PROYECTO TÉCNICO

Sistema de Monitorización de Red (NMS)

Sede Central — 60 puestos de trabajo

Supervisión centralizada de Red Telemática, UTM, VPN, Wi-Fi y CCTV

Enrique Calabozo Orea
Administrador de Sistemas TIC / Project Manager
Agosto 2026 • v1.0

Situación Actual

Infraestructura ya desplegada en la sede central, sin visibilidad centralizada de su estado.

Red Telemática (Core + VLAN)	Firewall / UTM Perimetral	VPN Site-to-Site	Wi-Fi Corporativo	CCTV (NVR/Cámaras)

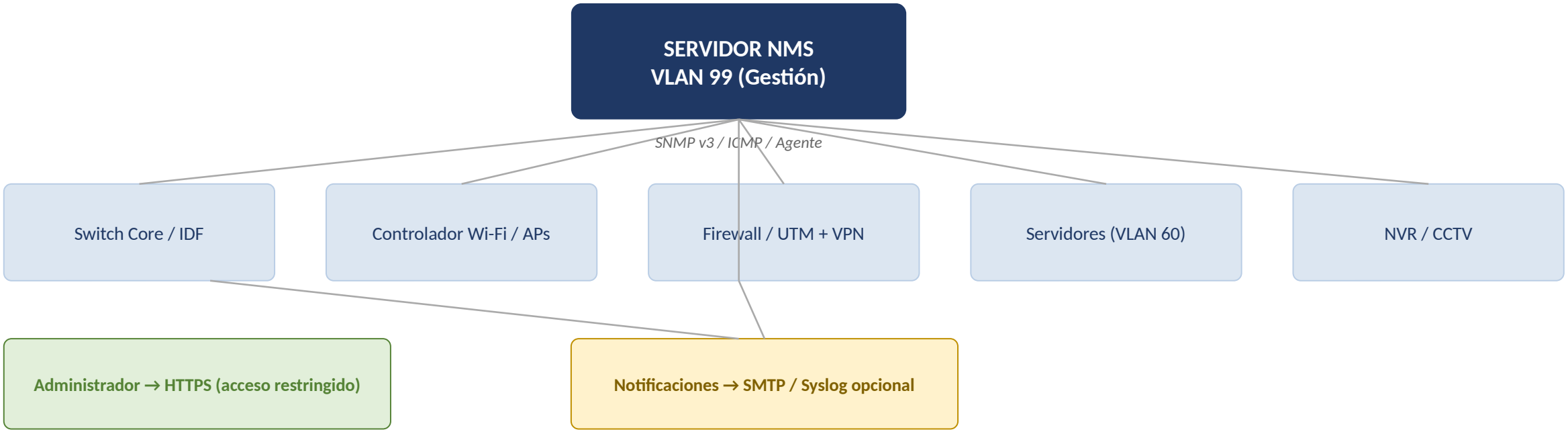
Problema identificado

No existe ningún sistema centralizado de supervisión: las incidencias se detectan por observación directa o notificación de usuarios, retrasando la respuesta ante caídas de enlace, saturación de CPU, fallos de VPN o degradación de servicios.

Objetivos del Proyecto

1. Desplegar el servidor NMS en la VLAN 99 (Gestión), con acceso restringido.
2. Monitorizar disponibilidad de switches, APs, UTM, servidores y NVR.
3. Supervisar CPU, memoria, temperatura y uso de enlaces.
4. Vigilar el estado de los túneles VPN Site-to-Site.
5. Generar alertas por severidad y notificaciones por correo.
6. Aplicar mínimo privilegio: SNMP de solo lectura y ACLs de acceso.

