sistema ha de ser capaç de realitzar una descoberta automatitzada de la xarxa per identificar tots els dispositius connectats i generar un inventari detallat. Aquest inventari ha d'incloure informació com el model, número de sèrie, versió de firmware, configuració de ports i estat operatiu. Així mateix, ha de ser capaç de generar i mantenir **mapes de topologia dinàmics** i interactius que reflecteixin les connexions físiques i lògiques (VLANs, enllaços agregats) entre els dispositius.
- **Configuració i Automatització:** La plataforma ha de facilitar l'automatització de les tasques de configuració. S'ha de permetre la creació de plantilles de configuració, l'aplicació de canvis de manera massiva a múltiples dispositius i la programació de tasques. Es requereix explícitament la funcionalitat d'**aprovisionament sense intervenció (Zero Touch Provisioning - ZTP)** per als nous equips, permetent que un commutador nou, en connectar-se a la xarxa, obtingui automàticament la seva configuració i versió de firmware des de la plataforma de gestió.

- **Monitorització Proactiva i Analítica:** El sistema ha de monitoritzar de manera contínua el rendiment de la xarxa, recopilant mètriques clau com l'ús de la CPU i memòria dels equips, la utilització de l'ample de banda dels enllaços, les taxes d'errors i els paquets descartats. Ha de disposar d'un sistema d'alarmes configurable que notifiqui el personal tècnic davant de fallades o degradacions del servei. A més, ha de proporcionar eines d'anàlisi i **emmagatzematge de dades històriques** per facilitar la resolució de problemes (*troubleshooting*), la planificació de capacitat i l'anàlisi de tendències.
- **Gestió de Firmware:** La plataforma ha de centralitzar i simplificar la gestió del cicle de vida del firmware dels commutadors. Ha de permetre l'arxiu de diferents versions de firmware, la distribució programada als dispositius i la verificació de la integritat de les actualitzacions, minimitzant el risc i l'impacte en el servei.

Implementació del Sistema de Control d'Accés a la Xarxa (NAC)

Per tal de donar compliment a les polítiques de seguretat de l'Ajuntament i als requisits de l'Esquema Nacional de Seguretat (ENS), és obligatòria la implementació d'una solució de **Control d'Accés a la Xarxa (NAC)**. Aquesta solució haurà d'estar perfectament integrada amb la plataforma de gestió ExtremeCloud IQ – Site Engine i ha de ser capaç de gestionar un mínim de **2000 dispositius concurrents**, tant cablejats com sense fils (tot i que la gestió de la xarxa sense fils no és objecte d'aquest contracte, el NAC ha d'estar preparat per a una futura integració).

El sistema NAC ha de proporcionar un control granular sobre quins dispositius i usuaris poden accedir a la xarxa i a quins recursos tenen permís, basant-se en polítiques de seguretat centralitzades. Les funcionalitats mínimes requerides són:

- **Visibilitat i Perfilat de Dispositius (Profiling):** El sistema ha de ser capaç d'identificar, classificar i perfilar automàticament qualsevol dispositiu que es connecti a la xarxa, fins i tot abans de l'autenticació. Per a això, ha d'emprar múltiples tècniques com l'anàlisi de les adreces MAC OUI, el *fingerprinting* del protocol DHCP, l'anàlisi de les capçaleres HTTP (User-Agent), i protocols de descoberta com LLDP. L'objectiu és classificar els dispositius en categories (p. ex., ordinador corporatiu, telèfon IP, impressora, dispositiu personal - BYOD, dispositiu IoT) per poder aplicar polítiques específiques.
- **Autenticació d'Usuaris i Dispositius:** El sistema ha de suportar múltiples mètodes d'autenticació per adaptar-se als diferents tipus de dispositius i usuaris.
  - **Autenticació basada en 802.1X:** Per a dispositius corporatius gestionats (ordinadors, portàtils), garantint una autenticació segura basada en credencials d'usuari o certificats digitals. La integració amb el directori actiu de l'Ajuntament (Microsoft Active Directory) a través del protocol **RADIUS** és un requisit indispensable.

  - **MAC Authentication Bypass (MAB):** Per a dispositius que no suporten 802.1X, com impressores, telèfons IP o càmeres, permetent una autenticació basada en la seva adreça MAC.
  - **Portal Captiu:** Per a la gestió d'usuaris convidats i l'autoregistre de dispositius personals (BYOD). El portal ha de ser personalitzable amb la imatge corporativa de l'Ajuntament.
- **Autorització i Aplicació de Polítiques Dinàmiques:** Un cop autenticat un usuari o dispositiu, el sistema NAC ha de ser capaç d'aplicar una política d'autorització granular i dinàmica. Això ha d'incloure, com a mínim:
  - **Assignació Dinàmica de VLAN:** Assignar el dispositiu a una VLAN específica en funció del seu perfil, el rol de l'usuari, la seva ubicació física o l'hora del dia. Per exemple, un usuari del departament de Recursos Humans es connectarà automàticament a la VLAN de RRHH, mentre que un convidat serà aïllat a la VLAN de convidats amb accés restringit a Internet.
  - **Aplicació d'ACLs Granulars:** Aplicar llistes de control d'accés (ACLs) o polítiques de tallafocs a nivell de port per restringir la comunicació entre dispositius o limitar l'accés a serveis crítics.
- **Avaluació de la Postura de Seguretat (Posture Assessment):** El sistema ha de ser capaç d'avaluar l'estat de compliment de seguretat dels dispositius que intenten accedir a la xarxa. Ha de poder verificar, mitjançant un agent lleuger o sense agent (agentless), aspectes com:
  - Versió del sistema operatiu i nivell de pegats de seguretat.
  - Estat de l'antivirus (instal·lat, en execució i actualitzat).
  - Existència de programari no autoritzat.
  - Activació del tallafocs local.

