Universidad de Buenos Aires

Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Seguridad en Sistemas Críticos, SWIFT

Autor: Ing. Gustavo Nicolás Morey

Tutor: Mgr. Juan Alejandro Devincenzi

Presentación: Octubre 2019

Cohorte: 2017

Declaración Jurada de origen de los contenidos:

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO

Resumen

El presente trabajo trata sobre la seguridad en el sistema SWIFT. Los múltiples ataques recibidos requieren que profesionales de la seguridad verifiquen el sistema detalladamente y en forma periódica. Para esto debemos empezar por el principio: SWIFT nunca fue atacado, fueron los bancos que utilizan el servicio. El ataque al *Swift Alliance Access* del Banco Central de Bangladesh fue el costo para detectar que el sistema de transferencias mundiales necesitaba ajustar su eslabón más débil en todo el mundo : las entidades. Este trabajo utiliza el método de análisis de capas para visibilizar las partes del sistema instalado en las entidades y plantea los riesgos asociados a los controles de varias normas de seguridad de sistemas informáticos. Se recopilan ataques reportados a entidades y sus controles comprometidos. Concluimos en este trabajo que los ataques a las entidades son del tipo *Advanced Persistent Threat* y que los RRHH correctamente preparados en conocimientos y procedimientos, en todas las áreas en relación al sistema crítico, son la mejor protección para cadenas productivas informatizadas.

Palabras claves: SWIFT, APT, SAA, Sistema Crítico, SC, Bangladesh, Alliance, *Advanced Persistent Threat*.

1. Primera Parte. Presentación del rompecabezas SWIFT

1.1 Estudio y empatía

La primera tarea del profesional de Seguridad Informática es ponerse en contacto con el sistema crítico a trabajar y los sectores que lo utilizan. El presente estudio analiza la seguridad en los sistemas críticos y utiliza como guía el sistema de transferencias electrónicas SWIFT.

Uno de los errores más comunes cuando se trata de asegurar un sistema crítico es preguntar por datos técnicos como por ejemplo, los protocolos y puertos. Luego con esta información se configuran los equipos de protección perimetral y los analizadores de eventos para esperar los mensajes de alertas en el correo, dando así por finalizada la tarea de seguridad. Generalmente, esta forma de trabajar pretende bloquear todos los servicios y parecería que apagar el sistema es la única opción segura, dando a entender que cualquier puerto permitido es una vulnerabilidad insalvable y no necesariamente es así.

El primer subproblema que se presenta es estudiar los requerimientos técnicos que recomienda el proveedor del sistema crítico (en adelante, “SC”) y sus opciones de configuración. El segundo subproblema es conocer cómo se utiliza en la organización, entender las necesidades del área operativa que utiliza el SC y cómo aportar valor a la entidad.

En tareas de Seguridad Informática (en adelante, “SI”) es recomendable desarrollar todas las herramientas que estén a nuestro alcance para lograr una comunicación fluida, transparente y fundamentalmente confiable con las partes operativas. Probablemente, los elementos se encuentran técnicamente bien asegurados, y aun así es necesario un cambio en los procedimientos para minimizar algún riesgo elevado existente; aquí es donde necesitamos la empatía para comprender,

negociar y producir el cambio propuesto o fundamentar la reevaluación del riesgo detectado en el análisis.

1.2 Primeros pasos

1.2.1 ¿Quién es SWIFT?

Society for Worldwide Interbank Financial Telecommunication (SWIFT) es una empresa cooperativa – sin fines de lucro - formada por miembros del mercado financiero: Bancos y otros. Con sede en Bélgica, su objetivo primario es brindar comunicaciones seguras para transportar instrucciones financieras entre sus miembros [1].

SWIFT fue creada el 3 de mayo del año 1973 por iniciativa de 200 entidades en 15 países, a fin de asegurar las comunicaciones internacionales financieras y expandir el negocio de manera segura: SWIFT comunica a la entidad miembro con las demás en el mundo, relacionándolas para hacer negocios financieros de distinto tipo.

El objetivo primario de la red SWIFT es garantizar la seguridad en las comunicaciones, controlando la autenticidad y confidencialidad de la información enviada y manteniendo una disponibilidad de los servicios cercana al máximo. En el año 1977 operó por primera vez y contaba con 500 miembros en 22 países. Ese primer año se traficaron 10 millones de mensajes. Más tarde, en los 80, la red traficaba 50 millones de mensajes de transacciones financieras por año [2].

Hoy, la red cuenta con más de 11.000 miembros en 200 países y territorios y transporta siete mil millones de mensajes anuales; la disponibilidad desde enero a junio de 2019 era de 99,999% [1]. Los números indicadores de SWIFT acompañan el crecimiento global de la economía, la definición de nuevos productos y la incorporación de nuevos mercados a la red. Estos números hablan de la criticidad del sistema SWIFT dentro del

mercado financiero mundial.

Actualmente SWIFT brinda comunicaciones financieras internacionales seguras, transporte seguro de sistemas de pagos, productos que dan valor a instituciones financieras o regiones económicas, frente a otros actores en el escenario financiero mundial. También ofrece servicios a corporaciones globales para que accedan a las entidades financieras, utilizando un mismo idioma mundial: los mensajes SWIFT.

1.2.2 Funcionamiento básico

Como se detalló, SWIFT es el actor que define, controla, mantiene y desarrolla los elementos necesarios para asegurar que el banco que dice ser A es A, que el banco B es B y que los mensajes fueron enviados y recibidos correctamente (o no) en las comunicaciones financieras que transitan la red. SWIFT es quien establece los procedimientos, las herramientas y mecanismos para asegurarse que solo ambos extremos, origen y destino tienen acceso a la información. Los miembros depositan la confianza en el sistema SWIFT en las tareas descriptas y deben cumplir con los requisitos obligatorios para beneficio de todas las partes que intervienen en el sistema y que también son los dueños de la cooperativa.

SWIFT no manipula ni custodia fondos de sus miembros, solo transporta de forma segura las órdenes de negocio enviadas de A hacia B mediante un esquema de mensajes para las diferentes operaciones de negocios de los actores financieros. SWIFT interconecta a los actores financieros del mundo implementando mecanismos de confidencialidad, autenticidad y disponibilidad de la información transportada. La confidencialidad de la información se logra mediante su encriptación, con certificados PKI administrados por SWIFT. La estructura PKI permite que los mensajes cifrados con clave pública sean descifrados por la clave privada correspondiente. Mediante el mantenimiento adecuado del certificado de

cifrado y descifrado garantizamos la confidencialidad de la información. Los miembros de la red pueden revocar certificados que fueron comprometidos y también crear nuevos, entre otras funciones, desde el portal correspondiente.

La autenticidad de los mensajes financieros se logra a través de certificados digitales para la firma de la información. SWIFT provee varios certificados de firma electrónica que utiliza en distintas etapas de las comunicaciones entre ella y la entidad, a fin de implementar el no repudio y certificar la autenticidad de la mensajería.

La red SWIFT asegura la disponibilidad de la información mediante varios mecanismos y en diferentes sectores de su sistema. Por ejemplo, los elementos de conectividad VPN son redundantes en alimentación, equipamiento y conectividad entre otras funciones. A nivel de instalación del sistema, SWIFT recomienda al usuario tener sistemas independientes para que trabajen con redundancia ante inconvenientes. Dentro de la red de SWIFT el proceso de Store-And-Forward cumple un papel clave: hasta que la información no sea aceptada por el nodo siguiente, no se descarta del anterior.

En el último año se trabajó mucho en la tecnología empleada para agilizar el movimiento de las transacciones, contemplando su importante volumen creciente. En la estructura de la red de SWIFT hay centros de conmutación y almacenamiento donde la mensajería es ruteada hacia sus puntos de salida. Ya en la cola de salida, el banco receptor puede ordenar la mensajería según diferentes criterios y esperar la disponibilidad del sistema instalado para entregarla en el orden de prioridades establecido previamente. Luego, ya en la entidad destino, la información financiera entregada por SWIFT es procesada internamente. Una orden transportada por SWIFT tarda segundos, o decenas de segundos para cruzar el globo. De

todas maneras, los mercados tienen horarios de operación específicos y establecidos por su regulador. Por ejemplo un mensaje desde Argentina a China puede llegar en segundos, pero ambos mercados operan con 12 horas de diferencia aproximadamente.

1.2.3 Entidades y mercado regulado por autoridades

Los actores del mercado financiero son entidades que manejan el capital de terceros y por esto regulados por la autoridad competente. En la República Argentina el mercado financiero está regulado por el Banco Central de la República Argentina (BCRA) estipulando sus funciones en la carta orgánica de la institución (Ley 24144, sancionada el 23/09/1992 y sus posteriores modificaciones) [3]. Las entidades adecuan su funcionamiento y riesgos a lo establecido por ley y normas del ente regulador.

1.2.4 Cómo conectarse a la red SWIFT. De qué manera ser parte de la red

SWIFT es una red que está disponible para entidades y organizaciones financieras que cumplan con los requisitos legales de sus respectivas jurisdicciones.

Para conectarse a la red se debe solicitar el ingreso a la asociación cooperativa SWIFT presentando los documentos requeridos que avalen la condición legal de la entidad como parte del mercado financiero. La solicitud será tratada por el órgano máximo de la cooperativa; una vez aprobada la solicitud, la entidad puede adquirir las licencias que requiera para formar parte de la red SWIFT. Regularmente SWIFT requiere presentar la documentación actualizada que certifique el estado de entidad financiera.

La entidad debe definir al menos dos representantes frente a SWIFT denominados oficiales de seguridad. Los oficiales de seguridad configuran los certificados digitales que identifican a la entidad en la red y la

representan legalmente frente a SWIFT.

1.3 Análisis el rompecabezas SWIFT

1.3.1 Primera pieza clave: conectividad a SWIFT

La conectividad se realiza mediante varios productos, que veremos en diferentes momentos del análisis. Uno de ellos es la conectividad vía VPN mediante soluciones *Swift Alliance Connect* [4]. SWIFT ofrece diferentes alternativas de conectividad e Internet es una de ellas desde hace pocos años [5]; otra alternativa utiliza líneas directas [6]; también hay soluciones de conectividad que mezclan líneas directas y líneas de Internet.

Los sistemas de comunicaciones SAC están formados por equipos terminadores de túneles que encriptan la información a enviar y se pueden conectar a múltiples proveedores de comunicaciones, ya sean de líneas directas y/o de servicios de Internet en función del producto elegido.

Otra opción para resolver el problema de la conectividad son las empresas autorizadas y auditadas regularmente por SWIFT, los *Service Bureau* [7] (SB) ofreciendo el servicio de acceso a los servicios de SWIFT. Además, las entidades financieras conectadas directamente a SWIFT pueden colaborar con otras para facilitarles el acceso a la red, compartiendo la infraestructura de conectividad. La opción del SB puede ser la mejor inicialmente en función del conocimiento específico necesario para realizar los primeros pasos en SWIFT.

La porción SAC del sistema, permite acceder a la red segura de SWIFT para transportar los paquetes en su red segura, *Secure IP Network* (SIPN) [16] y así poder utilizar el protocolo de servicios de la red SWIFT. Las cajas VPN, SAC, son la frontera física entre la institución y el proveedor de comunicaciones , son también la frontera lógica entre la institución y SWIFT mediante un canal virtual directo.

1.3.2 Otra pieza clave: cómo generar la mensajería financiera

La familia de software propuesto por SWIFT para administrar la mensajería financiera enviada y recibida por el banco se llama Swift Alliance Access [10]. La familia de gestión de mensajería, tiene un hermano mayor y otro menor, son Alliance Messaging Hub [11] y Swift Alliance Entry [12], respectivamente. También hay alternativas para gestionar la mensajería que son generadas por terceros y aprobadas por SWIFT. Para nuestro objetivo, esta familia de software, o su equivalente, se comporta de manera similar y lo llamaremos herramienta de gestión de mensajería financiera, SAA.

