XV REUNIÓN DE AUDITORES INTERNOS
DE BANCOS CENTRALES

“Auditoría a la gestión de la Implementación del Customer Security Program (CSP) de SWIFT”

BANCO CENTRAL DE CHILE, SANTIAGO, CHILE
SEPTIEMBRE 25 - 27, 2019

Auditoría a la gestión de la Implementación del Customer Security Program (CSP) de SWIFT

Luis José Orjuela y Marisol Alemán Bello
Auditoría General del Banco de la República

26 de septiembre de 2019

Dada la amenaza latente de ataques de ciberseguridad que ha tomado relevancia tras el ataque con malware ocurrido al Banco Central de Bangladesh (2016), SWIFT ha pedido acciones preventivas de parte de sus clientes, recordándoles su responsabilidad en cuanto a la seguridad de los sistemas internos que interactúan con la red SWIFT y además recomendándoles la implementación de ciertos controles de seguridad.

En mayo del 2016 SWIFT creó el Programa de Seguridad (CSP)

Los incidentes recientes relacionados con SWIFT y sector financiero (entre muchos otros sectores afectados) evidencian un incremento en la cantidad y sofisticación de ataques, así como también en el potencial impacto sobre las víctimas.

Ante esta situación el Banco de la República reforzó controles existentes y realizó varios ejercicios de evaluación de la infraestructura tecnológica y de los procesos operativos de las áreas de negocio que utilizan la plataforma SWIFT para el cumplimiento de las funciones misionales:

Administración de Reservas Internacionales

(Portafolio, Convenios y Organismos Internacionales)

Administración de Fondos Soberanos

Ejecución de la política Cambiara

Agencia Fiscal del Gobierno

Adicionalmente, en cuanto a gestión administrativa del Banco, la plataforma SWIFT soporta la realización de pagos internacionales de adquisición de bienes y servicios y gestión humana (nómina de pensionados y becarios en el exterior).

En desarrollo del Plan Estratégico del Banco 2017-2020, bajo el objetivo de *Optimizar el Sistema de Gestión de Seguridad de la Información,* se estableció el Programa de Ciberseguridad y creó el área de Ciberdefensa.

La Auditoría General ha definido ciclos operativos y de gestión de TI (68) para la evaluación de la gestión, estructura de control interno, cumplimiento y razonabilidad de los estados financieros de las operaciones del Banco.

El alcance de las evaluaciones de los ciclos operativos relacionados con los pagos internacionales(9) incluye el análisis de las nuevas amenazas y vulnerabilidades de riesgo cibernético con fuente en personas, procesos e infraestructura tecnológica.

Además de las evaluaciones que se venían realizando, a partir del 2017, se incluyó en el Plan Anual de la Auditoría General la evaluación de la implementación del Programa de Seguridad de SWIFT (CSP).

TEMAS

1. CSP: Un marco de controles de SWIFT
2. Implementación en el banco de la República
3. Enfoque de Auditoría al CSP
4. Conclusiones

1. CSP: EL MARCO DE CONTROLES DE SWIFT

Programa de Seguridad de SWIFT (CSP): El marco de controles

Para enfrentar el riesgo cibernético sistémico y mejorar la seguridad y la transparencia en la comunidad financiera global, Swift ha planteado el CSP considerando tres áreas:

1. Proteger y asegurar el entorno local de los clientes
2. Prevenir y detectar fraudes en las relaciones comerciales
3. Compartir información y prepararse continuamente contra futuras ciber amenazas .

El objetivo es limitar las oportunidades de ataques que exploten las vulnerabilidades de los ambientes locales de operación

Programa de Seguridad de SWIFT (CSP): El marco de controles

- SWIFT ha diseñado un marco de controles de seguridad para ayudar a los clientes a mejorar el nivel de ciberseguridad de su ambiente local.
- Estos controles están basados en los análisis de ciber-amenazas de inteligencia realizados en conjunto con expertos de la industria y con la retroalimentación de los usuarios, en línea con los estándares de seguridad existentes.
- Algunos de ellos son obligatorios y otros recomendados (buenas prácticas).

