Ajuntament de Matadepera

Exp núm: X2025008096
Contractació del servei de manteniment de la xarxa de comunicacions de l'Ajuntament de Matadepera (PPT).
Procediment obert simplificat. Tramitació ordinària.

PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA CONTRACTACIÓ DEL SERVEI DE MANTENIMENT INTEGRAL DE LA XARXA DE COMUNICACIONS I BOSSES D'HORES DE SERVERI TÈCNIC PER A L'AJUNTAMENT DE MATADEPERA

ÍNDEX

1 INTRODUCCIÓ I ANTECEDENTS

Aquest document estableix les prescripcions tècniques que han de regir la contractació del servei de manteniment de la infraestructura de xarxa de l'Ajuntament de Matadepera, així com el subministrament anual de material per a la seva renovació i millora.

La infraestructura de xarxa és un actiu crític que dona suport a tots els serveis digitals interns i externs de l'Ajuntament. La seva correcta gestió, seguretat i evolució són essencials per al funcionament de l'organització. Aquest plec busca garantir un servei d'alta qualitat, proactiu i alineat amb les necessitats tecnològiques de l'Ajuntament.

2 OBJECTE DEL PLEC

L'objecte d'aquest plec és definir les condicions tècniques per a la prestació dels següents serveis:

- **Servei integral de manteniment per a la infraestructura existent:** Actuacions centrades a garantir el funcionament, l'actualització i la seguretat de tota la xarxa de comunicacions que l'Ajuntament ja té operativa. Inclou el manteniment, optimització, substitució d'equips i ciberseguretat integral, així com la gestió de la connectivitat a Internet de totes les seus municipals, assumint la totalitat dels costos operatius i de gestió associats, com per exemple, la renovació i el manteniment de les llicències dels tallafocs (firewalls).
- **Bossa d'hores per ampliació de la infraestructura i nous serveis:** Pensada per a les actuacions que fan créixer la xarxa actual o hi afegeixen noves capacitats. Es gestiona mitjançant una bossa d'hores tècniques destinada a la instal·lació i posada en marxa de nou equipament de xarxa (com switches, routers, punts d'accés, etc.) i a la implementació de serveis addicionals que no estiguin inclosos en el manteniment ordinari del punt anterior.
- **Bossa d'hores per Formació i transferència de coneixement a l'equip municipal**: Es disposa d'una bossa de 20 hores anuals per a dur a terme tasques de formació i acompanyament personalitzat. L'objectiu final d'aquestes hores és realitzar una "transferència de coneixement" efectiva que permeti a l'equip intern guanyar progressivament la capacitat necessària per a l'autogestió dels actius de la xarxa i de la infraestructura de comunicacions municipal.

3 ABAST DEL SERVEI I INFRAESTRUCTURA ACTUAL

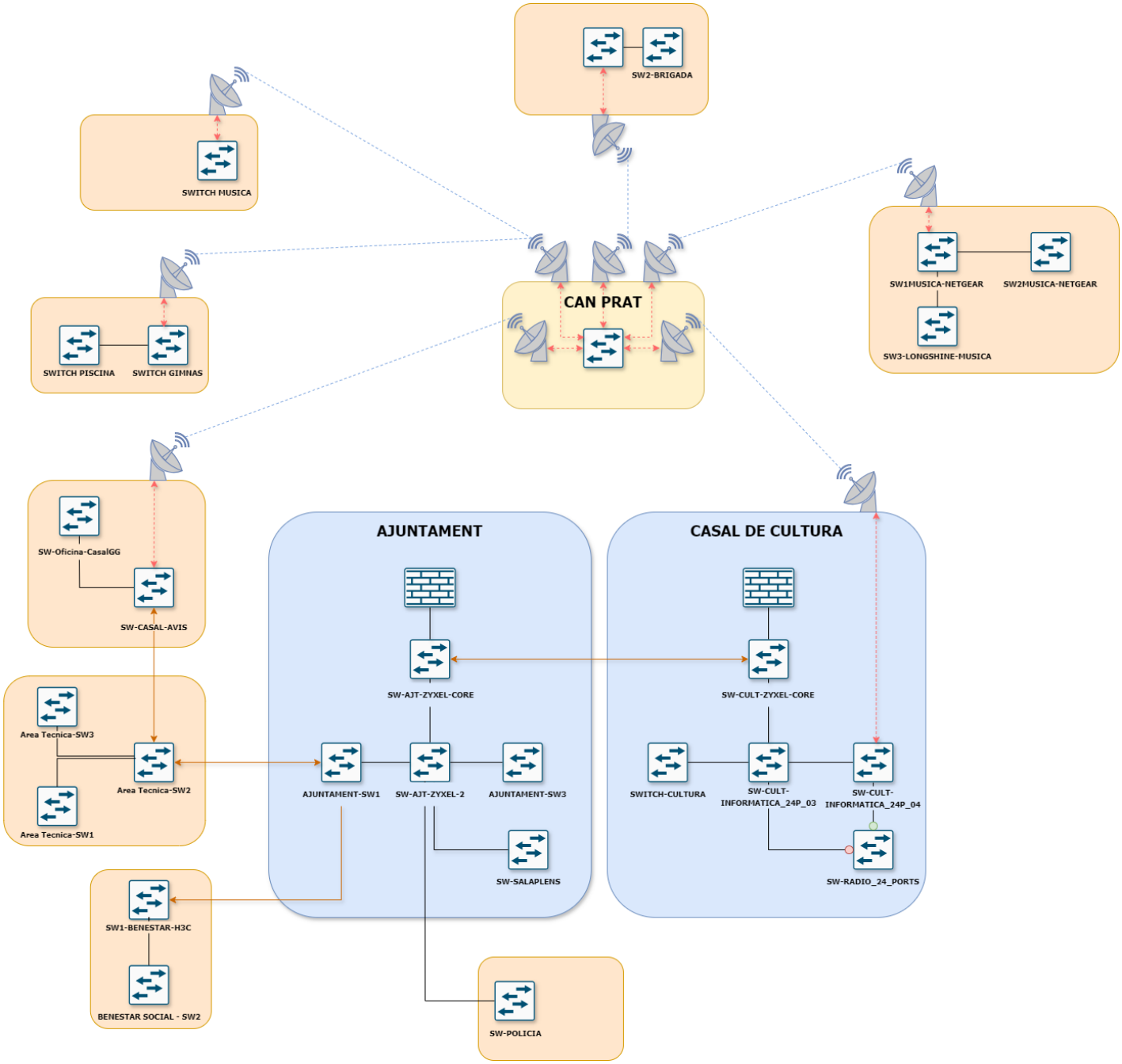
La infraestructura de xarxa de l'Ajuntament es basa en un model de nucli distribuït redundant. El servei abasta tots els actius de xarxa (commutadors, encaminadors, tallafocs, punts d'accés Wi-Fi, enllaços de fibra i radioenllaços) de les diferents seus

municipals, incloent l'Ajuntament, la Policia Local, el Casal de Cultura, l'Àrea Tècnica, Serveis Socials, i l'Escola de Música, entre d'altres.

3.1 Inventari dels Actius de Xarxa més representatius

Capa / Component	Model / Tecnologia	Quantitat / Distribució	Ubicació	Funció i Observacions
Nucli i Seguretat Perimetral: Tallafocs (Firewall)	SonicWall NSA 2700	2 (Clúster Actiu/Passiu)	Ajuntament (Actiu) / Casal de Cultura (Passiu)	Punt únic d'entrada/sortida a Internet. Gestiona seguretat perimetral (UTM), VPNs i enrutament principal. La configuració en alta disponibilitat (HA) garanteix la continuïtat del servei.
Nucli i Seguretat Perimetral: Commutadors de Nucli (Core)	Equips d'alta capacitat	2 (1 per seu principal)	Ajuntament / Casal de Cultura	Agregació de trànsit intern d'alta velocitat. Connecten directament amb els tallafocs i els commutadors de distribució de les seus principals.
Distribució i Accés (LAN): Commutadors d'Accés	Equips amb PoE	Múltiples unitats	Distribuïts a totes les seus (Ajuntament, Policia, Cultura, Àrea Tècnica, Benestar Social, etc.)	Proporcionen connectivitat directa als dispositius finals (PCs, telèfons IP, impressores). La majoria disposen de PoE per alimentar telèfons i APs Wi-Fi.
Xarxa Sense Fils (WLAN): Punts d'Accés Wi-Fi	Cambium Networks	Aprox. 50 unitats	Desplegats a tots els edificis municipals	Ofereixen cobertura Wi-Fi per a la xarxa corporativa i la xarxa de convidats.
Xarxa Sense Fils (WLAN): Controladora Wi-Fi	Cambium cnMaestro	1 (Servei Cloud)	Gestionada al núvol	Plataforma de gestió centralitzada per a la configuració, monitorització i actualització de tots els punts d'accés de la xarxa.
Interconnexió de Seus (WAN): Radioenllaç	WiMAX Cambium	Múltiples enllaços	Teulades dels edificis municipals	Creen una xarxa WAN privada per interconnectar les seus remotes amb el nucli. Utilitzen topologies punt a punt i punt-multipunt.

3.2 Mapa de Xarxa orientatiu:



3.3 Relació amb els mitjans de l'Ajuntament.

El Departament de Sistemes i Tecnologia de l'Ajuntament i l'empresa adjudicatària treballaran com a socis tecnològics. Existirà un interès compartit i una predisposició a

col·laborar per part dels tècnics municipals, que aportaran el context i la visió estratègica necessària per a l'alineament del servei.

Aquesta col·laboració, però, no dilueix les obligacions de l'adjudicatari. Com a expert i responsable del servei, l'empresa adjudicatària garantirà la totalitat de la prestació i el compliment dels nivells de servei, per la qual cosa haurà de disposar en tot moment dels mitjans propis necessaris.

S'espera que l'adjudicatari lideri la gestió proactiva. Les comunicacions dels tècnics municipals formen part del flux de treball col·laboratiu. Ara bé, un dels objectius del contracte és que l'adjudicatari detecti les incidències abans que ho facin els usuaris o el personal municipal.

Per exemple, si els tècnics municipals detecten un equip inoperatiu que no ha estat reportat per la monitorització de l'adjudicatari, s'interpretarà com una oportunitat de millora en els sistemes de vigilància de l'adjudicatari.

La confiança en aquest model de soci tecnològic es basarà en la capacitat de l'adjudicatari per aprendre i millorar. La recurrència en la detecció d'incidències per part del personal municipal, especialment si són problemes ja coneguts i evitables, es considerarà un incompliment significatiu de l'obligació de millora contínua i gestió proactiva.

4 DESCRIPCIÓ DEL SERVEI INTEGRAL DE MANTENIMENT

L'adjudicatari garantirà el funcionament òptim, la seguretat, el rendiment i l'evolució de la infraestructura de xarxes de l'Ajuntament i les seves seus externes. L'objectiu és assegurar un servei sòlid i eficient, minimitzant qualsevol temps d'interrupció mitjançant una gestió proactiva i una resposta ràpida, amb un compromís d'aplicació de les millors pràctiques per garantir la continuïtat del servei.

4.1 Rendiment i Continuïtat del Servei:

- **Temps de Resposta a Incidències i Monitorització**: L'adjudicatari garantirà uns temps màxims de resposta i resolució d'acord amb els Nivells de Servei (SLA) definits a l'apartat 7 d'aquest plec. El servei es basarà en una monitorització proactiva per anticipar-se a les incidències.
- **Monitorització i Gestió Proactiva:** L'adjudicatari ha de garantir que els paràmetres de rendiment dels enllaços troncals i els equips crítics es mantinguin dins de llindars acceptables (latència, pèrdua de paquets, ús de CPU/memòria, ample de banda consumit). Aquesta monitorització serà la base per anticipar-se a les incidències i els resultats d'aquesta monitorització, incloent gràfics d'evolució del consum i capacitat de la xarxa, a annexar en l'Informe Mensual de Servei.
- **Gestió d'Incidències i Informes de Causa Arrel (RCA):** Es garantirà el compliment estricte dels temps de resposta i resolució definits en els Nivells de

Servei (SLA). Per a les incidencies Crítica o Greus, es lliurarà un informe RCA en un termini màxim de 5 dies hàbils des de la seva resolució. Així mateix, la gestió de les peticions de servei s'atendrà dins dels terminis establerts a l'apartat de Nivells de Servei (apartat 7.2).