Els dispositius que no compleixin amb la política de seguretat definida hauran de ser automàticament **aïllats en una VLAN de quarantena o remediació**, on només tinguin accés a servidors d'actualització per poder corregir la seva postura abans de permetre'ls l'accés complet.

- **Gestió de Convidats:** La solució ha d'incloure un mòdul robust per a la gestió del cicle de vida dels usuaris convidats. Ha de permetre l'autoregistre a través del portal captiu, amb opcions de patrocini (un empleat intern ha d'aprovar l'accés) i la creació de comptes temporals amb dates de caducitat i limitacions d'ample de banda.

L'arquitectura de la solució NAC haurà de ser dissenyada en una configuració d'**alta disponibilitat (HA)** per garantir que una fallada en un dels components no provoqui una denegació de servei a la xarxa. Totes les llicències necessàries per a les funcionalitats descrites i per al nombre de dispositius especificat hauran d'estar incloses en la proposta de l'adjudicatari per a tota la durada del contracte.

8. Serveis de Manteniment i Explotació

El present capítol descriu el conjunt de serveis recurrents d'operació, administració, manteniment i suport que l'empresa adjudicatària haurà de prestar durant tota la vigència del contracte. Aquests serveis són fonamentals per garantir l'òptim funcionament, la disponibilitat, el rendiment i la seguretat de la infraestructura LAN i dels sistemes de seguretat perimetral de l'Ajuntament. L'objectiu és establir un marc de gestió proactiu i eficient que asseguri la continuïtat operativa dels serveis TIC municipals, minimitzi les interrupcions i permeti una evolució ordenada de la infraestructura.

El model de servei es basa en les millors pràctiques del mercat, com les definides en el marc de referència ITIL, i s'estructura en tres grans àmbits: el model de gestió del servei, els serveis d'operació i suport, i els serveis de manteniment i suport tècnic. L'adjudicatari haurà d'aportar tots els recursos humans i materials necessaris per a la correcta execució d'aquestes tasques, les quals s'entenen incloses en el preu del contracte.

8.1. Model de Gestió del Servei

Per garantir una comunicació fluida, una gestió eficient i una relació de col·laboració estratègica, l'adjudicatari haurà d'implementar un model de gestió de servei personalitzat, centralitzat i professional. Aquest model definirà els perfils, les responsabilitats, els canals de comunicació i el marc de governança del servei.

El servei s'ha de prestar a través d'una **finestra única de servei (Single Point of Contact - SPOC)**, que centralitzarà totes les comunicacions entre l'Ajuntament i l'adjudicatari per a la gestió d'incidències, peticions de servei, gestió de canvis i consultes tècniques. Aquesta finestra única ha d'estar accessible mitjançant un portal web de gestió de tiquets, correu electrònic i telèfon.

L'adjudicatari haurà d'assignar al servei un equip de professionals amb l'experiència i les certificacions adequades per a les tasques a realitzar. Com a mínim, s'hauran de definir i assignar els següents perfils:

- **Responsable del Servei (Service Manager):** Serà l'interlocutor principal de l'Ajuntament per a tots els aspectes contractuals i de gestió del servei. Serà el responsable últim de la qualitat del servei prestat, del compliment dels Acords de Nivell de Servei (ANS) i de la satisfacció del client. Haurà de liderar el Comitè de Seguiment del Servei, elaborar els informes de seguiment i proposar plans de millora contínua. Es requereix que aquest perfil tingui una experiència mínima de 5 anys en gestió de serveis TIC a administracions públiques i que estigui certificat, com a mínim, en **ITIL v4 Foundation**. La seva dedicació al servei ha de ser suficient per garantir una gestió proactiva i eficaç.
- **Enginyer/a especialista en Xarxes i Seguretat:** Serà el responsable tècnic de la infraestructura gestionada. Aquest perfil serà l'encarregat de resoldre les incidències de nivell avançat,

planificar i executar els canvis complexos, supervisar les actualitzacions de programari, i donar suport a les auditories de seguretat. Haurà de posseir un coneixement profund de les tecnologies implementades. Es requereix una experiència mínima de 5 anys en disseny, implementació i gestió d'infraestructures de xarxa i seguretat complexes, i posseir certificacions tècniques de nivell professional dels principals fabricants de la solució proposada (per exemple, **Extreme Certified Specialist - ECS, Check Point Certified Security Expert - CCSE** o equivalents).

- **Tècnics d'Operació i Suport:** Equip de tècnics encarregats de la monitorització del servei, la gestió d'incidències de primer i segon nivell, i l'execució de canvis estàndard. Hauran de tenir coneixements de les tecnologies gestionades i estar certificats en les tecnologies base (per exemple, **Extreme Certified Professional - ECP, Check Point Certified Security Administrator - CCSA** o equivalents).

