PROYECTO TÉCNICO

Sistema de Monitorización de Red (NMS)

Sede Central — 60 puestos de trabajo

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

Autor: Enrique Calabozo Orea

Administrador de Sistemas TIC / Project Manager

Fecha: Agosto 2026

Versión: 1.0

Índice

1. Introducción

El presente documento constituye la Memoria Técnica del proyecto “Sistema de Monitorización de Red (NMS) – Sede Central (60 puestos)”, cuyo objeto es dotar a la organización de una plataforma centralizada de supervisión (Network Monitoring System) que ofrezca visibilidad continua sobre el estado, disponibilidad y rendimiento de la infraestructura de red ya desplegada.

El NMS se integra de forma coherente con los proyectos previamente documentados: la Implantación de Red Telemática (60 puestos), el Firewall UTM Perimetral, la VPN Site-to-Site, el sistema de videovigilancia IP (CCTV) y la red Wi-Fi corporativa. Su función es supervisar de forma unificada todos estos sistemas, generando alertas tempranas ante degradaciones o caídas de servicio, sin sustituir ni modificar la funcionalidad de ninguno de ellos.

El documento sigue la estructura habitual de la documentación técnica de proyecto empleada en las certificaciones profesionales IFCT0410 / IFCT0510, e incluye memoria técnica, anexos numerados correlativamente y anexos de soporte a la ejecución, operación y aceptación del sistema.

2. Objetivos del Proyecto

2.1. Objetivo general

Desplegar un sistema de monitorización de red centralizado (tipo Zabbix, PRTG o equivalente) ubicado en la VLAN de Gestión, que descubra y supervise mediante SNMP/ICMP/agentes toda la infraestructura crítica de la sede central, generando alertas ante incidencias y ofreciendo paneles de visibilidad del estado de la red.

2.2. Objetivos específicos

- Desplegar el servidor NMS en la VLAN 99 (Gestión), con acceso restringido y HTTPS a la consola web.
- Descubrir y monitorizar la disponibilidad (up/down) de switch Core, switches de acceso, controlador Wi-Fi/APs, firewall/UTM, servidores y NVR de CCTV.
- Supervisar métricas de rendimiento: CPU, memoria, temperatura (si disponible) y uso de enlaces (tráfico in/out).
- Monitorizar el estado de los túneles VPN Site-to-Site (up/down).
- Controlar el espacio en disco de los servidores y del propio NMS.
- Supervisar servicios críticos (DHCP, DNS, VMS de CCTV) dentro del alcance del proyecto.
- Configurar umbrales de alerta por severidad y notificaciones por correo electrónico (y opcionalmente syslog/webhook).
- Definir retención de históricos (corto y largo plazo) y copias de seguridad de la configuración del NMS.
- Aplicar principio de mínimo privilegio: credenciales SNMP de solo lectura, ACL de acceso, usuarios con roles diferenciados.

3. Antecedentes y Situación Actual

La sede central dispone de una red telemática operativa para 60 puestos de trabajo, con Switch Core L3 en el MDF, switches de acceso en los IDF, controlador Wi-Fi con puntos de acceso, sistema de videovigilancia IP (NVR/cámaras), un firewall/UTM perimetral y una VPN Site-to-Site hacia una sucursal remota. El esquema de VLAN en producción es el siguiente:

VLAN	Nombre	Red / Máscara	Descripción
10	Datos	10.10.10.0/24	Puestos de usuario, equipos de oficina
20	Voz	10.10.20.0/24	Telefonía IP / centralita virtual
30	Wi-Fi Corporativo	10.10.30.0/24	Acceso inalámbrico de empleados
40	Wi-Fi Invitados	10.10.40.0/24	Acceso inalámbrico de visitantes (aislado)
50	Vídeo / CCTV	10.10.50.0/24	Cámaras IP, NVR/VMS
60	Servidores	10.10.60.0/24	Servidores internos y aplicaciones corporativas
99	Gestión	10.10.99.0/24	Gestión de electrónica de red; ubicación prevista del NMS

Actualmente no existe ningún sistema centralizado de supervisión: la detección de incidencias depende de la observación directa o de la notificación de los propios usuarios, lo que retrasa la identificación de caídas de enlace, saturación de CPU, fallos de VPN o degradación de servicios críticos. Esta carencia de visibilidad proactiva es la necesidad que este proyecto resuelve.

4. Descripción General del Proyecto

El proyecto consiste en el diseño, despliegue, configuración y puesta en producción de un servidor NMS (físico o virtual) ubicado en la VLAN 99 de Gestión, que descubra y monitorice mediante SNMP v2c/v3, ICMP y agentes (donde proceda) los elementos de la infraestructura existente.