- **Gestió de la Connectivitat a Internet:** L'adjudicatari actuarà com a interlocutor tècnic qualificat davant dels proveïdors de serveis d'Internet (ISP), gestionant qualsevol incidència i verificant el compliment dels acords de servei contractats per l'Ajuntament. Les polítiques de Qualitat de Servei (QoS) es mantindran optimitzades i la seva configuració haurà d'estar documentada al Dossier Tècnic de Xarxa.
- **Abast del Suport:** El servei cobrirà tots els actius de la xarxa, incloent el suport remot i presencial quan sigui necessari, amb els costos de desplaçament inclosos. Es realitzaran les visites sobre el terreny que siguin necessàries i com a mínim una de seguiment per semestre.
- **Cicle de Vida del Material**: Es gestionarà íntegrament el procés de tramitació de garanties i substitució de qualsevol component avariat, documentant cada gestió al sistema de tiqueting.

4.2 Seguretat

L'adjudicatari ha de garantir la seguretat, integritat i confidencialitat de la infraestructura de xarxa existent. L'enfocament del servei de seguretat és dual:

- Manteniment de la Seguretat Actual: Assegurar el funcionament robust, la gestió i l'actualització de les mesures de seguretat ja implementades a la infraestructura municipal.
- Mecanisme d'Evolució: Proveir un vehicle contractual (la bossa d'hores) per implementar noves capacitats de seguretat de forma controlada i projectitzada, si l'Ajuntament ho sol·licita.

Per aquest motiu, els serveis de seguretat es divideixen clarament en dos blocs contractuals:

A. Serveis de Seguretat Inclosos en el Servei Integral de Manteniment (Quota Fixa)

Aquest servei inclou totes les actuacions recurrents i correctives necessàries per garantir el funcionament, l'actualització i la seguretat de la infraestructura de xarxa existent i operativa en el moment d'inici del contracte.

Les tasques obligatòries incloses en aquesta quota fixa són:

- **Gestió de la Seguretat Perimetral i Interna:**
  - Realització d'una auditoria anual de les regles dels tallafocs perimetrals.

  - Gestió activa i actualització dels serveis de seguretat unificada (UTM) existents.
  - Manteniment de la documentació i justificació de cada regla (perimetral i interna) al Dossier Tècnic de Xarxa.
- **Gestió de Vulnerabilitats i Auditoria de Configuració:**
  - Realització d'una anàlisi semestral de vulnerabilitats dels actius de la xarxa.
  - Lliurament d'un informe semestral identificant vulnerabilitats (CVEs) i males configuracions (serveis insegurs, configuracions febles), el seu nivell de risc (CVSS) i el pla de mitigació proposat.
- **Resposta a Incidents de Seguretat:**
  - Assistència activa i amb la màxima celeritat en les tasques de contenció, anàlisi i recuperació en cas d'incident de seguretat sobre la infraestructura gestionada.
- **Gestió de Còpies de Seguretat de Configuracions:**
  - Garantia de recuperabilitat de tots els equips de xarxa i sistemes de gestió crítics mitjançant còpies de seguretat periòdiques de les seves configuracions.
  - Verificació de la funcionalitat d'aquestes còpies mitjançant una prova semestral de restauració sobre un entorn controlat.
- **Pla de Recuperació davant Desastres (DRP) de la Xarxa:**
  - Elaboració i manteniment d'un pla documentat per a la recuperació dels serveis de xarxa i seguretat crítics.
  - Revisió i validació anual d'aquest pla amb l'Ajuntament.

Incorporació de Nous Serveis al Manteniment:

Les nova funcionalitat, servei o plataforma de seguretat que s'implementi durant la vigència del contracte (ja sigui mitjançant la bossa d'hores de l'apartat 5 o per altres mitjans) passarà a ser considerada "infraestructura existent" un cop finalitzada la seva fase d'implementació i el seu manteniment s'incorporarà automàticament a aquesta quota fixa del servei integral.

B. Projectes d'Evolució i Noves Capacitats (Bossa d'Hores)

Aquest bloc descriu actuacions que no estan incloses en la quota fixa de manteniment, ja que es consideren projectes d'implementació que afegeixen noves capacitats de seguretat a la xarxa.

L'execució d'aquests projectes es finançarà a través de la bossa d'hores per a ampliació de serveis (descrita a l'apartat 5).

La següent llista és un exemple de serveis que es podrien implementar per evolucionar l'arquitectura de seguretat:

- Desplegament i configuració inicial d'eines de Detecció i Correlació d'Esdeveniments (SIEM/XDR).
- Projectes d'implementació de Microsegmentació interna.
- Creació d'una Xarxa Superposada (Overlay) per a accés segur (p. ex., basada en models Zero Trust com Tailscale, Headscale, Nebula...)

4.3 Gestió Estratègica i Documentació:

- **Gestió de Canvis Planificats:** Tota actuació planificada que pugui tenir un impacte significatiu en el servei haurà de ser documentada mitjançant una petició de canvi (RFC) als tècnics informàtics municipals.
- **Llibre de Documentació de la Xarxa:** L'adjudicatari és responsable de crear i mantenir un repositori centralitzat (Dossier Tècnic de Xarxa) amb tota la documentació rellevant, incloent inventari, diagrames L2/L3, configuracions, justificació de regles de tallafocs, etc.. Aquesta documentació és propietat de l'Ajuntament i ha d'estar permanentment actualitzada i accessible.
- **Informe Anual de Recomanacions i Pla de Millora:** Es lliurarà un informe anual que consolidi les dades operatives del servei i l'anàlisi del cicle de vida dels actius (EoL/EoS, aquest document es el full de ruta tecnològic integral, justificat i valorat per a l'evolució de la infraestructura.
- **Assessorament en Projectes:** Es prestarà suport i assessorament tècnic en la integració de nous serveis o tecnologies a la xarxa municipal, garantint la seva correcta implementació i documentació

4.4 Millora Contínua

- **Anàlisi Causa Arrel i Mesures Preventives:** Després de cada incidència Crítica o Greu, l'Informe de Causa Arrel (RCA) inclourà obligatòriament un apartat de "Mesures Correctores i Preventives", amb un pla d'acció calendaritzat.

5 Bossa d'hores per ampliació de la infraestructura i nous serveis

5.1 Objectiu, Dotació i Conceptes Coberts

Aquest apartat estableix l'objectiu, la dotació econòmica i les condicions d'ús de la bossa d'hores destinada a l'ampliació de la infraestructura de xarxa i a la implementació de nous serveis, sempre que aquests no estiguin inclosos en el servei integral de manteniment ordinari.

La dotació d'aquesta bossa es destina als serveis professionals (Hores Tècniques) i al material auxiliar necessari per a la seva execució. L'adquisició de l'equipament (com

ara routers, switchs, firewalls, etc.) es gestionarà a través de les partides d'inversió de l'Ajuntament.

Dotació Econòmica: El contracte inclou una partida anual de **6.500 € (IVA exclòs)**. Aquesta xifra constitueix un pressupost màxim, l'execució del qual es realitzarà sota demanda expressa de l'Ajuntament.

Conceptes Coberts:

- **Hores Tècniques:** Treballs d'instal·lació i configuració. Es facturaran segons el preu/hora ofertat per l'adjudicatari, amb el límit màxim establert en la licitació de 50 €/hora (IVA exclòs).
- **Material Auxiliar:** Components menors i fungibles indispensables per a la instal·lació (p. ex., cablejat de connexió, connectors, ancoratges).

5.2 Procediment de Gestió de Sol·licituds

Tota sol·licitud i comunicació es registrarà al sistema de tiqueting de l'adjudicatari per garantir-ne la traçabilitat, seguint els passos següents:

1. **Sol·licitud:** L'Ajuntament obre un tiquet on detalla la necessitat, aportant la informació tècnica de l'equip a instal·lar (fabricant, model), la seva ubicació i la funcionalitat desitjada.
2. **Presentació de Proposta (5 dies hàbils):** L'adjudicatari ha de presentar una proposta valorada que inclogui:
   - Estimació detallada d'hores tècniques i del material auxiliar.
   - Un pla de treball bàsic amb les fases principals de l'actuació.
3. **Avaluació de la proposta:** L'Ajuntament avaluarà la proposta i comunicarà la seva decisió (Aprovar, Sol·licitar modificacions o Rebutjar).

5.3 Execució, Garantia i Recepció del Servei

- **Inici dels Treballs:** Un cop aprovada la proposta, l'adjudicatari disposa de 10 dies hàbils per iniciar la instal·lació.
- **Model d'Adquisició i Integració:** S'estableix un model de col·laboració obert. L'Ajuntament pot adquirir l'equipament de xarxa al proveïdor que consideri més oportú. Com a soci tecnològic, es pot sol·licitar a l'adjudicatari la realització de la instal·lació i posada en marxa (amb càrrec a aquesta bossa d'hores) independentment de qui hagi subministrat l'equip. Si l'adjudicatari també és proveïdor d'equipament de xarxa, l'Ajuntament el podrà convidar a presentar oferta, sense que això suposi una preferència ni exclusivitat.
- **Recepció, Conformitat i Facturació:** La prestació finalitzarà amb la recepció de conformitat del Responsable del Contracte, un cop verificat el correcte funcionament de l'equip i l'actualització de la documentació de xarxa. Prèvia emissió de factura caldrà conformitat favorable.

5.4 Seguiment Econòmic i Gestió de Romanents

- **Seguiment:** L'informe mensual del servei ha d'incloure un apartat específic amb l'estat de la bossa d'hores: saldo inicial, consum del període i saldo final disponible en euros.
- **Gestió de Romanents:** La partida anual és un pressupost màxim, no una quantitat prepagada. Els fons no consumits en una anualitat seran transferibles al saldo de la següent, dins del període de vigència del contracte. La no execució total o parcial de la bossa en finalitzar el contracte no generarà cap dret de compensació econòmica per a l'adjudicatari.

5.5 Condicions d'Ús i Exclusions

- **Actuacions Incloses:** L'ús d'aquesta bossa es limita exclusivament a projectes de nova implementació, posada en marxa d'equipament nou o evolucions de la infraestructura que hagin estat prèviament sol·licitats i aprovats.
- **Actuacions Excloses:** No es podran imputar hores d'aquesta bossa a tasques considerades dins de la quota fixa del servei de manteniment.

6 BOSSA D'HORES PER A TRANSFERÈNCIA DE CONEIXEMENT:

Per tal d'incrementar la competència i l'autonomia de gestió de l'equip del Departament de Tecnologia i Sistemes Municipal, s'estableix una bossa de 20 hores anuals destinada a sessions programades i dedicades a la transferència de coneixement. Aquestes sessions tenen com objectiu de contribuir a la capacitat d'autogestió de la infraestructura.

Les activitats formatives es podran desenvolupar de dues maneres:

- **Sessions Telemàtiques Regulars:** Es proposa la realització de sessions telemàtiques setmanals d'aproximadament una hora, on els tècnics del Departament d'Informàtica puguin fer recorreguts guiats per les eines de gestió i configuració de la xarxa, així com resoldre dubtes i fer consultes.
- **Aprofitament de Visites Presencials:** Es podran planificar activitats de formació pràctica sobre el terreny, aprofitant les visites presencials que faci l'adjudicatari.

Condicions d'Ús:

- **Temàtica:** La temàtica a tractar serà definida per les necessitats dels tècnics municipals, sense cap altra limitació que l'abast dels actius i serveis objecte d'aquest contracte.

- **Exclusivitat:** El còmput d'hores només aplicarà a activitats de formació planificades i acceptades per l'Ajuntament. En cap cas es podran imputar hores d'aquesta bossa a actuacions derivades de la resolució d'incidències, instal·lacions o qualsevol altra tasca pròpia del servei de manteniment.

La sol·licitud i planificació de les sessions es coordinarà a través del sistema de tiqueting per garantir-ne la traçabilitat. L'adjudicatari haurà de reflectir l'estat de la bossa d'hores (saldo inicial, hores consumides, saldo final) a l'Informe Mensual de Servei. Les hores no consumides a finals d'any seran transferibles i acumulables a la bossa de l'any següent.

7 NIVELLS DE SERVEI (SLA)

7.1 Temps de Resposta i Resolució

L'horari de suport estàndard serà de dilluns a divendres de 8:00h a 17:00h, excloent festius nacionals i locals.

El còmput dels temps de resposta i resolució s'iniciarà en el moment en què la incidència quedi registrada al sistema de tiqueting de l'adjudicatari, ja sigui per detecció proactiva, per comunicació telefònica o per correu electrònic per part del personal de l'Ajuntament. És obligatori registrar totes les incidències, independentment de si l'avís prové dels tècnics municipals o de accions proactives de l'empresa de manteniment.