El objetivo es limitar las oportunidades de ataques que exploten las vulnerabilidades de los ambientes locales de operación

(CSP): El marco de controles de SWIFT

Objetivos de seguridad

Asegure su entorno

Conozca y limite el acceso

Detecte y responda

Estos objetivos consideran 8 principios de seguridad

(CSP): El marco de controles de SWIFT

Objetivos y Principios de seguridad

Asegure su entorno

- Restringir el acceso a internet
- Proteger los sistemas críticos del entorno general de TI
- Reducir la superficie de ataque y las vulnerabilidades
- Asegurar físicamente el entorno

Conozca y limite el acceso

- Prevenir amenazas que comprometan las credenciales
- Gestionar identidades y segregación de privilegios

Detecte y responda

- Detectar actividad irregular en los sistemas o registros de transacciones
- Plan de respuesta a incidentes e intercambio de información

(CSP): El marco de controles de SWIFT

27 Controles de seguridad obligatorios y recomendados (1/3)

30/09/2019

- Protección del Entorno de SWIFT
- Control de Cuentas privilegiadas de Sistema Operativo

1. Restringir el acceso a Internet y proteger sistemas críticos del entorno de TI general

2. Reducir la superficie de ataque y las vulnerabilidades

- Seguridad Interna de Flujo de datos
- Actualizaciones de Seguridad
- Fortalecimiento del Sistema
- Seguridad del Flujo de Datos del Servicio Interno
- Protección de Transmisión Externa de Datos
- Confidencialidad e Integridad de la Sesión del Operador
- Escaneo de Vulnerabilidades
- Subcontratación de Actividades Críticas
- Controles Empresariales de Transacciones

3. Asegurar físicamente el entorno

- Seguridad Física

ASEGURE SU ENTORNO

(CSP): El marco de controles de SWIFT

27 Controles de seguridad obligatorios y recomendados (2/3)

5. Gestionar identidades y segregación de privilegios

- Control de Acceso Lógico
- Gestión de Tokens
- Poceso de Verificación de Antecedentes del Personal
- Almacenamiento Físico y Lógico de Contraseñas

4. Prevenir amenazas que pongan en compromiso las credenciales

- Política de Contraseñas
- Autenticación de Múltiples Factores

CONOZCA Y LIMITE EL ACCESO

(CSP): El marco de controles de SWIFT

27 Controles de seguridad obligatorios y recomendados (3/3)

30/09/2019

- Protección contra Malware
- Integridad del Software
- Integridad de la Base de Datos
- Log de información y Monitoreo
- Detección de Intrusiones