El SAA, recibe la información desde el Back Office (BO) en forma manual o automática y crea la mensajería para su futuro tratamiento mediante el gestionador mensajería SAA. Una vez creada la mensajería se verifica mediante el contraste de valores en campos específicos. Si el mensaje creado es verificado correctamente puede enviar la orden a SWIFT o en su defecto, puede existir un paso más que se llama autorización. La autorización no requiere contrastar campos, es una inspección visual de la orden a enviar. Una vez autorizado el mensaje es enviado al corresponsal a través de la red. Los operadores o procesos que detecten un error en la información de la orden, la pueden modificar y el proceso de verificación/autorización se inicia nuevamente.

El flujo desde la creación, hasta la salida del mensaje, depende de cómo fue programado el tratamiento de las órdenes en la institución financiera.

Antes de acceder al medio de comunicación presentado como SAC, el SAA envía la información al siguiente software en la cadena que trabajará con los certificados y encriptaciones correspondientes. Estos son el SWIFT Alliance Gateway (SAG) [13] y el SWIFT Net Link (SNL) [14].

1.3.3 Completando el eslabón perdido entre SAA y SWIFT

Hasta aquí se presentaron dos partes importantes que forman el SC SWIFT a analizar en este trabajo: la gestión mediante el SAA y conectividad VPN a SWIFT mediante el SAC.

El SAA es la gestión de la mensajería financiera generada en la institución y el SAC es la conectividad VPN segura entre SWIFT y la institución mediante proveedores locales de comunicaciones e internet.

En los siguientes párrafos uniremos ambas partes, SAA y SAC mediante el eslabón perdido. Tal como se mencionó, SWIFT brinda a las entidades la funcionalidad de interconexión segura con el objetivo primario de intercambiar mensajería financiera. Si bien la entidad A envía un mensaje financiero a la entidad B, está implícito que la comunicación se realiza mediante los servicios de SWIFT. No hay una conexión directa entre A y B, existe un tercero transparente: SWIFT. El software de SWIFT no es un aplicativo que cumple su función aisladamente dentro de la institución.

SWIFT realiza, entre otras tareas, la conmutación de la mensajería, recibe la mensajería de A y en función de su destino, la entrega en B. Por esto último podemos asegurar que SWIFT es el primer servicio en la nube que existe previo a Internet. Antes de la existencia de SWIFT cada entidad financiera necesitaba un vínculo para conectarse con otra, la herramienta utilizada era el Telex mediante líneas analogicas. El resultado de la red vía Telex era del tipo mesh con un crecimiento exponencial de líneas, claves, tipos de sistemas de comunicaciones y problemas de seguridad, principalmente en las grandes entidades financieras que ofrecían servicios a otras. La solución de la cooperativa SWIFT resuelve parte de los problemas mediante un único vínculo de conectividad.

Los servicios que brinda SWIFT en el punto central se materializan mediante el protocolo de SWIFT utilizado por las entidades conectadas. La

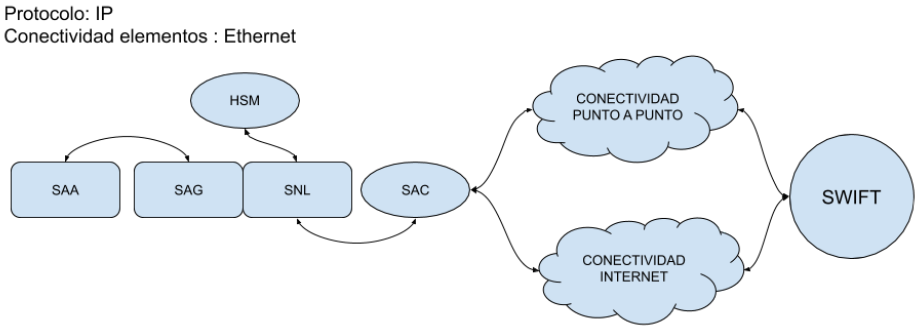
porción de software que implementa el protocolo en la entidad se denomina SWIFT Net Link (SNL). El SWIFT Alliance Gateway (SAG) es el eslabón entre la implementación de los servicios (SNL) y el software que gestiona la mensajería (SAA). El SAG ofrece una interfaz al SAA para realizar el proceso de envío y recepción de la mensajería financiera. Las respuestas del sistema central de SWIFT enviadas al SNL se entregan al SAG y así llegan las órdenes al SAA.

1.4 SWIFT en la nube

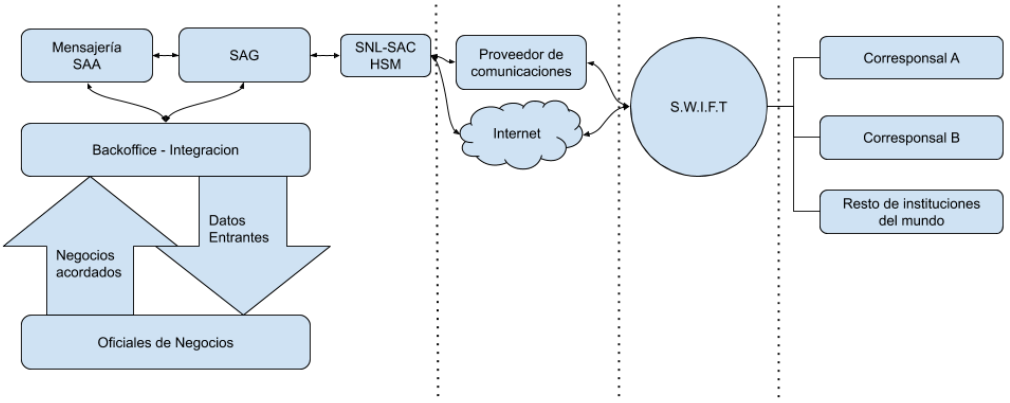
Además de los servicios de conmutación segura que emplean las entidades que utilizan un gestionador del tipo SAA, SWIFT ofrece servicios en la nube tanto para gestionar mensajería como para la conectividad. Técnicamente, estos productos pueden utilizarse como redundancias de los sistemas instalados o como medios de producción. En este segundo caso, la ventaja es no necesitar inversiones en equipamiento, licencias, personal y soporte especializado en SWIFT. La ventaja de la instalación local de los elementos de SWIFT es la configuración personalizada que puede hacer la entidad en cuanto a servicios y funcionalidades, agregando valor en la entidad dentro de su mercado frente a otras entidades. Cada entidad deberá analizar junto a las normativas locales que correspondan cuáles son los servicios normativamente factibles.

1.5 Ensamblaje de piezas

En función de lo analizado hasta aquí, se presentan los elementos en el siguiente gráfico:



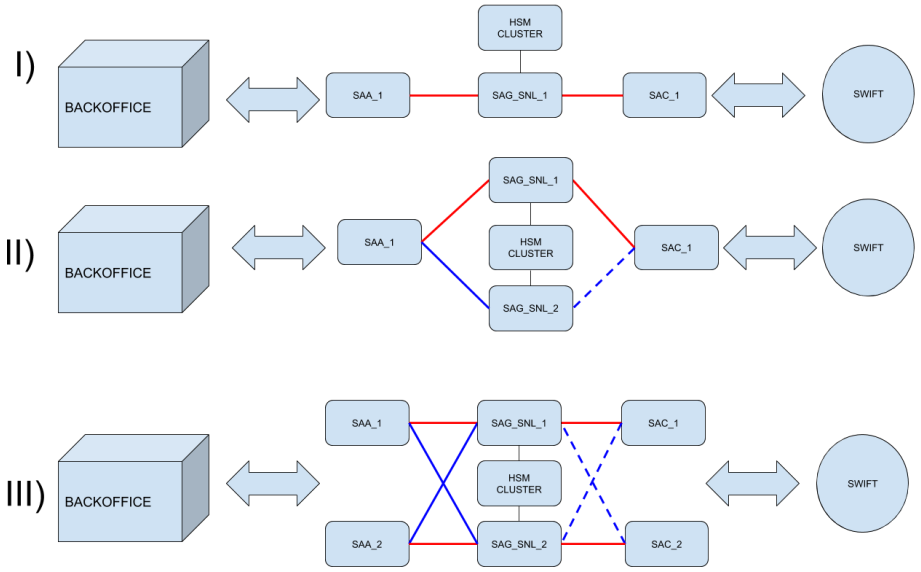
El SAA interactúa con el BO intercambiando la mensajería a enviar y recibir mediante la red.



Con respecto a la redundancia de elementos, en la figura siguiente, la cadena I) de elementos es la cadena simple, la cadena II) tiene redundancias de conectividad, mientras que la cadena III) tiene redundancias de conectividad y de software para gestionar la mensajería.

SWIFT permite la creación de *clusters* en los HSM y también de *clusters* de servidores donde se instala el software.

Otros ítems para agregar al rompecabezas son: el soporte de red, la interacción con los recursos humanos, los procedimientos que afectan a la



utilización de esta estructura de servicios, las diferentes áreas y gerencias con injerencia en el sistema SWIFT y en el mantenimiento de la red, hardware, sistema operativo e infraestructura SWIFT; el monitoreo del funcionamiento y de controles de seguridad, la conectividad con otros sistemas, el acceso de usuarios, verificadores y autorizadores. Todo ello en cumplimiento de las normativas del regulador del mercado, las leyes y las directivas internas de la institución.

No menos relevante será preparar a diario los datos para auditoría y el análisis de riesgos de la entidad. Trataremos estos temas en el siguiente capítulo, utilizando un marco que identifique los riesgos y genere puntos de control.

2. Segunda Parte. Análisis

2.1 Marcos y normas

La norma IRAM-ISO/IEC 27001[1] Requisitos para Gestión de la Seguridad de la Información [16] propone más de cien controles de seguridad. La norma *Framework for Improving Critical Infrastructure Cybersecurity* V1.1 2018[2] [17] y la norma, emitida por el Banco Central de La República Argentina, el texto ordenado "Requisitos Mínimos de Gestión, Implementación y Control de los Riesgos Relacionados con la Tecnología Informática, Sistemas de Información y Recursos Asociados para las Entidades Financieras"[3] [18] otros tantos más. Pretender aplicarlos en el análisis inicial es motivo de estancamiento y bloqueo en el curso de la tarea, además de costoso. A pesar que cada control apunta a temas diferentes, en un primer momento se realiza una aproximación a un conjunto limitado de controles que permitan visibilizar el estado inicial de la SI referente al sistema crítico.

El análisis y aplicación de la primera selección de controles ayuda a descubrir la metodología a emplear en nuestro SC. En posteriores iteraciones - ponderando los controles posibles en función de las políticas de seguridad de la entidad- se corregirá la primera aproximación realizada. Se deben priorizar las regulaciones dictadas por la autoridad del mercado, los requisitos de SWIFT y las normas que correspondan para evitar sanciones que dañen la reputación de la institución.

Como respuesta a los eventos de seguridad registrados en el año 2016, SWIFT desarrolló un programa que consta de tres partes. La primera parte es una guía de buenas prácticas para asegurar la infraestructura en

[1] 27001 en adelante

[2] NIST en adelante

[3] TO SGSI en adelante

cada institución, con puntos de control opcionales y otros obligatorios. La segunda parte es una autoevaluación o evaluación externa del estado actual de los controles específicos del sistema SWIFT; esta evaluación es compartida en la comunidad con la contraparte que lo solicite. La tercera parte es la publicación de análisis de eventos de seguridad a fin de prevenir y alertar a las entidades de la red sobre nuevas metodologías detectadas en los ataques a las instituciones financieras.

Este trabajo realiza un análisis del SC SWIFT mediante modelos de capas definidos más adelante, desglosando al sistema SWIFT. Este análisis puede ser un modelo aplicable a cualquier sistema siguiendo los mismos pasos, sea o no parte de una institución financiera para detectar sus componentes.