L'adjudicatari haurà de facilitar un organigrama detallat amb els noms, rols, dades de contacte, dedicació i certificacions de cada membre de l'equip assignat al servei. Qualsevol canvi en el personal clau (Responsable del Servei, Enginyer especialista) haurà de ser notificat i aprovat prèviament per l'Ajuntament.

8.2. Operació i Suport

Aquest bloc de serveis agrupa les tasques diàries necessàries per al funcionament i l'administració de la infraestructura.

Gestió de l'Inventari (Gestió de la Configuració):

L'adjudicatari serà responsable de crear i mantenir una **Base de Dades de Gestió de la Configuració (CMDB)** que contingui un inventari detallat i permanentment actualitzat de tots els elements de configuració (CI) sota l'abast del contracte. Aquesta CMDB haurà de ser accessible per al personal autoritzat de l'Ajuntament. Per a cada CI, s'haurà de registrar, com a mínim, la informació següent: identificador únic, fabricant, model, número de sèrie, versió del sistema operatiu/firmware, ubicació física (edifici, sala, armari rack), adreçament IP de gestió, data d'instal·lació, estat del cicle de vida (actiu, en magatzem, pendent de retirada), i informació sobre la garantia i el contracte de manteniment associat. Qualsevol canvi en la infraestructura (alta, baixa, modificació) haurà de quedar reflectit a la CMDB en un termini màxim de 48 hores.

Gestió de Canvis:

L'adjudicatari haurà d'implementar un procediment formal de gestió de canvis per a totes les modificacions que s'hagin de realitzar a la infraestructura. L'objectiu és minimitzar l'impacte negatiu dels canvis sobre el servei i garantir que es realitzen de forma controlada i documentada. El procediment haurà de distingir entre canvis estàndard (pre-aprovats, de baix risc), normals i d'emergència. Tota sol·licitud de canvi haurà de ser registrada a l'eina de gestió de tiquets i haurà

d'incloure, com a mínim: descripció del canvi, justificació, anàlisi d'impacte i risc, pla d'execució detallat (amb tasques i responsables), pla de proves per a la seva validació, i un pla de retorn (*rollback*) en cas de fallada. Els canvis normals requeriran l'aprovació explícita del personal tècnic de l'Ajuntament abans de la seva execució, que es realitzarà preferentment en finestres de manteniment acordades per minimitzar l'afectació als usuaris.

Monitorització Proactiva:

L'adjudicatari haurà d'implementar i operar una solució de monitorització centralitzada que permeti una supervisió constant i proactiva de tota la infraestructura gestionada. La monitorització haurà de cobrir, com a mínim, els següents aspectes:

- **Disponibilitat:** Verificació de l'estat (amunt/avall) de tots els dispositius de xarxa, enllaços WAN, i serveis de seguretat.
- **Rendiment:** Seguiment de mètriques clau com l'ús de CPU i memòria dels equips, la utilització de l'ample de banda dels enllaços troncals, les taxes d'errors i descartaments de paquets en les interfícies, i la latència de la xarxa.
- **Seguretat:** Monitorització dels logs dels tallafocs, del sistema SIEM i de l'eina NAC per a la detecció d'esdeveniments de seguretat, com intents d'intrusió, connexions no autoritzades o activitat maliciosa.
- **Capacitat:** Anàlisi de tendències per preveure futurs esgotaments de recursos (ports disponibles, potència PoE, capacitat de processament dels tallafocs, etc.).

El sistema de monitorització haurà d'estar configurat per generar alertes automàtiques davant de llindars predefinits. L'adjudicatari serà responsable d'analitzar aquestes alertes i actuar de forma proactiva per resoldre els problemes abans que impactin de manera significativa en el servei.

Elaboració d'Informes:

L'adjudicatari haurà de generar i lliurar a l'Ajuntament un conjunt d'informes periòdics sobre l'estat del servei. Com a mínim, s'inclouran:

- **Informe Mensual de Servei:** Aquest informe detallarà el compliment dels ANS durant el període, un resum de totes les incidències registrades (amb temps de resposta i resolució), la llista de canvis executats, gràfiques de rendiment i disponibilitat dels elements més crítics, i un resum de les alertes de seguretat més rellevants.
- **Informe Executiu Trimestral:** Orientat a la direcció, aquest informe presentarà una anàlisi de tendències a mitjà termini, l'estat de la capacitat de la infraestructura, recomanacions estratègiques per a la millora del servei (tecnològiques o de procés) i un resum de l'estat dels riscos de seguretat.

- **Informes a Demanda:** L'adjudicatari haurà de tenir la capacitat de generar informes específics a petició de l'Ajuntament per a anàlisis puntuals o auditories.

8.3. Manteniment i Suport Tècnic

Aquest conjunt de serveis té com a finalitat mantenir la infraestructura en un estat òptim de funcionament, resoldre les avaries que es produeixin i assegurar la seva evolució tecnològica.

Manteniment Preventiu:

L'adjudicatari haurà d'elaborar i executar un pla de manteniment preventiu anual. L'objectiu és identificar i corregir problemes potencials abans que causin una interrupció del servei. Aquest pla ha d'incloure, com a mínim, la revisió periòdica de les configuracions dels equips per assegurar que s'alineen amb les millors pràctiques; l'anàlisi de logs per detectar patrons anòmals; la verificació de l'estat de les fonts d'alimentació i sistemes de refrigeració; i la comprovació de la correcta execució de les còpies de seguretat de les configuracions.