6. Detectar actividad irregular en los sistemas o registros de transacciones

7. Plan de respuesta a incidentes e intercambio de información

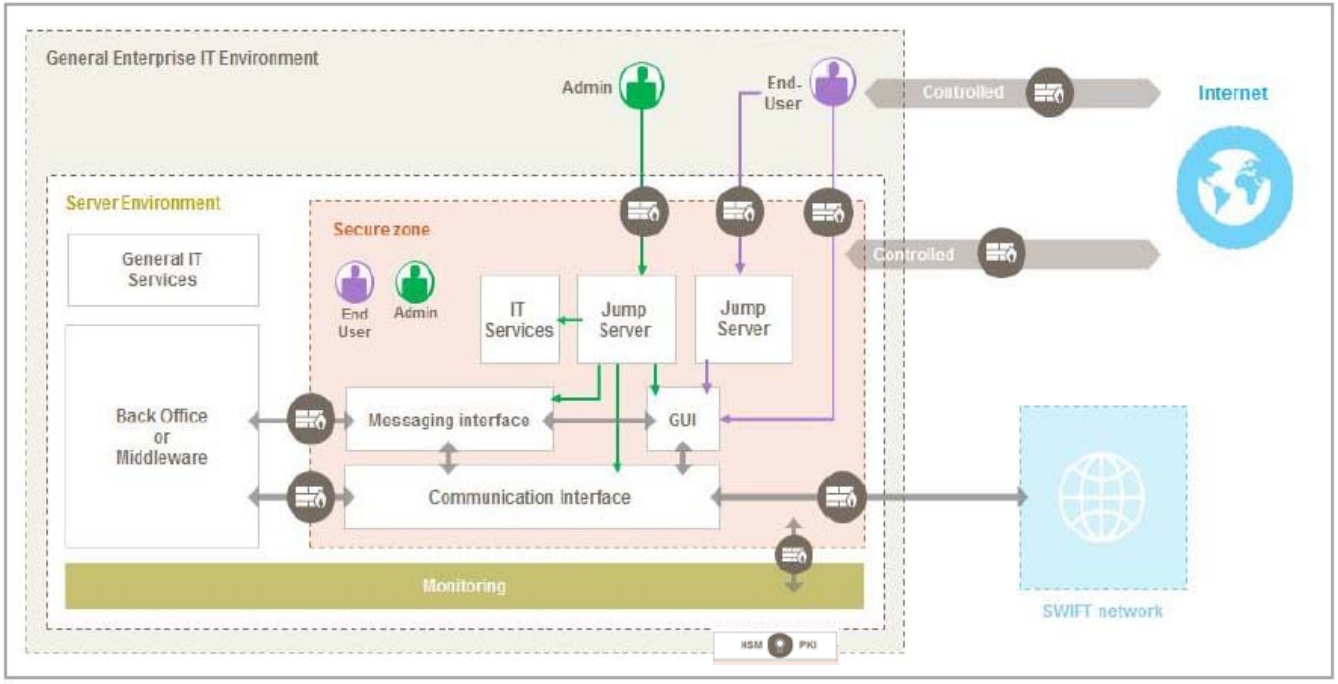
- Planeación de Respuesta a Incidentes Cibernéticos
- Capacitación y Concienciación en Temas de Seguridad
- Pruebas de Penetración
- Evaluación de escenarios de riesgo

DETECTE Y RESPONDA

(CSP): El marco de controles de SWIFT

ARQUITECTURA DE REFERENCIA

Arquitectura Tipo A1



Los usuarios deberán implementar todos los controles obligatorios que les resulten aplicables de acuerdo con las arquitecturas de referencia tipo A o tipo B

Marco de Controles de Seguridad para el Cliente de SWIFT 2019

(CSP): El marco de controles de SWIFT

Reducir la superficie de ataque y las vulnerabilidades

2.1 Seguridad interna del Flujo de Datos		Arquitecturas a las que aplica: A
Definición del control	Objetivo	Asegurar la confidencialidad, integridad y autenticidad de los flujos de datos entre las aplicaciones locales relacionadas con Swift y su vínculo con el PC del operador
	Componentes dentro del alcance	- PC del Operador - Componentes de la infraestructura relacionada con Swift
	Factores de riesgo	- Pérdida de confidencialidad de datos sensibles - Pérdida de integridad de datos sensibles - Tráfico no autenticado del Sistema - Acceso no autorizado
Guía de Implementación	Planteamiento del Control	Los mecanismos de confidencialidad, integridad y autenticación se implementan para proteger los flujos de datos aplicación a aplicación y operador a aplicación relacionados con Swift
	Contexto del Control	Los flujos de datos internos se protegen contra divulgación, modificación y acceso no intencional de los datos mientras se encuentran en tránsito
	Directrices para la implementación	…

(CSP): El marco de controles de SWIFT

Plan de Respuesta a incidentes e intercambio de información

7.1 Planeación de Respuesta a Incidentes		Arquitecturas a las que aplica: A y B
Definición del control	Objetivo	Asegurar un enfoque congruente y efectivo para la gestión de incidentes cibernéticos
	Componentes dentro del alcance	Control de la organización
	Factores de riesgo	Daño excesivo derivado de la preparación cibernética deficiente
Guía de Implementación	Planteamiento del Control	El usuario cuenta con un plan de respuesta a incidentes cibernéticos definido y comprobado
	Contexto del Control	La disponibilidad y la resiliencia adecuada resultan fundamentales para el negocio. A este respecto, definir y probar un plan de respuesta a incidentes cibernéticos es una forma muy efectiva de reducir el impacto y duración de un incidente cibernético real…
	Directrices para la implementación	…