2.2 Metodología empleada

El análisis contempla una fase inicial y cuatro ejes. La fase inicial consta de la primera tarea mencionada en todas las normas de seguridad: Identificación y relevamiento de activos. Con respecto al relevamiento de los activos, la norma del BCRA [18] reglamenta la existencia del inventario de activos en el punto 5.2 Inventario Tecnológico donde se clasifica la información en recursos de software, recursos de información, activos físicos y servicios descentralizados.

Los siguientes cuatro ejes del análisis propuesto se agrupan según los cuatro actores de la herramienta de negocios SWIFT en su operación: primero, el gobierno y sus normas, desde donde emanan las bases que materializan la seguridad de cada institución; segundo, la operación del sistema SWIFT, los roles del SC y los procedimientos de negocio de la institución; tercero, la infraestructura y su conocimiento, y por último, el eje

seguridad que incluye el tratamiento de eventos, monitoreo, verificación de controles y otros temas. La auditoría del sistema atraviesa los cuatro ejes.

Se desarrollan dos análisis del tipo de capas, *top-down*, donde definiremos dominios que nos ayudan a visibilizar las partes del sistema tanto para el análisis orientado al negocio como a la infraestructura, teniendo como principal capa a proteger aquella que contiene los datos.

2.3 Fase inicial: partes del sistema

Cómo mencionamos la norma TO SGSI del BCRA, el punto 5.2 Inventario tecnológico, contempla:

- Recursos de software
- Recursos de información
- Activos físicos
- Servicios tercerizados

Además de esta valiosa discriminación al realizar el inventario, la norma TO 4609 del BCRA, en su punto 5.2 Inventario tecnológico, detalla la importancia de identificar al propietario del activo y el nivel de criticidad de cada activo detectado.

El propietario del activo se define en la norma Política de Seguridad de la Información Modelo del ONTI [9], Propietario de la Información, que define a la persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información.

Se proponen como guía los siguientes puntos a relevar para la identificación de los activos del SC SWIFT.

➢ Recursos de software:

- Sistema Operativo.

- Herramientas de software empleadas en procedimientos de controles, Firmware de hardware empleado, relevamiento de versiones, configuraciones y funcionalidades como accesos remotos, USB, modos de arrancar, etc.
- envíos, etc.
- SWP, software de SWIFT, interfaz con cliente usuario.
- Software Integrador de *Back Office* con gestionador de mensajería financiera
- Software de Gestión de mensajería financiera, SAA
- Software de Comunicaciones, SAG, SNL
- Servicios de Autenticación
- Servicios de File Server
- Servicios de Impresión
- Otros servicios.

➢ Recursos de Información:

- Manuales
- Listados de problemas conocidos y su tratamiento
- Planos, diagramas.
- Procedimientos de mantenimiento
- Procedimientos de envío y recepción de mensajería financiera
- Métricas históricas
- Auditorías realizadas
- Relevamientos
- Fe de erratas

➢ Activos físicos:

- Estaciones de trabajo que acceden a los activos físicos
- Servidores SWP
- Servidores SAA
- Servidores SAG,SNL
- Servidores de integración
- Servidores de servicios
- Impresoras
- Equipos de Comunicaciones (SAC, etc.)
- Vínculos de datos
- *Switches* que forman las VLANs del sistema
- *Switches* por donde pasa el troncal de VLAN del sistema
- Elementos de seguridad (Firewalls, etc.)
- Otros equipos de conectividad
- Soportes de certificados PKI
- Soportes de autenticación de doble factor
- Infraestructura de soporte

➢ Servicios tercerizados:

- Soporte especializado SWIFT
- Mantenimiento edilicio, infraestructura
- Proveedores de mantenimiento de hardware de estaciones y servidores
- Proveedores de equipos de comunicaciones y sus servicios
- Proveedores de cableado
- Proveedores de vínculos

Se debe contemplar un conjunto de activos para producción y las correspondientes redundancias tanto de de servicio como edilicias. También se deberán contemplar los activos destinados a pruebas y a educación, si fuera requerido por la entidad.

Respecto al propietario de la información y de los activos, ambos roles son los generadores de novedades sobre el SC. Son roles responsables frente a la institución y deben trabajar coordinadamente para mantener la seguridad del SC. El propietario de la información, o de los datos, está más cerca de los negocios y creación de valor con la herramienta de negocios SWIFT. El propietario de los activos está más cerca de la infraestructura donde reside el soporte del SC.

La norma TO SGSI se refiere al propietario de activos, datos y procesos. El propietario de los procesos deberá proporcionar procesos actualizados a todas las partes: negocios, sistemas y seguridad. Los procedimientos deben generar una base documental para el posterior control de auditoría y evaluación resultados verificando el SC en un estado de riesgo deseado por la entidad.

2.4 Eje I: Gobernanza

Uno de los puntos críticos en seguridad es el grado de conciencia sobre su importancia en la institución. Hoy nadie puede ignorar que la tecnología empleada y sus métodos exponen la cadena de generación de valor a riesgos que la pueden afectar. En todos los mercados la tecnología es la herramienta de administración de las tareas productivas. En el mercado financiero, la tecnología empleada es también el depósito de la materia prima: los datos. De aquí la necesidad de estudiar los riesgos metódicamente para tenerlos presentes, detectados, evaluados, controlados y mitigados.

La minuciosidad del análisis para detectar riesgos, el grado de conciencia en temas de seguridad en la institución y su madurez cultural son factores necesarios de éxito en tareas de seguridad informática.

El Banco Central de la República Argentina, por medio de la norma TO SGSI [18], menciona la obligatoriedad de la existencia de políticas de seguridad que manejen los riesgos producidos por la tecnología empleada en la institución, responsabilizando así a la alta gerencia [18, punto 2.2].

La norma IRAM-ISO/IEC 27001 requiere que las políticas de seguridad sean definidas por los altos mandos de la organización, mostrando conciencia y decisión, liderando así las acciones respecto a la seguridad que las diferentes gerencias de la organización deben aplicar [16, punto 5 Liderazgo].

El marco desarrollado por NIST [17], en el apartado de *Governance* ID.GV-1 al 4 detalla puntos a relevar en la institución sobre la política de seguridad. Menciona la definición clara de la política y su comunicación al resto de la institución [17, ID.GV-1], los roles y responsabilidades definidas [17, ID.GV-2], las regulaciones [17, ID.GV-3] y los procesos de análisis de riesgos [17, ID.GV-4]. La renovación tecnológica hace imprescindible un análisis periódico de las políticas de cada institución.

2.5 Eje II: roles, RRHH, segregación de funciones, roles de negocio

Esta etapa analiza los roles que impactan en el SC SWIFT. En el análisis de capas propuesto a continuación se detectan los roles necesarios del SC para la parametrización de los elementos y la operación. La norma IRAM-ISO/IEC 27001 Tecnología de la información [16] en el control A6.1.2 menciona la necesidad de realizar la segregación de funciones teniendo en cuenta obligaciones y responsabilidades incompatibles. También lo menciona el marco originado por NIST, *Framework for Improving Critical*

Infrastructure Cybersecurity, en el punto PR.AC-4 [17]. La norma NIST propone el tratamiento de segregación de permisos y autorizaciones, utilizando los principios de menor privilegio y la separación de responsabilidades.

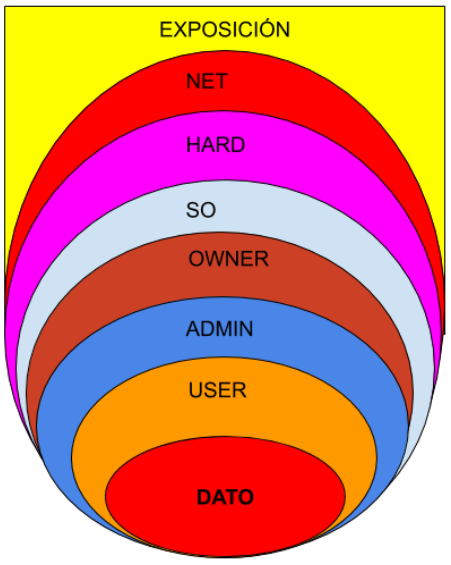
El marco regulatorio para el mercado bancario dispuesto por el BCRA en nuestro país detalla una segregación de tareas y de tareas incompatibles, en el apartado “2.5.4 Actividades y segregación de funciones. Incompatibilidades”, norma TO SGSI [18].

La segregación de tareas busca evitar la concentración de permisos como primera medida. Asimismo, esta segregación genera controles de la información en el flujo de tareas. La primera función es evitar la existencia de un superusuario en los hechos, donde el compromiso de las credenciales concentradas pone en riesgo a todo el sistema. Este riesgo también afecta a los socios de negocios de la institución y al mercado donde se desempeña en el caso del SC SWIFT. La segunda función aporta un valor agregado muy importante que es el autocontrol del flujo de la información procesada: control y seguimiento de la información en las diferentes etapas del proceso productivo.

Si se contempla la dinámica diaria en la operación del sistema mediante las áreas negocios, infraestructura, seguridad, auditoría y otras, cada una de ellas deberá implementar la segregación de tareas, según corresponda, asegurando el flujo de la información.

2.5.1 Análisis de capas *Top-Down* I: visibilización de roles

El siguiente análisis intenta detectar las capas donde los roles se involucran en el funcionamiento de los activos del SC. Utilizamos el sistema de capas, avanzando desde el exterior hacia los mensajes financieros.



Dominios detectados en un sistema informático por análisis de capas:

EXPOSICION: Capa de contacto a otros sistemas, y sistemas usuarios. Funcionalidades y servicios de elementos internos a la red de servicio. Contacto con otras redes de servicios como backoffice, Internet, red de PCs, clientes y proveedores de la institución.

NET : Configuraciones de red en firewalls, switches, cables, routers, wireless, IOT, etc, que forman la infraestructura de comunicaciones la red de servicio y también a los elementos que no forman parte del servicio crítico que están en contacto con el sistema.

HARD : Configuración y definiciones sobre el comportamiento del soporte físico donde la aplicación y sus clientes residen. Soportes electrónicos de datos, sistemas y servicios.

SO : Configuración de sistema operativo donde reside la aplicación y sus clientes. servers, estaciones, smartphones, etc.

OWNER : Usuario de SO que tiene la potestad de modificar el sistema instalado aplicando upgrades y realizar tareas de mantenimiento. Es el usuario de menor privilegio que permite el funcionamiento y configuración del sistema.

ADMIN : Configuración del software de negocios. Definición de perfiles, modificaciones de comportamiento, definición de puntos de contacto e interrelaciones con otros sistemas, etc.

USER : Usuario del software de negocios con permisos de operación.

DATO : Los datos que trabaja y almacena el sistema crítico manejados por los usuarios.

Se define a cada capa del modelo como dominio. Cada dominio detectado contiene un conjunto de elementos que tienen funcionalidades en común y en ellos identificamos los roles presentes que afectan al funcionamiento y seguridad del SC.

La capa superior del modelo es el dominio EXPOSICIÓN, que representa al exterior del activo. La capa inferior del modelo corresponde al conjunto de datos a proteger. El dominio de los datos se define con el nombre DATO. En cada activo que forma el SC, los dominios intermedios entre EXPOSICIÓN y DATA pretenden proteger y dar funcionalidad a la información del dominio DATO.

Descripción de los dominios

EXPOSICIÓN: todo lo externo al activo en contacto lógico o físico con el. Puede ser parte del mismo SC. Es el conjunto de elementos o servicios

que pueden interactuar con el activo.

NET: agrupa a todos los roles de elementos de infraestructura que permiten la interacción del activo crítico, sus protecciones y las configuraciones de conectividad del activo.

HARD: es la porción física del activo, su hardware. Se considera también su entorno físico de infraestructura. Detectamos aquí los roles referentes al mantenimiento de la porción física del activo.

SO: es la capa del sistema operativo del activo. Este dominio se centra en el software del sistema operativo, su administración, funcionamiento y lo referido a herramientas de virtualización, si existieran.