Arquitectura del Sistema de Monitorización

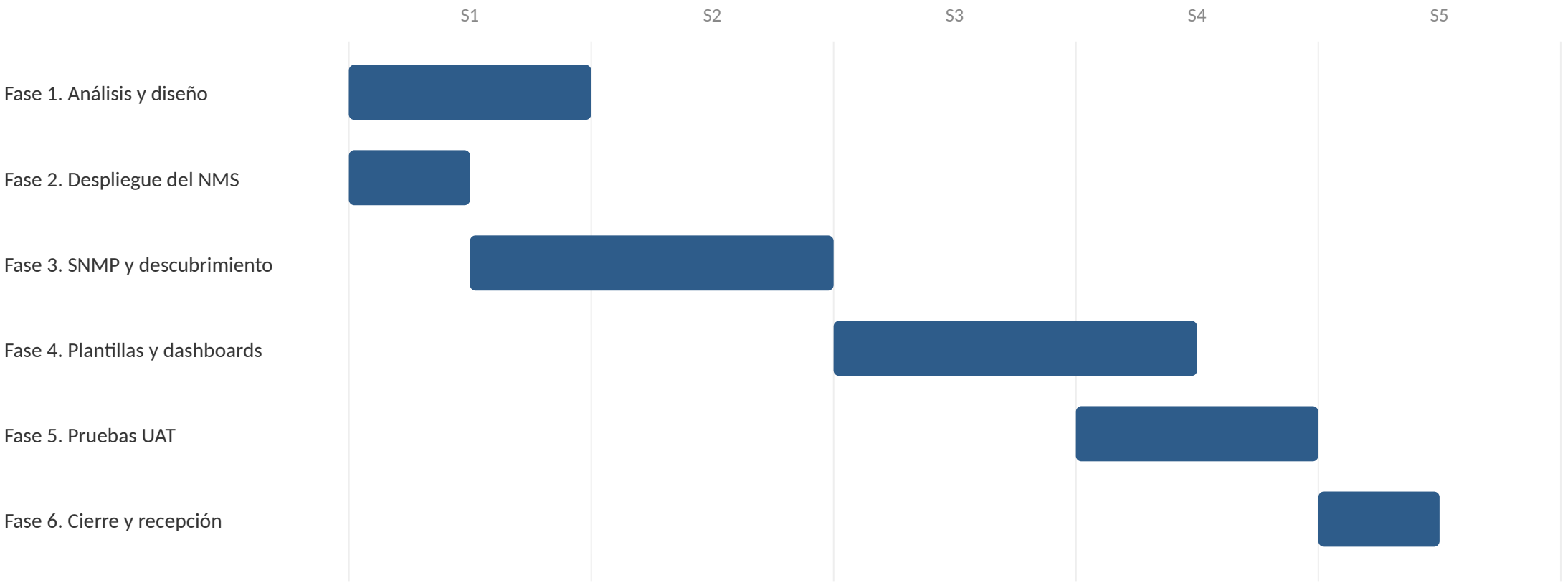


El NMS inicia el tráfico de monitorización hacia los equipos; ningún equipo inicia conexión hacia el NMS salvo traps/syslog expresamente permitidos.

