SWIFT Programa de seguridad de clientes 2020

pwc.com.ar

pwc

SWIFT Programa de seguridad de clientes 2020
Lo esencial

¿Qué es el programa de seguridad del cliente de SWIFT?

SWIFT Customer Security Programme (CSP)

El SWIFT CSP se centra en 3 áreas que se refuerzan mutuamente. Proteger y asegurar su entorno local (Usted), prevenir y detectar el fraude en sus relaciones comerciales (Sus contrapartes) y continuamente compartiendo información y preparándose para defenderse frente a futuras amenazas cibernéticas (Su comunidad).

Mientras las organizaciones siguen siendo los principales responsables de proteger su propio ambiente, SWIFT's CSP busca que la comunidad soporte la lucha contras los ciber-ataques.

¿Por qué es importante?

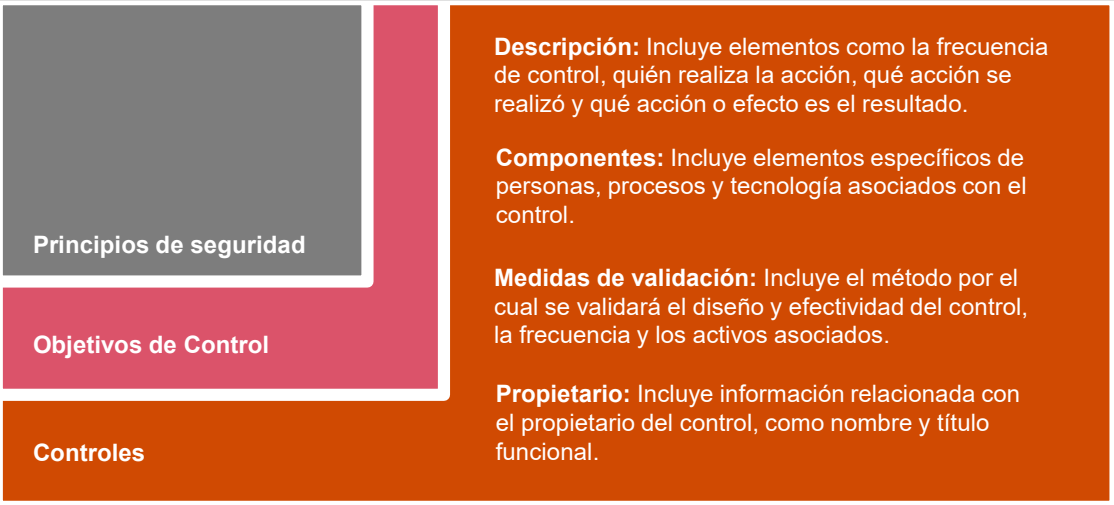
En respuesta a una serie de ataques cibernéticos y violaciones a lo largo de 2016, SWIFT ha identificado 16 controles de seguridad obligatorios y 11 opcionales para sus 11,000 clientes en todo el mundo. Se pedirá a todos los clientes que atestigüen que cumplen con los controles, y que los resultados se comparten con sus homólogos y reguladores. **En la Versión 2020, Los controles se han elevado a 31 en Total, de los Cuales 21 son Mandatorios y 10 Opcionales.**

Impacto

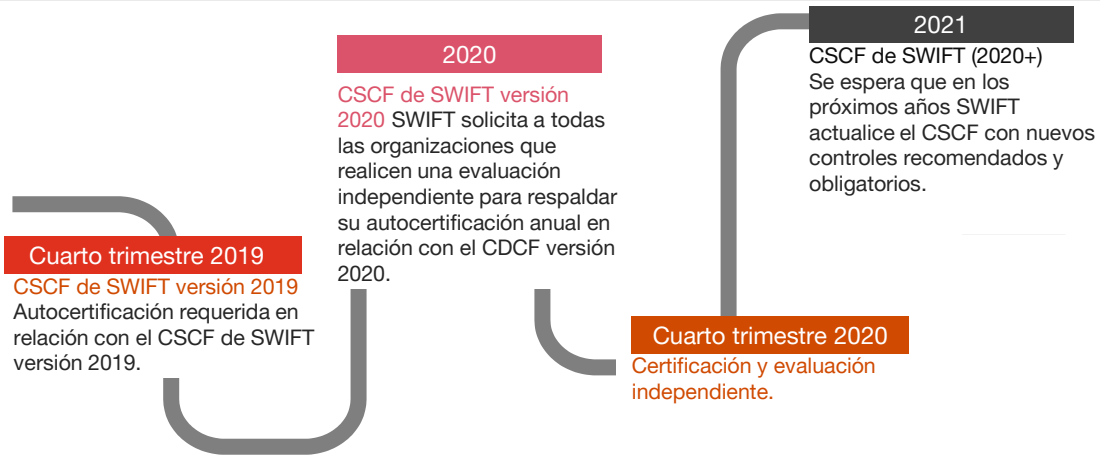
Los impactos variarán dependiendo de la madurez de la organización, del diseño del entorno SWIFT local y de la naturaleza de los controles existentes. Muchas organizaciones tendrán que remediar tanto las deficiencias técnicas como las relacionadas con los procesos.