OWNER: representa los permisos mínimos del dominio SO para que la porción de software del SC cumpla sus funciones en el activo que corresponda.

ADMIN: son los roles de parametrización del sistema. Se representan en este dominio los roles de parametrización y mantenimiento de la herramienta que corresponda.

USER: son los roles de negocio. El dominio USER representa a los roles de usuario de las herramientas que forman el SC. Mediante funciones de los roles de negocio aplicadas al dominio DATO se genera valor para la institución.

DATO: es el dominio que representa la información que utiliza o genera el SC.

Cada uno de estos dominios contiene riesgos de distinta naturaleza. Solamente visibilizando los roles y sus entornos podemos reconocer, identificar y tratar los riesgos generados.

2.5.2 Detección de roles en los diferentes dominios del modelo de capas

En el caso del SC SWIFT, el dominio DATO representa principalmente a la información relacionada con la mensajería financiera, pero también son los resguardos de datos históricos, credenciales y todo dato necesario para la generación de valor. El acceso al dominio DATO es el primer punto a considerar en la seguridad del sistema SWIFT. Se accede al dominio DATO a través del dominio USER y sus procedimientos. La manipulación del dominio DATO, respecto a la mensajería financiera, se realiza mediante la herramienta de gestión SAA. El dominio USER aglutina a los roles de usuario que cumplen funciones en el proceso de negocios mediante mensajería financiera. Profundizaremos en el dominio USER en el siguiente apartado.

Al considerar credenciales, resguardos, etc. dentro del dominio DATO, también debemos analizar los sistemas que los gerencian y sus procedimientos, tal como el SAA gerencia la mensajería, junto a los procedimientos definidos.

El dominio ADMIN representa al conjunto de roles existentes que parametrizan las diferentes partes del SC. Por ejemplo los administradores del gestionador de mensajes financieros, los administradores de software de apoyo a la tarea de tratamiento de mensajería financiera y todo administrador de activos que forme parte del SC. En el caso de la gestión de la mensajería financiera los usuarios privilegiados llamados izquierdo (LSO) y derecho (RSO), y aquellos delegados en las tareas de oficiales de seguridad, pertenecen claramente al dominio ADMIN. Los roles especiales, LSO y RSO, definidos en los SAA por SWIFT, no tienen permisos para crear mensajería financiera debido a incompatibilidad de funciones.

Cada una de las partes del rompecabezas de SWIFT tiene usuarios específicos de altos privilegios:

- Administradores de configuración LSO, RSO: SAA
- Administradores y usuarios de conf.: SWP
- Administradores de seguridad: SNL (O2M, certificados PKI)
- Administradores y usuarios de conf.: SAG
- Administradores y usuarios de conf.: HSM BOX SWIFT

A esta lista hay que agregar los usuarios de administración de los activos que la institución asigne al SC. Esta clasificación ayudará a mantener el cuidado sobre credenciales críticas ayudando a mantener el SC en zona de riesgo aceptable.

Una parte importante de la infraestructura del sistema SWIFT se configura mediante usuarios administrador izquierdo y derecho de las diferentes partes del sistema. Los roles de administrador izquierdo y derecho trabajan mediante controles mutuos sobre sus tareas, tienen el formato de trabajo llamado “de cuatro-ojos”. El principio de cuatro-ojos significa que el administrador izquierdo, o el derecho, configura un parámetro “Z” y el cambio realizado en la configuración del parámetro “Z” no tiene efecto hasta que el administrador opuesto confirme el cambio parametrizado. Este principio aporta transparencia - además de seguridad - al proceso de modificación de parámetros en los sistemas. Es una opción más segura que la del superusuario independiente y que hasta hoy conocemos en los sistemas operativos tradicionales. En algunos roles de seguridad del sistema SWIFT la opción de este principio de cuatro-ojos puede ser deshabilitada en función del criterio de costos, de la seguridad de cada institución y exigencias de entes reguladores. Deshabilitar esta opción implica ejecutar más controles en la utilización de usuarios de privilegio.

El dominio OWNER está formado por los roles del SO que tienen los privilegios necesarios para que cada elemento de software funcione correctamente y pueda ser mantenido adecuadamente. El usuario del SO perteneciente al dominio OWNER sólo puede ejecutar, actualizar y detener la pieza de software que le compete, no puede generar usuarios que manejen el sistema, ni modificar archivos del SC fuera de su zona de influencia. Se trata del resultado de aplicar la regla de menor privilegio al usuario de sistema operativo para que la pieza de software que maneja funcione correctamente en el hardware asignado. Así tenemos que cada herramienta tiene su propio usuario de sistema operativo con los menores privilegios posibles:

- *Owner* SAA
- *Owner* SNL y SAG
- *Owner* SWP
- *Owner* de Servicios Complementarios (autenticación, *file servers*, *print servers*, etc.).

Un objetivo de la definición de menor privilegio es también evitar que un rol diferente del OWNER pueda realizar modificaciones al software. Para esto necesitará que el administrador modifique los permisos otorgados. Hasta hace poco tiempo, el sistema SWIFT requería de un usuario del sistema operativo con los mayores privilegios posibles para su funcionamiento. La definición de OWNER, en SWIFT, se inició con los eventos de seguridad del año 2016.

El dominio SO aglutina los roles de superusuario del sistema operativo. Asimismo, se contemplan en este dominio los roles administradores de motores de virtualización, si este fuera el caso. Si bien estos roles no pueden crear mensajería en los procedimientos normales,

tienen privilegios suficientes para introducir mensajería al sistema dependiendo de cómo esté configurado el SAA, o bien pueden influir en la seguridad del sistema. También debemos contemplar en este dominio a los administradores de los SO de las máquinas que se utilizan para acceder al SC y de las bases de datos del sistema.

El dominio HARD representa a los roles que tienen contacto con la parte física de soporte del SC. Los roles de mantenimiento del hardware de los servidores y equipos de usuarios son un punto crítico a considerar. También forman parte de este dominio los roles de mantenimiento de los elementos de infraestructura física.

El dominio NET representa a los administradores, usuarios de configuración y monitoreo de las comunicaciones: LAN y WAN, *routers* y *firewalls*, *switches*, impresoras, VPN, etc. que interconectan al SC.

El dominio EXPOSICIÓN es el inventario de los servicios expuestos por el activo bajo análisis, los otros activos que interactúan con el primero y aquellos que potencialmente pudiesen interactuar.

En función del análisis de la información relevada de cada dominio y en cada activo, debemos detectar los riesgos a los que está expuesto el SC.

2.5.3 El dominio USER: roles de negocio

El dominio USER está formado por los roles que gestionan la mensajería financiera que forman el dominio DATO:

- Carga y Modificación
- Verificación de mensajería
- Autorización de mensajería
- RMA: relaciones con otros bancos

Rol Carga: Se refiere al permiso del usuario para crear un nuevo

mensaje dentro de la aplicación de mensajería. Una vez terminada la carga, el mensaje pasa a la siguiente instancia, por ejemplo Verificación. Si una etapa posterior detecta un error, la función Modificación lo puede solucionar corrigiendo el error detectado en el contenido del mensaje. Es posible configurar la herramienta SAA para que el mismo rol de carga del mensaje lo envíe a la red SWIFT sin otra instancia posterior. La configuración del tratamiento de los mensajes puede discriminar posibilidades de acción para distintos tipos de mensajes. Las herramientas de gestión SAA permiten ser configuradas de tal manera que todos, o bien determinados mensajes financieros, pasen a la red SWIFT directamente una vez ingresados al SAA.

Rol Verificación: La etapa de verificación del mensaje contrasta la información de campos del mensaje. Por ejemplo, fecha, valor, importe, moneda, números de cuenta, contraparte, etc., antes de enviarlos a SWIFT o a la siguiente etapa: Autorización.

El Verificador tiene información del mensaje que debe coincidir con aquella cargada durante su creación. Si coincide, el mensaje puede pasar al siguiente estado de Autorización, o ser enviado a SWIFT, dependiendo de la parametrización de la herramienta de mensajería. Si los datos ingresados no coincidiesen con aquellos del mensaje original, se puede pasar el mensaje a la etapa de modificación para su corrección o cancelarlo para generar uno nuevo.

Rol Autorización: Los mensajes llegan al estado de autorización por diferentes rutas. Una vez allí serán procesados por un operador con el perfil adecuado para ser enviados a la red SWIFT. Tal como en todos los estados del mensaje, el rol autorizador tiene las tres posibilidades disponibles: puede enviarlo a la red SWIFT, anular el mensaje o enviarlo a modificación para su corrección.

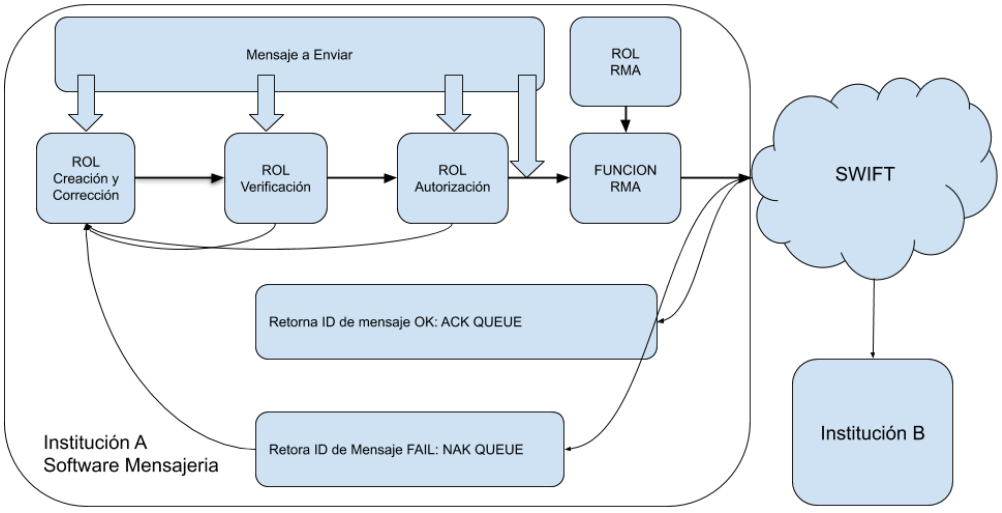
Todos los mensajes enviados por la institución a la red SWIFT se

identifican mediante un número identificador único y consecutivo, asignado por el servicio SWIFT.

Rol RMA: RMA (*Relationship Management Application*) es la función dentro del sistema SWIFT que permite el envío y recepción de mensajería que representa compromiso de valores con otras entidades. El rol de RMA es el permiso de manejo de las solicitudes de RMA de la institución.

Cómo se mencionó anteriormente, algunos mensajes SWIFT significan compromiso de valores custodiados por la entidad, otros son meramente informativos y no suponen ningún compromiso extra. Por defecto, ninguna de las entidades conectadas puede enviar mensajes que signifiquen un compromiso de valores a otra entidad. Entonces para poder enviar una orden sobre valores determinados, la entidad emisora debe haber sido autorizada por el receptor para realizar el envío. Una vez establecidas, las autorizaciones RMA vencerán solo si se lo especificó en el establecimiento de la relación. Toda relación RMA puede ser revocada en cualquier momento por cualquiera de las partes.

La función de enviar los requisitos de RMA a otras entidades y aceptar los recibidos le corresponde a quien maneje el rol RMA. Las claves intercambiadas deben ser revisadas periódicamente detectando las RMA innecesarias o las que puedan comprometer a la institución, ya sea por sanciones o por exposición. Asimismo, la función RMA permite un intercambio epistolar que se registra en el historial de claves RMA. La función RMA se puede granular por tipo de mensaje mediante el RMA Plus, mientras que el RMA simple incluye a la totalidad de los mensajes una vez otorgada la autorización de envío a la otra entidad. La relación de los roles se representa en el siguiente gráfico:



Los roles de creación, verificación y autorización representan los tres estados de la mensajería antes de ser firmada digitalmente por la entidad y enviada a la contraparte a través de la red de servicios SWIFT. Por lo tanto, si hay un error en cualquiera de las etapas o estados, se envía el mensaje para su corrección. Mínimamente, existen tres etapas para detectar errores en el flujo del mensaje financiero. Esto depende de la configuración paramétrica del SAA; puede que los roles de creación, verificación y autorización se cumplan en otra herramienta y el SAA pase a ser un túnel a SWIFT. Por esto es importante poner la atención en los roles y procedimientos, además de las herramientas.

