

A man and a woman are in an office setting, looking at a computer monitor. The man is pointing at the screen, and the woman is looking at it with a focused expression. The background shows large windows with a city view.

SWIFT CUSTOMER SECURITY PROGRAMME (CSP)

CSCF v2026

REFORÇAR A SEGURANÇA DAS OPERAÇÕES FINANCEIRAS GLOBAIS

Conformidade, Resiliência Operacional e Confiança no Ecosistema SWIFT

ENQUADRAMENTO

O que é o SWIFT Customer Security Programme?

O SWIFT Customer Security Programme (CSP) constitui o principal framework de cibersegurança da SWIFT para proteção da comunidade financeira global.

Criado para reforçar a resiliência dos utilizadores da rede SWIFT face à crescente sofisticação das ameaças cibernéticas, o programa define um conjunto de controlos de segurança obrigatórios e recomendados, que devem ser implementados por todas as organizações que utilizam a rede SWIFT.

Mais do que uma obrigação de conformidade, o CSP promove:

- Redução do risco de fraude financeira;
- Proteção dos fluxos de pagamentos;
- Reforço da confiança entre contrapartes;
- Melhoria contínua da maturidade de cibersegurança;
- Alinhamento com normas internacionais e regulamentos como DORA, NIS2 e ISO 27001.

CUSTOMER SECURITY CONTROLS FRAMEWORK (CSCF)

Assente em 3 objetivos, 7 princípios de segurança e 32 controlos:

• Proteger o seu ambiente

- Restringir o acesso à Internet e segregar sistemas críticos do ambiente geral de TI
- Reduzir a superfície de ataque e vulnerabilidades
- Proteger fisicamente o ambiente

• Conhecer e limitar o acesso

- Evitar o comprometimento das credenciais
- Gerir identidades e segregar privilégios

• Detetar e responder

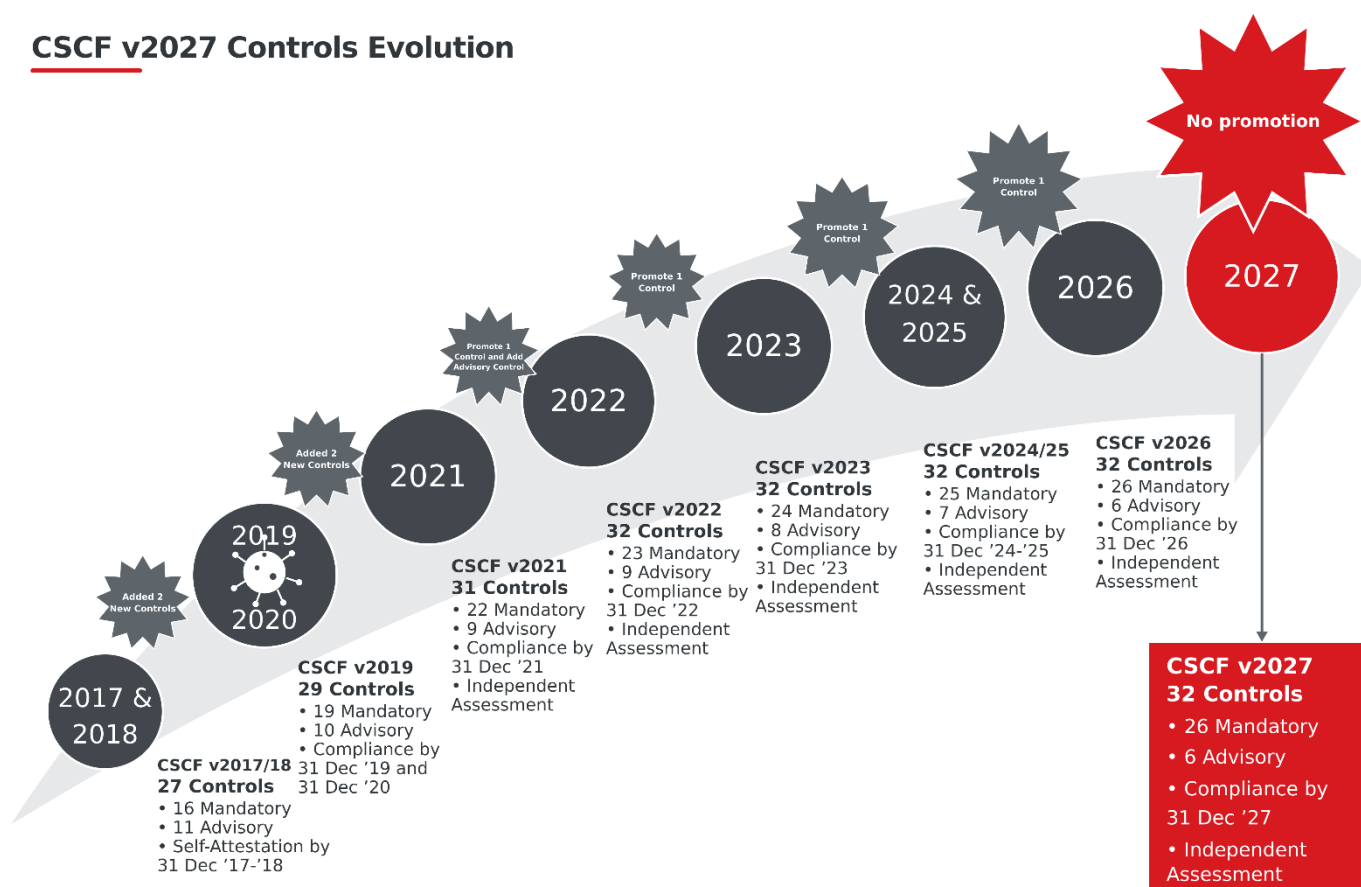
- Detetar atividade anómala em registos do sistema ou transações
- Planear a resposta a incidentes e a partilha de informação