Factores de éxito: Para tener éxito, se debe adoptar un enfoque detallado y sistemático, que incluya la colaboración a través de 3 líneas de defensa, liderazgo fuerte y un equipo diverso organizado.

Cyber security assurance framework



Cronología



SWIFT Programa de seguridad de clientes 2020
Capacidades de PwC

¿Cómo puede ayudar PwC?

1

Análisis de brecha
Realizamos una evaluación para determinar si existen controles que satisfacen los requisitos de SWIFT.

2

Remediación
Desarrollar flujos de trabajo para abordar las deficiencias de control identificadas a través de la tecnología y los cambios de procesos.

3

Atestiguamiento – Auto Certificación
Validación del cumplimiento exitoso de los controles de CSP y transición al equipo de cumplimiento en curso.

Servicios adicionales

Servicios de seguridad cibernética:

- Pruebas de penetración
- Evaluación técnica
- Prueba de respuesta a incidentes
- Evaluación de indicadores de incumplimiento

Servicios de garantía de cumplimiento:

- Informes de terceros bajo normas reconocidas (por ejemplo, SOC2, ISAE)
- Analíticos de confianza - Medir los niveles de confianza dentro de su base de clientes

¿Por qué PwC?

Equipo cohesivo que entiende SWIFT

PwC ha realizado un gran número de evaluaciones de seguridad basados en SWIFT a nivel mundial y contamos con un enfoque probado y entendimiento de como asegurar la infraestructura de SWIFT, manteniéndola funcional.

Experiencia probada en proyectos similares

PwC cuenta con sólida experiencia en reportes de atestiguamiento similares , esto bajo estándares internacionales reconocidos SOC II, NIST, PCI, ISO 27001.

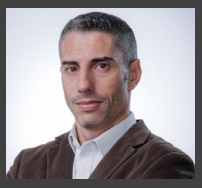
Experiencia técnica y base de conocimientos

PwC es la única empresa 'Big-4' con certificado de Consultoría de Seguridad Cibernética de la NCSC. PwC es único en su capacidad de aprovechar inteligencia de amenazas para construir y simular escenarios realistas de ataque cibernético.

Adaptarse a sus necesidades

PwC formulará y adaptará el enfoque que se adecue a las necesidades inmediatas y planes a futuro. Para cumplir con estos objetivos PwC provee un enfoque pragmático y puntos de vista balanceados que apoya en la priorización de las acciones asociadas.

Contactos



Diego Taich
CiberSeguridad & Tec. Managing Director

T: +54 (11) 4850 6834

E: diego.taich@pwc.com

Eduardo Ponce Paz
CiberSeguridad Senior Manager

T: +54 (11) 4850 6111

E: eduardo.s.ponce.paz@pwc.com

SWIFT Programa de seguridad de clientes 2020
Apéndice (1/2)

Descripción general del marco de control de seguridad de clientes de SWIFT Versión 2020.

Esta sección general establece el conjunto de controles de seguridad obligatorios y de asesoramiento. Los controles de seguridad obligatorios se basan en la guía existente y establecen una línea de base de seguridad. Los controles asesores son buenas prácticas opcionales que SWIFT recomienda para que cada usuario implemente en su entorno.