Tal como se describió anteriormente, RMA es la función que habilita los intercambios de mensajería financiera entre entidades. Los roles allí pueden ser configurados con el principio de cuatro-ojos: un operador crea la solicitud y otro la aprueba para la función de enviar mensajes RMA, lo mismo en la recepción de peticiones RMA, un operador la acepta y otro la activa dentro del sistema.

Como se puede observar, SWIFT realizó un trabajo importante en la segregación de funciones. Dependerá entonces de las instituciones, utilizar o

no los roles para fortalecer el sistema. Actualmente SWIFT está exigiendo a las entidades la segregación de funciones mediante requisitos de cumplimiento obligatorio y modificando el software : opciones de configuración que antes existían se anulan en versiones nuevas disminuyendo riesgos en las entidades.

2.6 Eje III: Infraestructura

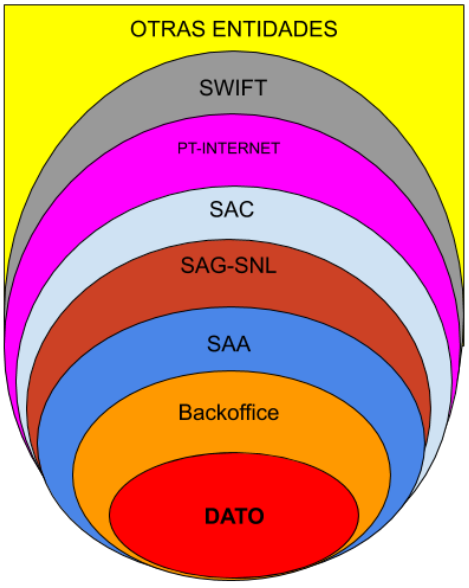
En esta etapa del análisis de seguridad del SC se estudia la infraestructura del sistema para detectar sus zonas vulnerables y los controles que podemos implementar. Para el estudio y modelización del SC se propone el sistema de capas desde el dominio DATO, contemplando esta vez, las capas de infraestructura del sistema en lugar de sus roles.

Si bien se realiza una división por funciones de infraestructura en base al sistema SWIFT el análisis puede emplearse a cualquier SC.

De la descripción de las partes del sistema SWIFT vemos dos grandes grupos: gestión y comunicaciones. Una vez que gestión entrega el mensaje a comunicaciones, el resto es una tarea que no requiere un rol operativo para llevarse adelante ya que involucra cifrados y firmas digitales que se realiza independientemente del mensaje financiero. Se agrupan entonces los elementos de comunicación en una función que llamaremos Función de Paquetización Segura. La agrupación por funcionalidades y definiciones ayuda a comprender los sistemas críticos y permite la modelización para estudiar la seguridad, detectando los dominios y estados críticos de la información. Las iteraciones periodicas de los análisis realizados en cada modelo y capa propuestos, permitirán optimizar tanto los recursos disponibles como la seguridad del SC expuesto al nivel de riesgo definido por la entidad.

2.6.1 Análisis de capas *Top-Down* II: flujo de la información

Las capas para el análisis se definirán considerando el flujo de la información en la infraestructura del SC. Los dominios propuestos son los siguientes:



Dominios detectados en un sistema informático por análisis de capas:

OTRAS ENTIDADES: Resto de los actores que se interconectan a la entidad mediante la red del sistema crítico.

SWIFT: Red de interconexión de servicios del sistema crítico.

PT-INTERNET: Proveedores de transporte de información. Son proveedores de vínculos directos autorizados por SW (Gold, Silver) y proveedores de Internet para Silver y Bronze.

SAC: Equipos de VPN entre la institución y SWIFT (SW) mediante el transporte que corresponda. Son los productos Bronze, Silver, Gold, etc.

SAG-SNL: Funcionalidades del sistema SW referentes a certificados, cifrado, protocolos de red..

SAA: Gestionador de mensajería financiera (MF). Porción de SC donde están definidos los roles para el tratamiento de la MF, sea manual o automatico.

BACKOFFICE: sistemas, o procedimientos, que consumen, proveen y procesan información para generar valor en la cadena de producción.

DATO :Los mensajes financieros y sus partes disponibles para consumo interno de la institución y otros datos para el funcionamiento del SC..

El dominio DATO está formado, entre otros, por los datos recibidos de otras entidades vía mensaje financiero y por los datos locales necesarios para enviar mensajería financiera a otras entidades. Los conjuntos de datos enviados y recibidos, implican procesos a ejecutar en la institución, materializados por la siguiente capa en el flujo de información, el dominio *Back Office*.

El dominio DATO es el mismo que en el análisis anterior, aquí enfatizamos en los datos de mensajería.

La información es procesada por el dominio *Back Office* donde se agrupa y complementa la información, iniciando el procedimiento de envío

de la orden a la contraparte, o bien iniciando el procedimiento interno que ordena un mensaje recibido.

El siguiente dominio gestiona la mensajería financiera, es decir, la crea, modifica, verifica, autoriza y dispone su envío. Respecto de mensajes recibidos, el gestionador de mensajería financiera no puede, y no debería, alterar los mensajes ingresados.

Los dominios SAG-SNL, SAC, PT-Internet son los elementos de comunicación y los agrupamos en una función que llamaremos: Función de Paquetización Segura, tanto para mensajes salientes como entrantes.

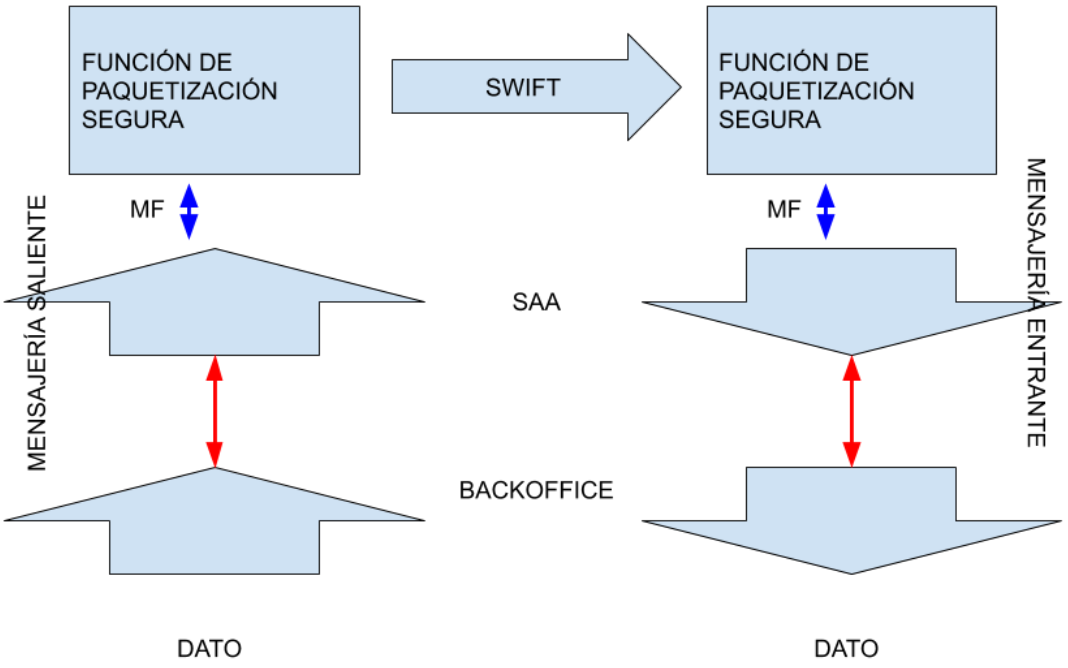
Esta función se encarga de la seguridad en la transmisión mediante encriptación y autenticación de los datos recibidos respecto del origen y destino, entre muchas otras tareas. Más adelante, se amplía información sobre la función definida.

El dominio SWIFT tiene varias funciones, entre ellas la de conmutar la mensajería para la entrega de cada mensaje, además de gestionar la disponibilidad, integridad, autenticidad y no repudio de cada orden o mensaje financiero en la red mediante su estructura de servicios de certificados PKI.

El dominio Otras Entidades representa a los corresponsales y a otros actores de la red de servicios SWIFT. Respecto de la información de mensajes recibidos, estos disparan tareas internas en la institución. Por ejemplo, la instrucción recibida puede ser una orden de débito o de crédito en una cuenta de un cliente que administre la entidad, o bien información sobre alguna cuenta de la institución en otra entidad.

2.6.2 Función de paquetización segura

La Función de Paquetización Segura está formada por los dominios SAG-SNL, SAC y PT-Internet. En estos dominios se realizan las tareas de



firma digital, verificación de firmas PKI, encriptación, uso de protocolos de los servicios de SWIFT y la tunelización segura de los datos hacia SWIFT para transmitir la mensajería financiera ya en formato de cápsula encriptada y firmada. También se realiza la recepción de paquetes de información encriptados vía SWIFT, se procede a la verificación de firmas y desencriptación de mensajes.

Si bien los vínculos de transporte vía Internet no tienen ninguna restricción respecto de la elección de proveedor, las líneas punto a punto son adquiridas solamente a ciertos proveedores aprobados por SWIFT.

El dominio PT-Internet es el medio de transporte que une la entidad con SWIFT. Si bien los proveedores de transporte son empresas autorizadas por SWIFT y elegidas por la institución, no hay traslado de responsabilidad sobre las mismas: SWIFT establece que la entidad es la responsable de la

información y debe tomar todos los recaudos necesarios.

En el dominio PTP-Internet la información está en un medio potencialmente hostil y depende de la robustez de la encriptación y de la solidez del protocolo de SWIFT para asegurar la seguridad informática de los datos transmitidos. Asimismo, la entidad debe verificar que los métodos ejecutados por el proveedor de comunicaciones contratado son adecuados, y se cumplen las mejores prácticas por parte del proveedor.

En el sentido entrante, es decir desde otras entidades en SWIFT y hacia la institución, la función de paquetización segura recibe la mensajería en el dominio PTP-Internet y la entrega al dominio SAC. El dominio SAC cumple la función de realizar un túnel seguro y encriptado entre la entidad y SWIFT. La primer verificación de la información la realiza la VPN en el dominio SAC que se conecta al dominio PT-Internet y al dominio SAG-SNL. El dominio SAG-SNL es la segunda verificación: la información recibida fehacientemente proviene de SWIFT, del emisor del mensaje y está destinada a la institución. El dominio SAG-SNL realiza funciones criptográficas complejas entregando la información verificada en base a su procedencia, destino e integridad del contenido, dando por finalizada la función de paquetización segura. El dominio SAC utiliza clave simétrica entre otros mecanismos de seguridad, mientras que el dominio SAG-SNL está basado en certificados PKI emitidos por SWIFT, validando origen y destino de las entidades en cada función solicitada a los servicios de la red SWIFT. Los mecanismos utilizados por SAG-SNL son firma y encriptación de la información mediante los certificados PKI emitidos por SWIFT. A esta estructura de certificados PKI se le agrega la certificación y encripción de la infraestructura SAC y además un certificado de conectividad del SNL identificando el elemento de comunicaciones SNL de la entidad.