Manteniment Correctiu (Gestió d'Incidències):

L'adjudicatari serà responsable de la resolució de totes les incidències que afectin la infraestructura gestionada, d'acord amb els temps de resposta i resolució definits als Acords de Nivell de Servei (ANS) d'aquest plec. El procés de gestió d'incidències ha d'incloure el registre, la categorització i priorització de la incidència, el diagnòstic, l'escalat a nivells superiors o al fabricant si s'escau, l'aplicació de la solució, la verificació amb l'usuari i el tancament. Per a les incidències crítiques, l'adjudicatari haurà de realitzar una **Anàlisi de Causa Arrel (RCA)** per identificar l'origen del problema i proposar accions per evitar la seva recurrència.

Gestió de Garanties i Suport del Fabricant:

L'adjudicatari serà l'únic responsable de gestionar totes les garanties del maquinari i els contractes de suport del programari amb els respectius fabricants durant tota la vida del contracte. Això inclou l'obertura i seguiment de tiquets de suport amb els fabricants (com Extreme Networks, Check Point, etc.), la gestió de la substitució de maquinari avariat (procés d'RMA), i l'escalat de problemes de programari complexos. L'Ajuntament no haurà d'interactuar directament amb els fabricants per a qüestions de suport.

Actualització de Programari i Microprogramari (Firmware):

L'adjudicatari serà responsable de mantenir actualitzats tots els components de programari i microprogramari de la infraestructura (sistemes operatius dels commutadors, versions dels tallafocs, firmwares dels controladors, etc.) a versions estables, segures i recomanades pels fabricants. Aquesta gestió inclou la planificació, prova i execució de les actualitzacions, seguint el procediment formal de gestió de canvis. L'adjudicatari haurà d'informar proactivament a

l'Ajuntament sobre les noves versions disponibles, especialment aquelles que corregeixen vulnerabilitats de seguretat crítiques, i planificar la seva instal·lació en les finestres de manteniment acordades.

Auditoria de Seguretat Bianual:

Amb una periodicitat de dues vegades l'any, l'adjudicatari haurà de realitzar una auditoria de seguretat completa de la infraestructura gestionada, la primera de les quals s'haurà de realitzar dins dels primers sis mesos del contracte. Aquesta auditoria ha de cobrir, com a mínim, una anàlisi de vulnerabilitats dels actius exposats, una revisió exhaustiva de les configuracions de seguretat dels commutadors, tallafocs i sistema NAC per verificar l'alineació amb les millors pràctiques del sector i els requisits de l'Esquema Nacional de Seguretat (ENS), i una revisió de la política de regles dels tallafocs per identificar regles obsoletes, redundants o excessivament permissives. El resultat de cada auditoria serà un informe detallat que identifiqui les troballes, classifiqui els riscos associats i proposi un pla d'acció concret amb recomanacions per a la seva mitigació. L'adjudicatari serà responsable de l'execució de les accions correctores acordades amb l'Ajuntament.

9. Pla d'Implantació i Migració

La implantació de la nova infraestructura LAN i la transició dels serveis de gestió de la seguretat representen un procés crític per a la continuïtat de les operacions de l'Ajuntament de Santa Coloma de Gramenet. Per aquest motiu, l'adjudicatari haurà de presentar i executar un Pla d'Implantació i Migració exhaustiu, que garanteixi una transició ordenada, eficient i amb el mínim impacte possible sobre els usuaris i els serveis municipals. Aquest pla ha de ser concebut sota una metodologia de gestió de projectes formal i ha de cobrir totes les fases, des de la planificació inicial fins a l'acceptació final de la solució i el lliurament de la documentació corresponent. La responsabilitat de l'execució exitosa del projecte recau íntegrament en l'adjudicatari, que haurà de coordinar tots els recursos tècnics i humans necessaris per complir amb els terminis i els objectius de qualitat establerts en aquest plec.

Un cop formalitzat el contracte, l'adjudicatari disposarà d'un termini màxim de quatre (4) setmanes per elaborar i presentar a l'Ajuntament un **Projecte Executiu** detallat. Aquest document serà la pedra angular de la implantació i haurà de ser validat i aprovat per l'Ajuntament abans de l'inici de qualsevol tasca d'instal·lació o migració. El Projecte Executiu ha d'incloure, com a mínim, els següents apartats:

9.1 Planificació Detallada del Projecte

L'adjudicatari haurà de lliurar un pla de treball detallat que serveixi com a full de ruta per a tot el procés d'implantació. Aquest pla s'haurà de presentar en format de **diagrama de Gantt** o similar, i haurà d'especificar de manera clara i concisa:

- **Fases del projecte:** Desglossament de les principals etapes del projecte, com ara l'anàlisi de detall, el disseny final, la provisió de material, la instal·lació, la configuració, la migració, les proves i l'entrada en servei.
- **Tasques i activitats:** Identificació de totes les tasques necessàries per a cada fase, amb una estimació de la seva durada i els recursos assignats.
- **Dependències i Fites (Milestones):** Definició de les interdependències entre tasques i l'establiment de fites clau que permetin mesurar el progrés del projecte, com ara "Recepció de l'equipament", "Finalització migració del Core" o "Acceptació del sistema NAC".
- **Cronograma:** Un calendari precís que indiqui les dates d'inici i finalització previstes per a cada tasca i fase, respectant el termini màxim d'implantació global establert en aquest plec.
- **Recursos assignats:** Identificació del personal tècnic que participarà en el projecte, amb els seus rols i responsabilitats.