Objetivos	Principios	Controles
Proteger su entorno	Restringir el acceso a Internet y proteger los sistemas críticos del entorno general de TI	**Obligatorio** **Protección del ambiente SWIFT–** Una zona segura segregada protege la infraestructura SWIFT de los compromisos y ataques más amplios en los entornos empresariales y externos. **Control de cuentas privilegiadas del sistema operativo –** El acceso a las cuentas del sistema operativo de nivel administrador se limita al máximo posible. El uso es controlado, monitoreado y sólo está permitido para actividades relevantes tales como instalación y configuración de software, mantenimiento y actividades de emergencia. En cualquier otro momento, se utiliza una cuenta con el acceso de menor privilegio. **Protección de plataforma de virtualización -** Plataforma de virtualización segura y máquinas virtuales (VM) que alojan componentes relacionados con SWIFT al mismo nivel que los sistemas físicos. **Opcional** **Restricción de Acceso a Internet -** Restringir el acceso a Internet desde las PCs del operador y otros sistemas dentro de la zona segura.
	Reducir la superficie de ataque y las vulnerabilidades	**Obligatorio** **Seguridad interna en el flujo de datos** – Se implementan mecanismos de confidencialidad, integridad y autenticación para proteger los flujos de datos relacionados con SWIFT relacionados y entre la aplicación y el operador. **Actualizaciones de seguridad** – Todo el hardware y software dentro de la zona segura y en las PC del operador están dentro del ciclo de vida de soporte, actualizaciones de software mandatorio y se aplican rápidamente actualizaciones de seguridad. **Hardening de los sistemas** – El fortalecimiento de seguridad se realiza en todos los componentes dentro del alcance. **Confidencialidad e integridad de la sesión del operador** – Se protege la confidencialidad e integridad de las sesiones interactivas del operador que se conecta a la zona segura. **Escaneo de Vulnerabilidades** – Los escaneados de vulnerabilidades de las zonas seguras y los sistemas de operadores de PC se realizan con una herramienta de análisis actualizada y de buena reputación. **Hardening de las Aplicaciones**– El fortalecimiento de seguridad de la Aplicación ,se realiza en todos los componentes dentro del alcance (mensajería, interfaces, etc). **Opcional** **Seguridad de flujo de datos de back-office** – Se implementan mecanismos de confidencialidad, integridad y autenticación mutua para proteger los flujos de datos entre aplicaciones de back office (o middleware) y componentes de infraestructura de SWIFT. **Protección de datos de transmisión externa** – Los datos sensibles relacionados con SWIFT que salen de la zona segura se cifran. **Subcontratación de actividades críticas** – Las actividades subcontratadas críticas están protegidas, al menos, con el mismo nivel de atención que si operaran dentro de la organización. **Controles comerciales de transacciones** – Implementación de controles a la gestión de relaciones de aplicaciones y detección de transacciones, prevención y control de validación para restringir la actividad de la transacción dentro de los límites esperados o de los negocios normales. **Controles comerciales de RMA -** Restringir la actividad de transacciones a contrapartes comerciales validadas y aprobadas.
	Proteger físicamente el ambiente	**Obligatorio** **Seguridad Física** – Controles de seguridad física para proteger el acceso a equipos sensibles, sitios de hosting y almacenamiento..

SWIFT Programa de seguridad de clientes 2020
Apéndice (2/2)

Objetivos	Principios	Controles
Conocer y limitar el acceso	Evitar el Compromiso de Credenciales	**Obligatorio** **Política de contraseñas** – Todas las cuentas de aplicaciones y sistemas operativos imponen contraseñas con parámetros tales como longitud, complejidad, validez y número de intentos fallidos de inicio de sesión. **Autenticación de múltiples factores** – La autenticación de múltiples factores se utiliza para el acceso interactivo de los usuarios a las aplicaciones y cuentas del sistema operativo relacionadas con SWIFT.
	Administrar identidades y segregar privilegios	**Obligatorio** **Control de acceso lógico** – Las cuentas se definen de acuerdo con los principios de seguridad del acceso a la necesidad de conocer, los privilegios mínimos y la separación de funciones. **Administración de Tokens** – Los tokens de autenticación se gestionan adecuadamente durante la emisión, revocación, uso y almacenamiento. **Almacenamiento de contraseñas físicas y lógicas** – Las contraseñas registradas para cuentas privilegiadas se almacenan en una ubicación física o lógica protegida, con acceso restringido según necesidad. **Opcional** **Proceso de evaluación del personal -** Asegure la confiabilidad del personal que opera el entorno local de SWIFT mediante la evaluación de antecedentes del personal.
Detectar y responder	Detectar actividad anómala en sistemas o registros de transacción	**Obligatorio** **Protección de Malware** – Software anti-malware de un proveedor de confianza se instala y se mantiene actualizado en todos los sistemas. **Integridad del Software** – La comprobación de la integridad del software se realiza a intervalos regulares en la interfaz de mensajería, la interfaz de comunicación y otras aplicaciones relacionadas con SWIFT. **Integridad de la Base de Datos** – Se realiza una comprobación de la integridad de la base de datos a intervalos regulares, en bases de datos que registran transacciones de SWIFT. **Registro y monitoreo** – Se implementan capacidades para detectar actividad anómala y se dispone de un proceso o herramienta para almacenar y revisar registros con frecuencia. **Opcional** **Detección de intrusos** – La detección de intrusos se implementa para detectar acceso de red no autorizado y actividad anómala.
	Plan para la respuesta a incidentes y el intercambio de información	**Obligatorio** **Planificación de respuesta a ciber incidentes** – La organización tiene un plan de respuesta a incidentes cibernéticos definido y probado. **Formación y sensibilización en materia de seguridad** – Se realizan sesiones anuales de concientización sobre la seguridad para todos los miembros del personal, incluida la capacitación específica para roles de SWIFT con acceso privilegiado. **Opcional** **Pruebas de Penetración** – Las pruebas de penetración de aplicaciones, host y redes se realizan dentro de la zona segura y en las PCs del operador. **Evaluación del riesgo de escenario** – Se llevan a cabo periódicamente evaluaciones de riesgos basadas en escenarios para mejorar la preparación para la respuesta a incidentes y para aumentar la madurez del programa de seguridad de la organización.