

Tabla 3. Marco de gestión de riesgos para automatizaciones

Código del riesgo	Riesgo identificado	Medida de control principal	Tipo de medida de control	Tipo de acción frente al riesgo	Prioridad	Responsable principal	Alcance
R1	Pérdida de datos o configuraciones por ausencia de respaldo previo	Implementar respaldos obligatorios antes de cualquier cambio en automatizaciones (NAS + OneDrive + verificación).	Tecnológica / Administrativa	Mitiga / Evita	Crítica	Analista SOC / Líder SOC	Todas las automatizaciones que modifiquen scripts, configuraciones o flujos en producción.
R2	Bloqueo o suspensión de servicios externos (ej. WhatsApp corporativo)	Definir límites de frecuencia y volumen de envío; uso de ambientes de prueba y listas de destinatarios controladas.	Tecnológica / Administrativa	Mitiga	Alta	Analista SOC	Automatizaciones que interactúan con plataformas externas de mensajería o notificación.
R3	Fallos de integración entre sistemas (plataformas)	Validar credenciales, rutas, APIs y conexiones en entorno de pruebas; monitoreo de logs y alertas ante errores.	Tecnológica	Mitiga	Alta	Analista SOC	Integraciones entre SOAR, Grafana, FGT, NAS, OneDrive y otras plataformas relacionadas.
R4	Generación de reportes erróneos o incompletos	Definir criterios de aceptación; revisión de consultas y filtros de tiempo; validación de reportes por un segundo revisor.	Administrativa / Tecnológica	Mitiga	Alta	Analista SOC / Líder SOC	Automatizaciones de generación y envío de reportes operativos o de monitoreo.
R5	Envío duplicado o masivo de correos automatizados	Configuración correcta de tareas programadas; pruebas con destinatarios de prueba; monitoreo inicial tras despliegue.	Tecnológica	Mitiga	Alta	Analista SOC	Automatizaciones que utilizan correo electrónico como canal de notificación.
R6	Falta de trazabilidad y documentación de automatizaciones	Implementar registro centralizado de automatizaciones, control de versiones y formatos de documentación obligatoria.	Administrativa	Mitiga / Evita	Alta	Líder SOC	Todas las automatizaciones creadas o modificadas en el SOC.

Fuente: Elaboración propia