Cómo se observa en el gráfico, luego de la recepción, la función

paquetización segura entrega la información al gestionador de mensajería financiera, SAA, para su proceso y posterior entrega al dominio *Back Office* desde donde se nutrirá el dominio DATO. Además del tratamiento criptográfico mencionado, la función de paquetización segura se aplican varias de las herramientas de SI para asegurar la autenticidad, integridad y disponibilidad de la información:

Disponibilidad: Un gestionador de mensajería financiera (SAA) puede tener dos o más cadenas de paquetización segura, disponibles y configuradas. Si esta función que está siendo utilizada pierde conectividad con SWIFT es reemplazada automáticamente por la segunda cadena sin pérdida de información.

Confidencialidad: El esquema de certificados PKI utilizado garantiza la confiabilidad mediante la utilización de claves pública-privada. TLS es un opción disponible sí necesitamos utilizarlo.

Integridad: Se traduce como la inalterabilidad de la información generada en origen. Para esto SWIFT utiliza un esquema criptográfico que combina claves de ambas entidades y campos críticos del mensaje para calcular un valor resultado que identifica unívocamente el contenido del mismo.

La función de paquetización segura también es utilizada para tareas administrativas. Estas tareas incluyen la creación, mantenimiento y recuperación de los certificados PKI, la asignación de roles a estos certificados y la auditoría de tareas con cada certificado.

2.6.3 Segregación y menor privilegio

Toda infraestructura representa un conjunto ordenado de recursos para cumplir determinada tarea, cada recurso cumplirá un rol dentro del orden mencionado. Nuevamente se observa que los principios de

segregación y menor privilegio son factibles de aplicar, esta vez, al conjunto de recursos informáticos.

El resultado de aplicar el principio de segregación a los activos críticos de la red hace que debamos separar de la infraestructura general, la porción correspondiente al SC y también sus servicios. Así lo recomiendan las normas IRAM-ISO/IEC 27001 en el punto 13.1 Gestión de seguridad de la red. También lo menciona el marco originado por NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, en el punto PR.AC-5 [17].

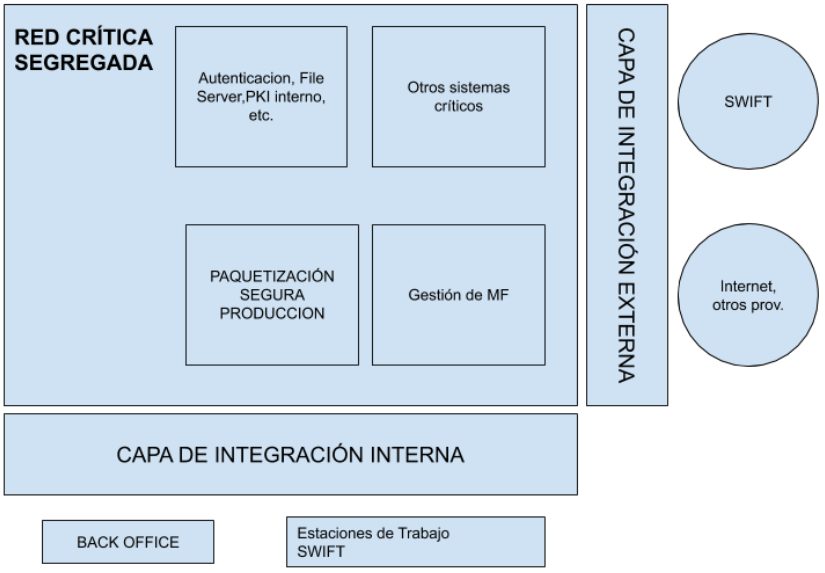
Tal como se mencionó, se verifica la necesidad de separar las funciones de servicio del SC de aquellas funciones de los sistemas no críticos. No realizar la segregación de los servicios tiene al menos dos consecuencias, ambas negativas: genera un costo elevado al tratar a los servicios comunes como críticos o aumenta el riesgo de incidentes al exponer a los SC mediante estos servicios comunes.

Resulta necesario entonces separar los servicios brindados a los sistemas críticos de los no críticos y diferenciarlos de los mismos servicios para sistemas no críticos, optimizando así los riesgos y los recursos. Se observa la posibilidad de tener servicios comunes a los servicios críticos ya que tendrán el mismo tratamiento en procedimientos, recursos y respuesta a eventos de seguridad detectados.

El principio de segregación y el de menor privilegio aplicado a los roles en la infraestructura reduce la exposición de los SC a otras infraestructuras con múltiples resultados positivos, entre ellos: mejora en la detección de eventos provenientes de SC, con la consecuente detección temprana de ataques e independización de zonas de infraestructura en caso de compromiso de alguna de ellas. Toda solicitud recibida por el SC no puede ser ignorada y será tramitada. En caso que la solicitud recibida no sea correcta, se analizará y corregirá de inmediato, mediante los controles

correctivos oportunos registrando los eventos que correspondan.

El siguiente gráfico ubica las funciones y los servicios externos necesarios.



2.6.4 DATO, *Back Office* y Gestión de mensajes

El dominio DATO es el conjunto de información financiera formada por la información recibida desde las contrapartes, la información a enviar en curso y la mensajería efectivamente enviada.

La información recibida por la institución es el conjunto de información que dispara procesos internos. Los procesos internos implican la ejecución de procedimientos locales, por ejemplo, realizar débitos, créditos, etc. en cuentas de terceros que administra la entidad, respuesta a solicitudes o negocios ofrecidos en mensajería recibida y también posiblemente, generar nuevos mensajes financieros hacia otras entidades.

El dominio *Back Office* es el responsable de la ejecución de dos tipos de procesos, ya sea preparar el envío de órdenes financieras a otras

entidades o impactar localmente en los procedimientos de la institución en función de los datos recibidos.

El SAA implementa métodos que aseguran el intercambio de información con el dominio *Back Office*. Estos métodos utilizan clave simétrica, con o sin encriptación. De esta manera aseguramos que la información recibida por el SAA es la generada por el *Back Office* que posee la clave simétrica y el protocolo convenido para el intercambio. El método de autenticación, con o sin encriptación, es válido en ambas direcciones.

Para la generación de mensajería, luego de la gestión realizada en el SAA se entregan las órdenes generadas a la función de paquetización segura para su envío a SWIFT. Para la recepción, los mensajes se validan en la función de paquetización segura y se entregan al gestionador SAA, que mediante protocolos de autenticación, entregan la información al back office para los procesos necesarios. Claramente de no existir autenticación entre SAA y Back Office se pierde parte de la seguridad implementada en la función de paquetización segura.

2.6.5 Internet y proveedores externos a la infraestructura

Debemos contemplar que SWIFT es un proveedor externo a la institución y si bien hay varios mecanismos técnicos que aseguran que estamos conectados al SWIFT proveedor de servicios, todo evento de seguridad con esta entidad externa debe clarificarse inmediatamente, documentando el evento en detalle, y si corresponde, informando a SWIFT mediante los canales de comunicación establecidos por éste. Hace unos pocos años, la red de SWIFT tenía una infraestructura de comunicaciones independiente. Hoy la red Internet es la que interconecta principalmente a las entidades ya sea por vínculos o por equipamiento en proveedores. Conectar a Internet un SC de cualquier naturaleza es una tarea que se debe

realizar tomando los recaudos necesarios, ya que Internet es una importante fuente de servicios y un medio para reducir costos pero también una fuente inagotable de riesgos. Internet - para el servicio crítico SWIFT - es el medio donde el *SAC Bronze* y *SAC Silver* crean la VPN por la que viajan los mensajes financieros entrantes y salientes de la institución. Además de transportar mensajes financieros, Internet es el medio que nos conecta con la información y alertas de SWIFT a través de su sitio web. SWIFT provee, mediante su sitio en Internet, indicadores de compromiso (IOC) y otros servicios, que pueden configurarse para que los sistemas de la entidad adquieran información automáticamente. Para los IOC se puede implementar la obtención de datos automáticos mediante STIX y TAXII.

En síntesis, para SWIFT la conectividad a Internet es una fuente de información y comunicación. Ciertamente, el acceso a Internet debe estar acotado a los sitios y direcciones públicas de SWIFT.

2.7 Eje IV: Seguridad Informática

El actor Seguridad Informática en el SC SWIFT que utiliza la institución será el recolector de eventos y derivará su tratamiento a quien corresponda. Cada evento debe ser analizado en función de evidenciar riesgos materializados en alguna medida, cada evento debe ser clasificado y generar una base de conocimiento para el futuro, robusteciendo el sistema en función del conocimiento adquirido.

Los eventos automáticos de red, los del SC, los del control perimetral y aquellos observados por cada uno de los roles generan los incidentes que nutren la gestión de eventos.

Todo evento, por inocente que parezca, es información valiosa para detectar cualquier posible compromiso. El tratamiento de eventos de seguridad requiere de procedimientos claros y coordinados en la institución,

renovándose estos al detectar posibles mejoras en función de la experiencia diaria. El entrenamiento y concientización de todas las partes relacionadas al SC respecto de la seguridad es un aporte al grado de madurez de la institución robusteciendo la seguridad. El entrenamiento sobre buenas prácticas en seguridad es muy importante como también la difusión de los procedimientos actuales a las partes involucradas.

El área SI debe analizar el contenido de los procedimientos, sus controles y también del cumplimiento de cada uno de ellos mediante métricas establecidas. Se deben analizar periódicamente los resultados de métricas definidas para indicar el estado de riesgo actual de cada SC y de sus servicios asociados.

La generación de reportes del estado de la seguridad del SC por parte del área SI informando a la alta gerencia y a las demás áreas involucradas respecto de tareas, eventos y estado del SC es crítico para mantener informados a los responsables finales del estado de situación pudiendo así, los responsables, definir tareas correctivas según las necesidades planteadas. Los reportes periódicos son un medio de coordinación de esfuerzos entre las partes.

3. Tercera parte: Riesgos detectados, cómo mitigarlos

La detección de riesgos se lleva a cabo estudiando los controles propuestos en el anexo A de la norma ISO 27001 [18] y el sistema SWIFT. En el siguiente análisis se presentan los generadores de riesgos detectados y se proponen sus tratamientos posibles. No se trata de una evaluación de los riesgos respecto de su severidad, ni de su probabilidad de ocurrencia y repetición, ya que esto requiere la definición de un marco de información que escapa al alcance de este trabajo. El presente análisis se trata simplemente de un listado de puntos a verificar en cada entidad para detectar si los generadores de riesgos listados existen o no. Por ejemplo la generación de riesgos por falta de políticas sobre la gestión de la seguridad en el mercado bancario es poco probable o bien existirá una fuerte observación hacia la entidad. La primer etapa en la evaluación de un riesgo es visibilizarlo, muchas veces la falta de madurez impide visibilizar determinado riesgo, otras veces políticamente no conviene que el riesgo exista, y entonces no existe, según el proverbio popular sin autor cierto:

"Los muertos que vos matáis/ gozan de buena salud."

Lo que se intenta visibilizar son los posibles generadores de riesgos para que en un primer chequeo la institución se autoevalue en función sí contempla o no contempla algún análisis, o mitigación, sobre el generador de riesgo propuesto y detectar otros que pueden gozar de muy buena salud.

3.1 Políticas de seguridad de la información

En los inicios de la seguridad de la información, en lo que respecta a los elementos de las computadoras o de la red, se pensaba que la SI era un tema meramente técnico, y de seguir buenas prácticas, se asemejaba a la idea de asegurar la información dentro de un buen cofre.

Actualmente, los organismos de incidencia global como el NIST, la ISO 27001 y también la norma del BCRA TO SGSI, destacan la necesidad de políticas que definan el tratamiento de la seguridad de la información dentro de la organización mediante políticas que incluyen y exceden largamente las buenas prácticas tecnológicas, basándose en principios como segregación de roles, menor privilegio, tratamiento de eventos y muchos temas más.

Generadores de riesgo: Falta de organismos de control en la institución. Comité de seguridad sin definición de integrantes o bien sin funcionamiento al menos periódico. Procedimientos poco claros. Mala o nula comunicación de las políticas de SI al resto de los integrantes de la institución. Implementación parcial de procedimientos. No hay definición o recolección de métricas sobre las políticas y procedimientos de la SI.