El alcance del proyecto comprende:

- Definición de la arquitectura del sistema de monitorización y su ubicación en la VLAN de Gestión.
- Selección de requisitos mínimos de la plataforma NMS (dimensionamiento por número de hosts/métricas).
- Configuración de credenciales SNMP de solo lectura y ACLs de acceso a los equipos gestionados.
- Descubrimiento e incorporación de los elementos a monitorizar: switches, APs, firewall/UTM, servidores, NVR, enlaces VPN, UPS/PDU (si disponen de SNMP).
- Definición de plantillas de monitorización, umbrales de alerta por severidad y reglas de notificación.
- Configuración de mapas de red y paneles (dashboards) de estado.
- Definición de política de retención de históricos y copia de seguridad de la configuración del NMS.
- Pruebas de aceptación (UAT), documentación final y entrega formal mediante Acta de Recepción Provisional.

Quedan fuera de alcance: la sustitución de los equipos monitorizados, el despliegue de un SIEM completo y la correlación avanzada de eventos de seguridad, que se consideran proyectos independientes.

5. Solución Técnica Propuesta

5.1. Ubicación y arquitectura

El servidor NMS se despliega como máquina virtual (opción recomendada) o equipo físico dedicado, ubicado en la VLAN 99 (Gestión). Desde esta posición dispone de visibilidad hacia el resto de VLANs mediante reglas específicas de firewall/UTM que permiten únicamente el tráfico de monitorización necesario (SNMP, ICMP, y agentes) en sentido NMS → equipos monitorizados, y el acceso administrativo a la consola web en sentido restringido hacia el NMS.

5.2. Protocolos de monitorización

- SNMP v3 (preferible) o v2c con comunidad de solo lectura no trivial, para switches, APs, UTM/firewall, UPS/PDU compatibles.
- ICMP (ping) para verificación básica de disponibilidad de todos los elementos.
- Agentes ligeros (NMS agent) en servidores Linux/Windows para métricas de CPU, memoria, disco y servicios locales, donde SNMP no sea suficiente.
- Syslog (opcional) para centralizar eventos adicionales de los equipos que lo soporten, complementando al UTM perimetral.

5.3. Elementos monitorizados

Elemento	Método	Métricas clave
Switch Core L3 (MDF)	SNMP v3 + ICMP	Disponibilidad, CPU, memoria, uso de puertos, temperatura
Switches de acceso (IDF)	SNMP v3 + ICMP	Disponibilidad, uso de puertos, errores de interfaz
Controlador Wi-Fi / APs	SNMP v3 + ICMP / API	Disponibilidad, nº de clientes asociados, uso de canal
Firewall / UTM perimetral	SNMP v3 + syslog	Disponibilidad, CPU, memoria, sesiones, estado VPN
Túneles VPN Site-to-Site	SNMP / API del UTM	Estado del túnel (up/down), tráfico cursado
Servidores (VLAN 60)	Agente + SNMP	CPU, memoria, disco, servicios críticos (DHCP/DNS/VMS)
NVR / VMS de CCTV	SNMP + ICMP	Disponibilidad, espacio de grabación, estado de cámaras
UPS / PDU (si disponen de SNMP)	SNMP v2c/v3	Estado de alimentación, autonomía de batería, temperatura

5.4. Umbrales y severidades de alerta

Severidad	Ejemplo de disparador	Notificación
Disaster	Elemento crítico caído (Core, UTM, NVR) > 2 min	Correo inmediato + repetición cada 15 min hasta resolución
High	Túnel VPN caído; servicio crítico (DHCP/DNS) no responde	Correo inmediato
Average	CPU > 85% sostenido 10 min; uso de enlace > 80%	Correo en horario laboral
Warning	Disco > 75%; temperatura por encima de umbral normal	Correo diario agrupado
Information	Reinicio de equipo, cambio de configuración detectado	Registro en panel, sin correo

5.5. Notificaciones

El canal principal de notificación es el correo electrónico, con distribución diferenciada por severidad y horario. De forma opcional, se habilita el envío de alertas por webhook o syslog hacia un sistema SIEM o hacia el propio UTM perimetral, permitiendo una futura correlación de eventos.

5.6. Retención y copias de seguridad

Se define una retención de histórico detallado (alta resolución) de 30 días y una retención de histórico agregado (tendencias) de 12 meses, suficiente para análisis de capacidad sin comprometer el rendimiento del NMS. La configuración del NMS (hosts, plantillas, usuarios, umbrales) se respalda de forma automática y diaria, con retención mínima de 90 días de copias.

5.7. Seguridad

- Credenciales SNMP de solo lectura, distintas por segmento cuando sea posible, sin comunidades por defecto ("public").
- Acceso a la consola web del NMS únicamente vía HTTPS, restringido por IP de origen y con usuarios nominales por rol (administrador, operador, solo lectura).
- Reglas de firewall/UTM específicas que permiten sólo el tráfico de monitorización estrictamente necesario, en el sentido NMS → equipos.
- Registro de auditoría de accesos y cambios de configuración del propio NMS.

