¿Cómo mitigar las brechas que abre la tecnología?

SWIFT CSP evaluación independiente

The better the question. The better the answer.
The better the world works.

Building a better working world

La Sociedad para las Comunicaciones Interbancarias y Financieras Mundiales (SWIFT, por sus siglas en inglés) se describe a sí misma como un proveedor de "una red para transferir valores con un enfoque confiable, seguro y protegido", que establece los estándares internacionales para la sintaxis de los mensajes financieros, provee una red segura para la transmisión de mensajes entre las instituciones financieras y desarrolla software para conectar la red SWIFT.

Generalidades

Como respuesta al fraude en Bangladesh del 2016, SWIFT como parte de su política ha implementado el Programa de Seguridad para Clientes (CSP, por sus siglas en inglés), para abordar riesgos cibernéticos de pagos globales y mejorar la confianza dentro de la comunidad SWIFT, incluyendo las instituciones financieras, así como otras grandes corporaciones conectadas a la red. Su marco laboral subyacente establece una serie de controles de seguridad diseñados a ayudar a los clientes a protegerse contra amenazas cibernéticas, así como a asegurar la infraestructura local usada para acceder a la red SWIFT. Bajo la CSP, SWIFT requiere que todos los clientes, de forma anual, autoevalúen su postura de cumplimiento dentro de la herramienta Know Your Customer (KYC), que es utilizada por SWIFT y por las contrapartes de los clientes (p.e., otros bancos o corporaciones), para analizar los resultados de la auto evaluación.

Actualmente, se requiere que los clientes SWIFT realicen auto evaluaciones con poco o ningún involucramiento de las unidades de negocio asociadas a la primera línea de defensa (generalmente, áreas financieras, tesorería). A inicios de julio del 2021, las actualizaciones al CSP requieren que los clientes obtengan una evaluación independiente contra el marco de SWIFT de forma anual, para informar a la alta gerencia del estado actual de seguridad del ambiente SWIFT. Esto puede llevarse acabo de las siguientes maneras:

- **Una evaluación externa** por una organización externa independiente que tenga experiencia en las evaluaciones de ciberseguridad existentes, así como evaluadores individuales con certificaciones relevantes en la industria de seguridad. Un ejemplo de esta evaluación externa sería el reporte de certificación de un Cybersecurity Program Assessment.
- **Una evaluación interna** por una función de usuario de segunda o tercera línea de defensa (cumplimiento, auditoría interna), independiente de la primera línea de defensa que será evaluada. Aquellos que realicen la evaluación deben poseer experiencia reciente y relevante en la evaluación de los controles de ciberseguridad.

El CSP de SWIFT requerirá de una evaluación independiente para informar a la alta gerencia de la auto evaluación. Por lo tanto, EY ha desarrollado un enfoque metodológico para cubrir esta necesidad.

Preparándose para el 2021

Los ciberataques se están volviendo cada vez más sofisticados dentro de la comunidad financiera. La arquitectura SWIFT instalada dentro del entorno de las entidades de los clientes permite la comunicación de mensajes financieros (p.e., transferencias electrónicas entre entidades financieras), debido al incremento de conexiones fuera de la red de la entidad, presenta un aumento en la superficie de exposición mediante la ejecución de vectores de ataque que podrían ser materializados (explotados). De no estar propiamente asegurados, existe el riesgo de fraudes electrónicos, asociados a cambios no autorizados al monto o al receptor de los fondos durante los pasos finales del proceso de transferencia de SWIFT.

EY está preparada para ayudar a las entidades a cubrir esta necesidad, actualmente cuenta con una red de profesionales con conocimiento y experiencia en el sector financiero, en materia de ciberseguridad, cumplimiento regulatorio y el manejo de riesgos tecnológicos, quienes están en la capacidad de llevar a cabo una evaluación SWIFT CSP.

Reporte de evaluación SWIFT CSP – uso y beneficios

El reporte de evaluación permite la reducción de tiempo y costos necesarios para abordar los requerimientos en materia de seguridad de SWIFT, así como el estado de seguridad del ambiente SWIFT basado en riesgos a los clientes y otras contrapartes al permitir que las entidades demuestren que los controles implementados son los apropiados para mantener la postura de seguridad.

¿Cuáles son los requisitos para una evaluación independiente del SWIFT CSP?