Cada controlo é definido em conformidade com normas reconhecidas de segurança da informação, como ISO 27002, PCI DSS, SOC2 e NIST CSF.

Os controlos aplicáveis, obrigatórios e recomendáveis, variam conforme a solução de conectividade SWIFT implementada.

O QUE MUDA NO CSCF v2026?

CSCF v2027 Controls Evolution



© Swift

PRINCIPAIS ALTERAÇÕES

A versão 2026 do Customer Security Controls Framework (CSCF) introduz novos requisitos focados na proteção dos fluxos de dados de pagamentos e no reforço da segurança dos componentes que ligam os sistemas internos das organizações à infraestrutura SWIFT.

As alterações refletem a evolução das ameaças cibernéticas e a necessidade de proteger pontos tradicionalmente menos controlados dentro da cadeia de processamento de pagamentos.

DESTAQUES 2026

- Novo controlo obrigatório sobre os fluxos de dados entre sistemas SWIFT e Back Office
- Requisitos obrigatórios para Customer Client Connectors
- Maior foco na proteção contra ameaças potenciadas por Inteligência Artificial
- Preparação para a transição futura para criptografia pós-quântica



CONTROLO 2.4

Proteção dos Fluxos de Dados do Back Office

AGORA OBRIGATÓRIO

Uma das mudanças mais relevantes do CSCF 2026 é a obrigatoriedade da primeira fase do controlo 2.4 - Back Office Data Flow Security.

O objetivo é assegurar:

- Confidencialidade
- Integridade
- Autenticidade

dos dados trocados entre:

- Infraestrutura SWIFT
- Middleware
- Sistemas de Back Office

O que é esperado?

As organizações deverão garantir:

- Encriptação forte das comunicações;
- Proteção ponta a ponta ou por segmento;
- Monitorização dos fluxos de pagamentos;
- Inventário completo das ligações existentes;
- Avaliação contínua dos riscos associados aos canais de comunicação.

ROADMAP SWIFT

2026 Proteção obrigatória para novos fluxos de dados.

2028 (previsto) Extensão dos requisitos aos fluxos de dados existentes (legacy).