Aquest pla ha de ser realista i consensuat amb l'equip tècnic de l'Ajuntament per garantir la seva viabilitat. Qualsevol desviació sobre el pla aprovat haurà de ser comunicada, justificada i acceptada formalment per l'Ajuntament.

9.2 Pla de Migració de la Infraestructura

Aquest és un dels components més crítics del projecte. El pla de migració ha de descriure amb el màxim detall el procediment tècnic per substituir l'equipament existent i transicionar els serveis cap a la nova plataforma, **minimitzant en tot moment la interrupció del servei**. Totes les intervencions que puguin causar talls de servei s'hauran de planificar fora de l'horari laboral (preferiblement en horari nocturn o durant el cap de setmana) i requeriran l'aprovació explícita de l'Ajuntament.

El pla de migració haurà d'abordar, com a mínim:

- **Migració del Core de xarxa:** Descripció del procés per substituir els xassís actuals per la nova arquitectura Spine-Leaf. S'haurà de detallar l'estratègia a seguir (p. ex., implementació en paral·lel, migració per fases) per assegurar que no es produeixi una pèrdua de connectivitat durant el procés.
- **Renovació dels commutadors d'accés:** Planificació de la substitució dels equips de planta a les diferents seus municipals, coordinant-se amb els usuaris i responsables de cada edifici per minimitzar les molèsties.
- **Migració del sistema de gestió i NAC:** Detall del procés de migració de la plataforma de gestió actual a la nova versió (ExtremeCloud IQ) i la implementació del nou sistema de Control d'Accés a la Xarxa (NAC), incloent la fase de perfilat inicial dels dispositius i la posterior activació progressiva de les polítiques de control.
- **Pla de Rollback (Marxa enrere):** Per a cada etapa crítica de la migració, s'haurà de definir un pla de *rollback* detallat. Aquest pla ha de descriure els passos tècnics necessaris per revertir

els canvis i tornar a l'estat operatiu anterior a la intervenció en cas que sorgeixin problemes greus que impedeixin la finalització exitosa de la migració.

9.3 Pla de Proves i Validació

Un cop finalitzada la instal·lació i configuració de la nova infraestructura, l'adjudicatari haurà de dur a terme un protocol de proves exhaustiu per verificar que la solució compleix tots els requisits tècnics i funcionals definits en aquest plec. L'inici de l'explotació del servei no serà possible fins que aquestes proves hagin estat superades amb èxit i l'Ajuntament hagi emès l'Acta d'Acceptació formal.

El pla de proves haurà d'incloure, entre d'altres:

- **Proves d'Infraestructura:** Verificació de la connectivitat física, el correcte funcionament dels enllaços troncals, les proves de redundància (simulació de fallada de fonts d'alimentació, enllaços, commutadors Spine) i la validació de l'alimentació PoE als ports designats.
- **Proves de Rendiment:** Mesurament de l'ample de banda i la latència entre punts clau de la xarxa per assegurar que el rendiment s'ajusta a l'esperat.
- **Proves Funcionals:** Validació de la correcta configuració de les VLAN, l'enrutament entre elles, les llistes de control d'accés (ACLs), el funcionament dels protocols de xarxa i la correcta operativa del sistema NAC (autenticació 802.1x, assignació dinàmica de VLAN, etc.).
- **Proves de Gestió:** Comprovació de totes les funcionalitats de la plataforma de gestió, incloent la correcta visualització de l'inventari, la monitorització en temps real, la generació d'alertes i la creació d'informes.
- **Proves d'Acceptació d'Usuari (UAT):** L'Ajuntament definirà un conjunt de casos de prova que seran executats conjuntament amb l'adjudicatari per donar la conformitat final a la solució.

9.4 Lliurament de Documentació Tècnica (As-Built)

A la finalització del projecte, l'adjudicatari haurà de lliurar un dossier complet de documentació "as-built" que reflecteixi de manera fidedigna l'estat final de la infraestructura implementada. Aquesta documentació és propietat de l'Ajuntament i ha de ser lliurada en format digital editable. El contingut mínim de la documentació serà:

- **Diagrames de xarxa:** Mapes de la topologia física (ubicació d'equips a racks, cablejat) i lògica (arquitectura Spine-Leaf, enllaços entre equips).
- **Pla d'adreçament IP i VLANs:** Documentació detallada de l'esquema d'adreçament IP, subxarxes i la definició de totes les VLANs implementades, amb la seva funció.
- **Inventari detallat:** Llistat complet de tot l'equipament (hardware i software) instal·lat, incloent-hi models, números de sèrie, versions de firmware/software, i informació sobre llicències i garanties.

- **Fitxers de configuració:** Còpia de seguretat dels fitxers de configuració finals de tots els dispositius de xarxa.
- **Manuals d'operació:** Guies i procediments bàsics per a l'administració i operació diària de la plataforma per part del personal tècnic de l'Ajuntament.
- **Informe de resultats de les proves:** Documentació formal que reculli els resultats de totes les proves executades durant la fase de validació, incloent l'acta de signatura de l'UAT.