Tratamiento: Asistencia mediante entes reguladores. Buscar apoyo para el desarrollo de políticas en asociaciones de instituciones comunes. Contratar servicios externos. Reuniones periódicas que fijan objetivos, miden avances y corrigen desvíos para encauzar las políticas en la institución. Definición desde la alta gerencia de las áreas y responsables necesarios para el desarrollo e implementación de las definiciones de políticas de seguridad de la información.

3.2 Aspectos organizativos. Roles

Este control se refiere a la estructura de roles que necesita la herramienta de producción para funcionar en forma segura, en este caso analizamos los roles del SC SWIFT.

Generadores de riesgo: Vulnerabilidad del sistema por concentración de roles/credenciales. Asignar funciones incompatibles. Resistencia al cambio. Funcionamiento en forma de compartimientos estancos: en detrimento de la formación, concientización de los recursos y medidas de tipo organizativo. Asignación de roles supuestamente segregados crean un superusuario en la operación diaria: por ejemplo todas las tareas de negocios, o credenciales críticas, concentradas en un área de la institución.

Tratamiento: Establecer los roles en áreas de negocio donde el flujo del proceso realice el control de la información: asignar los roles en distintas áreas colaborativas realiza un control en línea de la información (roles de carga, verificación y autorización distribuidos). Diferenciar mensajería por corresponsal, monto, tipo de negocio, etc. ayuda a segregar roles. Utilizar definición de zonas en SAA para separar, diferenciar y ordenar el tratamiento de mensajería en roles. Segregar los roles de RMA, tratamiento de mensajería y configuración según corresponda. Asimismo, realizar la segregación de funciones dentro de cada una de las áreas responsables de las operaciones de negocios, infraestructura, SI y auditoría para permitir un autocontrol en el flujo de la información y aumentar la probabilidad de detectar y prevenir eventos.

3.2.1 Incompatibilidad de funciones

Según la norma TO SGSI [18] del Banco Central de la República Argentina para el mercado financiero, en la sección 2 “Organización funcional y gestión de tecnología informática y sistemas”, punto 2.5.4

“Actividades y segregación de funciones, incompatibilidades”, se detallarán las incompatibilidades entre los roles dentro de un sistema informático, con la finalidad de mantenerlo en una zona segura y de bajo riesgo operativo.

La sección 2.5.5 de la norma, define los roles que forman todo sistema informático. Asignaremos las funciones de utilización del SC para generar valor - dentro de la institución - a los roles Usuario Final y Data Entry del cuadro mencionado en la norma TO SGSI [18]. Ambos roles están representados en la columna Negocio del cuadro que sigue a continuación.

En base a funciones de los roles, el know-how necesario para llevar adelante cada tarea con un riesgo bajo y las incompatibilidades de funciones entre roles de cada subdominio que emanan de la norma TO SGSI, se propone la siguiente segregación de responsabilidades: ver tabla en Anexo I.

3.2.2 Credenciales críticas

Las tareas indicadas desde el ID 2.2 hasta el ID 2.8 en la tabla del Anexo I, corresponden a roles incompatibles con el envío de mensajería financiera. Las credenciales ligadas a las tareas descriptas tienen habilitadas funciones de configuración, mantenimiento, ABM de usuarios, realizar nuevas instalaciones, entre muchas más. Estas credenciales deben permanecer custodiadas y asignadas específicamente a responsables de la institución según la matriz propuesta o bien por la matriz de incompatibilidades que defina la institución en función de sus necesidades y requerimientos de negocios. Los procedimientos internos deben garantizar que el propietario designado del activo esté informado de las modificaciones y de las nuevas instalaciones realizadas o a realizar. Con las credenciales asignadas en custodia, se puede no solamente realizar una nueva instalación, sino también asignar nuevos roles a usuarios existentes, modificar métodos de autenticación, asignar claves nuevas a los usuarios con roles de tratamiento de mensajería. La propuesta realizada, en la

descripción de la tabla anterior, de involucrar a auditoría de sistemas en el procedimiento de utilización de las credenciales, incentiva el trabajo en equipo y da transparencia al proceso de gestión de cambios. Es necesario contar con un resguardo seguro de las credenciales críticas, donde la solicitud de alguna de ellas genere registros informáticos automáticos informando a los involucrados en el sistema SWIFT. La finalización de la tarea iniciada con la solicitud de credenciales críticas debe estar plasmada en un informe técnico de la tarea realizada y la conformidad de los involucrados junto al propietario o custodio del activo.

3.3 Seguridad ligada a los Recursos Humanos

Los RRHH serán las principales herramientas de la institución para llevar adelante el funcionamiento seguro del SC. Su evaluación periódica, concientización en seguridad, formación respecto de los procedimientos y conocimientos necesarios para su rol asignado es muy importante para mantener el SC en zona segura.

Generadores de riesgo: Comportamiento en redes sociales. Resistencia al cambio. Ingeniería social. Estabilidad social y familiar.

Tratamiento: Contener mediante profesionales a los recursos en caso de contingencias familiares, sociales y de salud. Concientizar al personal relacionado a los sistemas críticos sobre la exposición en redes sociales. Los ataques en búsqueda de credenciales pueden iniciarse en los elementos personales expuestos. Monitorear el comportamiento de los RRHH en SC para actuar proactivamente en la concientización y prevención. Cumplir con las normas de privacidad que correspondan para fortalecer la estructura de RRHH. Tal como lo ilustra el control anterior (Roles), la segregación de funciones le dará robustez a la estructura. Se puede realizar una evaluación periódica de los recursos afectados al SC.

3.4 Gestión de activos

Inventario de activos, los activos que forman el SC deberán estar identificados.

Generadores de riesgo: Inventario incompleto. Desconocimiento de las partes constitutivas del SC y sus soportes informáticos, de comunicaciones, servicios, RRHH y procedimientos.

Tratamiento: Analizar y estudiar las partes del sistema permite revelar los elementos del SC. Llevar a cabo controles periódicos y analizar las tareas realizadas que afecten al SC para detectar activos no contemplados. Servicios de consultoría externa para detección de faltantes en el inventario del SC. Recomendaciones del proveedor del SC.

3.4.1 Propiedad de los activos

La asignación de propietario a los activos determina el responsable de cada uno de los activos.

Generadores de riesgo: Falta de coordinación de actividades en activos productivos frente a riesgos detectados. No hay propietario formalmente designado. Falta de comunicación de tareas y responsabilidades al propietario. Falta de comunicación del propietario con el resto de las áreas de trabajo sobre el SC.

Tratamiento: Designar propietarios según especialidad, para esto podemos utilizar la información brindada en el TO SGSI del BCRA. Se propone asignar:

Propietario de la información: designar un RRHH que pertenezca a los roles de negocios.

Propietario de los activos físicos: designar un RRHH que pertenezca a los roles de infraestructura.

Propietario de procedimientos: designar un RRHH que pertenezca a los roles de procedimientos y riesgos.

Es necesario designar, entre los tres propuestos, un propietario coordinador. Se propone que sea el propietario de la información definido el que coordina las tareas con los demás propietarios en función de las necesidades del negocio de la institución. Cada propietario informa al grupo sobre las novedades y necesidades en sus especialidades.

Se reportan las novedades y tareas programadas a SI, para evaluar la evolución del SC y generar reportes que correspondan.

3.5 Control de accesos

Generadores de riesgo: Debilidad en sistema de autenticación. Falta de control en fortaleza de credenciales. Cuentas habilitadas sin utilización. Reutilización de credenciales. Compromiso de credenciales.

Tratamiento: Acceder al sistema SWIFT mediante doble factor de autenticación en los roles correspondientes a los dominios USER y ADMIN. Configurar modo de autenticación de doble factor embebido en SAA y SAG, o bien un sistema de autenticación externo con doble factor. Configurar O2M con acceso vía doble factor de autenticación. Configurar las restricciones horarias a cada rol. Analizar el registro de autenticaciones positivas, negativas y las modificaciones de credenciales. Definir los entornos físicos y controles perimetrales para autenticación y operación. Aquellos días sin operación financiera, bloquear el acceso de la institución a SWIFT mediante función Login/Select.En las instituciones que trabajen con token HSM o con tokens personales, desconectarlos y guardarlos en lugar seguro al no utilizar el sistema SWIFT. No identificar a las credenciales de los roles con reglas que permitirían identificar a los individuos y sus funciones. En caso de compromiso del sistema de autenticación externa, evaluar la posibilidad de

activar credenciales locales. Analizar los eventos para detectar intentos fallidos y posibles ataques por reutilización de claves (por ejemplo, al restaurar backup anteriores o que hayan sido modificados). Custodiar y mantener las credenciales genéricas. Asignar roles de credenciales genéricas a roles delegados en cuentas identificadas. Establecer procedimientos a ejecutar en caso de credenciales comprometidas.

SWIFT brinda una lista de hardware y aplicaciones compatibles con la implementación de SHA256 en la funcionalidad embebida TOTP para doble factor. LDAP y RADIUS son alternativas de autenticación con el agregado necesario para contar con doble factor.

En las versiones actuales, LSO y RSO inhabilitadas pueden ser recuperadas con el soporte de SWIFT (en versiones anteriores no existía tal posibilidad y el único camino era la reinstalación del software). Es importante analizar eventos de utilización de la nueva funcionalidad descrita periódicamente. Los elementos de autenticación deben estar configurados para verificar que las contraseñas elegidas por los usuarios cumplen las normas de complejidad adecuada y permiten el listado de palabras y/o caracteres especiales denegados.

3.5.1 Uso de herramientas con privilegios

Estas herramientas modifican datos o parámetros en el SC mediante procedimientos alternativos ya que las funcionalidades normalmente utilizadas no funcionan o no corrigen el error.

Generador de riesgo: Soporte de SWIFT provee código para utilizar herramientas con privilegios sobre bases de datos Oracle y herramientas de software que modifican parámetros o datos del SC.

Tratamiento: Verificar periódicamente evidencias de la utilización de estas herramientas mediante la búsqueda de eventos en los diferentes elementos de software, en los registros de acceso a soporte de SWIFT y en

las herramientas de mantenimiento de certificados WebAccess (O2M) por parte de Seguridad y Auditoría.

3.6 Criptografía

La utilización de criptografía protege a la información, garantiza su integridad y verifica la autenticación. El cuidado y resguardo de las claves junto a los métodos computacionales empleados es altamente crítico para proteger y recuperar la información cuando sea requerido.

Generadores de riesgo: Certificados de la institución comprometidos. Comunicaciones no encriptadas. No se utiliza autenticación de datos antes de procesarlos. Pérdida de comunicación con SWIFT por vencimiento de certificados de conectividad o encripción. No hay procedimientos de mantenimiento de certificados internos o de SWIFT. Desconocimiento sobre el manejo y control de certificados en la institución. Procedimientos poco claros en la delegación de la conectividad vía *service bureau* de SWIFT y el mantenimiento de los certificados.

Tratamiento: Capacitaciones sobre funcionamiento de SWP, SNL, SAG, O2M y SAA. Preparar y verificar procedimientos claros y detallados sobre el mantenimiento de certificados. Establecer procedimientos de verificación periódica del estado de los certificados de conectividad a SWIFT mediante el SAG y O2M. Definición de responsables de certificados y sus tareas de mantenimiento periódicas. Auditoría de tareas mediante O2M y logs de los sistemas que forman el SC. Verificación del estado de los soportes físicos de los certificados ya sean HSM BOX o HSM Token. Identificar los HSM Token en inventario de activos y su resguardo. Los certificados PKI utilizados dentro de la red SWIFT tienen fortaleza igual o superior a RSA 4K (anteriormente RSA 2K). Aquellos que no migren a certificados 4k para mediados de 2022, no se podrán conectar a la red. Procedimientos claro en caso de corrupción de un token para su recupero,

procedimientos claros para la revocación en caso de sospechar compromiso de certificados. Los certificados PKI que identifican a la institución deben ser manejados por los oficiales de seguridad de la institución.