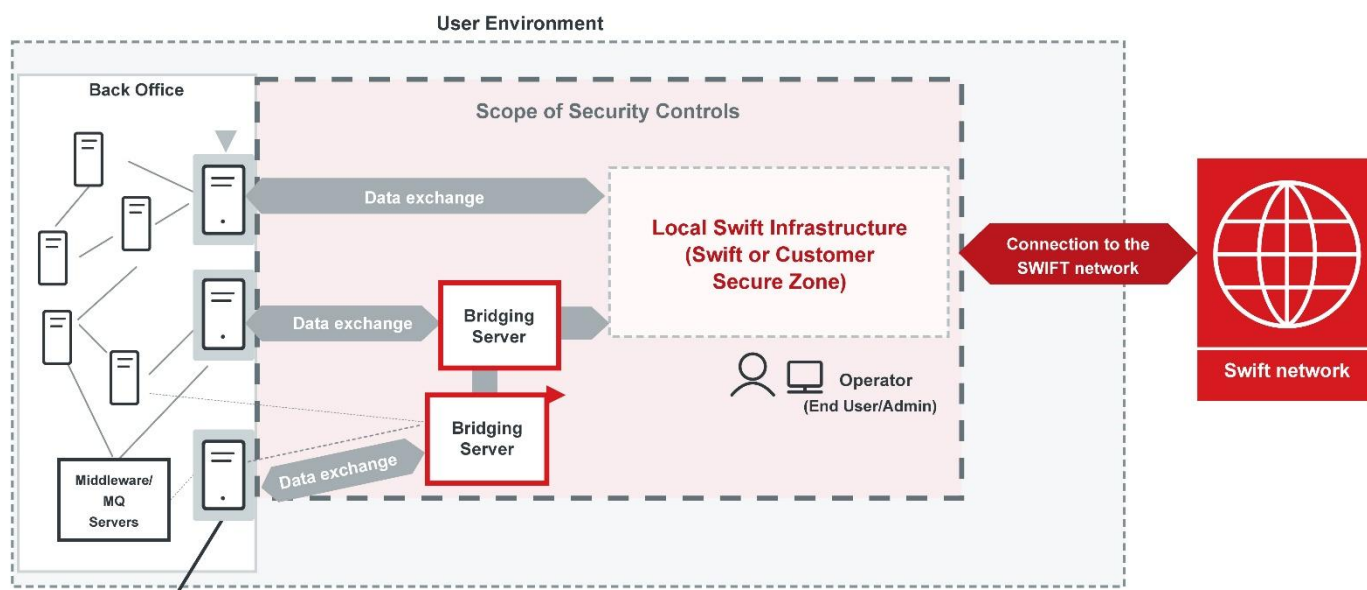


Diagrama que mostra as fases de implementação do controlo 2.4

CUSTOMER CLIENT CONNECTORS

DA RECOMENDAÇÃO À OBRIGATORIEDADE

As organizações que utilizam integração automática ou semi-automática de pagamentos, tipicamente enquadradas numa arquitetura Tipo A4, são agora obrigadas a atestar a conformidade do componente Customer Client Connector, nos controlos aplicáveis.

Um *Customer Client Connector* é um componente utilizado para estabelecer comunicações automatizadas entre sistemas internos e a infraestrutura SWIFT ou os respetivos componentes intermédios.

Exemplos frequentes incluem:

- Clientes IBM MQ;
- Clientes SFTP;
- APIs de integração;
- Ferramentas de transferência de ficheiros;
- Componentes de middleware utilizados nos processos de pagamento.

Caso não sejam adequadamente protegidos, podem tornar-se um vetor de ataque para:

- Interceção de mensagens financeiras;
- Manipulação de instruções de pagamento;
- Compromisso da integridade dos dados;
- Movimentação lateral para sistemas críticos.

Porque é que esta alteração é relevante?

- Os Customer Client Connectors representam frequentemente um dos pontos de ligação entre ambientes altamente controlados e sistemas corporativos de negócio.

Ao tornar estes componentes obrigatoriamente avaliáveis, a SWIFT reforça a proteção dos fluxos de pagamentos fora da zona tradicionalmente mais protegida da infraestrutura SWIFT.



