SWIFT CSCF v2026 / Control 7.3A

Probar una vez, satisfacer a muchos: la prueba de penetración SWIFT CSCF v2026 7.3A como ejercicio transversal a los regímenes

Cambridge Cyber International / 2026

Desde el ciclo 2026 del SWIFT Customer Security Programme, el Control 7.3A (Penetration Testing) lleva consigo una guía elaborada por la comunidad que fija el alcance y los escenarios de prueba que se esperan de una institución conectada a lo largo de un ciclo trienal continuo (SWIFT 2025). Leído de forma aislada, es una línea de atestación más que satisfacer. Leído frente al panorama regulatorio más amplio, es la prueba de una única dirección de marcha: los supervisores de la Unión Europea, los Estados Unidos y Canadá están convergiendo hacia pruebas guiadas por la inteligencia e informadas por las amenazas como la manera en que una institución demuestra que sus controles funcionan en lugar de limitarse a existir. Este artículo sostiene que una institución que se prepara para la prueba de penetración 7.3A debería diseñar esa prueba una sola vez, según un estándar de vanguardia, y cosechar la misma evidencia frente al Digital Operational Resilience Act (DORA), la segunda directiva sobre seguridad de las redes y de la información (NIS2), la regulación de ciberseguridad del New York State Department of Financial Services (23 NYCRR Part 500) y la Guideline B-13 del Office of the Superintendent of Financial Institutions, usando el Cybersecurity Framework versión 2.0 del National Institute of Standards and Technology de los Estados Unidos (NIST CSF 2.0) como columna vertebral común.

El problema de una lectura del 7.3A como casilla que marcar

Una institución conectada que trata cada régimen como una obligación separada paga una penalización estructural. Define el alcance de una prueba de penetración SWIFT de forma estrecha a la zona segura, encarga una prueba de resiliencia DORA por separado, responde a un cuestionario de NYDFS sobre pruebas anuales y prepara evidencia para un supervisor canadiense según un cuarto calendario. Cada encargo repite el mismo reconocimiento, las mismas reglas de enfrentamiento, el mismo ciclo de remediación, y cada uno produce evidencia en una forma que el régimen siguiente no acepta. El coste no es solo económico. Las pruebas fragmentadas producen una imagen fragmentada del riesgo, porque ningún ejercicio aislado ve a la institución como la vería un verdadero adversario: de extremo a extremo, a través del back office, las estaciones de trabajo de los operadores, la interfaz de mensajería y la conexión a la red.

El argumento aquí es que la convergencia ahora visible entre los principales regímenes vuelve obsoleto el enfoque fragmentado. La guía 7.3A, el régimen de pruebas guiadas por las amenazas de DORA, la expectativa guiada por la inteligencia de OSFI y el mandato anual de NYDFS no son cuatro pruebas distintas. Son cuatro expresiones de supervisión de una única idea, y una institución que diseña según la más exigente de ellas, y registra el resultado frente a un marco compartido, puede satisfacer las demás como subproducto.

Qué espera ahora el Control 7.3A de SWIFT CSCF v2026

El Control 7.3A se sitúa en el Customer Security Controls Framework como un control consultivo cuyo objetivo es validar la resiliencia operativa de la infraestructura relacionada con SWIFT del usuario, identificando las vulnerabilidades que podrían conducir a un compromiso de la zona segura o del back office (SWIFT 2025). La sustancia del cambio de 2026 no es un nuevo número de control, sino una guía más nítida sobre cómo debe definirse el alcance de la prueba y qué escenarios debe cubrir. El marco ahora articula un conjunto de escenarios de prueba que deben ejercitarse a lo largo de un ciclo trienal, de modo que una institución no pueda satisfacer el control con un único escaneo externo estrecho repetido anualmente. La expectativa es que, a lo largo del ciclo, el programa cubra las pruebas a nivel de aplicación de la interfaz de mensajería y los componentes relacionados, las pruebas de infraestructura de la zona segura y su segmentación, y las rutas humanas y de las estaciones de trabajo de los operadores que las intrusiones reales explotan.

