CUANDO LA IA ATACA

SWIFT en la mira.

¿Cómo los controles del Customer Security Control Framework 2026 responden a las amenazas generadas por inteligencia artificial — y por qué la mayoría de las instituciones financieras aún no están preparadas?

06 DE JUNIO DE 2026

5 MINUTOS DE LECTURA

1185 PALABRAS

RESUMEN EJECUTIVO

La IA generativa ha transformado el panorama de amenazas cibernéticas en el sector financiero — de forma permanente.

Lo que antes requería equipos especializados de atacantes, hoy se ejecuta con herramientas de IA accesibles, baratas y muy efectivas.

Para las instituciones conectadas a la red SWIFT, esto no es una amenaza futura. Es una realidad operativa del presente y futuro.

ESTE ARTÍCULO DESTACA LOS VECTORES DE ATAQUE MÁS RELEVANTES Y LAS ACCIONES QUE LAS ORGANIZACIONES DEBEN PRIORIZAR.

La IA ha reescrito las reglas del *ataque cibernético.*

16%

de brechas de seguridad ya involucran ataques impulsados por IA.

IBM COST OF A DATA BREACH REPORT · 2025

97%

de organizaciones afectadas carecían de controles de acceso adecuados.

NIST ADVERSARIAL AI RESEARCH · 2025

80%

de grandes instituciones financieras fallaron su evaluación inicial del CSP en 2025.

DELOITTE CSP ASSESSMENTS · 2025

En las últimas décadas, la seguridad en los sistemas de mensajería financiera, incluyendo SWIFT, se construyó sobre un principio claro: el atacante necesita tiempo, recursos y conocimiento especializado. La inteligencia artificial generativa ha eliminado esas barreras de entrada de forma permanente.

En la actualidad, un atacante puede generar correos de phishing personalizados en segundos, automatizar el reconocimiento de infraestructura SWIFT y evadir los propios sistemas de detección mediante técnicas de manipulación a los modelos de seguridad.

Para el ecosistema SWIFT, los riesgos son especialmente graves. La red mueve billones de dólares diariamente; una ventana de compromiso de apenas minutos puede traducirse en pérdidas irreversibles.

El 80% de las grandes instituciones financieras evaluadas en 2025 fallaron su primera evaluación CSP, según artículo publicado por Deloitte en abril de 2026. Este dato no refleja únicamente brechas técnicas, sino que la velocidad a la que evolucionan las amenazas supera la cadencia de los ciclos de cumplimiento tradicionales.

VECTORES DE RIESGO CLAVE

Principales amenazas de IA para SWIFT.

> *“ El 97% de las organizaciones afectadas por ataques de IA carecían de controles de acceso adecuados para hacerle frente a este tipo de ataques. ”*

01

CRÍTICO

Phishing Hiperpersonalizado

La IA genera mensajes adaptados al perfil exacto del destinatario usando datos públicos y patrones internos filtrados. Los filtros de correo tradicionales no los detectan.

02

CRÍTICO

Deepfakes de Autorización

Simulación de voz y video de ejecutivos para eludir verificación de transferencias de alto valor. El CSCF 2026 lo aborda explícitamente en el Control 7.2.

03

ALTO

Evasión de Controles de IA

Técnicas adversariales que manipulan modelos de detección de fraude para clasificar ataques activos como transacciones legítimas. Ataques a la lógica de los sistemas.

04

ALTO

Automatización de Ataques

Agentes de IA realizan reconocimiento continuo de infraestructura SWIFT e intentos de intrusión a velocidades que superan cualquier respuesta humana.

RECOMENDACIONES

Lo que las organizaciones deben hacer ahora.

El CSCF 2026 provee el marco regulatorio, pero la respuesta ante amenazas de IA requiere decisiones más allá del área de tecnología.

1 Elevar gobernanza de IA a riesgo sistémico.

El Comité de Riesgos debe revisar periódicamente la exposición a ataques de IA sobre SWIFT. Sin un patrocinador directivo, los esfuerzos permanecen fragmentados.

CSCF 2026 · CONTROL 1.1 · GOBERNANZA

2 Implementar MFA resistente a ingeniería social por IA.

Los esquemas MFA tradicionales son vulnerables ante deepfakes y phishing de IA. Migrar a MFA basado en hardware (FIDO2) para accesos privilegiados es urgente.

CSCF 2026 · CONTROL 4.2 · AUTENTICACIÓN

3 Deepfakes en programas de entrenamiento.

Exigido en el Control 7.2. El personal debe desarrollar criterios de verificación ante instrucciones inusuales, independientemente de su apariencia de legitimidad.

CSCF 2026 · CONTROL 7.2 · CONCIENCIACIÓN

4 Evaluación de brechas antes del tercer trimestre.

La atestación abre el 1 de julio de 2026. El 80% falló en 2025. Actuar ahora evita el costo reputacional y el escrutinio regulatorio ante contrapartes.

CSCF 2026 · KYC-SA · ATESTACIÓN

5 Inventariar sistemas de IA en el entorno SWIFT.

Todo sistema de IA que interactúe con flujos SWIFT debe estar documentado y bajo gobierno explícito. Sin inventario, no hay superficie de ataque conocida.

CSCF 2026 · CONTROL 2.4 · FLUJOS BACK-OFFICE

RISCCO

CONCLUSIÓN

La IA no espera. *El CSCF 2026 tampoco.*

El vínculo entre la inteligencia artificial generativa y la criticidad de la infraestructura SWIFT crea una ventana de riesgo que no existía hace años atrás. Los atacantes ya no necesitan expertise técnico avanzado: la IA facilita los ataques mientras las organizaciones siguen operando con procesos diseñados la era antes de la IA.

El CSCF 2026 representa el reconocimiento formal de SWIFT de que el perímetro se ha expandido y que las amenazas son fundamentalmente distintas. Sin embargo, el marco no se implementa solo: requiere voluntad ejecutiva, inversión y cultura organizacional donde la seguridad sea responsabilidad de todos.

Las instituciones que traten el cumplimiento SWIFT como un check-list se exponen no solo a sanciones regulatorias, sino a convertirse en el eslabón débil de un ecosistema que depende de la confianza colectiva.

MENSAJE CLAVE

La IA que sus competidores usan para eficiencia operativa, los atacantes la usan para comprometer infraestructura crítica.

CONTACTOS

Panamá, Centroamérica y El Caribe

Antonio Ayala I.
CEO
aayala@riscco.com

Rubén Fernández
Gerente de Consultoría
rfernandez@riscco.com

Marinelda Morales
Gerente Comercial
mmorales@riscco.com

República Dominicana y Puerto Rico

Eury Valdez
Asesor Comercial
efvaldez@riscco.com

Acerca de RISCCO

RISCCO es una firma de consultoría internacional e independiente, comprometida con transformar la forma en que las organizaciones gestionan el riesgo y adoptan la Inteligencia Artificial. Combinamos un enfoque riguroso en GRC (Gobernanza, Riesgo y Cumplimiento) con analítica de datos avanzada e Inteligencia Artificial para ayudar a nuestros clientes a anticipar riesgos, fortalecer la gobernanza y resolver desafíos complejos. Con sede en Panamá y presencia en seis países, en 2026 cumplimos 17 años sirviendo a más de 200 organizaciones líderes en Centroamérica y el Caribe.

Rigor internacional. Ejecución ágil. Impacto medible.
Pensamos como estrategas. Ejecutamos como especialistas.

riscco.com