- **Temps de Resposta:** Temps màxim des de l'inici del còmput fins que un tècnic qualificat ha registrat la incidència i ha iniciat les actuacions de diagnòstic
- **Temps de Resolució:** Temps màxim des de l'inici del còmput fins que el servei afectat es restableix de forma permanent.

Tipus d'Incidència	Descripció	Temps de Resposta (Inici actuacions)	Temps de Resolució (Restabliment servei)
Crítica	Impedeix que més del 50% dels treballadors municipals puguin operar amb normalitat o, Afecta directament a més de 10.000 ciutadans (p. ex., caiguda de la vlan VoIP municipal).	1 hora natural.	4 hores naturals.
Greu	Impedeix que més del 5% dels treballadors municipals puguin operar amb normalitat o, Afecta directament a més de 1.000 ciutadans (p. ex.,	4 hores laborables.	8 hores laborables.

Tipus d'Incidència	Descripció	Temps de Resposta (Inici actuacions)	Temps de Resolució (Restabliment servei)
	caiguda de múltiples punts d'accés Wi-Fi públic).		
Lleu	Impedeix que menys del 5% dels treballadors municipals puguin operar amb normalitat o, Afecta directament a menys de 1.000 ciutadans (p. ex., caiguda d'un únic punt d'accés Wi-Fi públic).	8 hores laborables.	48 hores laborables.

7.2 Termini de Resolució per a Peticions de Servei que no tinguin categoria d'incidencia:

A diferència de les incidències (avaries o interrupcions no planificades), les peticions de servei corresponen a sol·licituds que no són crítiques per a la continuïtat del servei (p. ex., alta d'un punt de xarxa, consulta tècnica).

- **Descripció:** Qualsevol sol·licitud registrada al sistema de tiqueting que no sigui classificada com a incidència.
- **Temps de Resolució Màxim:** 5 dies hàbils des de la sol·licitud.

7.3 Mecanisme de Millora Contínua

Per garantir que el servei no només resol problemes sinó que també aprèn d'ells per evitar que es repeteixin, s'estableix el següent mecanisme de millora contínua:

- **Anàlisi de Causa Arrel:** Després de cada incidència Crítica o Greu, l'Informe de Causa Arrel haurà d'incloure obligatòriament un apartat de "Mesures Correctores i Preventives", amb un pla d'acció calendaritzat per implementar les solucions que evitin la seva recurrència.
- **Seguiment i Control:** L'estat d'implementació d'aquestes mesures preventives serà un punt obligatori a tractar en la reunió de seguiment mensual del servei, garantint així un control sobre la seva execució.
- **Aplicació de mesures**: L'objectiu dels informes de Causa Arrel és prevenir la reincidència d'incidències evitables i les mesures descrites hauran de ser implementades de forma efectiva.

8 SEGURETAT DE LA INFORMACIÓ

L'adjudicatari està obligat al compliment de la normativa de protecció de dades (RGPD) i de l'Esquema Nacional de Seguretat (ENS), així com a garantir la

confidencialitat absoluta de tota la informació a la qual tingui accés. Aquest deure té la consideració d'obligació contractual essencial i en conseqüència, el seu incompliment serà causa directa de resolució del contracte.

9 ENTREGABLES i DOCUMENTACIÓ DEL SERVEI:

Entregable	Termini de Lliurament	Criteris d'Acceptació i Contingut
Pla de Transició i Desplegament	15 dies naturals des de l'inici del contracte	Ha d'incloure: cronograma detallat de la presa de control, matriu de contactes, pla de desplegament d'eines de monitorització i tiqueting, i procediment per a l'assumpció de la gestió.
Informe Inicial d'Auditoria i Dossier Tècnic de Xarxa	6 mesos des de l'inici del contracte	Ha d'incloure: inventari auditat (marca, model, S/N, versió FW, IP, ubicació física), diagrames L2 (VLANs, enllaços) i L3 (enrutament), anàlisi de riscos inicials i un pla d'acció de millora immediata. L'acceptació requerirà una validació per mostreig del 10% dels equips crítics. El dossier ha de ser un reflex fidel de l'estat real de la xarxa
Actualització del Dossier Tècnic	15 dies naturals després de cada canvi rellevant	Ha d'incloure: El registre del canvi realitzat (RFC), la data, el responsable, i l'actualització de l'inventari i els diagrames afectats. Per a nou equipament instal·lat, aquesta actualització haurà d'incorporar la documentació tècnica específica de la instal·lació (plànols, ubicació, esquemes de connexió, etc.).
Informe Mensual de Servei –punt 12.2-	Dins dels 5 primers dies hàbils de cada mes	Ha d'incloure: resum executiu, un apartat d'autoavaluació de compliment dels SLA i entregables, llistat d'incidències, actuacions realitzades, estat de la bosses d'hores i materials, i un resum de l'estat de la seguretat.
Informe de Causa Arrel (RCA) -punt 7-	5 dies hàbils després de la resolució d'una incidència Crítica o Greu	Ha d'incloure: cronologia detallada de l'incident, descripció de la causa arrel identificada, accions de contenció i resolució aplicades, impacte funcional que va tenir i les mesures preventives per detectar i evitar la seva repetició.
Informe Estratègic i de Recomanacions (Inicial i Anual) –punt 13-	Versió Inicial als 6 mesos, després 1 cada final d'any (desembre)	-Versió Inicial: Correspon a l'"Informe de Proposta de Millora Estratègica". Ha d'incloure l'anàlisi de la situació actual, la proposta d'arquitectura futura i un full de ruta plurianual. -Actualització Anual: Ha d'actualitzar el pla estratègic i incloure l'anàlisi de salut de la xarxa, l'anàlisi del cicle de vida dels equips (EoL/EoS) i un pla de renovació. Com a annexos, inclourà l'auditoria de regles de tallafocs i la validació del DRP.
Pla de Devolució del Servei –punt 14-	Amb la oferta de licitació, actualitzable.	Contingut lliure i basat en la proposta que faci el licitador per a obtenir una bona puntuació, en tot cas serà actualitzat amb l'input que aporti el tècnic informàtic responsable del contracte una vegada adjudicat el contracte.

Nota informativa: Per simplificar la càrrega documental, el tènic municipal responsable del contracte podrà eximir del lliurament formal d'informes i entregables si la informació ja és accessible i està actualitzada a les eines de gestió del servei (accessibles per l'Ajuntament segons l'apartat 12.3).

10 PLA D'IMPLANTACIÓ I TRANSICIÓ

Durant el primer mes de contracte, l'adjudicatari haurà de realitzar les següents tasques:

- Reunió d'inici amb el responsable del contracte.
- Revisió i assumpció de la gestió de tots els elements de la xarxa.
- Desplegament de les seves eines de monitorització.

Durant els primer sis mesos de contracte, l'adjudicatari haurà de realitzar les següents tasques:

- Tasques requerides per entregar l'Informe Inicial d'Auditoria i Dossier Tècnic de Xarxa.

11 GARANTIA DELS EQUIPS SUBMINISTRATS

Tot l'equipament subministrat haurà de comptar amb una garantia mínima de 2 anys o la garantia estàndard del fabricant si aquesta fos superior.

La responsabilitat de tramitar la garantia de l'equipament nou recaurà sobre el proveïdor que l'ha subministrat. Si el proveïdor ha estat l'adjudicatari, aquest gestionarà la garantia. Si ha estat un tercer, la gestionarà l'Ajuntament.

12 PLA D'EXPLOTACIÓ DEL SERVEI

12.1 Objectiu del Pla d'Explotació:

Aquest pla defineix el marc de treball, la metodologia, els processos i les eines per a l'operació del servei. Els procediments aquí detallats constitueixen els requisits mínims que l'adjudicatari ha de complir.

12.2 Gestió del Servei

La gestió del servei es basarà en una relació de col·laboració contínua entre el personal de l'Ajuntament i l'equip de l'adjudicatari.

- Reunions de Seguiment basades en Entregables:
  - **Reunió Operativa**: S'organitzarà una reunió operativa dins dels 5 dies hàbils posteriors al lliurament de cada Informe Mensual de Servei. L'objectiu principal serà revisar l'informe, analitzar el compliment dels SLA,

estudiar les incidències més rellevants, planificar les properes actuacions i validar el compliment dels SLA i entregables.

- **Reunió Estratègica**: Es realitzarà una reunió estratègica dins dels 10 dies hàbils posteriors al lliurament de l'Informe Estratègic i de Recomanacions (tant la versió inicial als 6 mesos com les actualitzacions anuals). El seu objectiu serà avaluar l'estat general de la infraestructura, debatre les propostes de millora, i revisar la planificació i l'execució de les bosses d'hores.

12.3 Eines de Gestió del Servei

L'adjudicatari haurà de proporcionar i mantenir, com a mínim, les següents eines durant tota la vigència del contracte:

- **Sistema de Monitorització:** Una plataforma que permeti la vigilància 24x7x365 de l'estat i el rendiment dels actius de xarxa, amb un sistema d'alertes automàtiques.
- **Sistema de Tiqueting:** Un portal accessible per registrar i consultar l'estat de les incidències i peticions, garantint la traçabilitat de totes les comunicacions.
- **Control de la Infraestructura:** L'adjudicatari assignarà un rol administrador de màxims privilegis al responsable del contracte en les eines software i hardware utilitzades per a la prestació del servei.

12.4 Processos Operatius Clau

1. Gestió d'Incidències i Manteniment Correctiu

Aquest procés descriu el cicle de vida complet per al tractament de qualsevol avaria o interrupció no planificada del servei.

A. Obertura i Registre d'Incidències:

- Canals de Comunicació: El personal de l'Ajuntament podrà comunicar les incidències a través de:
  - Un número de telèfon d'atenció prioritària per a incidències de caràcter Crític, el licitador obrirà ticket al finalitzar la trucada.
  - El portal de tiqueting o un correu electrònic designat per a incidències de caràcter Greu o Lleu.
- Horari de Recepció:
  - El canal telefònic per a incidències Crítiques estarà operatiu 24x7x365.
  - La resta de canals estaran operatius durant l'horari de servei estàndard (dilluns a divendres de 8:00h a 17:00h).

B. Procés de Resolució:

1) Registre i Priorització: Tota incidència es registrarà al sistema de tiqueting i es classificarà com a Crítica, Greu o Lleu, determinant així l'SLA aplicable.
2) Diagnòstic i Comunicació: L'adjudicatari realitzarà el diagnòstic i comunicarà un pla d'acció inicial.

3) Resolució (Remota i Presencial): Es prioritzarà la resolució remota. Si es requereix intervenció física, es mobilitzarà un tècnic a la seu corresponent. L'objectiu és restablir el servei dins dels temps definits en aquest plec.
4) Tancament i Documentació: Un cop verificada la solució amb l'Ajuntament, es tancarà el tiquet, documentant la solució i, per a les incidències crítiques s'fegirà un informe de Causa Arrel (RCA).

C. Exemples Servei Correctius:
- Radioenllaç WiMAX: diagnòstic i solució de pèrdues de connectivitat, problemes de rendiment (latència, pèrdua de paquets) i la gestió de la substitució de maquinari avariat.
- Firewalls: resolució de problemes de connectivitat per regles, fallades de túnels VPN, problemes de rendiment del dispositiu i restabliment del servei en cas de fallada del clúster d'alta disponibilitat.
- Switchs: Inclou la resolució de fallades de ports, problemes de VLANs, PoE, bucles de xarxa i incidències en punts d'accés Wi-Fi o la seva controladora.

2. Gestió de Peticions de Servei que no tenen caràcter d'incidencia

Correspon a les sol·licituds que no són incidències (p. ex., alta d'un punt de xarxa, consulta tècnica). Aquestes peticions es registraran sempre a través del sistema de tiqueting i executades per l'adjudicatari en un termini de 5 dies hàbils (apartat 7.2)

3. Gestió de Canvis

Correspon a modificacions significatives sobre la infraestructura (p. ex., actualització de firmware d'un equip de nucli). Aquests canvis requeriran una proposta documentada amb anàlisi d'impacte i pla de retorn (rollback), una aprovació formal per part de l'Ajuntament i una planificació en una finestra de treball de baix impacte.

12.5 Qualitat del Servei i Transferència de Coneixement:

Documentació Tècnica: El contractista haurà de mantenir permanentment actualitzada la documentació tècnica de la xarxa d'acord amb els informes previstos en el punt 9. La falta en el lliurament d'informes i entregables en temps i forma pot comportar penalitats.

Transferència de Coneixement: Amb l'objectiu que els tècnics municipals guanyin competència en la gestió de la infraestructura, l'adjudicatari oferirà una borsa de 20 hores anuals per a consultes, formació o activitats que contribueixin a millorar l'autonomia del personal. La temàtica concreta serà definida pel responsable del contracte.