De ello se siguen dos consecuencias de diseño. Primera, el alcance debe definirse frente a la zona segura y sus fronteras de confianza en lugar de frente a un rango de red conveniente, porque el propósito del control es demostrar que un atacante no puede pivotar desde el back office hacia la capa de mensajería. Segunda, la prueba debe ser realizada por una parte competente y suficientemente independiente, y sus hallazgos deben alimentar un ciclo de remediación rastreado cuyo cierre es en sí mismo evidencia. El control es consultivo en lugar de obligatorio para cada tipo de arquitectura, pero para las instituciones que se autoatestan frente a él, el evaluador esperará ver alcance, método, hallazgos y remediación como un registro coherente, no como un certificado.

Los cuatro regímenes vecinos

DORA y las pruebas de penetración guiadas por las amenazas

El Digital Operational Resilience Act exige a todas las entidades financieras dentro de su ámbito probar regularmente sus sistemas de tecnología de la información y la comunicación, y exige al subconjunto de entidades significativas realizar pruebas avanzadas por medio del threat-led penetration testing (TLPT) al menos cada tres años (European Parliament and Council 2022a). El TLPT está guiado por la inteligencia: una simulación controlada de red team contra sistemas de producción en vivo, modelada sobre las tácticas, técnicas y procedimientos de verdaderos actores de amenazas, realizada según una metodología para la cual el marco TIBER-EU es la referencia europea (European Central Bank 2018). La institución que prepara una prueba 7.3A según un estándar guiado por las amenazas, con inteligencia de amenazas actual dando forma a sus escenarios, ya está construyendo la columna vertebral de una prueba DORA, diferenciándose principalmente en el alcance formal y en la gobernanza de supervisión que envuelve a un TLPT designado.

NIS2 y la excepción de tipo lex specialis

La segunda directiva sobre seguridad de las redes y de la información eleva el nivel de base para la gestión del riesgo de ciberseguridad y la notificación de incidentes entre las entidades esenciales e importantes, y las autoridades nacionales pasaron de la transposición a la supervisión activa a lo largo de 2026 (European Parliament and Council 2022b; European Commission 2025). Para las entidades financieras el punto práctico es de precedencia: DORA es lex specialis, y el artículo 4 de la NIS2 le cede el paso allí donde las reglas del sector financiero sean al menos equivalentes. Por tanto, una institución debería tratar DORA como el régimen operativo de pruebas de resiliencia, reconociendo a la vez que las entidades del grupo fuera del perímetro financiero, como una filial tecnológica compartida, pueden permanecer dentro de la NIS2 y beneficiarse de la misma evidencia de pruebas.

Estados Unidos: NYDFS Part 500 y expectativas FFIEC

La regulación de ciberseguridad del New York State Department of Financial Services exige a cada entidad cubierta realizar pruebas de penetración de sus sistemas de información al menos anualmente, tanto desde dentro como desde fuera de las fronteras de los sistemas, sobre la base de la evaluación de riesgo de la entidad (New York State Department of Financial Services 2023). La regulación enmendada ha endurecido aún más las expectativas en materia de gobernanza y de pruebas (Ropes and Gray 2026). A nivel federal, el Federal Financial Institutions Examination Council no impone una regla fija, pero trata las pruebas de penetración por partes cualificadas e independientes como una expectativa del examinador y un indicador de madurez dentro de su Information Security booklet (Federal Financial Institutions Examination Council 2016). La institución que satisface el 7.3A según un estándar elevado, probando tanto desde dentro como desde fuera de la frontera con una cadencia definida, produce

exactamente los artefactos que un examinador de NYDFS y un examen FFIEC esperan.

Canadá: OSFI Guideline B-13

La Guideline B-13 del Office of the Superintendent of Financial Institutions, en vigor desde el 1 de enero de 2024, exige a las instituciones financieras reguladas a nivel federal identificar las vulnerabilidades mediante pruebas regulares, y para las instituciones con huellas tecnológicas significativas espera pruebas de penetración guiadas por la inteligencia y por las amenazas y ejercicios de red team que simulen ataques realistas de múltiples fases (Office of the Superintendent of Financial Institutions 2022). La B-13 está basada en resultados y no fija ninguna cadencia prestablecida, de modo que la institución evidencia el cumplimiento a través de la calidad y el realismo de sus pruebas en lugar de su frecuencia. Es el mismo estándar guiado por la inteligencia que DORA y la guía afinada del 7.3A expresan, lo que convierte a la B-13 en el miembro canadiense de la misma familia en lugar de una obligación separada.

