SWIFT CSCF v2026 · Control 7.3A

# Lista de verificação de preparação para o teste de penetração do Controlo 7.3A do SWIFT CSCF v2026

## 1. Definir o âmbito por consequência

- ☐ O ambiente SWIFT está inventariado: zona segura, interface de mensagens, estações de trabalho dos operadores, a ligação à rede e os sistemas de back-office que a alimentam.
- ☐ As vias de ataque são classificadas pela consequência de um comprometimento, não pela facilidade de teste.
- ☐ O âmbito é definido em relação à zona segura e aos seus limites de confiança, de modo que o teste prove que um atacante não pode pivotar do back-office para a camada de mensagens.
- ☐ O teste está planeado ao longo do ciclo de cenários de três anos, cobrindo vias de aplicação, infraestrutura e humanas.

## 2. Enquadrar com inteligência de ameaças

- ☐ A inteligência atual sobre os atores que visam as mensagens financeiras informa os cenários do teste.
- ☐ Os cenários ensaiam vias de intrusão plausíveis e nomeadas, em vez de classes genéricas de vulnerabilidades.
- ☐ A base de inteligência está documentada, de modo que o teste se qualifique como dirigido por ameaças ao abrigo do DORA e do OSFI B-13.

## 3. Executar conforme o padrão mais exigente

- ☐ O teste é executado tanto a partir de dentro como de fora dos limites dos sistemas, cumprindo a expectativa do NYDFS Part 500.
- ☐ O teste é realizado por uma parte competente e suficientemente independente.
- ☐ As regras de envolvimento, a autorização e os controlos de segurança para testar sistemas em produção estão documentados e aprovados.
- ☐ É estabelecida e registada uma cadência definida, satisfazendo em simultâneo o mínimo anual do NYDFS e o ciclo do SWIFT.

## 4. Medir as suas próprias defesas

- ☐ O exercício mede se a monitorização detetou a intrusão simulada, não apenas o que foi encontrado.
- ☐ O desempenho de resposta e contenção é registado face às funções de Detetar e Responder.
- ☐ As lacunas de deteção são registadas como constatações por direito próprio.

## 5. Fechar o ciclo e arquivar a evidência

- ☐ As constatações entram num ciclo de remediação com acompanhamento, com responsáveis e datas.
- ☐ O encerramento da remediação é evidenciado, não apenas afirmado.
- ☐ O registo completo (âmbito, cenários, narrativa de ataque, constatações, remediação, desempenho de deteção) é arquivado uma única vez sobre a espinha dorsal do NIST Cybersecurity Framework 2.0.
- ☐ O registo único é etiquetado para cada regime: SWIFT 7.3A, DORA, NYDFS Part 500, OSFI B-13.