Marco de Controles de Seguridad para el Cliente de SWIFT 2019

2. Implementación en el Banco de la República

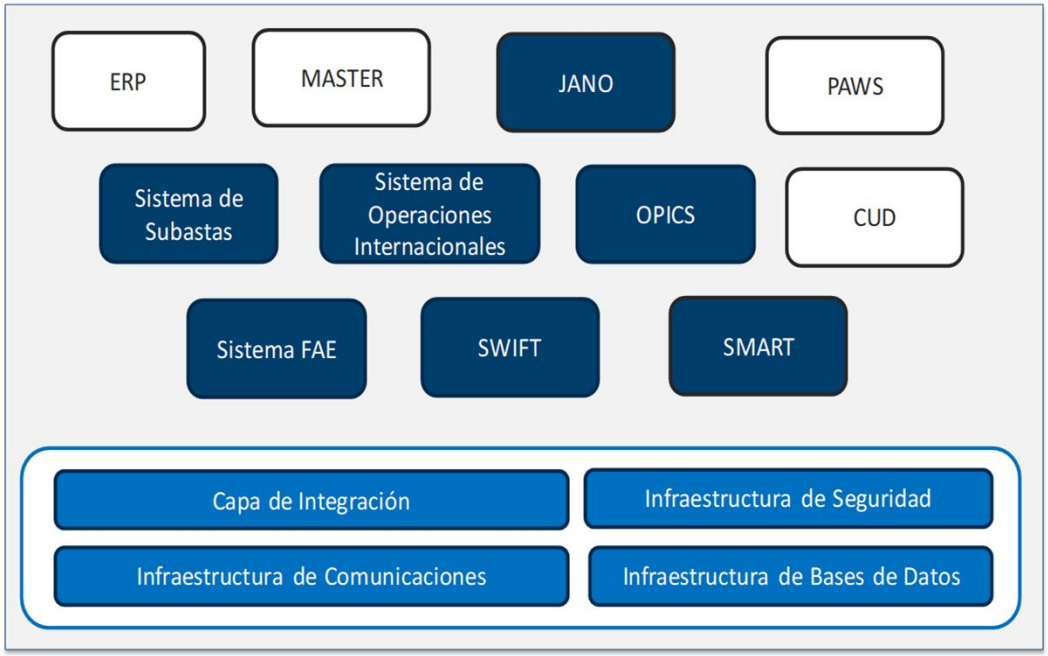
Implementación en el Banco de la República

Proceso de declaración y cumplimiento

Diciembre 31 2017	*Fecha máxima para reportar la autoevaluación del nivel de cumplimiento de los controles obligatorios de seguridad*
Diciembre 31 2018	*Fecha máxima para revaluar y confirmar el cumplimiento de los controles obligatorios de seguridad*

Implementación en el Banco de la República

Arquitectura de Solución Swift en el contexto de TI del BR



El Banco de la República cuenta con más de 195 servicios de tecnología

- 21 servicios de infraestructura
- 28 servicios de capa media
- 144 sistemas de negocio
- múltiples herramientas de monitoreo

