

ANEXO 6 – Manual de Operación y Mantenimiento

6.1. Acceso y gestión

- Acceso administrativo a la consola web únicamente vía HTTPS, restringido por IP de origen desde la VLAN 99 o IP del personal TIC autorizado.
- Cuentas nominales por técnico, con rol diferenciado (administrador, operador, solo lectura); prohibido el uso de cuentas genéricas compartidas.
- Registro de auditoría de todos los accesos y cambios de configuración.

6.2. Gestión de alertas y escalado

- Alertas de severidad Disaster/High: notificación inmediata por correo al personal TIC de guardia; repetición periódica hasta resolución o reconocimiento.
- Alertas de severidad Average/Warning: notificación agrupada en horario laboral, revisión diaria por el equipo de sistemas.
- Procedimiento de escalado: si una alerta crítica no se reconoce en 30 minutos, se notifica al responsable de sistemas TIC como segundo nivel.

6.3. Copias de seguridad

- Backup automático diario de la configuración del NMS (hosts, plantillas, usuarios, umbrales), exportado a repositorio externo al propio servidor.
- Backup adicional manual antes de cualquier cambio relevante (actualización de versión, cambios masivos de plantillas).
- Retención mínima de 90 días de copias de configuración.

6.4. Mantenimiento periódico

- Revisión mensual de falsos positivos y ajuste de umbrales por tipo de equipo.
- Revisión trimestral del inventario de hosts monitorizados, dando de baja equipos retirados y de alta los nuevos.
- Actualización de la plataforma NMS según calendario de parches del fabricante/proyecto, en ventana de mantenimiento planificada.
- Purga automática de históricos conforme a la política de retención (30 días detalle / 12 meses agregado).

6.5. Procedimiento ante incidencias

Incidencia	Procedimiento
Alerta de disponibilidad (equipo down)	Verificar conectividad física/lógica, comprobar SNMP/ICMP desde el propio NMS, escalar si persiste
Exceso de falsos positivos en un host	Revisar umbral configurado, ajustar según comportamiento normal del equipo, documentar el cambio
Fallo de envío de notificaciones	Verificar configuración SMTP, comprobar cola de alertas, reenviar manualmente si procede
Saturación de recursos del propio NMS	Revisar métricas de CPU/memoria/disco del NMS, reducir frecuencia de sondeo o ampliar recursos de la VM