Así como en muchos otros marcos de seguridad que existen actualmente (NIST, ISO, etc.), un marco de control también es la base de la CSP. El Marco de Controles de Seguridad para Clientes SWIFT (CSCF, por sus siglas en inglés) se divide en objetivos, principios y controles. Los controles están subdivididos en una serie común de controles de seguridad mandatorios y opcionales, y el número de controles evaluados dependerá del tipo de arquitectura utilizada por cada cliente SWIFT.

Architecture A		
A1 – Completa A2 – Parcial A3 – Conector SWIFT	**22 mandatorios** (Proteja su entorno: 11; conozca y limite el acceso: 5; detectar y responder: 6	**9 opcionales** (Proteja su entorno: 5; conozca y limite el acceso: 1; detectar y responder: 3
A4 – Conector de Cliente	**15 mandatorios** (Proteja su entorno 8; conozca y limite su acceso: 3; detectar y responder: 4	**8 opcionales** (Proteja su entorno 5; conozca y limite su acceso: 1; detectar y responder: 2
Architecture B		
B – No local user footprint	**14 mandatorios** (Proteja su entorno 6; conozca y limite su acceso: 5; detectar y responder: 4	**8 opcionales** (Proteja su entorno 4; conozca y limite su acceso: 1; detectar y responder: 2

SWIFT en números

37.9m de mensajes (FIN) al día 1[1]

11,000+ instituciones conectadas a la plataforma SWIFT[2]

200+ países o territorios conectados[2]

[1] https://www.swift.com/about-us/swift-fin-traffic-figures
[2] https://www.swift.com/about-us

Estadísticas de fraude SWIFT

El **40%** de las entidades "confían" en detectar ataques a la plataforma SWIFT[3]

$380m en pérdidas por pagos fraudulentos desde el 2016[3]

El **60%** de los bancos estadounidenses han sido blanco de fraude por medio de SWIFT[3]

[3] https://www.eastnets.com/news/eastnets-swift-cyber-fraud-survey-report-reveals-more-than-4-out-5-banks-are-targeted

Marco SWIFT para los controles de seguridad de los clientes

3 objetivos

- Aseguramiento del entorno
- Controles de acceso
- Detectar y responder

8 principios

- Restringir el acceso a Internet
- Proteger los sistemas críticos del entorno de TI
- Reducir la superficie de ataque y las vulnerabilidades
- Proteger físicamente el entorno
- Evitar el compromiso de las credenciales
- Administrar las identidades y segregar privilegios
- Detectar la actividad anómala en sistemas o registros de transacciones
- Planear la respuesta a incidentes y el intercambio de información

31 controles

SWIFT también ha definido responsabilidades mínimas de los clientes, así como de los asesores que realicen las revisiones independientes:

Responsabilidades de los asesorest – el asesor debe proveer a los clientes con:

- Un reporte formal describiendo la confirmación del asesor del cumplimiento de cada control, junto con la documentación de las situaciones relevantes que se deberían de llevar en la implementación.
- Una carta complementaria confirmando que el trabajo fue realizado con la objetividad e independencia requerida.

Las responsabilidades de los clientes SWIFT – Elegir al asesor que considere los siguientes aspectos:

- Que el asesor sea independiente y libre de cualquier conflicto de interés.
- Que la firma o departamento interno que lleva a cabo la evaluación tenga experiencia reciente (12 meses atrás) y relevante a la hora de ejecutar evaluaciones relacionadas con ciberseguridad dentro del marco del CSCF.
- Que el equipo de trabajo encargado de llevar a cabo la evaluación tenga al menos una certificación relevante a nivel profesional (CISA, CISSP, CISM, etc.).

¿Cuáles desafíos enfrentan las organizaciones?

Muchas organizaciones no tienen la capacidad, el criterio de independencia o la competencia requerida, dado que las funciones que ejecutan actualmente de segunda o tercera línea no les permitan realizar las evaluaciones SWIFT, o que simplemente no tengan la experiencia o la formación profesional.