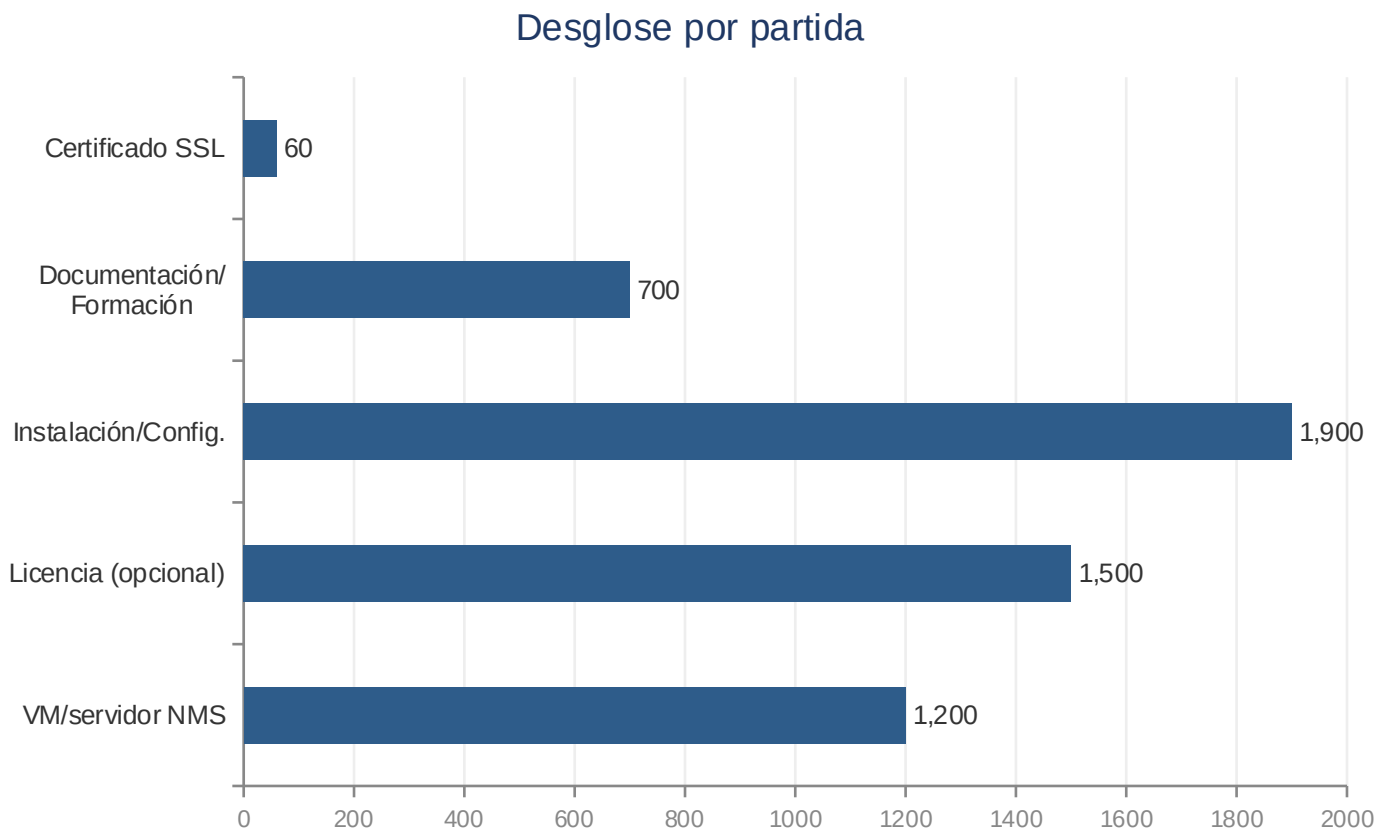
Umbrales y Severidades de Alerta

Disaster	Elemento crítico caído > 2 min
High	Túnel VPN caído; servicio crítico no responde
Average	CPU > 85% sostenido 10 min
Warning	Disco > 75%; temperatura anómala
Information	Reinicio o cambio de configuración

Plan de Ejecución (5 semanas)



Presupuesto Estimado



TOTAL (con licencia)

6.473,50 €

(con IVA 21%)

TOTAL (open-source)

4.658,50 €

(con IVA 21%)

Plataforma open-source (Zabbix/LibreNMS) sin coste de licencia reduce el total en ~1.200-1.500€.

Principales Riesgos

ID	Riesgo	Criticidad
R1	Credenciales SNMP expuestas	6
R2	Saturación del NMS por exceso de métricas	6
R3	Exceso de falsos positivos (fatiga de alertas)	6
R7	Retraso en obtención de acceso SNMP a equipos	4
R8	Desactualización de plantillas ante cambios	4
R4	Pérdida de configuración por fallo del servidor	3
R5	Acceso no autorizado a la consola web	3
R6	Impacto en rendimiento por sondeo excesivo	2

Escala de criticidad

- Alta (6–9)
- Media (3–4)
- Baja (1–2)

Criticidad = Probabilidad × Impacto (escala 1–3 cada uno).

Pruebas de Aceptación (UAT)

10 casos de prueba (P-N01–P-N10) con criterio PASS/FAIL medible. Aceptación: 100% PASS antes de la recepción provisional.

- ☑ P-N01 Descubrimiento completo de hosts
- ☑ P-N02 Detección de caída de switch de acceso
- ☑ P-N03 Detección de caída de túnel VPN
- ☑ P-N04 Umbral de CPU alta en switch Core
- ☑ P-N05 Umbral de disco en servidor
- ☑ P-N06 Envío de notificación por correo
- ☑ P-N07 Panel/dashboard refleja estado real
- ☑ P-N08 Acceso restringido a consola web
- ☑ P-N09 Copia de seguridad de configuración
- ☑ P-N10 Retención de históricos según política

Conclusiones

- ✓ Aporta visibilidad proactiva de la que hoy carece la organización.
- ✓ Coherente con el direccionamiento y VLAN ya desplegadas – sin modificar la infraestructura existente.
- ✓ Ubicado en la VLAN de Gestión conforme a las buenas prácticas de segmentación.
- ✓ Se recomienda revisar los umbrales durante los primeros meses para reducir falsos positivos.