ANEXO 4 – Matriz de Riesgos

Escala: Probabilidad e Impacto valorados de 1 (bajo) a 3 (alto). Criticidad = Probabilidad × Impacto. Verde: 1–2 (bajo) · Ámbar: 3–4 (medio) · Rojo: 6–9 (alto).

ID	Riesgo	Prob.	Imp.	Criticidad	Mitigación	Contingencia
R1	Credenciales SNMP expuestas o con comunidades por defecto	2	3	6	SNMP v3 con autenticación/cifrado, comunidades no triviales, ACL por IP	Rotación inmediata de credenciales y auditoría de accesos
R2	Saturación del NMS por exceso de métricas mal dimensionadas	2	3	6	Dimensionamiento con margen (sección 6), revisión de intervalos de sondeo	Ampliación de recursos de la VM o reducción de frecuencia de sondeo
R3	Exceso de falsos positivos que generan fatiga de alertas	3	2	6	Umbrales calibrados en UAT, periodo de ajuste tras la puesta en producción	Revisión y reajuste de umbrales por tipo de equipo
R4	Pérdida de la configuración del NMS por fallo del servidor	1	3	3	Copia de seguridad diaria automática de la configuración	Restauración desde la última copia válida
R5	Acceso no autorizado a la consola web del NMS	1	3	3	HTTPS, restricción por IP, roles de usuario diferenciados	Bloqueo de cuenta y auditoría de accesos
R6	Impacto en el rendimiento de los equipos monitorizados por sondeo excesivo	1	2	2	Intervalos de sondeo ajustados por criticidad del equipo	Reducción de la frecuencia de sondeo en el equipo afectado
R7	Retraso en la obtención de acceso SNMP a determinados equipos	2	2	4	Solicitud anticipada de credenciales/ACL en fase 1	Monitorización provisional sólo por ICMP hasta resolver el acceso
R8	Desactualización de plantillas ante cambios en la infraestructura	2	2	4	Procedimiento de actualización de inventario en cada proyecto nuevo	Revisión trimestral de hosts y plantillas activas