13 Informe de Proposta de Millora Estratègica

13.1 Objectiu de l'Informe

Un dels objectius clau d'aquest contracte és que l'adjudicatari actuï com un soci tecnològic estratègic, acompanyant l'Ajuntament en la modernització de la seva infraestructura. Per materialitzar-ho, s'estableix el següent cicle de vida per a la planificació estratègica:

- **Informe Inicial d'Auditoria i Dossier Tècnic de Xarxa:** L'adjudicatari lliurarà una primera versió completa i detallada d'aquest informe als sis mesos de l'inici del servei. Aquest document inicial servirà com a projecte integral i base per a l'evolució de la xarxa.
- **Actualització Anual Integrada:** Cada any i de forma successiva, les actualitzacions anuals d'aquest pla s'integraran dins de l'"Informe Anual de Recomanacions", consolidant tota la visió estratègica en un únic document anual per optimitzar i simplificar la documentació.

13.2 Contingut i Estructura de l'Informe de Proposta de Millora Estratègica

L'informe haurà de desenvolupar els següents apartats:

1. **Anàlisi i Diagnòstic de la Situació Actual:** Anàlisi crítica de l'arquitectura de xarxa existent, identificant punts febles, colls d'ampolla i riscos.
2. **Proposta d'Arquitectura Tècnica Futura:** Presentació d'una visió per a la xarxa futura, incloent un diagrama de la nova topologia, model d'enrutament i justificació tècnica.
3. **Pla de Segmentació i Seguretat:** Proposta detallada de l'esquema de VLANs i polítiques de seguretat per millorar el control del trànsit.
4. **Full de Ruta d'Implementació Plurianual:** Presentació d'un pla d'implementació realista i per fases, alineat amb la durada del contracte. S'ha de detallar la planificació per anualitats i la seva vinculació amb la bossa anual d'hores per a la instalació de nous equips i o serveis de xarxa de 6.500 € (sense iva), proposant com optimitzar aquesta inversió.
5. **Anàlisi de Beneficis:** Justificació de com la solució proposada millora la fiabilitat, el rendiment, la seguretat i l'escalabilitat de la xarxa municipal.

14 Pla de Devolució del Servei

L'adjudicatari haurà de presentar, com a part de la seva memòria tècnica, una proposta de Pla de Devolució del Servei, la qual serà valorada en el procés de licitació. L'objectiu d'aquest pla és garantir una transició ordenada en finalitzar el contracte, assegurant el traspàs efectiu de tots els coneixements, dades, documents i informació necessaris per a la continuïtat de la prestació.

Un cop adjudicat el contracte, el responsable tècnic municipal revisarà el pla proposat i podrà requerir a l'adjudicatari que hi incorpori les actualitzacions necessàries per garantir-ne la viabilitat.

El compliment satisfactori d'aquest pla, acreditat mitjançant un informe favorable dels tècnics municipals, serà una condició indispensable per procedir a la devolució de la garantia definitiva.

15 Annex 1: Ejemplo Memoria Técnica evaluable mediante criterios sujetos a juicio de valor

ÍNDEX

1 Preámbulo: Marco Conceptual y Realismo de la Propuesta

Esta memoria técnica se presenta como respuesta al apartado de criterios sujetos a juicio de valor, que suma hasta 25 puntos sobre 100. Se entiende que el objetivo de esta sección es evaluar no solo la capacidad técnica del licitador, sino también su visión, metodología y, fundamentalmente, su alineamiento con los objetivos estratégicos a largo plazo del Ayuntamiento.

Esta propuesta parte de una situación inicial de insuficiencia de medios propios que no permite al equipo informático municipal dedicar el tiempo necesario a la gestión proactiva de la red, abocándolo a un modelo reactivo. Por lo tanto, el objetivo de este contrato es dual: garantizar la continuidad del servicio a corto plazo y, simultáneamente, construir un ecosistema de red que sea sostenible y autogestionable por el equipo actual a largo plazo.

Se es plenamente consciente del conflicto de intereses inherente a este tipo de evaluaciones: la necesidad de presentar una propuesta ambiciosa para obtener la máxima puntuación, contra el riesgo de elevar los requisitos mínimos del servicio con propuestas que podrían ser irrealistas o difícilmente materializables. La filosofía adoptada para abordar este conflicto se basa en la total transparencia. Cada herramienta, proceso y mejora que se detalla a continuación no es una mera declaración de intenciones, sino un compromiso firme y realista, fundamentado en la experiencia previa en la implementación de estos ecosistemas.

En consecuencia, **se entiende y se acepta que las mejoras propuestas en esta memoria elevan los requisitos mínimos de la prestación del servicio, convirtiendose en nuevas obligaciones para el licitador, tal y como se establece en los pliegos (Memòria punto 15.5)**.

2 Resumen Ejecutivo

Esta memoria técnica presenta una hoja de ruta estratégica para transformar la gestión de la red del Ayuntamiento, evolucionando desde el actual modelo operativo, reactivo y dependiente de proveedores externos, hacia un paradigma proactivo, automatizado y, en última instancia, autónomo. La propuesta está diseñada para dar respuesta directa a los dos objetivos fundamentales:

> **-En el corto plazo**, estabilizar la infraestructura actual y garantizar la continuidad del servicio mediante un soporte experto y fiable;
>
> **-En el largo plazo,** capacitar al equipo técnico interno del Ayuntamiento con las herramientas, procesos y conocimientos necesarios para alcanzar la plena autonomia para la gestion y mantenimineto de las infraestructuras de red municipales.

Para ello, se propone un modelo de colaboración en el que nuestro rol es el de un socio estratégico temporal. El éxito de nuestra intervención no se medirá por la perpetuación de

un contrato de mantenimiento, sino por la progresiva autosuficiencia del personal del Ayuntamiento. El objetivo final, a lo largo de un horizonte de cuatro años, es que el equipo municipal sea capaz de gestionar, mantener y evolucionar su infraestructura de red de forma autónoma, segura y eficiente.

La estrategia se fundamenta en la implantación de un ecosistema tecnológico integrado, basado en estándares abiertos y soluciones de código abierto líderes en la industria, como Netbox, Ansible y LibreNMS. Este marco de trabajo se desplegará sobre una infraestructura de red estandarizada en hardware MikroTik, una elección estratégica que gracias a sus APIs permite implementar una gestion de red moderna basada en la filosofía de Infraestructura como Código (IaC) y garantiza la sostenibilidad económica y el alineamiento con las directivas europeas. A través flujos de trabajo basados en IaC, se establecerán procesos auditables, seguros y colaborativos que no solo modernizarán la gestión de la red, sino que servirán como un mecanismo intrínseco para la transferencia continua de conocimiento al equipo técnico municipal.

3 Estratégia y Modelo de Colaboración

3.1 Situación Actual y Retos

La situación actual de la infraestructura de red del Ayuntamiento se caracteriza por una serie de desafíos interconectados que limitan su estabilidad, seguridad y capacidad de evolución:

- **Falta de Documentación y Observabilidad:** La ausencia de una documentación centralizada, precisa y viva de la infraestructura de red hace que la resolución de incidencias sea lenta y compleja. Es imposible garantizar la estabilidad de un sistema que no se comprende en su totalidad.
- **Heterogeneidad de la Infraestructura:** La coexistencia de múltiples marcas y modelos de hardware, cada uno con sus propias particularidades de gestión, incrementa la carga cognitiva del personal técnico y dificulta la estandarización de procedimientos.
- **Pérdida de Conocimiento Interno:** El modelo de mantenimiento histórico ha provocado una externalización del conocimiento operativo. El *expertise* reside en las emprsas y técnicos externos que prestan el servicio de mantenimiento de red, lo que ha erosionado progresivamente la capacidad del personal municipal para gestionar de forma autónoma la infraestructura del Ayuntamiento, generando una fuerte dependencia de terceros.
- **Modelo de Gestión Reactivo ("Break-Fix"):** La operativa actual se basa en la intervención manual tras un fallo. Este modelo es ineficiente, costoso y no previene las interrupciones del servicio, que a menudo son descubiertas por los propios usuarios finales.

Estas condiciones crean un círculo vicioso de dependencia y fragilidad, esta memoria propone un plan de 4 años que consigue corregir estas carencias.

3.2 Nuestra Visión: Un Socio para la Soberanía Tecnológica

Nuestra propuesta redefine la relación tradicional entre proveedor y cliente. No aspiramos a ser un simple ejecutor de tareas de mantenimiento, sino un catalizador para la

transformación digital y la consecución de la soberanía tecnológica del Ayuntamiento. **Nuestro éxito se define por la eventual obsolescencia de nuestra función de soporte diario.**

Este modelo, lejos de ser un mal negocio para el licitador, se sustenta en un marco de colaboración transparente y mutuamente beneficioso. Entendemos que la transformación requiere una inversión continua. Por ello, el contrato contempla una bolsa de horas anual de 6.500 € (IVA excluido), destinada precisamente a la implementación remunerada de estas mejoras, como la instalación de nuevo equipamiento o la puesta en marcha de servicios adicionales. Este mecanismo asegura que nuestro rol como socio estratégico no solo se centre en la transferencia de conocimiento, sino que también nos permita liderar y facturar por el trabajo de evolución de la red, alineando nuestros incentivos con el objetivo de mejora continua del Ayuntamiento.

Este modelo de colaboración se basa en dos pilares fundamentales:

- **Colaboración Supervisada:** Durante toda la duración del contrato, trabajaremos en estrecha colaboración con el equipo informàtico municipal. Cada acción, cada despliegue y cada configuración se realizarán de forma conjunta. El enfoque no será solo ejecutar la tarea, sino explicar el "porqué" detrás de cada decisión, transfiriendo la lógica y la filosofía del nuevo modelo de gestión.
- **Transferencia Continua de Conocimiento:** El objetivo principal de este plan es el empoderamiento del equipo interno. La documentación no será un entregable final, sino una consecuencia natural del proceso de Infraestructura como Código. La formación no consistirá en cursos teóricos aislados, sino en un aprendizaje práctico y continuo, utilizando el entorno de laboratorio ("gemelo digital") y participando activamente en la gestión real de la red a través de los nuevos flujos de trabajo.

3.3 El Doble Mandato: Estabilidad a Corto Plazo, Autonomía a Largo Plazo

Entendemos la necesidad crítica de equilibrar la transformación a largo plazo con las exigencias operativas del día a día. Por ello, nuestro plan se estructura en dos fases paralelas:

- **Fase 1 (Estabilización y Fundamentos):** Desde el primer día, proporcionaremos el soporte reactivo "break-fix" necesario para garantizar la disponibilidad y estabilidad de la infraestructura de red actual. Este servicio de contingencia actuará como una red de seguridad, generando la confianza y el espacio necesarios para que el equipo municipal pueda dedicar tiempo a la asimilación del nuevo modelo sin la presión constante de las incidencias urgentes.
- **Fase 2 (Transformación y Empoderamiento):** Simultáneamente, comenzaremos la implantación de la arquitectura y los procesos descritos en esta memoria. A medida que el nuevo modelo proactivo y automatizado se consolide, la frecuencia y el impacto de las incidencias disminuirán drásticamente. Esto reducirá de forma natural y progresiva la necesidad del soporte reactivo de la Fase 1, facilitando el objetivo final de que el equipo municipal sea plenamente autónomo.

Comparativa de Modelos de Gestión de Red

Característica	Modelo Reactivo/Tradicional (Actual)	Modelo Proactivo/Automatizado (Propuesto)
Documentación	Inexistente, desactualizada o en hojas de cálculo dispersas. Fuente de error.	Viva, centralizada y en formato código (Netbox). Fuente Única de Verdad (SoT).
Gestión de Cambios	Manual, ad-hoc, sin validación previa. Alto riesgo de error humano.	Controlado, auditable, validado en un laboratirio gemelo digital antes del despliegue (GitOps).
Detección de Fallos	Reactiva. Reportada por los usuarios tras la interrupción del servicio.	Proactiva. Detectada por el sistema de monitorización (LibreNMS) antes del impacto.
Configuración	Inconsistente, dependiente del técnico. Propensa a la arrastrar errores històricos.	Consistente. Estandarizada, declarativa y aplicada por automatización (Ansible).
Rol del Personal de TI	"Apagafuegos". Dedicado a resolver incidencias.	Ingeniero/Estratega. Dedicado a mejorar y evolucionar el servicio.
Dependencia	Alta dependencia de proveedores externos y su conocimiento tácito.	Autosuficiencia. El conocimiento está codificado en los procesos y herramientas.
Coste del Servicio	Gasto operativo recurrente e impredecible.	Inversión estratégica con un retorno medible en eficiencia y capacitación.