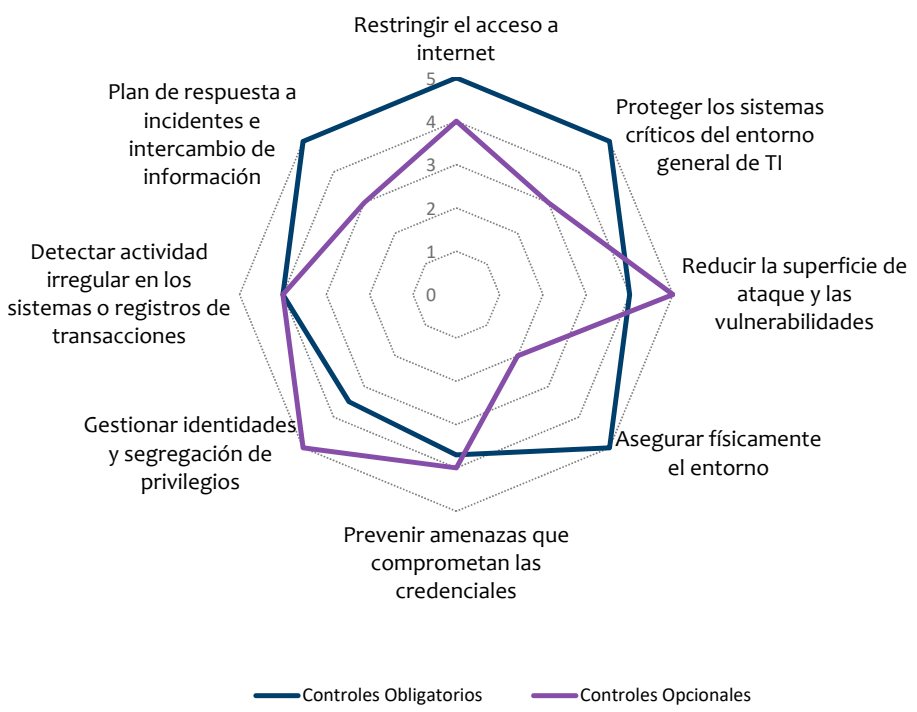
Actualmente 6 sistemas de negocio (aplicaciones) interactúan con SWIFT

Implementación en el Banco de la República

Actividades previas realizadas en el Banco

- Autoevaluación inicial del estado de implementación de controles de acuerdo con el Customer Security Program- CSP de SWIFT
- Evaluaciones externa de seguridad
  - Estaciones de trabajo
  - Infraestructura
- Definición de una estrategia de Implementación : Formulación del Proyecto.

Ejemplo de Autoevaluación Controles CSP en una organización



Implementación en el Banco de la República

Proyecto de Implementación

Objetivo del Proyecto	Lineamiento del Banco
Reforzar controles de seguridad en plataforma de operación crítica (SWIFT) a partir del cumplimiento de los controles mandatorios establecido en el ***Customer Security Program (CSP)***.	**Gestión de Riesgos**: Actuar de manera oportuna y preventiva propendiendo por una respuesta efectiva al riesgo con el fin de apoyar el logro de los objetivos, la toma de decisiones y la continuidad de la operación del Banco

La formulación de un proyecto garantizaba asignación de recursos multidisciplinarios, la coordinación de actividades y la adecuada toma de decisiones

Implementación en el Banco de la República

Proyecto de Implementación

Metas del Proyecto

- Identificar la brecha entre la situación actual y los controles obligatorios del CSP.
- Implementar los cambios necesarios en la infraestructura y operación de negocio para alcanzar los niveles de cumplimiento requerido.
- Completar el proceso de autoevaluación dentro de los límites de tiempo establecidos por SWIFT. En el 2017 y 2018.
- Proponer un proceso para la autoevaluación periódica establecido en el CSP, que se incorpore a las labores regulares de las áreas involucradas.

Restricciones

- La fecha máxima para terminar el proceso de autoevaluación era 31 de diciembre de 2017.
- Los ajustes a la situación existente debían realizarse utilizando de forma eficiente la tecnología disponible y con el menor impacto en la plataforma y procesos de negocio

La formulación de un proyecto garantizaba asignación de recursos multidisciplinarios, la coordinación de actividades y la adecuada toma de decisiones

