SWIFT

Customer Security Controls Framework (CSCF) y Customer Security Programme (CSP)

El panorama de amenazas y fraudes financieros y bancarios se adapta y evoluciona y, si bien todos los clientes son responsables de proteger sus propios entornos, SWIFT ha establecido el programa de seguridad denominado *Customer Security Programme (CSP)* para ayudarlos en la lucha contra los ciberataques.

El curso se basa en la última actualización de SWIFT Customer Security Controls Framework (CSCF) y Customer Security Programme (CSP).

SEGU·INFO
SEGURIDAD DE LA INFORMACION

educacion.segu-info.com.ar

Objetivos generales

Este curso está orientado a conocer el *SWIFT Customer Security Controls Framework (CSCF)*, *Customer Security Programme (CSP)* y el *Independent Assessment Framework* (ISF) compuestos de controles de seguridad obligatorios, recomendaciones y buenas prácticas para los usuarios de SWIFT.

Requisitos previos

Conocimiento básico sobre seguridad de la información, auditoría, gestión del riesgo y SWIFT.

Público Objetivo

El curso está orientado a administradores de bases de datos, especialistas en redes, y personas vinculadas al análisis, diseño, arquitectura SWIFT, así como a los responsables de tecnología y seguridad de la información de la organización.

Finalizado el curso, el asistente será capaz de:

- Conocer y entender los controles de CSCF y el CSP
- Entender las amenazas y vulnerabilidades a las que está expuesta cualquier infraestructura y red SWIFT
- Reconocer y detectar de manera proactiva las falencias de la implementación
- El proceso y los plazos para enviar la conformidad a la aplicación *KYC-Security Attestation* de SWIFT
- Acciones y contramedidas en caso de incumplimiento en presentación de informes

Material a entregar

Presentaciones utilizadas durante el curso en formato digital.

Duración y Modalidad

Este curso teórico/práctico tiene una duración de **8 horas** y la modalidad de cursada es presencial y/o remota. También puede ser desarrollado ***in-company***.

Instructor

Cristian Borghello es Licenciado en Sistemas (UTN), desarrollador, Certified Information Systems Security Professional (CISSP), Certificate of Cloud Security Knowledge (CCSK), y Cyber Security Foundation Professional Certificate (CSFPC).

Actualmente es Director de **Segu-Info**, **Segu-Kids, ODILA y Antiphishing.la** y se desempeña como consultor independiente en Seguridad de la Información.

Ha brindado cursos y dictado congresos y seminarios nacionales e internacionales sobre la temática.

Temario

- Introducción y arquitectura de SWIFT
- Tipos de mensajes
- Casos conocidos de ataques y vulnerabilidades en SWIFT
- Controles obligatorios vs recomendaciones
- Superficie de ataque y factores y escenarios de riesgo
- Controles de seguridad obligatorios y recomendados
- Tipo de arquitectura
- CSCF, CSP e ISF
- Roles y Responsabilidades
- Restringir el acceso a Internet
- Proteger sistemas críticos del entorno de TI general
- Reducir la superficie de ataque y las vulnerabilidades
- Asegurar físicamente el entorno
- Prevenir amenazas a las credenciales
- Gestionar identidades y segregación de privilegios
- Detectar actividad irregular en los sistemas o registros de transacciones
- Plan de respuesta a incidentes e intercambio de información
- Guías de mejores prácticas de seguridad
- Conclusiones