SWIFT CSCF v2026 / Control 7.3A

Testar uma vez, satisfazer muitos: o teste de intrusao do SWIFT CSCF v2026 Controlo 7.3A como exercicio multi-regime

Cambridge Cyber International / 2026

Do ciclo de 2026 do SWIFT Customer Security Programme, o Controlo 7.3A (Teste de Intrusao) traz orientacao impulsionada pela comunidade que fixa o ambito e os cenarios de teste esperados de uma instituicao conectada ao longo de um ciclo continuo de tres anos (SWIFT 2025). Lido isoladamente, isto e mais uma linha de atestacao a satisfazer. Lido face ao panorama regulatorio mais amplo, e prova de uma unica direcao de marcha: os supervisores na Uniao Europeia, nos Estados Unidos e no Canada estao a convergir para o teste guiado por inteligencia e informado por ameacas como a forma de uma instituicao provar que os seus controlos funcionam, em vez de meramente existirem. Este artigo defende que uma instituicao que se prepara para o teste de intrusao 7.3A deve conceber esse teste uma so vez, segundo um padrao de excelencia, e colher a mesma prova face ao Regulamento sobre a Resiliencia Operacional Digital (DORA), a segunda Diretiva relativa a Seguranca das Redes e da Informacao (NIS2), o regulamento de cibersseguranca do New York State Department of Financial Services (23 NYCRR Parte 500) e a Diretriz B-13 do Office of the Superintendent of Financial Institutions, usando a versao 2.0 do Cybersecurity Framework do National Institute of Standards and Technology dos Estados Unidos (NIST CSF 2.0) como espinha comum.

O problema de uma leitura do 7.3A como caixa a assinalar

Uma instituicao conectada que trata cada regime como uma obrigacao separada paga uma penalizacao estrutural. Define o ambito de um teste de intrusao SWIFT estreitamente para a zona segura, encomenda um teste de resiliencia DORA separado, responde a um questionario do NYDFS sobre teste anual e prepara prova para um supervisor canadiano num quarto calendario. Cada compromisso repete o mesmo reconhecimento, as mesmas regras de envolvimento, o mesmo ciclo de remediacao, e cada um produz prova numa forma que o regime seguinte nao aceita. O custo nao e so dinheiro. O teste fragmentado produz uma imagem fragmentada do risco, porque nenhum exercicio singular ve a instituicao como um adversario real veria: de ponta a ponta, atravessando o back office, as estacoes de trabalho dos operadores, a interface de mensagens e a ligacao a rede.

O argumento aqui e que a convergencia agora visivel entre os principais regimes torna obsoleta a abordagem fragmentada. A orientacao 7.3A, o regime de teste guiado por ameacas da DORA, a expectativa guiada por inteligencia da OSFI e o mandato anual do NYDFS nao sao quatro testes diferentes. Sao quatro expressoes supervisoras de uma so ideia, e uma instituicao que conceba para a mais exigente delas, e registe o resultado contra um quadro partilhado, pode satisfazer as restantes como subproduto.

O que o Controlo 7.3A do SWIFT CSCF v2026 agora espera

O Controlo 7.3A situa-se no Customer Security Controls Framework como um controlo de aconselhamento cujo objetivo e validar a resiliencia operacional da infraestrutura relacionada com SWIFT do utilizador, identificando vulnerabilidades que poderiam levar ao comprometimento da zona segura ou do back office (SWIFT 2025). A substancia da mudanca de 2026 nao e um novo numero de controlo, mas orientacao mais nitida sobre como o teste deve ser definido no ambito e que cenarios deve cobrir. O quadro articula agora um conjunto de cenarios de teste a exercer ao longo de um ciclo de tres anos, de modo a que uma instituicao nao possa satisfazer o controlo com uma unica varredura externa estreita repetida anualmente. A expectativa e que, ao longo do ciclo, o programa cubra o teste ao nivel da aplicacao da interface de mensagens e dos componentes relacionados, o teste da infraestrutura da zona segura e da sua segmentacao, e os caminhos humanos e das estacoes de trabalho dos operadores que as intrusoes reais exploram.

Seguem-se duas consequencias de conceao. Primeiro, o ambito tem de ser definido face a zona segura e aos seus limites de confianca, e nao face a um intervalo de rede conveniente, porque o proposito do controlo e provar que um atacante nao pode pivotar do back office para a camada de mensagens. Segundo, o teste tem de ser conduzido por uma parte competente e suficientemente independente, e as suas conclusoes tem de alimentar um ciclo de remediacao rastreado cujo encerramento e ele proprio prova. O controlo e de aconselhamento e nao obrigatorio para todos os tipos de arquitetura, mas para as instituicoes que se autoatestam face a ele, o avaliador esperara ver ambito, metodo, conclusoes e remediacao como um registo coerente, e nao um certificado.