3. Enfoque de Auditoría al CSP

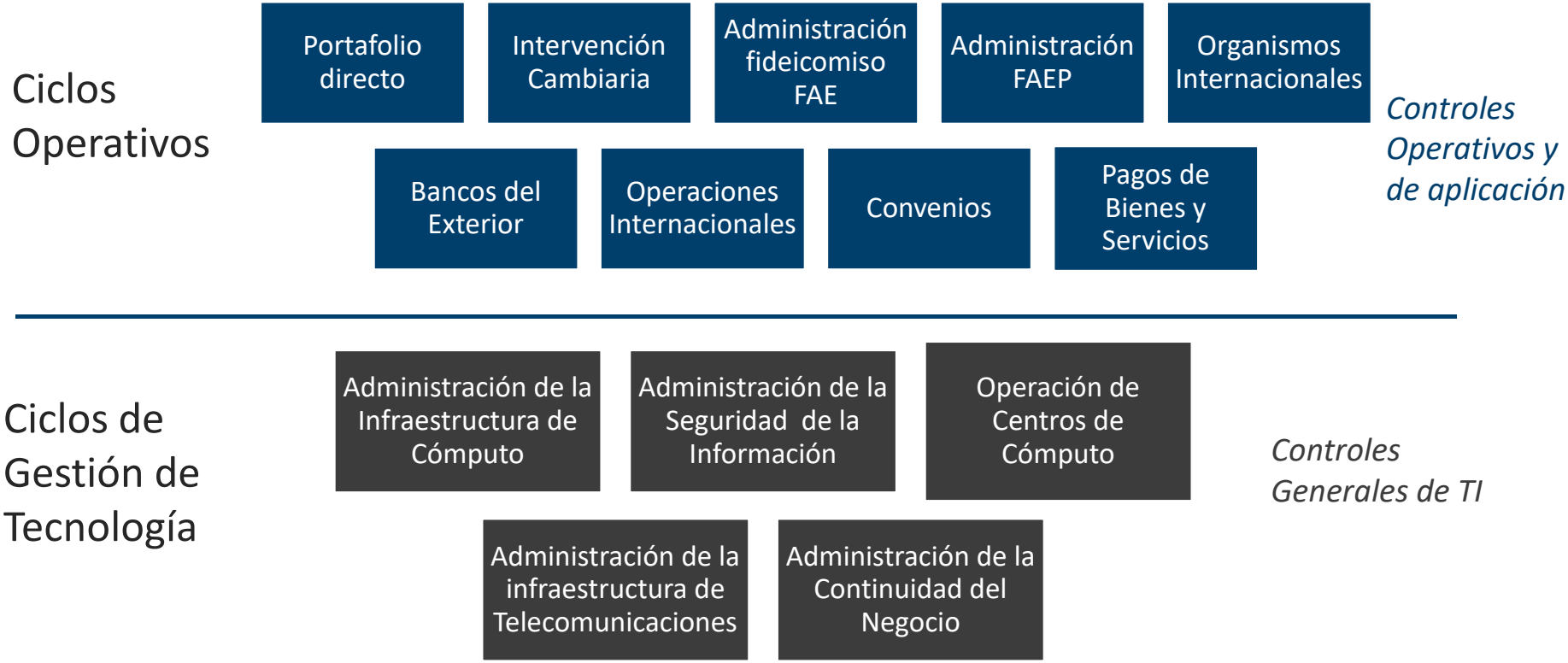
Enfoque de Auditoría al CSP

1. Auditoría a la gestión del Proyecto de Implementación del Programa de Seguridad de Swift (CSP)
   - Cumplimiento de la *autodeclaración* – Diciembre 2017
   - Cumplimiento de la *autodeclaración de cumplimiento* Diciembre 2018
   - Conformación del equipo de trabajo
   - Asignación de recursos
   - Gestión de Riesgos
   - Monitoreo Gerencial
2. Enfoque de Auditoría a los 27 controles
   - Evaluación de controles implementados en el contexto operativo
   - Seguimiento a las actividades asociadas
   - Seguimiento al reporte a los niveles gerenciales
3. Evaluaciones en el Contexto de Ciberseguridad