Algunos desafíos adicionales que hemos identificado de evaluaciones previas:

- Las organizaciones no están siempre conscientes de sus códigos de identificación de negocio (BIC, por sus siglas en inglés), cuántos tienen, quiénes son los dueños o quiénes los utilizan.
- La identificación de los diferentes componentes del sistema de mensajería SWIFT (tecnológicas y empresariales), no está siempre bien definida.
- La documentación es insuficiente para respaldar la certificación hecha por medio de la herramienta de Certificación de Seguridad KYC (KYC-SA) en caso de que SWIFT u otro tercero solicite más detalles sobre la solicitud.
- No toda la infraestructura de SWIFT está apropiadamente ubicada dentro de una (zona segura).
- Los aspectos importantes de riesgo del SWIFT no están siempre considerados bajo el contexto de objetivo de control y los requerimientos necesarios para la implementación.

¿Cuáles son las consecuencias del incumplimiento?

- Si la solicitud de auto evaluación en la herramienta KYC-SA está incompleta, ésta puede ser visible para las contrapartes.
- Las organizaciones están utilizando información de riesgo de la contraparte (un tercero) sobre SWIFT KYC-SA para informar las decisiones de gerencia de riesgos de terceros. El incumplimiento podría tener amplio impacto en la relación con terceros.
- Los reguladores de cada país pueden solicitar acceso a la información de certificación SWIFT CSP.
- SWIFT se reserva el derecho a desconectar a los usuarios de la red, o realizar evaluaciones presenciales, estipuladas por SWIFT.
- El marco laboral del CSP está diseñado bajo un enfoque de controles clave para el manejo de los riesgos de ciberseguridad al sistema SWIFT. El incumplimiento expone a la entidad a la materialización ciberataque.

Cómo puede ayudar el equipo de EY

Contamos con profesionales de EY, que tienen experiencia en el desarrollo de estas evaluaciones de SWIFT, trabajando en conjunto con entidades del sector financiero, para mejorar la postura de seguridad y el ambiente de control del sistema de mensajería SWIFT.

Preguntas clave que deberían hacerse

- ¿Tengo el personal apropiadamente calificado y certificado para llevar a cabo la evaluación?t
- ¿La evaluación está siendo realizada por una función independiente?
- Para mediados del 2021, ¿Puedo asegurar que estaré cumpliendo con todos los controles mandatorios de SWIFT CSP v2021?
- ¿He considerado el cumplimiento de los controles opcionales, que podrían ser mandatorios en el futuro?
- ¿Sé quién es el propietario de mi infraestructura SWIFT?, ¿Cuántos BICs tiene mi organización y de qué forma son utilizados?
- ¿Tiene la organización un plan para gestionar de manera continua el cumplimiento de SWIFT?

Contactos:

Miguel Caldentey
Socio
Consultor en Tecnología
Miguel.caldentey@pa.ey.com

Enrique Mendoza
Manager
Consultor en Tecnología
Enrique.mendoza.diaz1@pa.ey.com

EY | Construyendo un mejor mundo de negocios

EY existe para construir un mejor mundo de negocios, ayudando a crear valor a largo plazo para sus clientes, su gente y la sociedad en general, así como también para construir confianza en los mercados de capitales.

Por medio de datos y tecnología, los equipos diversos e incluyentes de EY, ubicados en más de 150 países, brindan confianza a través de la auditoría y ayudan a los clientes a crecer, transformarse y operar.

El enfoque multidisciplinario en auditoría, consultoría, legal, estrategia, impuestos y transacciones, busca que los equipos de EY puedan hacer mejores preguntas para encontrar nuevas respuestas a los asuntos complejos que actualmente enfrenta nuestro mundo.

EY se refiere a la organización global y podría referirse a una o más de las firmas miembro de Ernst & Young Global Limited, cada una de las cuales es una entidad legal independiente. Ernst & Young Global Limited, una compañía del Reino Unido limitada por garantía, no proporciona servicios a clientes. Para conocer la información sobre cómo EY recaba y utiliza los datos personales y una descripción de los derechos que tienen las personas conforme a la ley de protección de datos, ingrese a ey.com/privacy. Las firmas miembro de EY no ofrecen servicios legales en los casos en que las leyes locales lo prohíban. Para obtener mayor información acerca de nuestra organización, ingrese a ey.com.

Organización Regional: Costa Rica - Tel. +(506) 2208-9800 **| El Salvador** - Tel. +(503) 2248-7000 **| Guatemala** - Tel. +(502) 2386-2400
Honduras - Tel. +(504) 2232-9100 **| Nicaragua** - Tel. +(505) 2253-8430 **| Panamá** - Tel. +(507) 208-0100
República Dominicana - Tel. +(809) 472-3973