Os quatro regimes vizinhos

A DORA e o teste de intrusao guiado por ameacas

O Regulamento sobre a Resiliencia Operacional Digital exige que todas as entidades financeiras abrangidas testem regularmente os seus sistemas de tecnologias de informacao e comunicacao, e exige que o subconjunto de entidades significativas realize teste avancado por meio de teste de intrusao guiado por ameacas (TLPT) pelo menos de tres em tres anos (European Parliament and Council 2022a). O TLPT e guiado por inteligencia: uma simulacao controlada de equipa vermelha contra sistemas de producao em funcionamento, modelada nas taticas, tecnicas e procedimentos de agentes de ameaca reais, conduzida sob uma metodologia para a qual o quadro TIBER-EU e a referencia europeia (European Central Bank 2018). A instituicao que prepara um teste 7.3A segundo um padrao guiado por ameacas, com inteligencia de ameacas atual a moldar os seus cenarios, ja esta a construir a espinha de um teste DORA, diferindo sobretudo no ambito formal e na governanca supervisora que envolve um TLPT designado.

A NIS2 e a excecao lex specialis

A segunda Diretiva relativa a Seguranca das Redes e da Informacao eleva a base da gestao do risco de ciberssegurança e da comunicacao de incidentes entre entidades essenciais e importantes, e as autoridades nacionais passaram da transposicao para a supervisao ativa durante 2026 (European Parliament and Council 2022b; European Commission 2025). Para as entidades financeiras, o ponto pratico e de precedencia: a DORA e lex specialis, e o artigo 4.o da NIS2 cede-lhe lugar onde as regras do setor financeiro sao pelo menos equivalentes. Uma instituicao deve, portanto, tratar a DORA como o regime operativo de teste de resiliencia, reconhecendo ao mesmo tempo que entidades do grupo fora do perimetro financeiro, como uma subsidiaria tecnologica partilhada, podem permanecer dentro da NIS2 e beneficiar da mesma prova de teste.

Os Estados Unidos: a Parte 500 do NYDFS e as expectativas do FFIEC

O regulamento de ciberssegurança do New York State Department of Financial Services exige que cada entidade abrangida realize teste de intrusao dos seus sistemas de informacao pelo menos anualmente, tanto a partir do interior como do exterior dos limites dos sistemas, com base na avaliacao de risco da entidade (New York State Department of Financial Services 2023). O regulamento alterado apertou ainda mais as expectativas de governanca e de teste (Ropes and Gray 2026). Ao nivel federal, o Federal Financial Institutions Examination Council nao impoe uma regra fixa, mas trata o teste de intrusao por partes qualificadas e independentes como uma expectativa do examinador e um indicador de maturidade no seu manual de Information Security (Federal Financial Institutions Examination Council 2016). A instituicao que satisfaca o 7.3A segundo um padrao elevado, testando tanto a partir do interior como do exterior do limite numa cadencia definida, produz exatamente os artefactos que um

examinador do NYDFS e um exame do FFIEC esperam.

O Canada: a Diretriz B-13 da OSFI

A Diretriz B-13 do Office of the Superintendent of Financial Institutions, em vigor desde 1 de janeiro de 2024, exige que as instituicoes financeiras reguladas a nivel federal identifiquem vulnerabilidades atraves de teste regular, e para instituicoes com pegadas tecnologicas significativas espera teste de intrusao guiado por inteligencia e por ameacas e exercicios de equipa vermelha que simulem ataques realistas de multiplas fases (Office of the Superintendent of Financial Institutions 2022). A B-13 e baseada em resultados e nao fixa cadencia, pelo que a instituicao evidencia conformidade atraves da qualidade e do realismo do seu teste, e nao da sua frequencia. Este e o mesmo padrao guiado por inteligencia que a DORA e a orientacao afinada do 7.3A exprimem, o que faz da B-13 o membro canadiano da mesma familia, e nao uma obrigacao separada.

Uma espinha: mapear os regimes no NIST CSF 2.0

Nenhum regulador financeiro singular governa tanto os Estados Unidos como o Canada, pelo que uma instituicao transfronteirica precisa de uma referencia neutra reconhecida em ambos. A versao 2.0 do Cybersecurity Framework do NIST e essa referencia: voluntaria, amplamente adotada de ambos os lados da fronteira, e organizada em torno de seis funcoes, Governar, Identificar, Proteger, Detetar, Responder e Recuperar (National Institute of Standards and Technology 2024). Usada como espinha, permite a uma instituicao registar um programa de teste de intrusao e exprimir o resultado no vocabulario que cada regime compreende. O teste de intrusao fala mais diretamente a Identificar, ao revelar vulnerabilidades, e a Detetar e Responder, ao medir se a monitorizacao e a resposta da instituicao apanham e contem efetivamente uma intrusao realista. A funcao Governar carrega as regras de envolvimento, a independencia e a comunicacao ao conselho que os cinco regimes exigem. A Tabela 1 torna a convergencia concreta.