6. Especificaciones Técnicas

Requisitos mínimos orientativos de la plataforma NMS, dimensionados para 60 puestos + infraestructura asociada (aprox. 40–60 hosts monitorizados, 2.000–3.500 métricas activas):

Parámetro	Requisito mínimo orientativo
vCPU / CPU	4 vCPU
Memoria RAM	8 GB
Almacenamiento	150 GB SSD (sistema + base de datos de históricos)
Sistema operativo	Linux (distribución compatible con la plataforma NMS elegida)
Hosts monitorizados (capacidad objetivo)	≥ 80 (margen de crecimiento sobre 40–60 actuales)
Métricas/ítems activos (capacidad objetivo)	≥ 5.000
Protocolos soportados	SNMP v2c/v3, ICMP, agente propio, syslog, HTTP(S) API
Alta disponibilidad	No requerida en fase inicial; backup diario de configuración
Acceso administrativo	HTTPS, restringido por IP, roles diferenciados
Retención histórico detallado / agregado	30 días / 12 meses

7. Plan de Ejecución y Cronograma

El proyecto se ejecuta en 6 fases a lo largo de 5 semanas. El detalle de tareas, duración y diagrama se recoge en el Anexo 3 – Cronograma.

Fase	Descripción	Duración
1	Análisis, inventario de elementos a monitorizar y diseño	1 semana
2	Despliegue del servidor NMS (VM) e instalación base	0,5 semana
3	Configuración de credenciales SNMP y descubrimiento de red	1 semana
4	Plantillas, umbrales, alertas y dashboards	1 semana
5	Pruebas de aceptación (UAT) y ajuste fino	1 semana
6	Documentación final, formación y recepción provisional	0,5 semana

8. Presupuesto Estimado

El desglose completo se recoge en el Anexo 2. Resumen por partidas:

Partida	Importe (sin IVA)
Servidor NMS (VM dedicada o hardware si se opta por físico)	1.200,00 €

Partida	Importe (sin IVA)
Licencias de la plataforma NMS (si aplica; 3 años)	1.500,00 €
Instalación, configuración y descubrimiento de red	1.900,00 €
Documentación, pruebas y formación	700,00 €
TOTAL (sin IVA)	**5.300,00 €**
IVA (21%)	1.113,00 €
TOTAL (con IVA)	**6.413,00 €**

Nota: si se opta por una plataforma open-source (Zabbix, LibreOMS) sin coste de licencia, la partida de licencias se reduce a soporte/actualizaciones opcional, disminuyendo el total en aproximadamente 1.200–1.500 €.

9. Gestión de Riesgos

La matriz completa de riesgos se detalla en el Anexo 4. Se identifican 8 riesgos, siendo los de mayor criticidad la exposición de credenciales SNMP y la saturación del NMS por exceso de métricas mal dimensionadas.

10. Plan de Calidad y Pruebas

Se define un Plan de Pruebas de Aceptación (UAT) con casos de prueba identificados (P-N01, P-N02…) y criterio PASS/FAIL medible, recogido en el Anexo 9. Las pruebas cubren: descubrimiento correcto de todos los elementos del alcance, generación de alertas dentro de los tiempos objetivo, correcto envío de notificaciones, funcionamiento de los dashboards y validación de la retención/backup de configuración.

11. Documentación a Entregar

- Memoria técnica del proyecto (este documento).
- Anexo 1 – Arquitectura del sistema de monitorización.
- Anexo 2 – Presupuesto detallado.
- Anexo 3 – Cronograma.
- Anexo 4 – Matriz de riesgos.
- Anexo 5 – Inventario de elementos monitorizados y métricas clave.
- Anexo 6 – Manual de Operación y Mantenimiento.
- Anexo 7 – Inventario de equipos del propio sistema NMS.
- Anexo 8 – Configuración base / plantillas.
- Anexo 9 – Plan de Pruebas de Aceptación (UAT).
- Anexo 10 – Acta de Recepción Provisional.

12. Conclusiones

El despliegue del sistema de monitorización de red aporta a la organización la visibilidad proactiva de la que carecía, permitiendo detectar degradaciones y caídas de servicio antes de que impacten de forma significativa en los usuarios. La solución propuesta es coherente con el direccionamiento y las VLAN ya desplegadas, se ubica en la VLAN de Gestión conforme a las buenas prácticas de segmentación, y no requiere modificar la electrónica de red ni los sistemas ya existentes (Red Telemática, UTM, VPN, CCTV, Wi-Fi).

Se recomienda revisar periódicamente los umbrales de alerta durante los primeros meses de operación, con el fin de reducir falsos positivos y ajustar la sensibilidad del sistema a la realidad operativa de la sede.

13. Anexos

Los anexos numerados del 1 al 10 se desarrollan a continuación de esta memoria.