SWIFT CSCF v2026 · Control 7.3A

Lista de comprobación de preparación para la prueba de penetración del Control 7.3A de SWIFT CSCF v2026

1. Definir el alcance por consecuencia

- ☐ El entorno SWIFT está inventariado: zona segura, interfaz de mensajería, estaciones de trabajo de los operadores, la conexión a la red y los sistemas de back-office que la alimentan.
- ☐ Las rutas de ataque se clasifican por la consecuencia de un compromiso, no por la facilidad de prueba.
- ☐ El alcance se define frente a la zona segura y sus límites de confianza, de modo que la prueba demuestre que un atacante no puede pivotar desde el back-office hacia la capa de mensajería.
- ☐ La prueba está planificada a lo largo del ciclo de escenarios de tres años, cubriendo rutas de aplicación, infraestructura y humanas.

2. Enmarcar con inteligencia de amenazas

- ☐ La inteligencia actual sobre los actores que tienen como objetivo la mensajería financiera informa los escenarios de la prueba.
- ☐ Los escenarios ensayan rutas de intrusión plausibles y nombradas en lugar de clases genéricas de vulnerabilidades.
- ☐ La base de inteligencia está documentada, de modo que la prueba califique como dirigida por amenazas bajo DORA y OSFI B-13.

3. Ejecutar conforme al estándar más exigente

- ☐ La prueba se ejecuta tanto desde dentro como desde fuera de los límites de los sistemas, cumpliendo la expectativa de NYDFS Part 500.
- ☐ La prueba la realiza una parte competente y suficientemente independiente.
- ☐ Las reglas de enfrentamiento, la autorización y los controles de seguridad para probar sistemas en producción están documentados y aprobados.
- ☐ Se establece y registra una cadencia definida, satisfaciendo a la vez el mínimo anual de NYDFS y el ciclo de SWIFT.

4. Medir sus propias defensas

- ☐ El ejercicio mide si la supervisión detectó la intrusión simulada, no solo lo que se encontró.
- ☐ El rendimiento de respuesta y contención se registra frente a las funciones de Detectar y Responder.
- ☐ Las brechas de detección se registran como hallazgos por derecho propio.

5. Cerrar el ciclo y consignar la evidencia

- ☐ Los hallazgos entran en un ciclo de remediación con seguimiento, con responsables y fechas.
- ☐ El cierre de la remediación se evidencia, no solo se afirma.
- ☐ El registro completo (alcance, escenarios, narrativa de ataque, hallazgos, remediación, rendimiento de detección) se archiva una sola vez sobre la columna vertebral del NIST Cybersecurity Framework 2.0.
- ☐ El registro único se etiqueta para cada régimen: SWIFT 7.3A, DORA, NYDFS Part 500, OSFI B-13.