Una columna vertebral: mapear los regímenes sobre NIST CSF 2.0

Ningún regulador financiero único gobierna tanto los Estados Unidos como Canadá, de modo que una institución transfronteriza necesita una referencia neutral reconocida en ambos. El NIST Cybersecurity Framework versión 2.0 es esa referencia: voluntario, ampliamente adoptado a ambos lados de la frontera y organizado en torno a seis funciones, Govern, Identify, Protect, Detect, Respond y Recover (National Institute of Standards and Technology 2024). Usado como columna vertebral, permite a una institución registrar un solo programa de prueba de penetración y expresar el resultado en el vocabulario que cada régimen comprende. La prueba de penetración habla de forma más directa a Identify, al hacer aflorar las vulnerabilidades, y a Detect y Respond, al medir si la supervisión y la respuesta de la institución realmente captan y contienen una intrusión realista. La función Govern lleva las reglas de enfrentamiento, la independencia y el reporte al consejo que los cinco regímenes exigen. La Tabla 1 vuelve concreta la convergencia.

Tabla 1. Un programa de prueba de penetración, cuatro regímenes, una columna vertebral

Dimensión	SWIFT 7.3A	DORA TLPT	NYDFS Part 500	OSFI B-13	NIST CSF 2.0
Naturaleza	Control consultivo	Obligatorio para entidades	Regla obligatoria	Expectativa basada en	Referencia voluntaria
Cadencia	Ciclo de escenarios trienal	Al menos cada 3 años	Al menos anual	Sin cadencia fija	No prescrita
Método	Basado en escenarios, foco en la zona segura	Red team guiado por la inteligencia	Interior y exterior, basado en el riesgo	Guiado por la inteligencia, red team	Funciones y resultados
Independencia	Parte competente e independiente	Proveedores acreditados	Interno o externo cualificado	Aseguramiento independiente	Resultado de gobernanza
Evidencia principal	Alcance, hallazgos, remediación	Escenarios de amenaza, narrativa del ataque, remediación	Informe de prueba, cadencia de remediación	Realismo y resultado de la prueba	Resultados mapeados

La lectura a lo largo de cada fila es la tesis: diseña la prueba según el estándar más exigente en cada columna, método guiado por la inteligencia, alcance consciente de la zona segura, cobertura interior y exterior, ejecución independiente, remediación rastreada, y el único registro resultante satisface a los cinco.

Un modelo de preparación guiado por el riesgo

La guía 7.3A invita a una lectura de cumplimiento, en la que la institución hace el mínimo que el control nombra. La lectura más valiosa, y la que los supervisores recompensan cada vez más, está guiada por el riesgo: la prueba de penetración es el instrumento usado para hacer aflorar y retirar las exposiciones más consecuentes de la institución, y el cumplimiento es el subproducto de hacerlo bien.

La preparación comienza con una línea de base de riesgo y alcance. La institución inventaría su patrimonio relacionado con SWIFT, la zona segura, la interfaz de mensajería, las estaciones de trabajo de los operadores, la conexión a la red y los sistemas de back office que la alimentan, y clasifica las rutas según la consecuencia de un compromiso en lugar de según la facilidad de probarlas. Esto produce un alcance definido por dónde residen el dinero y la confianza, que es también el alcance que un verdadero adversario elegiría, y que se alinea con la postura guiada por las consecuencias de la B-13 y la postura basada en el riesgo de NYDFS.

A continuación viene el encuadre de inteligencia de amenazas. La inteligencia actual sobre los actores que apuntan a la mensajería financiera da forma a los escenarios, de modo que la prueba ensaya intrusiones plausibles en lugar de genéricas. Este es el paso que convierte una prueba de penetración en una prueba guiada por las amenazas, y es el paso que vuelve creíble el mismo ejercicio bajo DORA y B-13.