4. Arquitectura Filosófica y Tecnológica

4.1 Principios Fundamentales

La transformación propuesta se sustenta en un conjunto de principios y procediminetos que permiten estandarizar y simplificar la gestion operativa de las infraestructuras.

- **Infraestructura como Código (IaC):** La configuración de la red dejará de ser un estado manual y frágil en los dispositivos para ser definida en ficheros de texto legibles por humanos (YAML). Estos ficheros se gestionan en un sistema de control de versiones (Git), lo que permite tratar la infraestructura con el mismo rigor que el desarrollo de software: es versionable, repetible, auditable y colaborativa. Cada cambio queda registrado, eliminando la ambigüedad y reduciendo drásticamente el error humano.
- **Ecosistema Open Source:** La selección de herramientas se basa en soluciones de código abierto. Esta estratégia elimina el riesgo de "vendor lock-in" (dependencia de un único proveedor), garantiza la sostenibilidad a largo plazo y da acceso a una vasta comunidad global de conocimiento, talento y soluciones compartidas y auditables. El Ayuntamiento no quedará cautivo de licencias propietarias ni de las hojas de ruta

comerciales de fabricantes que podrían poner en jaque la estabilidad municipal por discontinuar productos o servicios.

- **Agnosticismo de Proveedor:** Aunque en esta propuesta se aboga por la estandarización en hardware MikroTik por el grado de madurez de su ecosistema de APIs, la arquitectura de gestión (Netbox, Ansible, LibreNMS) es intrínsecamente agnóstica. Los mismos principios y herramientas podrían utilizarse en el futuro para gestionar equipos de otros fabricantes si fuera necesario, protegiendo la inversión realizada en procesos y conocimiento por su transferibilidad.

Esta arquitectura desacoplada permite que si en el futuro el Ayuntamiento decidiera incorporar o migrar a otro fabricante de hardware, todo el marco de gestión, la lógica de automatización y la fuente de la verdad podrían ser preservados. Esta preservación de la inversión en procesos y conocimiento del personal reduce drásticamente el coste y el riesgo de futuras migraciones tecnológicas, una ventaja decisiva para una administración pública centrada en el valor a largo plazo.

4.2 El Círculo Virtuoso de la Automatización

La fortaleza de nuestra propuesta no reside en cada herramienta de forma aislada, sino en su integración sinérgica, que crea un bucle de retroalimentación y mejora constante.

- **Netbox (La Intención):** Actúa como el cerebro del sistema. Define el estado deseado de la red de forma declarativa. Aquí se documenta qué dispositivos existen, cómo se conectan, qué direcciones IP utilizan y qué servicios deben ofrecer. Es la Fuente Única de Verdad (SoT), todo bajo una interfaz de usuario intuitiva y amigable.
- **Ansible (La Acción):** Es el motor de automatización, las manos del sistema. Lee la "intención" definida en Netbox y la traduce en comandos de configuración específicos para los dispositivos de red, aplicando el estado deseado de forma precisa, consistente e idempotente.
- **LibreNMS (La Verificación):** Son los ojos del sistema. Monitoriza de forma continua el estado real y el rendimiento de la red. Sus datos permiten verificar que el estado aplicado por Ansible se corresponde con la realidad operativa y su sistema de alarmas alerta de forma proactiva sobre cualquier desviación o degradación del servicio, cerrando así el círculo.

Este ciclo **Intención -> Acción -> Verificación** transforma la gestión de red de una tarea artesanal a un proceso de ingeniería predecible y fiable mediante iteraciones que mejoran de forma continua el sistema.

4.3 La Fuente Única de Verdad (SoT): Netbox - El Cerebro de la Red

Para eliminar la ambigüedad, los errores y la obsolescencia de las hojas de cálculo y la documentación manual, es imperativo establecer un repositorio central, autoritativo y programable. Netbox es una herramienta diseñada específicamente con un modelo de datos exhaustivo para la infraestructura de red y sus APIs permiten una facil integracion con el resto de herramientas de nuestra propuesta.

Intent-Based Networking: La implementación de Netbox como SoT materializa el concepto de Redes Basadas en la Intención. El enfoque se desplaza de la configuración manual e imperativa de cada dispositivo ("*configura este puerto en modo troncal*") a la declaración de

un objetivo de alto nivel en Netbox ("*este servidor se conecta a este puerto del switch y necesita acceso a estas VLANs*"). La automatización se encarga del resto.

Así se elimina la documentación obsoleta, garantiza la consistencia de la configuración y se habilita la automatización basada en datos.

4.4 El Motor de Automatización: Ansible - Las Manos de la Red

Ansible se ha consolidado como el estándar de facto para la automatización de TI por su simplicidad (utiliza el formato YAML, fácil de leer y escribir), su naturaleza sin agentes (no requiere instalar software en los dispositivos de red) y su extensísimo ecosistema de módulos, con un soporte robusto para una amplia gama de fabricantes de red.

Idempotencia: Un principio fundamental de Ansible es la idempotencia. Esto significa que ejecutar un playbook (un script de automatización) múltiples veces produce el mismo resultado que ejecutarlo una sola vez. Si una configuración ya está en el estado deseado, Ansible no realiza ningún cambio. Esta propiedad es crucial para la seguridad y la predictibilidad de las operaciones automatizadas, ya que permite ejecutar los playbooks de forma segura en cualquier momento para garantizar el cumplimiento del estado deseado.

Gestión Centralizada y "API-First": La capacidad de Ansible para gestionar RouterOS (el sistema operativo de Microtik) es proporcionada por la libreria **`community.routeros`**, que contiene un conjunto de módulos para interactuar con dispositivos MikroTik. Estos módulos utilizan principalmente uno de dos métodos de conexión subyacentes: `network_cli`, que se conecta a través de SSH y simula la interacción con la CLI, o una conexión directa a la API de RouterOS.

La conexión **`network_cli`**, utilizada por el módulo **`community.routeros.command`**, permite a los ingenieros enviar comandos de la CLI de RouterOS en bruto. Aunque aparentemente sencillo para quienes están familiarizados con la CLI, este enfoque está plagado de peligros en un entorno automatizado a gran escala ya que las tareas de `routeros_command` a menudo no son idempotentes.

Por lo tanto, esta arquitectura debe construirse sobre un mandato que priorice la API (*API-first*). La API de RouterOS proporciona una interfaz estructurada y programática para la configuración.

Módulos de Ansible como **`community.routeros.api`**, **`community.routeros.api_modify`** y **`community.routeros.api_find_and_modify`** aprovechan esta API para manipular objetos de configuración específicos en lugar de simplemente enviar cadenas de texto a una terminal.

Este método es inherentemente más declarativo y fiable. Permite a los *playbooks* consultar el estado de un objeto, compararlo con el estado deseado de NetBox y realizar cambios precisos.

Este enfoque proporciona la base sólida necesaria para construir *playbooks* verdaderamente idempotentes que puedan ejecutarse de forma segura y repetida.

El módulo `command` debe tratarse como una herramienta de último recurso, reservada únicamente para comandos "show" simples que no modifiquen la configuración o para

configurar características que aún no están expuestas a través de los módulos de API más avanzados.

Este principio no es simplemente una buena práctica; es un requisito previo para lograr el objetivo de gestionar la red únicamente con Ansible de una manera segura y escalable.

Inventario Dinámico: Ansible no operará sobre una lista estática de equipos. Se configurará el plugin de inventario dinámico de Netbox, que permite a Ansible consultar a Netbox en tiempo real cada vez que se ejecuta. Esto asegura que la automatización siempre se basa en la información más actualizada de la Fuente Única de Verdad, incluyendo nuevos dispositivos, cambios de IP o cualquier otra modificación registrada en Netbox.

4.5 La Plataforma de Observabilidad: LibreNMS - Los Ojos de la Red

Se requiere una solución de monitorización completa, de código abierto y altamente extensible para proporcionar visibilidad en tiempo real del estado y rendimiento de la red. LibreNMS basado en SNMP permite el descubrimiento automático de dispositivos así como la configuración de alerta personalizables.

En nuestro ecosistema, LibreNMS trasciende la simple recepción de alertas. Sus datos sobre el tráfico, la latencia, la utilización de la CPU y la memoria de los dispositivos sirven como un mecanismo de verificación del mundo real. Confirma que la "intención" definida en Netbox y "aplicada" por Ansible se traduce en una red que funciona como se espera. Esto permite una gestión proactiva, detectando cuellos de botella o degradaciones del servicio antes de que los usuarios los perciban, transformando el modelo de trabajo de "apagar fuegos" a "prevenirlos".

5 MikroTik para estandarización y predictibilidad pressupuestaria.

La elección de MikroTik no es una mera preferencia de hardware, sino una decisión estratégica fundamentada en un diferenciador técnico clave que hace viable toda nuestra propuesta de automatización: **su API REST nativa, completa y universalmente disponible en toda su gama de productos a un coste inigualable.**

Este factor es el requisito indispensable sobre el que se construye nuestro modelo de gestión. Mientras que otros fabricantes reservan sus capacidades de automatización para equipos de gama alta con costes prohibitivos, o directamente carecen de una interfaz de programación robusta, MikroTik la ofrece de serie. **Intentar implementar un sistema de Infraestructura como Código (IaC) con Netbox y Ansible en otro fabricante de red, dentro de un rango de coste similar, sería, en la práctica, inviable.** La API de RouterOS es la piedra angular que nos permite transformar la gestión de red de un ejercicio manual y reactivo a un proceso programático, declarativo y eficiente.

Nuestra propuesta, por tanto, no es solo sobre el hardware, sino sobre la adopción de un paradigma de gestión de red moderno, eficiente y escalable.

5.1 Allanando la curba de aprendizaje de RouterOS

Abstracción: El pilar de nuestra propuesta es una potente capa de abstracción que elimina la complejidad inherente a la gestión de redes. Mientras que la interfaz nativa de RouterOS es robusta, requiere conocimientos específicos (Winbox/RouterOS CLI) la curba de aprendizaje es pronunciada y poco transferible a otros ecosistemas. Nuestra arquitectura supera este desafío:

Intención sobre Comandos: El personal técnico no interactuará directamente con la sintaxis de RouterOS. En su lugar, utilizará Netbox como fuente única de verdad (SSoT) para definir el estado deseado de la red de forma declarativa (p. ej., asignar una VLAN a un puerto o reservar una IP).

El Rol Clave de la API: La "magia" ocurre cuando Ansible traduce esta intención en configuración real. Esto es posible gracias a que RouterOS expone una API REST completa y nativa, una característica excepcional que lo distingue de otros fabricantes. Esta API permite una gestión programática profunda del equipo, algo que es prácticamente inexistente en dispositivos de un rango de coste similar.

Así complejidad técnica queda encapsulada en la automatización, no en el operador.

Estandarización: El principal beneficio operativo radica en la homogeneidad del ecosistema. Al estandarizar la infraestructura de red (routers, switches, firewalls y puntos de acceso) en MikroTik, toda la gestión se consolida bajo un único y potente sistema operativo: RouterOS.

Esto reduce drásticamente la carga cognitiva del equipo técnico municipal. En lugar de dominar las interfaces, comandos y particularidades de múltiples fabricantes, solo necesitan aprender y perfeccionar un sistema. Esta unificación simplifica radicalmente la gestión diaria, el mantenimiento, la resolución de incidencias y la formación, garantizando una mayor agilidad y eficiencia operativa.

5.2 El Modelo de Licencia Perpetua

MikroTik opera con un modelo de licenciamiento perpetuo. Al adquirir un dispositivo de hardware, se incluye una licencia de RouterOS de por vida, con derecho a todas las futuras actualizaciones de software sin coste adicional. No existen cuotas anuales de mantenimiento ni suscripciones obligatorias para acceder a funcionalidades básicas o críticas, el principio que aplica es “own what you buy”.

Este modelo contrasta radicalmente con la tendencia dominante en la industria, donde los grandes fabricantes están migrando funcionalidades esenciales a modelos de suscripción anual basadas en su cloud propietario. Este enfoque introduce imprevisibilidad, riesgos presupuestario y de continuidad de operaciones. Un aumento de precios en las licencias o la decisión del fabricante de mover una característica de seguridad necesaria a un nivel de suscripción superior puede dejar a la administración en una posición de "rescate por parte del vendedor" ("vendor ransom"), forzada a aceptar costes crecientes para mantener operativos servicios esenciales. El modelo de MikroTik proporciona una previsibilidad y un control total sobre el coste total de propiedad (TCO) respaldando sus declaraciones con un sólido historial.