Visión integradora y coordinación de las diferentes actividades de la Auditoría Informática

Enfoque de Auditoría al CSP

Marco Metodológico de las evaluaciones relacionadas con SWIFT



Enfoque de Auditoría al CSP

Marco Metodológico de las evaluaciones relacionadas con SWIFT

- Portafolio Directo
- Intervención Cambiaria
- Pago de Bienes y servicio
- Administración Fideicomiso FAE
- Bancos del Exterior

- Seguridad Interna del flujo de datos

- Controles Empresariales de Transacciones
  - Conciliación de registros contables y extractos de cuentas

Operaciones Internacionales

- Seguridad del Flujo de Datos del Servicio Interno
- Confidencialidad e Integridad de la sesión del operador
- Control de Acceso Lógico
  - Mínimo Privilegio
  - Segregación de Funciones
  - Gestión de novedades de usuarios
- Controles Empresariales de Transacciones
  - Control de Horarios
  - Envió de mensajes de Confirmación MT 910

Ciclos Operativos

Controles Operativos, Tecnológicos y de Aplicación

Enfoque de Auditoría al CSP

Marco Metodológico de las evaluaciones relacionadas con SWIFT

30/09/2019

Administración de la Infraestructura de Cómputo

- Control de Cuentas Privilegiadas del Sistema Operativo
- Fortalecimiento del Sistema
- Política de Contraseñas
- Autenticación de Múltiples Factores
- Integridad de la Base de Datos

Operación de Centros de Cómputo

- Seguridad Física

Administración de la Continuidad del Negocio

- Planeación de Respuesta a Incidentes Cibernéticos

Administración de la infraestructura de Telecomunicaciones

- Protección del Entorno de SWIFT

Administración de la Seguridad de la Información

- Protección del Entorno de SWIFT
- Protección contra Malware
- Integridad del Software
- Log de información y Monitoreo
- Detección de Intrusiones
- Almacenamiento Físico y Lógico de Contraseñas
- Planeación de Respuesta a Incidentes Cibernéticos
- Capacitación y Concienciación en Temas de Seguridad
- Pruebas de Penetración
- Evaluación de Escenarios de Riesgo

Ciclos de Gestión de Tecnología

Controles Generales de TI

Enfoque de Auditoría al CSP

Evaluaciones en el Contexto de Ciberseguridad

Auditoría al Proceso de gestión de seguridad de la información.

- Auditoría al Programa de Ciber-Seguridad Corporativo alineado con marco referencia NIST
- Auditoría al Programa de Sensibilización (Personas-Procesos-Tecnología).
- Auditoría a la Seguridad de la infraestructuras críticas del Banco (Swift y otros Sistema de Pagos)
- Auditoría a la implementación de los controles críticos de ciberseguridad (20 controles CIS)
- Auditoría al Sistema de Gestión de Seguridad de la Información – SGSI basado en la norma ISO 27001.

Enfoque de Auditoría al CSP

Evaluaciones en el Contexto de Ciberseguridad

Auditoría al Proceso de gestión de seguridad de la información.

- Auditoría al Cumplimiento normas y regulaciones: Superintendencia Financiera y Leyes de Delitos informáticos y Protección datos personales
- Auditoría a la Configuración, administración y funcionamiento de los controles operativos y tecnológicos de seguridad informática.
- Auditoría a las actividades de análisis de los incidentes de seguridad, pruebas de hacking ético y gestión de vulnerabilidades.
- Visita instalaciones proveedor del servicio de monitoreo de seguridad 7x24 – SOC (Security Operation Center).

Conclusiones

- El Programa de Seguridad de SWIFT (CSP) robustece la estructura de control de la plataforma Swift minimizando los nuevos riesgos de ciberseguridad.
- Es un labor continua y permanente que incorpora el análisis de las nuevas amenazas y vulnerabilidades de riesgo cibernético.
- La Auditoría al CSP es un enfoque integral y permanente apoyado en las evaluaciones a los ciclos operativos y de gestión de tecnología informática.