Aquesta documentació haurà de ser mantinguda i actualitzada per l'adjudicatari durant tota la vigència del contracte davant de qualsevol canvi o modificació realitzada.

10. Acords de Nivell de Servei (ANS)

Aquest apartat estableix els compromisos de qualitat que l'adjudicatari haurà d'assumir en la prestació del servei. Els Acords de Nivell de Servei (ANS) constitueixen una part fonamental del contracte, ja que defineixen de manera objectiva, mesurable i verificable els estàndards de rendiment i disponibilitat de la infraestructura i els serveis gestionats. L'objectiu és garantir que l'Ajuntament de Santa Coloma de Gramenet rep un servei de qualitat, proactiu i alineat amb les seves necessitats operatives.

L'incompliment dels indicadors aquí definits comportarà l'aplicació de les penalitzacions econòmiques descrites en aquest mateix apartat, sense perjudici d'altres responsabilitats que es puguin derivar de l'execució del contracte. L'adjudicatari haurà de proporcionar les eines necessàries per al mesurament continu dels indicadors i facilitar l'accés a l'Ajuntament per a la seva verificació.

10.1. Marc General i Metodologia de Mesura

La gestió i el seguiment dels ANS es realitzarà en el si del Comitè de Seguiment del Servei. La metodologia per al mesurament i càlcul dels indicadors es regeix pels següents principis:

- **Mesurament Continu:** Els paràmetres seran mesurats de forma contínua mitjançant les eines de monitorització i gestió de l'adjudicatari, les quals hauran de ser accessibles per al personal tècnic de l'Ajuntament per a tasques de consulta.
- **Període de Càlcul:** El període de càlcul per als indicadors recurrents serà el mes natural.
- **Temps d'Aturada Justificada:** No es computarà com a temps d'indisponibilitat o retard en la resolució aquell període en què la prestació del servei es vegi impedida per causes de força major, accions de tercers aliens a l'adjudicatari o per requeriment explícit de l'Ajuntament (per exemple, per a la realització de proves). Aquest temps es considerarà "temps d'aturada justificada" i s'haurà de documentar i aprovar pel Comitè de Seguiment. De la mateixa manera, les intervencions preventives programades i acordades amb l'Ajuntament fora de l'horari productiu no computaran com a indisponibilitat.

- **Responsabilitat de l'Adjudicatari:** L'adjudicatari serà l'únic responsable del compliment dels ANS. En la proposta presentada s'haurà d'incloure el detall de la metodologia i les eines que utilitzarà per al seu seguiment.

10.2. Tipificació d'Incidències i Nivells de Criticitat

Per a una correcta aplicació dels ANS, es defineix una classificació de les incidències en funció del seu impacte sobre el servei, així com una diferenciació de les seus i sistemes segons la seva criticitat.

Classificació de la Criticitat de Sistemes i Seus:

- **Sistemes Crítics:** Són aquells components la fallada dels quals provoca una interrupció total o molt severa del servei a una part significativa de l'organització. Es consideren crítics:
  - La infraestructura de Core (commutadors *Spine* i *Leaf*).
  - Els sistemes de seguretat perimetral (plataforma Check Point Quantum Maestro).
  - La plataforma de publicació d'aplicacions (ADC NetScaler).
  - El sistema SIEM.
  - Els commutadors d'accés de seus considerades crítiques, com la Casa Consistorial o les dependències de la Policia Local.
- **Sistemes Estàndard:** La resta d'equipaments d'accés/planta no inclosos en la categoria anterior.

Classificació de la Severitat de les Incidències:

- **Incidència de Criticitat MOLT GREU:** Qualsevol incident que provoqui:
  - La pèrdua total de connectivitat en un o més **Sistemes Crítics**.
  - La caiguda completa dels sistemes de seguretat perimetral, ADC o SIEM.
  - La indisponibilitat de més del 50% dels commutadors d'accés d'una mateixa seu.
- **Incidència de Criticitat GREU:** Qualsevol incident que provoqui:
  - La pèrdua de redundància en qualsevol **Sistema Crític**.
  - Una degradació severa i persistent del rendiment de la xarxa que afecti un nombre significatiu d'usuaris (>25%).
  - La caiguda d'un commutador d'accés en una seu estàndard.
  - La fallada parcial d'un component dels sistemes de seguretat que no provoqui una caiguda total però sí una pèrdua de funcionalitat rellevant (ex: caiguda d'un servei VPN crític).
- **Incidència de Criticitat LLEU:** Qualsevol incident de menor impacte, com:
  - La fallada d'un port d'un commutador d'accés.
  - Problemes de rendiment esporàdics o que afecten un únic usuari.
  - Errors en la configuració que no afecten la disponibilitat del servei.

10.3. Indicadors Clau de Rendiment (KPI)

A continuació es detallen els indicadors clau de rendiment que seran objecte de mesurament i seguiment.

10.3.1. Atenció i resposta a consultes

A continuació es defineixen els paràmetres ANS amb relació a l'atenció i respostes a consultes.

Temps màxim de resposta comercial / consulta	
Definició	Temps màxim transcorregut des de la petició d'oferta de serveis / projectes per part de l'Ajuntament fins a la recepció d'aquesta per part de l'adjudicatari. L'Ajuntament podrà considerar com no retornades aquelles ofertes que no s'adeqüin a la sol·licitud. L'Ajuntament podrà en cas de necessitat sol·licitar resposta de forma urgent.