5.3 Track record y Compliance NIS2

- MikroTik tiene un historial demostrado de proporcionar soporte de software para su hardware durante periodos excepcionalmente largos. Es común que dispositivos con más de una década de antigüedad continúen recibiendo actualizaciones de seguridad y funcionalidades de RouterOS. Esta política protege la inversión del Ayuntamiento, maximiza la vida útil del hardware y evita los ciclos de obsolescencia forzada.
- La Directiva NIS2 exige a las organizaciones del sector público que evalúen y gestionen rigurosamente los riesgos asociados a la seguridad de su cadena de suministro. Optar por un proveedor tecnológico con sede en la UE (Letonia) simplifica este cumplimiento, mitiga los riesgos geopolíticos asociados a la cadena de suministro y se alinea con las estrategias europeas de soberanía digital.

5.4 Análisis de Alternativas (VyOS)

En una estrategia que se basa en de IaC, VyOS se presenta como una alternativa robusta que destaca en.

- **Excelencia en IaC**: Un sistema operativo diseñado para la automatización, con una CLI transaccional (con *commit* y *confirm*) y módulos de Ansible maduros.
- **Alto Rendimiento en Routing**: Al desplegarse sobre hardware x86 potente (con aceleración por software vía DPDK), puede gestionar enormes volúmenes de tráfico, superando en esta tarea específica a la mayoría de CPUs de MikroTik.

Sin embargo, para los objetivos de este contrato (la gestión integral de la red de un Ayuntamiento), la arquitectura de VyOS presenta tambien las siguientes desventajas:

- **Estandarización parcial:** El pilar de nuestra propuesta es la estandarización total (routers, *switches*, firewalls, puntos de acceso, etc..) bajo un único SO. VyOS al ser solamente un software para hardware x86 no permite cubrir todas los casos de uso requeridos (por ejemplo switches de acceso, puntos de acceso Wi-Fi). Su adopción forzaría la introducción de un segundo o tercer fabricante para cubrir la red de acceso a expensas de la estandarización mantenibilidad.
- **CPU vs. ASIC**: VyOS procesa tráfico por software (CPU) mientras que los equipos MikroTik se basan en ASICs (hardware dedicado) para el procesando de tráfico a velocidad de línea. Si bien és perfectamente posible mover datos y trafico de red con CPUs operando VyOS, para cubrir un mismo requisito funcional se precisaría hardware más potente (y caro) y que consumiría mas energía que los equipos ASIC de Microtik.

Si bien VyOS es superior para *routing* de software a gran escala, MikroTik es una solución que combina una API de automatización universal con un ecosistema de hardware completo bajo un mismo OS (routers, switches, firewalls, Aps..) y un modelo de coste perpetuo, siendo la opción mas adecuada para el caso de uso de estandarización y eficiencia que busca la Administración.

6 Seguridad, Validación y Auditoría desde el Diseño

El objetivo es que, en un plazo de 4 años, estas bases (las Fuentes de Verdad de identidad y dispositivos) estén tan consolidadas que la transición a un modelo *overlay Zero Trust* sea un paso lógico y viable. Este enfoque permite validar y desplegar políticas de seguridad granulares de forma fiable y sin caídas de servicio desde el primer día, sentando las bases para una arquitectura de seguridad de próxima generación."

6.1 El Ecosistema de Herramientas (Framework)

El modelo de Confianza Cero se apoya en la interoperabilidad de las siguientes herramientas, cada una cumpliendo un rol específico:

- **Fuentes de Verdad (SOT):** Son las bases de datos maestras que definen el estado deseado.
  - **Active Directory (AD):** Actúa como **SOT de Identidad**. Responde a la pregunta: "¿Quién es este usuario y a qué grupos pertenece?".
  - **NetBox:** Actúa como **SOT de Infraestructura**. Responde a la pregunta: "¿Qué es este dispositivo, dónde debería estar conectado y está autorizado?".
- **Automatización y Gestión del Cambio:**
  - **Ansible:** Es la herramienta de automatización (las "manos") que aplica las configuraciones a los dispositivos de red.
  - **GitLab CI:** Es el orquestador de CI/CD (el "cerebro") que gestiona todo el flujo de trabajo de validación y despliegue.
- **Validación y Pruebas:**
  - **Proxmox VE + MikroTik CHR:** Forman el **"Gemelo Digital"**, un entorno de laboratorio seguro para probar cambios sin impacto en producción.
- **Auditoría de Seguridad y Vulnerabilidades:**
  - **Sara (RouterOS Security Inspector):** Herramienta de análisis de configuración integrada en el *pipeline* de CI/CD para detectar automáticamente malas prácticas, servicios inseguros o CVEs antes de que un cambio se apruebe.
- **Detección, Respuesta y Observabilidad:**
  - **SIEM/XDR:** Plataforma centralizada que **correlaciona logs** (Firewalls, AD, NAC) para detectar anomalías e incidentes de seguridad.
  - **LibreNMS:** Herramienta de observabilidad (los "ojos") que verifica el estado operativo de la red después de un cambio.

Este ecosistema garantiza que ningún cambio se aplique a producción sin una validación previa funcional y una auditoría de seguridad.

6.2 El Gemelo Digital: Laboratorio Proxmox y CHR

El mayor riesgo en la gestión de redes es la introducción de cambios en el entorno de producción sin una validación previa. Un error de configuración puede provocar la interrupción de servicios críticos para el Ayuntamiento y sus ciudadanos. Por ello, es innegociable disponer de un entorno de laboratorio donde probar cada cambio de forma segura antes de desplegarlo en la red de producción.

Se propone la implementación de un servidor de virtualización basado en Proxmox VE. En este servidor se creará un "gemelo digital" de la red del Ayuntamiento, una réplica virtual exacta de la infraestructura de producción.

Se crearan maquinas virtuales para simular los equipos de red. La viabilidad y fiabilidad de este gemelo digital se basa imagenes Cloud Hosted Router (CHR) de MikroTik. El punto crítico y diferenciador es que el CHR no es un emulador ni un simulador que intenta aproximar el comportamiento de RouterOS. Es, literalmente, **el mismo código binario que se ejecuta en el hardware físico (RouterBOARD)**. Esta paridad de software 1:1 es la garantía fundamental de que un cambio validado con éxito en el laboratorio se comportará de forma idéntica cuando se despliegue en la red de producción.

6.3 El Flujo de Trabajo de Gestión de Cambios

Todo cambio en la red seguirá un proceso estructurado y auditable, diseñado para garantizar la seguridad y la coherencia. El siguiente flujo describe el ciclo de vida de un cambio típico, como la asignación de una nueva VLAN a un puerto de switch:

- **Paso 1: Declaración de la Intención (SOT).** El proceso comienza y termina en las Fuentes de Verdad (SOT). Para cambios de infraestructura (como una VLAN), el ingeniero modifica los datos en Netbox (SOT de Infraestructura). Para cambios de identidad, la fuente es Active Directory (SOT de Identidad). Esta es la única ubicación donde se define el cambio.
- **Paso 2: Disparo de la Automatización.** Una modificación en Netbox dispara un webhook que inicia un pipeline de CI/CD en GitLab CI. Alternativamente, el proceso puede ser iniciado manualmente.
- **Paso 3: Generación del Cambio Propuesto.** El pipeline ejecuta el playbook de Ansible relevante en modo de verificación (--check y --diff) contra el inventario dinámico de producción. Adicionalmente se ejecuta automáticamente la herramienta Sara (RouterOS Security Inspector) contra la configuración propuesta para detectar servicios inseguros (p.ej., Telnet, RoMON), configuraciones débiles (SNMP 'public') o CVEs conocidas. Esta acción no realiza ningún cambio, pero genera un informe preciso de los comandos que Ansible *ejecutaría* para alinear la realidad con la nueva intención de Netbox.
- **Paso 4: Validación Automatizada en el Gemelo Digital.** El mismo playbook se ejecuta contra el entorno del gemelo digital. Pruebas automatizadas verifican que el cambio se aplica correctamente y no introduce efectos secundarios no deseados (p. ej., mediante pruebas de conectividad).. Crucialmente, se realizan pruebas de persistencia de acceso: tras aplicar el cambio, se verifica que el dispositivo sigue siendo gestionable.
- **Paso 5: Revisión Humana y Aprobación.** El informe "diff" del Paso 3 y los resultados de las pruebas del Paso 4 se presentan para su revisión por pares o por un responsable técnico. Este es un punto de control humano crucial antes de afectar a la producción.
- **Paso 6: Aplicación Auditada en Producción.** Tras la aprobación, el pipeline ejecuta el playbook de Ansible. Antes de aplicar cualquier modificación, el pipeline ejecuta una **tarea de respaldo automático**, exportando la configuración activa del

dispositivo y almacenándola de forma versionada (ej. en GitLab) como un punto de restauración seguro. A continuación, el cambio se aplica de forma idempotente. Todo el proceso, desde la intención hasta su aplicación, queda registrado y es completamente auditable.

- **Paso 7: Verificación del Estado Post-Cambio.** Finalmente, herramientas de observabilidad como LibreNMS verifican que el estado operativo del dispositivo es el esperado y que las métricas de rendimiento se mantienen dentro de los umbrales normales.

La siguiente tabla visualiza este flujo de trabajo:

Paso	Acción	Actor/Herramienta	Artefacto	Ubicación
1	Declarar Intención	Ingeniero de Red	Asignación VLAN/Interfaz modificada	Interfaz/API de Netbox
2	Disparar Proceso	Webhook de Netbox / Operador	Disparo de Tarea CI/CD	Plataforma CI/CD
3	Generar Plan	Ansible (Modo Check)	Informe "Diff" de Configuración	Log de Tarea CI/CD
4	Validar Plan	Ansible, Pruebas Automatizadas	Resultados de Pruebas	Gemelo Digital
5	Aprobar Plan	Responsable Técnico	Aprobación en Ticket/Chat	Sistema de Gestión de Cambios
6	Aplicar Intención	Ansible (Modo Live)	Configuración Aplicada	Red de Producción
7	Verificar Estado	LibreNMS	Métricas Operativas, Estado	Plataforma de Observabilidad

6.4 Casos de Uso

A continuación, se detallan casos de uso prácticos que ilustran cómo el flujo de trabajo definido se aplica a operaciones de red comunes, mejorando la seguridad, la eficiencia y la fiabilidad.

6.4.1 Caso de Uso 1: Aprovisionamiento "Zero-Touch" de un Nuevo Switch

Este proceso transforma la adición de nuevo hardware de una tarea manual y propensa a errores a un flujo de trabajo seguro y validado.

- **Paso 1: Declaración de la Intención.** Un técnico accede a Netbox y crea un nuevo objeto de dispositivo para el switch que se va a instalar. Rellena sus datos: nombre, modelo, número de serie, ubicación (sede, rack) y asociando las VLANs correspondientes. El dispositivo se marca con el estado "Planificado".
- **Paso 2: Disparo de la Automatización.** Al guardar el nuevo dispositivo en Netbox con estado "Planificado", un webhook notifica al sistema de CI/CD, que inicia el pipeline de aprovisionamiento.
- **Paso 3: Generación del Cambio Propuesto.** El pipeline ejecuta un playbook de Ansible en modo --check y --diff. Como el dispositivo es nuevo, el "diff" generado es la configuración completa y estandarizada que se le aplicará, incluyendo nombre, IP de gestión, servidores NTP, VLANs, seguridad de puertos, etc.
- **Paso 4: Validación Automatizada en el Gemelo Digital.** El pipeline provisiona una nueva instancia de CHR (Cloud Hosted Router) en el laboratorio Proxmox. A continuación, ejecuta el playbook de Ansible contra esta instancia virtual, aplicando la configuración generada. Se ejecutan tests automatizados para verificar que la configuración es sintácticamente correcta y que responde a pings en su IP de gestión.
- **Paso 5: Revisión Humana y Aprobación.** Un responsable técnico recibe una notificación con el plan de configuración (el "diff") y el resultado exitoso de las pruebas en el gemelo digital. Tras revisar que todo es correcto, aprueba el despliegue.
- **Paso 6: Aplicación Auditada en Producción.** Un técnico de campo instala físicamente el switch en el rack y conecta un único cable a un puerto de aprovisionamiento. El switch arranca, obtiene una IP por DHCP y se registra en la red. El pipeline, al recibir la aprobación, ejecuta el mismo playbook en modo normal contra la IP del nuevo switch físico, aplicando la configuración de forma segura y consistente.
- **Paso 7: Verificación del Estado Post-Cambio.** Una vez configurado, el playbook notifica a LibreNMS, que añade automáticamente el nuevo switch a la monitorización. En minutos, empieza a recopilar métricas de CPU, tráfico y estado de los puertos, confirmando que el dispositivo está operativo y saludable.