AMEAÇAS EMERGENTES

INTELIGÊNCIA ARTIFICIAL (FRONTIER AI)

As organizações enfrentam um novo paradigma de risco.

Os modelos avançados de IA estão a aumentar:

- Velocidade dos ataques;
- Automatização de exploração de vulnerabilidades;
- Escala dos incidentes;
- Sofisticação dos ataques direcionados.

Embora a SWIFT não introduza controlos específicos para IA no CSCF 2026, reforça a necessidade de:

- Implementação rigorosa dos controlos existentes;
- Detecção precoce de incidentes;
- Resposta rápida;
- Gestão contínua de vulnerabilidades.

CRIOGRAFIA PÓS-QUÂNTICA (PQC)

A computação quântica representa uma transformação tecnológica capaz de comprometer algoritmos criptográficos atualmente considerados seguros.

RISCO PRINCIPAL

"Harvest Now, Decrypt Later"

Os atacantes podem:

1. Capturar dados hoje;
2. Armazená-los;
3. Desencriptá-los futuramente com recursos quânticos.

O QUE FAZER?

As organizações devem começar a:

- Inventariar ativos criptográficos;
- Avaliar dependências criptográficas;
- Desenvolver roadmaps de migração;
- Preparar iniciativas de crypto-agility.

A SWIFT pretende suportar a transição da comunidade financeira para padrões pós-quânticos até 2030.



O PROCESSO DE DECLARAÇÃO (*ATTESTATION*) SWIFT

O QUE DEVE SABER

Todos os utilizadores SWIFT devem proceder à submissão da declaração anual através da plataforma **KYC Security Attestation (KYC-SA)**.

CALENDÁRIO

1 Julho a 31 Dezembro

Período oficial para a declaração anual.

Mesmo em situação de não conformidade, a organização deve submeter a declaração.

PORQUE É IMPORTANTE?

A informação é partilhada:

- Com as contrapartes financeiras;
- Com a SWIFT;
- Com as autoridades de supervisão aplicáveis.

BENEFÍCIOS DA CONFORMIDADE CSP

Muito além da conformidade

Benefícios estratégicos

- Redução do risco operacional
- Prevenção de fraude financeira
- Reforço da confiança dos clientes
- Melhoria da maturidade de cibersegurança
- Alinhamento com DORA, NIS2 e ISO 27001
- Proteção dos processos críticos de pagamentos
- Demonstração de compromisso junto do mercado



PORQUÊ A BDO?

Especialização reconhecida pela SWIFT

- SWIFT CSP Certified Assessors integrados na equipa global BDO;
- Presença no diretório oficial de Certified Assessors da SWIFT;
- Center of Excellence Internacional dedicado ao SWIFT CSP;
- Experiência comprovada no setor financeiro e sistemas de pagamentos;
- Competências complementares em DORA, NIS2 e ISO 27001;
- Abordagem prática, focada na segurança e na conformidade.

Transformamos conformidade em valor

Mais do que apoiar a declaração anual, ajudamos as organizações a reforçar a sua resiliência operacional, reduzir riscos e aumentar a confiança no seu ecossistema de pagamentos.

ENTRE EM CONTACTO CONNOSCO



César Benú Soares

Manager | TRA

cesar.soares@bdo.pt

+351 937 990 127



Rute Miriam Neto

Manager | TRA | SWIFT

CSP Certified Assessor

rute.neto@bdo.pt

+351 932 301 733

A BDO & Associados, SROC, S.A., a BDO Consulting, Lda., a BDO Outsourcing, Serviços de Contabilidade e Organização, S.A., a BDO II ADVISORY, S.A., a BDO EnviEstudos, S.A. e a BDO, Domingues & Associado, SROC, Lda., sociedades registadas em Portugal, são membros da BDO International Limited, sociedade inglesa limitada por garantia, e fazem parte da rede internacional BDO de firmas independentes. BDO é a marca da rede internacional BDO e para cada uma das Firms Membro BDO.

www.bdo.pt