Temps màxim de resposta comercial / consulta	
Aplicació	$Temps\_resposta\_comercial = T_{resposta} - T_{sol\cdot licitud} - T_{aturada}$

10.3.2. Peticions de provisions I Administració

A continuació es defineixen els paràmetres ANS amb relació a la provisió i administració dels serveis.

Temps màxim de provisió	
Definició	Temps màxim transcorregut entre la sol·licitud d'un servei per part de l'Ajuntament i l'entrega del mateix. Es podran definir diferents temps màxims de provisió en cas que el servei sol·licitat impliqui instal·lacions de més equips.
Aplicació	$Temps\_provisió = T_{entrega} - T_{sol\cdot licitud} - T_{aturada}$

Modificacions dels serveis	
Definició	Temps màxim transcorregut entre la sol·licitud de modificació d'un servei per part de l'Ajuntament i la modificació d'aquest per part de l'adjudicatari.
Aplicació	$Temps\_modificació = T_{modificació} - T_{sol\cdot licitud} - T_{aturada}$

Temps màxim de suspensió o baixa del servei	
Definició	Temps màxim transcorregut entre la sol·licitud d'una suspensió i baixa d'un servei per part de l'Ajuntament i l'execució de la mateixa.
Aplicació	$Temps\_suspensió\_baixa = T_{execució} - T_{sol\cdot licitud} - T_{aturada}$

10.3.3. Disponibilitat dels Sistemes

Aquest indicador mesura el percentatge de temps que els sistemes han estat operatius i accessibles durant el període de mesura.

%Disponibilitat global dels serveis	
Definició	Percentatge de temps mensual en el que estan disponibles els serveis globalment.
Aplicació	$Disponibilitat\_global(mensual) = \frac{\sum_{i}^{N} Disponibilitat_i}{N}$ N: Número total de serveis.

% Disponibilitat individual dels serveis	
Definició	Percentatge de temps mensual en el que estan disponibles els serveis individualment.
Aplicació	$Disponibilitat\_individual(mensual) = \frac{(T_{total} - T_{nodisp})}{T_{total}} \cdot 100$

10.3.4. Avaries

Aquests indicadors mesuren l'agilitat de l'adjudicatari per atendre i solucionar els problemes que sorgeixin. El temps comença a comptar des del moment en què la incidència és registrada al sistema de gestió de tiquets de l'adjudicatari. A continuació es defineixen els paràmetres ANS amb relació a les avaries dels serveis i de les operacions.

Resposta a incidències	
Definició	Temps màxim transcorregut entre la notificació d'una incidència i el reconeixement o negació d'aquesta per part de l'adjudicatari.
Aplicació	$Temps\_resposta\_incidències = T_{resposta} - T_{notificació} - T_{aturada}$

Resolució d'avaries molt greus	
Definició	Temps màxim transcorregut entre la notificació d'una incidència d'avaria molt greu i la resolució d'aquesta per part de l'adjudicatari.
Aplicació	$Temps\_resolució\_incidències\_molt\_greus = T_{resposta} - T_{notificació} - T_{aturada}$

Resolució d'avaries greus	
Definició	Temps màxim transcorregut entre la notificació d'una incidència d'avaria greu i la resolució d'aquesta per part de l'adjudicatari.
Aplicació	$Temps\_resolució\_incidències\_greus = T_{resposta} - T_{notificació} - T_{aturada}$

10.3.5. Facturació

A continuació es defineixen els paràmetres ANS amb relació a la facturació dels serveis proporcionats:

Errors en la facturació periòdica	
Definició	Verificació de l'existència d'errors en la facturació periòdica rebuda. Es verificarà que es facturin els serveis disponibles en aquell moment, així com l'aplicació precisa de les tarifes pactades.
Aplicació	$\%errors\_en\_facturació = \frac{Facturació\_OPERADOR - Facturació\_REAL}{Facturació\_OPERADOR} \cdot 100$ Facturació_OPERADOR: Facturació periòdica en € enviada pel proveïdor. Facturació_REAL: Facturació periòdica real en € demostrable.

10.3.6. Presentació d'informes

A continuació es defineixen els ANS amb relació a la presentació d'informes:

Termini d'entrega d'informes/inventari	
Definició	Termini màxim per entregar els informes/inventari sol·licitats en el present plec.
Aplicació	$Temps\_entrega\_informes = T_{entrega} - T_{màx} - T_{aturada}$

10.4. Sistema de Penalitzacions

L'Ajuntament i l'adjudicatari acordaran el procediment detallat i forma d'abonament de les penalitzacions pactades per l'incompliment dels nivells de servei a l'inici de la prestació dels serveis.

L'Ajuntament es reserva el dret a modificar i incorporar nous compromisos de qualitat de servei, així com definir nous serveis en base a:

- L'aplicació de penalitzacions similars a serveis comparables.
- L'aplicació de penalitzacions per a nous serveis segons els paràmetres pactats per serveis comparables i els ANS obtinguts.