Resultado: Se garantiza que cada nuevo dispositivo se despliega con una configuración estandarizada, validada y sin errores, eliminando el riesgo asociado a la configuración manual, a la vez que se genera toda la documentacion y actualización del inventario de red.

6.4.2 Caso de Uso 2: Despliegue de una Nueva VLAN

Este caso ilustra el flujo completo para un cambio que afecta a múltiples dispositivos de la infraestructura.

- **Paso 1: Declaración de la Intención.** Un técnico de red define la nueva VLAN (p.ej., VLAN 150 - "Dependencias Policiales") en Netbox, le asigna un prefijo de red y la asocia a los puertos troncales y de acceso correspondientes en varios switches.

- **Paso 2: Disparo de la Automatización.** El técnico inicia manualmente el pipeline "Gestionar VLANs" desde la interfaz de GitLab CI, especificando el ID de la nueva VLAN como parámetro.
- **Paso 3: Generación del Cambio Propuesto.** El pipeline ejecuta el playbook de gestión de VLANs en modo --check --diff contra la red de producción. El informe "diff" muestra con precisión los comandos add que se ejecutarán en cada uno de los switches afectados para crear la VLAN y asignarla a los puertos correctos.
- **Paso 4: Validación Automatizada en el Gemelo Digital.** El mismo playbook se ejecuta sobre el gemelo digital. Tras aplicar el cambio, se lanzan pruebas de conectividad automatizadas: dos máquinas virtuales de prueba conectadas a los switches virtuales correspondientes verifican que pueden comunicarse entre sí en la nueva VLAN 150, y que no han perdido conectividad en otras VLANs.
- **Paso 5: Revisión Humana y Aprobación.** El informe "diff" y el log de las pruebas de conectividad exitosas se presentan al responsable de TI. Al verificar que el cambio propuesto es correcto y que no causa daños colaterales, lo aprueba formalmente en el sistema de gestión de cambios.
- **Paso 6: Aplicación Auditada en Producción.** Tras la aprobación, se ejecuta el paso de despliegue del pipeline. Ansible se conecta a los switches de producción y aplica los cambios de forma idempotente.
- **Paso 7: Verificación del Estado Post-Cambio.** LibreNMS detecta las nuevas interfaces lógicas de la VLAN 150 en los switches y comienza a graficar su tráfico. El estado de los puertos afectados se monitoriza para asegurar que siguen activos y sin errores.

Resultado: Un cambio crítico y distribuido se despliega con riesgo mínimo, validando no solo la sintaxis de la configuración, sino también su impacto funcional antes de tocar la red real.

6.4.3 Caso de Uso 3: Auditoría Continua y Remediación de "Configuration Drift"

Este caso no sigue el flujo de cambio, sino que es un proceso complementario que utiliza las mismas herramientas para garantizar la integridad de la red.

1. **Detección Periódica:** Diariamente, de forma programada, un pipeline de "Auditoría" ejecuta un playbook de Ansible en modo --check --diff contra todos los dispositivos de la red. Este playbook no pretende aplicar ningún cambio, solo comparar el estado real con el estado deseado documentado en Netbox.
2. **Generación de Informes:** Si un dispositivo tiene una configuración que no coincide con la definida en Netbox (por ejemplo, un cambio manual de emergencia no revertido), Ansible genera un "diff" que resalta la discrepancia.
3. **Alerta y Análisis:** Si el informe "diff" no está vacío, el sistema genera una alerta de alta prioridad para el equipo de TI, adjuntando los detalles de la desviación. Esto permite un análisis inmediato para determinar si el cambio fue malicioso, accidental o un error operativo.
4. **Remediación Controlada:** Para corregir la deriva, no se aplica una reversión automática. En su lugar, el operador utiliza el informe para crear una intención de cambio en Netbox que refleje el estado correcto. A continuación, se sigue el **flujo de trabajo de gestión de cambios estándar (Pasos 1-7)** para reaplicar la configuración aprobada, garantizando que incluso la corrección de un error se haga de forma segura y auditable.

Resultado: Se establece un sistema de autovigilancia que detecta proactivamente cualquier desviación no autorizada, manteniendo la red en un estado conocido, seguro y alineado con la documentación, un requisito clave para normativas como el Esquema Nacional de Seguridad (ENS).

6.4.4 Caso de Uso 4: Gestión de la Calidad del Servicio (QoS) y SLAs con Proveedores

Este caso demuestra el valor de la capa de observabilidad (Paso 7 del flujo) como una herramienta de gestión estratégica.

1. **Monitorización Objetiva:** LibreNMS no solo monitoriza el estado de los dispositivos internos, sino que también realiza pruebas activas y continuas (cada minuto) contra los enlaces de los proveedores de Internet (ISP). Mide KPIs críticos como latencia, jitter y pérdida de paquetes hacia destinos externos fiables.
2. **Definición de Umbrales (SLAs):** En el sistema se configuran los umbrales definidos en los Acuerdos de Nivel de Servicio (SLA) con cada proveedor. Por ejemplo, una alerta si la latencia supera los 40ms o la pérdida de paquetes es mayor del 1% durante más de cinco minutos.
3. **Detección Proactiva de Degradación:** Cuando el rendimiento de un enlace viola un umbral, LibreNMS genera una alerta automática, a menudo antes de que los usuarios lo noten. El sistema recopila y almacena datos históricos de forma continua.
4. **Gestión de Incidencias Basada en Datos:** Al abrir una incidencia con un ISP, el equipo técnico del Ayuntamiento no se basa en reportes subjetivos ("Internet va lento"). En su lugar, presenta datos empíricos e irrefutables: *"Desde las 14:02 UTC, nuestro sistema de monitorización registra un aumento sostenido de la pérdida de paquetes al 5% en su enlace. Adjuntamos los gráficos que lo demuestran, que muestran un claro incumplimiento del SLA pactado."*

Resultado: Se empodera al Ayuntamiento con datos objetivos para exigir el cumplimiento de los contratos, acelerar la resolución de incidencias y garantizar una alta calidad del servicio para los ciudadanos y el personal.

6.4.5 Caso de Uso 5: Modificación Crítica de Reglas de Firewall (Prevención de Bloqueo)

Un ingeniero de red define una nueva política de firewall que, por error, bloquea el acceso de gestión, creando un riesgo de bloqueo lock-out del terminal.

- **Paso 1: Declaración de la Intención.** El ingeniero define la nueva (y defectuosa) política de firewall en el repositorio de configuración centralizado, que actúa como la fuente de la verdad para estas políticas.
- **Paso 2: Disparo de la Automatización.** Al guardar el cambio en el repositorio, un webhook notifica a la plataforma de CI/CD, que inicia automáticamente el pipeline de validación y despliegue.

- **Paso 3: Generación del Cambio Propuesto.** El pipeline ejecuta Ansible en modo check & diff. Se genera un informe que muestra los comandos exactos que se aplicarían, resaltando la eliminación de la regla de acceso de gestión.
- **Paso 4: Validación Automatizada en el Gemelo Digital.** Esta es la fase crítica donde se previene el error: El playbook de Ansible aplica la configuración propuesta a la réplica virtual del firewall (el gemelo digital). A continuación, una tarea específica de Prueba de Persistencia de Acceso intenta establecer una nueva sesión de gestión (SSH/API) con el gemelo digital. La conexión falla (timeout), la prueba se marca como FALLIDA, y todo el pipeline se detiene.
- **Paso 5: Revisión Humana y Aprobación.** Este paso no se alcanza. El fallo automático en el paso anterior impide que el cambio sea presentado para aprobación. La acción del ingeniero es recibir una notificación de "Pipeline Fallido" y revisar los logs para entender por qué.
- **Paso 6: Aplicación Auditada en Producción.** No se ejecuta. El cambio ha sido bloqueado de forma segura en la fase de validación.
- **Paso 7: Verificación del Estado Post-Cambio.** No se ejecuta, ya que no se ha realizado ningún cambio en la red de producción.

Resultado: Se consigue neutralizar un error operativo grave de forma proactiva y sin intervención humana. El cambio nunca llega a ser aprobado ni, por supuesto, desplegado. El sistema no confía en que un revisor humano detecte el error. La comprobación de seguridad es una parte obligatoria y automatizada del proceso. Se evita una crisis (la pérdida de control sobre el firewall principal) en lugar de tener que solucionarla bajo presión. Se fomenta la confianza en la automatización como un mecanismo más seguro que la intervención manual para cambios críticos.

6.4.6 Caso de Uso 6: Recuperación de Emergencia Tras un Bloqueo (Gestión Fuera de Banda)

Este caso de uso no sigue el framework estándar de gestión de cambios (Pasos 1-7), ya que se trata de una reacción a un incidente imprevisto, no de un cambio planificado. Las acciones se clasifican en una secuencia lógica de recuperación que se apoya en las herramientas del ecosistema.

Un dispositivo de red crítico ha quedado inaccesible por la red normal debido a un error de configuración manual.

- **Paso de Detección (Relacionado con el ecosistema del Paso 7: Verificación)** La plataforma de observabilidad (LibreNMS) detecta la pérdida de conectividad con el dispositivo y genera una alerta crítica. El equipo de red confirma el bloqueo.
- **Paso de Activación del Plan (Acción Manual de Emergencia)**. Un ingeniero ejecuta manualmente un playbook de Ansible específico para la recuperación, utilizando un inventario que apunta a la red de Gestión Fuera de Banda (OOB).
- **Paso de Restauración (Utiliza artefactos del Paso 6: Aplicación).** El playbook de emergencia realiza la recuperación: Se conecta de forma segura al dispositivo a través de la red OOB. Accede a GitLab para buscar y recuperar el último respaldo de configuración válido, que fue generado como artefacto durante la última ejecución

exitosa del **Paso 6** de un cambio anterior. Aplica esta configuración "buena" en el dispositivo, borrando el estado defectuoso.

- **Paso de Verificación Final (Similar en objetivo al Paso 7: Verificación)** El propio playbook comprueba que el acceso a través de la red de producción se ha restablecido. La plataforma de observabilidad (LibreNMS) confirma que el dispositivo vuelve a estar operativo y deja de alertar.

Resultado: Se consigue recuperar el control total de un activo crítico en cuestión de minutos, de forma remota y fiable, revirtiendo un fallo que manualmente podría tardar horas en resolverse. La organización dispone de un mecanismo robusto para recuperarse de fallos graves, garantizando la continuidad del servicio. Se minimiza el tiempo de inactividad de la gestión, pasando de un problema de horas (con desplazamiento físico) a una solución de minutos. La recuperación automatizada elimina el riesgo de errores humanos bajo presión, asegurando que se aplican los pasos y la configuración correctos en todo momento.

6.4.7 Caso de Uso 7: Control de Acceso de Usuario, NAC y Zero Trust

(no hay suficiente personal para gestionar las incidencias de un NAC y PKI)

~~Este caso ilustra la interacción diaria del NAC con las SOTs para un usuario.~~

~~**Escenario:** Un empleado conecta su portátil (autorizado) a un puerto de la red.~~

- ~~**Paso 1: Detección.** El switch detecta la conexión e inicia una petición 802.1X al NAC (PacketFence).~~
- ~~**Paso 2: Consulta SOT Identidad.** NAC valida las credenciales del usuario contra Active Directory (vía LDAP). AD confirma: "Usuario 'J.Doe' es válido y pertenece al grupo 'Contabilidad'".~~
- ~~**Paso 3: Consulta SOT** Infraestructura. NAC consulta la MAC del portátil contra NetBox (vía API). NetBox confirma: "Dispositivo 'LT-JDoe-01' está inventariado y autorizado".~~
- ~~**Paso 4: Decisión y Provisión.** El motor de políticas de NAC toma la decisión: "Usuario válido + Dispositivo válido = Acceso total". PacketFence ordena al switch (vía RADIUS) que coloque el puerto en la VLAN 20 (Contabilidad).~~

~~**Escenario Alternativo (Fallo):** Un invitado conecta un portátil personal (no autorizado).~~

- ~~**Pasos 1 y 2:** Ocurren igual.~~
- ~~**Paso 3 (Fallo):** NAC consulta la MAC contra NetBox. NetBox responde: "Dispositivo 'MAC-Invitado' no encontrado".~~
- ~~**Paso 4 (Decisión):** El motor de NAC decide: "Usuario válido + Dispositivo NO autorizado = Acceso restringido". PacketFence ordena al switch que coloque el puerto en la VLAN 99 (Invitados), que solo tiene salida a Internet.~~

~~**Resultado:** Se aplica el principio de Confianza Cero. El acceso no se concede por defecto; se verifica *cada conexión* contra las Fuentes de Verdad (Identidad e Infraestructura) antes de aplicar una política de acceso granular.~~

7 Plan de Acción y Casos de uso

7.1 Plan de Implantación y Transición (Primeros 90 Días)

Para materializar esta visión, se propone un plan de acción concreto y medible para los tres primeros meses de servicio. Este plan está diseñado para construir los cimientos del nuevo modelo de gestión mientras se garantiza la estabilidad del entorno actual.