La ejecución luego despliega los escenarios a lo largo del ciclo trienal que la guía 7.3A describe, cubriendo las rutas de aplicación, infraestructura y humanas, desde dentro y desde fuera de la frontera, por una parte independiente, según reglas de enfrentamiento documentadas. La institución mide no solo lo que se encontró sino si su propia detección y respuesta vieron suceder la prueba, porque esa medición es la evidencia que las funciones Detect y Respond exigen.

Por último, la remediación y la evidencia cierran el círculo. Los hallazgos entran en un ciclo de remediación rastreado cuyo cierre se registra, y el registro completo, alcance, escenarios, narrativa del ataque, hallazgos, remediación y rendimiento de detección, se archiva una sola vez frente a la columna vertebral NIST CSF 2.0 y se etiqueta para cada régimen. La institución que completa este círculo no ha aprobado una prueba. Ha construido un reutilizable activo probatorio de resiliencia.

Nuestro servicio de evaluación SWIFT CSP define el alcance y ejecuta la prueba 7.3A según este estándar, y PenTeva valida y rastrea los hallazgos hasta su cierre, de modo que la evidencia se sostenga bajo cualquiera de los cuatro regímenes. Allí donde el modelado de resiliencia DORA esté dentro del ámbito, DORA-MAST lleva la misma evidencia al cuadro de la resiliencia operativa.

Conclusión

La guía afinada del 7.3A se comprende mejor no como un requisito SWIFT aislado, sino como una única expresión de supervisión de un movimiento global hacia las pruebas guiadas por la inteligencia e informadas por las amenazas. Una institución que diseña su prueba de penetración 2026 según ese estándar, define su alcance según la consecuencia, la enmarca con inteligencia de amenazas actual, la ejecuta de forma independiente a través de la zona segura y registra el resultado frente a un marco compartido, puede satisfacer DORA, la NIS2 donde aún se aplica, NYDFS Part 500 y OSFI B-13 a partir del mismo ejercicio. El pen test deja de ser un coste de cumplimiento recurrente y se convierte en el instrumento a través del cual la institución encuentra y retira los riesgos que importan. Prueba una vez, satisface a muchos.

Acrónimos

CSCF, Customer Security Controls Framework (SWIFT). CSP, Customer Security Programme (SWIFT). DORA, Digital Operational Resilience Act. FFIEC, Federal Financial Institutions Examination Council. ICT, Information and Communication Technology. NIS2, Network and Information Security Directive (second). NIST CSF, National Institute of Standards and Technology Cybersecurity Framework. NYDFS, New York State Department of Financial Services. OSFI, Office of the Superintendent of Financial Institutions. SWIFT, Society for Worldwide Interbank Financial Telecommunication. TIBER-EU, Threat Intelligence-Based Ethical Red Teaming (European framework). TLPT, Threat-Led Penetration Testing.

References

European Central Bank (2018). TIBER-EU Framework. https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

European Commission (2025). NIS2 Directive: transposition in EU countries. https://digital-strategy.ec.europa.eu/en/policies/nis-transposition

European Parliament and Council (2022a). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). https://eur-lex.europa.eu/eli/reg/2022/2554/oj

European Parliament and Council (2022b). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2). https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Federal Financial Institutions Examination Council (2016). Information Technology Examination Handbook: Information Security. https://ithandbook.ffiec.gov/it-booklets/information-security/

National Institute of Standards and Technology (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

New York State Department of Financial Services (2023). Cybersecurity Requirements for Financial Services Companies, 23 NYCRR Part 500 (as amended). https://www.dfs.ny.gov/system/files/documents/2023/03/23NYCRR500_0.pdf

Office of the Superintendent of Financial Institutions (2022). Guideline B-13: Technology and Cyber Risk Management. https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/technology-cyber-risk-management

Ropes and Gray (2026). NYDFS-regulated entities face stronger cybersecurity regulations. https://www.ropesgray.com/en/insights/alerts/2026/01/nydfs-regulated-entities-face-stronger-cybersecurity-regulations

SWIFT (2025). Customer Security Controls Framework v2026, Customer Security Programme. https://www.swift.com/myswift/customer-security-programme-csp