Checklist de Automatización de Seguridad Multicloud

Use esta lista para verificar el nivel de madurez de sus procesos de automatización de seguridad en entornos multicloud (Azure y AWS). Está orientada a roles de gestión y cumplimiento. Responda cada pregunta con 'Sí' o 'No'.

1. Gobernanza y planificación de la automatización

[ ] ¿Existe una política formal de automatización de seguridad aprobada por la dirección? (Sí / No)

[ ] ¿Se han evaluado los riesgos potenciales de la automatización (falsos positivos, impacto operativo)? (Sí / No)

[ ] ¿Se han definido roles y responsables claros para la automatización de seguridad? (Sí / No)

[ ] ¿Existe un comité que revisa periódicamente las reglas de automatización? (Sí / No)

2. Integración de plataformas y monitoreo unificado

[ ] ¿Todos los registros y alertas están centralizados en una plataforma SIEM común? (Sí / No)

[ ] ¿Se monitorean continuamente las configuraciones inseguras en cada nube? (Sí / No)

[ ] ¿Los hallazgos de seguridad se centralizan en un solo panel multicloud? (Sí / No)

[ ] ¿Existe integración bidireccional entre nubes para eventos críticos? (Sí / No)

3. Identificación de escenarios de automatización

[ ] ¿Se tiene un inventario de alertas críticas que podrían automatizarse? (Sí / No)

[ ] ¿Se han definido criterios de activación claros para cada tipo de alerta? (Sí / No)

[ ] ¿Se ha documentado la acción deseada por tipo de incidente? (Sí / No)

[ ] ¿Los responsables de cumplimiento participan en la definición de automatizaciones? (Sí / No)

Sheyla Leacock – Carlos Solís Salazar

4. Diseño de playbooks y flujos de respuesta

[ ] ¿Existen playbooks de respuesta que actúan sobre recursos en Azure y AWS? (Sí / No)

[ ] ¿Los flujos automatizados incorporan validaciones o aprobaciones? (Sí / No)

[ ] ¿Cada paso de los playbooks está mapeado a políticas internas o controles normativos? (Sí / No)

[ ] ¿Se usan plantillas o estándares de la industria como base de los flujos? (Sí / No)

5. Control de accesos e identidades

[ ] ¿Las cuentas usadas en automatizaciones siguen el principio de mínimo privilegio? (Sí / No)

[ ] ¿Se revisan periódicamente los privilegios de cuentas de automatización? (Sí / No)

[ ] ¿Se segregan los entornos de pruebas y producción en la automatización? (Sí / No)

[ ] ¿Las cuentas con privilegios altos tienen autenticación multifactor habilitada? (Sí / No)

6. Cumplimiento normativo y auditoría

[ ] ¿Todas las acciones automatizadas quedan registradas en logs de auditoría? (Sí / No)

[ ] ¿Se generan reportes automáticos de cumplimiento a partir de estos registros? (Sí / No)

[ ] ¿Cada automatización está mapeada a un control de cumplimiento específico? (Sí / No)

[ ] ¿Se validan las implicaciones legales de las acciones automáticas de alto impacto? (Sí / No)

7. Pruebas, simulacros y validación

[ ] ¿Se prueban los playbooks en entornos seguros antes de habilitarlos en producción? (Sí / No)

[ ] ¿Se realizan simulacros periódicos que validen el comportamiento automatizado? (Sí / No)

[ ] ¿Se revisan y actualizan las reglas disparadoras de automatizaciones regularmente? (Sí / No)

[ ] ¿Se documentan lecciones aprendidas después de cada incidente o prueba? (Sí / No)

8. Monitoreo y mejora continua

[ ] ¿Se monitorea el éxito o fallo de las automatizaciones en tiempo real? (Sí / No)

[ ] ¿Existen procedimientos de respaldo manual si una automatización falla? (Sí / No)

[ ] ¿Se revisan y actualizan periódicamente las reglas de automatización? (Sí / No)

[ ] ¿Se presentan métricas de automatización a la alta dirección? (Sí / No)

9. Capacitación y concientización

[ ] ¿El equipo de seguridad está capacitado en las herramientas de automatización usadas? (Sí / No)

[ ] ¿El equipo de gestión/compliance entiende cómo funcionan los flujos automatizados? (Sí / No)

[ ] ¿Los equipos de TI y usuarios clave conocen qué acciones están automatizadas? (Sí / No)

[ ] ¿Se promueve una cultura de mejora continua y reporte de errores en automatización? (Sí / No)

✅ SISTEMA DE PONDERACIÓN:
- Cada “Sí” = 1 punto
- Cada “No” o en blanco = 0 puntos
- Total máximo de puntos posibles: 36 (9 secciones × 4 preguntas)

Modelo de Madurez de Automatización en Seguridad Cloud

Nivel 0 - Reactivo

- Rango de puntos: 0 - 10 puntos

Automatización inexistente o mínima. Las acciones son manuales. No hay visibilidad integrada ni gobernanza. Alto riesgo de incumplimiento.

Nivel 1 - Inicial

- Rango de puntos: 11 - 18 puntos

Hay algunas automatizaciones aisladas, sin estandarización. No están alineadas con políticas ni revisadas por compliance. Riesgo medio-alto.

Nivel 2 - Controlado

- Rango de puntos: 19 - 26 puntos

La organización cuenta con automatizaciones bien definidas, algunas integradas entre nubes. Se monitorea la efectividad, pero aún falta integración con cumplimiento normativo.

Nivel 3 - Orquestado

- Rango de puntos: 27 - 32 puntos

Los flujos de automatización están estandarizados, gobernados, y auditados. Hay integración entre plataformas y reportes automáticos. Se reacciona rápido y con trazabilidad.

Nivel 4 - Optimizado

- Rango de puntos: 33 - 36 puntos

La automatización está alineada con la estrategia de seguridad y cumplimiento. Simulacros, métricas, revisión continua y mejora constante. Tiempo de respuesta mínimo y alta resiliencia.