Tabela 1. Um programa de teste de intrusao, quatro regimes, uma espinha

Dimensao	SWIFT 7.3A	DORA TLPT	NYDFS Parte 500	OSFI B-13	NIST CSF 2.0
Natureza	Controlo de aconselhamento	Obrigatorio para entidades	Regra obrigatoria	Expectativa baseada em	Referencia voluntaria
Cadencia	Ciclo de cenarios de 3 anos	Pelo menos de 3 em 3 anos	Pelo menos anual	Sem cadencia fixa	Nao prescrita
Metodo	Baseado em cenarios, foco na zona segura	Equipa vermelha guiada por inteligencia	Interior e exterior, baseado no risco	Guiado por inteligencia, equipa vermelha	Funcoes e resultados
Independencia	Parte competente e independente	Fornecedores acreditados	Interno ou externo qualificado	Garantia independente	Resultado de governanca
Prova primaria	Ambito, conclusoes, remediacao	Cenarios de ameaca, narrativa de ataque, remediacao	Relatorio de teste, cadencia de remediacao	Realismo e resultado do teste	Resultados mapeados

A leitura ao longo de cada linha e a tese: conceba o teste segundo o padrao mais exigente em cada coluna, metodo guiado por inteligencia, ambito ciente da zona segura, cobertura de interior e exterior, execucao independente, remediacao rastreada, e o registo singular resultante satisfaz os cinco.

Um modelo de preparacao guiado pelo risco

A orientacao 7.3A convida a uma leitura de conformidade, em que a instituicao faz o minimo que o

controlo nomeia. A leitura mais valiosa, e aquela que os supervisores recompensam cada vez mais, e guiada pelo risco: o teste de intrusao e o instrumento usado para revelar e retirar as exposicoes mais consequentes da instituicao, e a conformidade e o subproduto de fazer isso bem.

A preparacao comeca com uma base de risco e ambito. A instituicao inventaria o seu patrimonio relacionado com SWIFT, a zona segura, a interface de mensagens, as estacoes de trabalho dos operadores, a ligacao a rede e os sistemas de back office que a alimentam, e classifica os caminhos pela consequencia do comprometimento, e nao pela facilidade do teste. Isto produz um ambito definido por onde estao o dinheiro e a confianca, que e tambem o ambito que um adversario real escolheria, e que se alinha com a postura guiada pela consequencia da B-13 e com a postura baseada no risco do NYDFS.

Segue-se o enquadramento por inteligencia de ameacas. A inteligencia atual sobre os agentes que visam as mensagens financeiras molda os cenarios, de modo a que o teste ensaie intrusoes plausiveis em vez de genericas. Este e o passo que transforma um teste de intrusao num teste guiado por ameacas, e e o passo que torna o mesmo exercicio credivel ao abrigo da DORA e da B-13.

A execucao corre depois os cenarios ao longo do ciclo de tres anos que a orientacao 7.3A descreve, cobrindo caminhos de aplicacao, de infraestrutura e humanos, a partir do interior e do exterior do limite, por uma parte independente, sob regras de envolvimento documentadas. A instituicao mede nao so o que foi encontrado, mas se a sua propria detecao e resposta viram o teste acontecer, porque essa medicao e a prova que as funcoes Detetar e Responder exigem.

Por fim, a remediacao e a prova fecham o ciclo. As conclusoes entram num ciclo de remediacao rastreado cujo encerramento e registado, e todo o registo, ambito, cenarios, narrativa de ataque, conclusoes, remediacao e desempenho de detecao, e arquivado uma so vez contra a espinha NIST CSF 2.0 e marcado para cada regime. A instituicao que completa este ciclo nao passou um teste. Construiu um ativo de prova de resiliencia reutilizavel.

O nosso servico de avaliacao SWIFT CSP define o ambito e corre o teste 7.3A segundo este padrao, e a PenTeva valida e rastreia as conclusoes ate ao encerramento, para que a prova resista sob qualquer dos quatro regimes. Quando a modelacao de resiliencia DORA esta no ambito, a DORA-MAST leva a mesma prova para a imagem da resiliencia operacional.

Conclusao

A orientacao afinada do 7.3A entende-se melhor nao como um requisito SWIFT isolado, mas como uma expressao supervisora de um movimento global rumo ao teste guiado por inteligencia e informado por ameacas. Uma instituicao que conceba o seu teste de intrusao de 2026 segundo esse padrao, o defina no ambito pela consequencia, o enquadre com inteligencia de ameacas atual, o execute de forma independente atravessando a zona segura e registe o resultado contra um quadro partilhado, pode satisfazer a DORA, a NIS2 onde ainda se aplica, a Parte 500 do NYDFS e a OSFI B-13 a partir do mesmo exercicio. O teste de intrusao deixa de ser um custo recorrente de conformidade e torna-se o instrumento atraves do qual a instituicao encontra e retira os riscos que importam. Testar uma vez, satisfazer muitos.

Acronimos

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

(segunda). 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 (quadro europeu). TLPT, Threat-Led Penetration Testing.

Referencias

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