L'aplicació de les penalitzacions per part de l'adjudicatari dels serveis es basa en els següents criteris d'aplicació:

- Les penalitzacions es faran efectives mitjançant un abonament addicional a la facturació periòdica emesa. L'aplicació de les penalitzacions als serveis afectats per incompliment dels nivells de servei establerts, es realitzarà en base a com a mínim allò especificat a **l'Annex L3 – Compromisos de qualitat de servei**, amb la proposta realitzada.
- L'adjudicatari està obligat a l'abonament de les penalitzacions.
- Les diferents penalitzacions a aplicar sobre un servei tenen caràcter acumulatiu, i totes les penalitzacions a aplicar dintre del període i del contracte són també acumulatives. En el moment de licitar s'haurà d'especificar en la seva proposta el límit màxim global de penalització com un % de la facturació anual global que està disposat a assumir, essent el mínim establert del **10% de la facturació anual global sense IVA.**

- Mensualment, en base a la informació enviada pel proveïdor es calcularan les penalitzacions de la següent manera:
    - Cada ANS disposarà d'un valor mínim o valor màxim, segons paràmetre de compliment.
    - Una vegada superat el valor mínim o valor màxim, segons paràmetre, s'aplicarà una penalització lineal segons la definició establerta.

El detall d'aplicació de les penalitzacions, els valors del paràmetre, valor mínims o valors màxims, la penalització establerta per a cada paràmetre, s'indica a l'**Annex L3 – Compromisos de qualitat de servei**.

L'Ajuntament podrà realitzar auditories periòdiques dels paràmetres oferts amb personal propi o recursos externs, amb aquest motiu el proveïdor estarà obligat a facilitar la informació requerida i la realització dels treballs associats per realitzar aquestes comprovacions i col·laborar amb els mitjans necessaris.

- En cas que el resultat de la auditoria presenti diferències superiors a un 10% en contra del proveïdor dels serveis, es podrà sol·licitar aplicar la penalització que correspongui al paràmetre en qüestió.
- En cas de no aportació de la informació requerida dintre dels terminis pactats, l'Ajuntament podrà aplicar una penalització corresponent al 10% sobre la facturació global mensual.

11. Formació i Transferència de Coneixement

Un dels objectius fonamentals d'aquest contracte és garantir que, un cop finalitzada la implantació, el personal tècnic del Departament de Sistemes d'Informació de l'Ajuntament de Santa Coloma de Gramenet disposi dels coneixements i les competències necessàries per a l'operació, gestió bàsica i supervisió de la infraestructura renovada. Per aquest motiu, la transferència de coneixement és un element essencial del servei i haurà de ser planificada i executada amb la màxima qualitat.

L'empresa adjudicatària haurà de presentar, juntament amb el pla d'implantació, un **Pla de Formació detallat**, que haurà de ser validat pel personal tècnic de l'Ajuntament abans de la seva execució. Aquest pla haurà d'estar dissenyat específicament per a l'entorn implementat i orientat a les tasques operatives que haurà de realitzar l'equip tècnic municipal. La formació haurà de ser eminentment pràctica, impartida en modalitat presencial a les dependències municipals i utilitzant l'entorn de producció o, si s'escau, un entorn de laboratori que en sigui una rèplica fidel.

El contingut mínim que haurà de cobrir el Pla de Formació s'estructurarà en els següents blocs temàtics:

1. **Arquitectura General de la Solució:** Una sessió inicial que proporcionarà una visió global de la nova arquitectura de xarxa basada en el model Spine-Leaf. Es tractaran els conceptes clau de la topologia, els mecanismes de redundància, el flux de trànsit, la segmentació de la xarxa mitjançant VLANs i els protocols utilitzats, per tal que el personal tècnic comprengui el disseny de la solució en el seu conjunt.
2. **Operació i Configuració dels Equipaments LAN:** Formació específica sobre els commutadors de Core (Spine i Leaf) i d'accés instal·lats. Aquesta capacitació haurà de cobrir, com a mínim: la interfície de línia de comandes (CLI), la configuració bàsica de ports, la gestió de VLANs, l'apilament (stacking) si s'aplica, la diagnosi i resolució de problemes de primer nivell (troubleshooting) i els procediments per a la substitució física d'un equip en cas d'avaria.
3. **Administració de la Plataforma de Gestió Centralitzada:** Aquest mòdul és de vital importància i ha de proporcionar una capacitació exhaustiva sobre l'eina de gestió (per exemple, ExtremeCloud IQ). La formació ha de permetre al personal municipal realitzar tasques com la visualització de l'estat de la xarxa, la monitorització del rendiment dels equips, la gestió d'alarmes i notificacions, l'aplicació de plantilles de configuració, la gestió centralitzada del microprogramari (firmware) i la generació d'informes d'ús i rendiment.
4. **Gestió i Operació del Sistema de Control d'Accés a la Xarxa (NAC):** Formació dedicada a la gestió de la solució NAC implementada. Aquest bloc haurà de capacitar el personal de l'Ajuntament per administrar el cicle de vida dels dispositius a la xarxa, incloent-hi la creació i modificació de polítiques de perfilat, autenticació i autorització per a diferents tipus d'usuaris i dispositius (corporatius, convidats, BYOD), la gestió del portal captiu per a convidats, i l'anàlisi dels logs per a la resolució d'incidències d'accés.

L'adjudicatari haurà de proporcionar tota la documentació utilitzada durant les sessions formatives (presentacions, manuals, guies de laboratori) en format digital i en català. Així mateix, el personal formador haurà de ser personal tècnic certificat i amb experiència demostrable en la implantació i gestió de les tecnologies objecte de la formació.