Periodo	Hitos Clave	Actividades Detalladas
Semanas 1-3	Descubrimiento y Estabilización Inicial	- Realizar una auditoría exhaustiva de la red "as-is" para documentar todos los dispositivos, configuraciones y conexiones existentes. - Establecer los canales de comunicación y el protocolo de actuación para el servicio de soporte reactivo "break-fix". - Desplegar la infraestructura de servidores base que albergarán las herramientas de gestión (Netbox, Ansible, LibreNMS, Proxmox).
Semanas 4-7	Despliegue de Herramientas y Población de la SoT	- Instalar y configurar las instancias de Netbox, Ansible (con AWX/Tower para la gestión centralizada) y LibreNMS. - Realizar la población inicial de Netbox con los datos descubiertos en la fase de auditoría, estableciendo la primera versión de la Fuente Única de Verdad. - Configurar el entorno de Gemelo Digital en Proxmox, desplegando las primeras instancias de MikroTik CHR.
Semanas 8-12	Primeros Flujos de Automatización y Formación	- Desarrollar los primeros playbooks de Ansible para tareas de "solo lectura": backups de configuración automatizados, auditorías de versiones de software, etc. - Implementar y validar el inventario dinámico que conecta Ansible con Netbox. - Realizar la primera sesión de formación práctica y colaborativa con el equipo técnico municipal, enfocada en el uso de Netbox para documentar la red y la comprensión de la filosofía IaC. - Desarrollar y probar exhaustivamente en el gemelo digital el primer caso de uso de "escritura": la estandarización de la configuración de servicios básicos (NTP, Syslog, Banners de acceso) en todos los dispositivos.

7.2 Modelo de Mantenimiento Proactivo y Automatizado

El concepto de "mantenimiento" se transforma radicalmente. En lugar de revisiones manuales periódicas, se implementa un sistema de vigilancia y mantenimiento continuo basado en la automatización:

- **Auditoría Continua de Configuración:** Se programarán playbooks de Ansible para que se ejecuten de forma periódica (diaria o semanalmente) en modo de verificación (--check y --diff). Estos playbooks compararán la configuración real de cada dispositivo con el estado deseado definido en Netbox y Git. Cualquier desviación o "configuration drift" será detectada y reportada automáticamente, permitiendo una remediación inmediata.
- **Vigilancia Proactiva del Rendimiento:** Las alertas de LibreNMS se configurarán no solo para detectar fallos completos (un dispositivo caído), sino también para identificar degradaciones de rendimiento (alta latencia, pérdida de paquetes, utilización de CPU anómala). Esto permite intervenir antes de que los problemas afecten a los usuarios.
- **Mantenimiento Evolutivo:** El esfuerzo de mantenimiento se centrará en mejorar y ampliar la cobertura de la automatización. Por ejemplo, creando nuevos playbooks para auditar el cumplimiento de políticas de seguridad, automatizar actualizaciones de firmware o añadir nuevas métricas de monitorización a LibreNMS.

8 Ciberseguridad y Plataforma de Futuro

8.1 Seguridad por Capas

La ciberseguridad no es un producto, sino un proceso continuo que debe estar integrado en cada aspecto de la gestión de la red. Se propone una estrategia de "seguridad por capas" que aprovecha la automatización para garantizar una postura de seguridad robusta y consistente.

- **Capa 1 (Fundacional): Gestión de Vulnerabilidades y Hardening Automatizado.** La base de una red segura es una configuración robusta y actualizada. Se utilizarán playbooks de Ansible para aplicar de forma sistemática y auditable configuraciones de "hardening" en todos los dispositivos: desactivar servicios inseguros (ej. Telnet), forzar el uso de protocolos cifrados (SSH, HTTPS), configurar políticas de contraseñas robustas y desplegar parches de seguridad de forma controlada.
- **Capa 2 (Perimetral):** La gestión de las reglas del firewall se tratará como código, permitiendo su versionado, auditoría y despliegue controlado a través del flujo GitOps. En fases posteriores y gracias a la bolsa de horas para ampliación de equipos y servicios de red se podran desplegar e integrar la gestión de Firewalls de Aplicaciones Web (WAF) y Sistemas de Detección/Prevención de Intrusiones (IDS/IPS).
- ~~**Capa 3 (no hay suficiente personal para mantener un NAC y PKI): Control de Acceso a la Red (NAC) 802.1X.** Para combatir las amenazas internas y el acceso de dispositivos no autorizados, se propone la implementación del estándar 802.1X. Este sistema requiere que cualquier dispositivo (ordenador, teléfono, etc.) que se conecte a un puerto de red físico o a la red Wi-Fi se autentique contra un servidor central (RADIUS) antes de que se le conceda acceso. Esto asegura que solo dispositivos y~~

~~usuarios autorizados y conocidos puedan operar en la red interna. RouterOS de MikroTik puede actuar como cliente RADIUS, y el propio sistema puede albergar un servidor RADIUS o integrarse con soluciones existentes como Active Directory.~~

- **Capa 4 (Avanzada - Futuro): Microsegmentación y "Zero Trust".** La base de IaC establecida es el prerrequisito para adoptar arquitecturas de seguridad más avanzadas como la microsegmentación. Esta técnica permite crear políticas de firewall granulares entre servidores y servicios dentro de la propia red local, limitando drásticamente el movimiento lateral de un posible atacante, en línea con la filosofía "Zero Trust".
- **Capa 5 (Procedimental):** La tecnología se complementará con el desarrollo y formalización de Planes de Respuesta a Incidentes (SIRP) y Planes de Recuperación ante Desastres (DRP), asegurando que el Ayuntamiento esté preparado para actuar de forma coordinada y eficaz ante cualquier contingencia de seguridad.

8.2 Una Plataforma para el Futuro

Es fundamental entender que esta propuesta no entrega un producto final y estático, sino que construye una plataforma de gestión de red evolutiva. La combinación de Infraestructura como Código (IaC), una Fuente Única de Verdad (SoT) fiable y flujos de trabajo automatizados sienta las bases sólidas para futuras innovaciones y mejoras continuas.

Para materializar esta evolución, el contrato contempla una bolsa anual de 6.500 € (sin IVA) destinada exclusivamente a la mejora y adaptación de la plataforma. Esta partida permitirá, ademàs de implementar nuevos equipos de red, remunerar el diseño y la implementación de nuevas funcionalidades y servicios a propuesta del Ayuntamiento o del adjudicatario, tales como:

- El desarrollo de nuevos playbooks de Ansible para automatizar tareas complejas.
- La integración con otros sistemas municipales mediante las API de NetBox.
- La creación de scripts personalizados para la generación de informes o auditorías de seguridad.
- La adaptación de la plataforma a nuevas tecnologías o necesidades operativas.

Este mecanismo asegura que el Ayuntamiento y la empresa adjudicataria trabajen en consonancia por un objetivo común: hacer evolucionar la infraestructura de red de manera ágil y alineada con las necesidades estratéticas. Una vez consolidada la gestión básica, esta colaboración financiada permitirá abordar retos futuros con el mismo paradigma, como la implementación de redes superpuestas (overlay) seguras (p. ej., ZeroTier o Tailscale) para el teletrabajo o la interconexión de sedes, construyendo sobre las herramientas y el marco económico ya establecidos en este contrato.

9 Medición del Éxito y Conclusión

9.1 KPIs de Transformación

El éxito de esta propuesta no puede medirse con las métricas de un contrato de mantenimiento tradicional (como el número de tickets resueltos). El objetivo es la transformación, por lo que se deben adoptar Indicadores Clave de Rendimiento (KPIs) que reflejen la reducción de la necesidad de intervención y el aumento de la capacidad de

resolución y gestion de los técnicos informáticos municipales en las redes y sistemas del municipio.

Este cambio en la medición del valor posiciona el contrato no como un gasto operativo recurrente, sino como una **inversión estratégica en la capacidad institucional del Ayuntamiento**. No se están "alquilando manos", se está "adquiriendo el conocimiento, los procesos y las herramientas" para ser autónomos.

Categoría	KPI	Métrica	Objetivo a 4 Años
Reducción de Incidencias	Tiempo Medio Entre Fallos (MTBF)	Aumento del tiempo (horas) entre incidencias críticas.	Aumento significativo.
	Nº de incidencias P1/P2 por mes	Reducción del número absoluto de incidencias de alto impacto.	Reducción drástica.
	% de cambios que causan incidencias	Porcentaje de cambios desplegados que resultan en un fallo.	Tender a cero.
Eficiencia y Autonomía	Tiempo para desplegar un nuevo servicio/VLAN	Tiempo desde la solicitud hasta la disponibilidad del servicio.	De días/horas a minutos.
	% de infraestructura en la SoT	Porcentaje de dispositivos y conexiones documentados en Netbox.	100%.
	Nº de intervenciones reactivas requeridas	Número de veces que se requiere nuestro soporte "break-fix".	Reducción progresiva hasta ser excepcional.

9.2 Conclusión: El Ayuntamiento en 4 Años

Al finalizar el periodo de cuatro años de esta colaboración estratégica, el Ayuntamiento habrá experimentado una transformación fundamental en la gestión de su infraestructura tecnológica. La red habrá pasado de ser una fuente de incertidumbre y un lastre operativo a convertirse en un activo digital sólido, observable, seguro y ágil.

El escenario final será el de un equipo técnico municipal plenamente empoderado, que domina no solo las herramientas, sino la filosofía de la gestión moderna de redes. Gestionarán su infraestructura a través de procesos estandarizados, seguros y auditables, definidos como código y validados antes de cada despliegue. La documentación ya no será una tarea pendiente, sino un resultado intrínseco y siempre actualizado de su trabajo diario. La capacidad para desplegar nuevos servicios se habrá acelerado exponencialmente, permitiendo al departamento de TI responder con agilidad a las necesidades cambiantes del Ayuntamiento y sus ciudadanos.

En definitiva, al cabo de cuatro años, el Ayuntamiento habrá alcanzado la soberanía tecnológica sobre uno de sus activos más críticos. La dependencia de proveedores externos para la operativa diaria será cosa del pasado. Nuestra relación, una vez cumplido con éxito este objetivo, podrá evolucionar hacia un rol de consultoría estratégica de alto nivel, ayudando al Ayuntamiento a afrontar los futuros retos tecnológicos desde una posición de fortaleza y autonomía. La inversión detallada en esta memoria no es, por tanto, un coste de mantenimiento, sino la construcción de una capacidad interna sostenible que generará un valor creciente para el Ayuntamiento durante muchos años.

Valoració:

La proposta rep la màxima puntuació per presentar un projecte integral i estratègic que va molt més enllà d'una simple prestació de serveis. Es posiciona com un veritable soci tecnològic per a l'Ajuntament, prioritzant el seu interès a llarg termini mitjançant un compromís explícit amb la transferència de coneixement i garantint la propietat de les dades municipals des del primer dia, fet que assenta les bases per a una autèntica sobirania tecnològica.

Aquesta visió es materialitza en un ecosistema tecnològic integrat i coherent, basat en estàndards oberts que eviten la dependència de proveïdors (*vendor lock-in*). Això permet transformar la gestió de xarxes (NetOps) d'un model reactiu a un de proactiu, basat en dades i totalment auditable. La solidesa de la proposta es reforça amb una selecció de maquinari que respon a una visió estratègica a llarg termini, on es prioritza la responsabilitat fiscal i el retorn de la inversió, i s'introdueixen mecanismes robustos de mitigació de riscos com el bessó digital per garantir l'estabilitat del servei.

Per articular tot aquest conjunt, es presenta un model operatiu complet i pragmàtic, acompanyat d'un pla de transició realista i un manteniment profundament automatitzat, la qual cosa es traduirà en operacions més ràpides, segures i eficients per al personal informàtic.

Finalment, tot el sistema està protegit per un enfocament de seguretat holístic i modern. S'aplica el principi de Defensa en Profunditat amb una estratègia multicapa que combina la gestió de vulnerabilitats, la protecció perimetral avançada i, de manera crucial, la implementació de principis Zero Trust, assegurant una protecció robusta i auditable de tots els actius digitals de l'Ajuntament.