3.7 Seguridad física y ambiental

El acceso físico a los elementos del SC se debe restringir a lo necesario y mediante personal calificado. La protección del entorno físico es crítico junto a detectores de humo, agua, temperatura, gases, etc.

Generadores de riesgo: Acceso físico a los activos críticos sin control o no autorizado. Compromiso de servidores vía interfaz USB, elementos de hardware maliciosos, elementos de infraestructura física. Relevamiento incompleto de activos críticos o no identificados físicamente. Modificaciones en conectividad física o lógica (cableado).

Tratamiento: Generar y analizar registros automáticos de acceso físico y lógico a equipamiento crítico. Acceso a credenciales lógicas, físicas, etc. mediante control o custodia.Procedimientos de aviso preventivo de tareas en áreas físicas de custodia. Control y reporte de tareas físicas y lógicas realizadas. Establecer el sistema cuatro-ojos en las instalaciones y tareas físicas de áreas críticas. Definir áreas físicas restringidas para protección de activos críticos y áreas de transición de criticidad. Analizar exhaustivamente todo nuevo activo que se incorpore a la zona crítica antes de ingresar a producción. Establecer las ventanas horarias de mantenimiento de infraestructura física y ambiental para que no afecten a los sistemas productivos críticos.

3.8 Seguridad en las operaciones

3.8.1 Documentación de procedimientos

Establecer las formas de realizar las tareas, sus recursos, periodicidad, reportes, métricas resultantes, condiciones, etc.

Generadores de riesgo: Procedimientos desactualizados o no implementados. No hay unificación o repositorio único de procedimientos, distintas versiones distribuidas de los procedimientos. Inexistencia de procedimientos documentados o aprobados frente a eventos de seguridad. Inexistencia de documentación de paso de producción a contingencia y su retorno a producción. Los procedimientos en contingencia no contemplan las incompatibilidades entre roles (Ver aspectos organizativos). No hay procedimientos verificados por los roles que los deberán ejecutar.

Tratamiento: Definir propietario de procedimientos. Verificar procedimientos actuales, corregirlos si fuera necesario. Definir repositorio común y comunicar a los RRHH que deberán ejecutarlos. Definir métricas de utilización de procedimientos y evaluarlas periódicamente. Verificación periódica de procedimientos.

3.8.2 Separación de entornos desarrollo, pruebas y producción

Esto evita el acceso no autorizado a los equipos productivos y a sus datos de trabajo. Evita riesgos en equipos productivos. La no existencia de elementos de prueba pone en riesgo al sistema productivo.

Generadores de riesgo: Activos productivos inoperables por inconvenientes en instalaciones de parches de SWIFT, parches de SO, nuevas versiones, pruebas de sistemas. Contingencias no disponibles (ídem anterior). Acceso de personal de desarrollo a equipos productivos. Elementos de desarrollo instalado en elementos productivos. Diferencias entre elementos productivos y elementos de prueba.

Tratamiento: Definir entornos idénticos al productivo para verificar las modificaciones a realizar sin afectar activos productivos. No utilizar activos de contingencia como ambientes de prueba de nuevas versiones, parches, etc.

En caso de realizar desarrollo de elementos de software evitar las herramientas de desarrollo y los fuentes de código en los elementos del sistema.

3.8.3 Protección contra código malicioso

Generadores de riesgo: No instalar protectores contra código malicioso. No atender las vulnerabilidades detectadas por fabricante o nuevas formas de ataque. Desactivar la protección contra código malicioso para determinadas tareas.

Tratamiento: Instalar software para prevenir código malicioso e intrusiones, manteniéndolo correctamente actualizado. Atender las vulnerabilidades publicadas por el proveedor y los métodos propuestos para mitigarlas. Instalar parches de seguridad de SC y SO, previa verificación del procedimiento de instalación, y su funcionalidad final, en los equipos de prueba. Configurar adecuadamente la distribución de eventos. Enviar eventos de las herramientas de detección a repositorios seguros para su análisis. Configurar la carga automática de patrones de ataques y compromiso, detectados por SWIFT en herramientas automáticas (STIX-TAXII). Verificar periódicamente la integridad de los sistemas de SWIFT y sus bases de datos mediante los comandos adecuados. Configurar controles de integridad durante el arranque de cada elemento de software del SC. Forzar regularmente los errores conocidos para verificar el correcto funcionamiento del chequeo de integridad y de la cadena de eventos y alertas que debe disparar. Analizar todo evento correspondiente a los activos del SC. Analizar información sobre modus operandi de últimos ataques registrados por SWIFT y realizar las comprobaciones locales que correspondan.

3.8.4 Resguardo

Generadores de riesgo: Falla de hardware. Falla de disco. Corrupción de archivos o disco. Mensajería financiera archivada y eventos del sistema.

Tratamiento: Respecto a los certificados de conectividad, realizar periódicamente una copia de seguridad de SNL mediante los comandos de línea correspondientes, por ejemplo: Snl_backup. Complemento: copiar certificados de SNL en lugar seguro. Respecto a SAG y SAA, realizar copias diarias de configuraciones. Según la política de la institución los mensajes ya cursados o completados deben extraerse del server SAA y guardarse en lugar seguro para consultas posteriores. Los resguardos realizados con el software de SWIFT de SAA son encriptados y solo los puede recuperar la misma licencia de la institución. La nueva modalidad de carga de mensajería SWIFT utiliza los mensajes anteriores como template: Extraer de la base interna de mensajería períodos que tengan errores de transmisión para evitar repetirlos. La opción SWIFT DataBase Recovery permite guardar mensajería completa y en curso en backup en línea: en caso de inconvenientes con el sitio de producción, la mensajería podrá transferirse al sitio de contingencia.

La herramienta de backup de base de datos del SAA no guarda mensajes sino la configuración del SAA. El restore de la base de datos del SAA actualiza la configuración y el estado de los partners de SAA. El restore de la configuración elimina eventos anteriores en el equipo: Salvar la información histórica antes de aplicar restore de configuración. Realizar un backup de configuración antes de trabajar en SAA/SAG. En el caso de utilizar el restore de la configuración amas instalaciones deben tener el mismo certificado en la versión actual.

Realizar los backup de SNL luego de cada renovación de certificados. Realizar backup de SAA y SAG antes y después de cada cambio de versión;

ambos son críticos y los backups de versiones anteriores dejan de ser válidos para la nueva versión.

3.8.5 Vulnerabilidades técnicas

Generadores de riesgo: Nuevas vulnerabilidades detectadas en activos del SC. Contemplar software y hardware del SC como también sus elementos de comunicaciones como switches, routers, impresoras y todo elemento que permita vulnerabilidades.

Tratamiento: Una vez identificados los activos del SC (Inventario) analizar las comunicaciones y actualizaciones emitidas por el fabricante que corresponda. Desafectar activos sin soporte de fabricante. Detección periódica de vulnerabilidades y su análisis.

Las vulnerabilidades solucionadas con cada parche de software están identificadas por SWIFT en cada documento de la versión. Analizar regularmente las noticias y alertas de seguridad publicadas por SWIFT en su sitio web para sus productos y servicios.

3.8.6 Restricciones a la instalación de software

Generadores de riesgo: Presencia de software malicioso en elementos agregados por usuario para realizar tareas productivas. Análisis de vulnerabilidades técnicas incompleto. roles de negocios acceden a credenciales críticas del SC y las emplean para agregado de elementos de software.

Tratamiento: Relevamiento periódico de software instalado en cada activo del SC. Comunicar las modificaciones o agregados de elementos de software realizados a todos los sectores involucrados en el SC.

3.8.7 Controles de la auditoría de sistemas de la información

Generadores de riesgo: Desconocimiento del SC. Tareas productivas permiten controles parciales. Falta de registro preciso de actividades con credenciales críticas. Registros de eventos no informatizados.

Tratamiento: Capacitar a personal de auditoría en los SC de la institución. Se propone que auditoría de sistemas forme parte del equipo de trabajo, mediante un monitoreo activo, al momento de emplear las credenciales críticas del SC listadas en el punto 6. Aspectos Organizativos. Cómo mencionamos antes esto permite a la auditoría relevar evidencias sobre la ejecución procedimientos y tareas con credenciales críticas en los diferentes elementos del SC: SWP, SAA, SAG, SNL, SAC, O2M y actividades en la herramienta swift.com.

Las áreas de Seguridad, Negocios e Infraestructura deben preparar reportes para el área de auditoría documentando las actividades en el SC. Las áreas de control de acceso físico deben generar reportes de acceso físico a las áreas críticas. En cuanto a los accesos a los elementos del SC se recomienda generar un informe técnico que describa la tarea realizada e incluir el conforme del ejecutante y del cliente interno controlante de dicha tarea.

3.9 Seguridad en las telecomunicaciones.

3.9.1 Controles internos. Controles de red

Generadores de riesgo: Adulteración de información en reposo. Envío de órdenes incorrectas a corresponsales. Ejecución local de tareas basadas en información falsa o adulterada.

Tratamiento: Además del control de permisos de los SO,claramente vulnerables, utilizar criptografía en la protección de información y autenticación de datos. El repositorio del dominio DATO debe autenticar los datos recibidos y realizar una verificación criptográfica de integridad antes de ser utilizados. Existencia de procedimientos en dominio Back Office para verificar la fidelidad de la información. Implementación en el dominio Back Office del protocolo de autenticación e integridad de la información intercambiada con el gestionador de mensajería SAA. La tecnología

disponible en SAA es HMAC-256 y AES256-GCM. Para datos en zona segura, puede no requerirse encriptación. Fuera de ella, la encriptación es necesaria para mantener la confidencialidad e integridad y autenticidad de los datos. Dentro de la zona segura es necesaria la autenticación de los datos intercambiados.

3.9.2 Seguridad de los servicios de red (Seguridad de la red del SC).

Generadores de riesgo: Intercambio de información con activos maliciosos o incorrectos. Adulteración de información en tránsito. Interceptación de comunicaciones.

Tratamiento: Configurar la clave simétrica en la interconexión de activos: SAA y SAG soportan un mecanismo criptográfico que autentica los servidores y asegura la identidad de cada extremo de la conexión mediante clave simétrica y certificados. La tecnología mencionada también verifica la integridad de los mensajes intercambiados y soporta el principio de cuatro ojos. En este contexto, el principio de cuatro ojos permite asegurar que se necesitan dos oficiales de seguridad para definir la comunicación SAA-SAG que enviará la mensajería financiera a SWIFT. Es recomendable desarrollar una CA en la institución para manejar los certificados de identificación de los activos del SC y no utilizar los autogenerados con las herramientas de SWIFT. Establecer certificados en cada SWP relacionados a la CA interna. Para asegurar la confidencialidad de la conexión se habilita la opción de encriptado en la configuración de la comunicación: protocolo TLS. Restringir las comunicaciones entre las estaciones de trabajo mediante firewalls del SO, u otros activos de interconexión de las estaciones que permitan bloqueo de comunicaciones de datos.

3.9.3 Segregación de redes

Generador de riesgos: Exposición activos críticos a elementos de la red fuera del SC.

Tratamiento: Segregar redes críticas de los SC de las no críticas. Establecer protecciones perimetrales internas. Definir servicios de red para zonas críticas en función de riesgo de exposición y criticidad en el negocio. Segregar redes de acceso a los SC mediante estaciones definidas. Autenticar estaciones de trabajo.

Es crítico segregar, física y lógicamente, los ambientes productivos, alternativos y de pruebas frente al riesgo de compromiso malicioso de uno de ellos.

Aplicar el concepto de hardening en los elementos de redes es una herramienta útil para desactivar vulnerabilidades existentes.

Segregar las funciones del SC en elementos físicamente separados controlando el tráfico entre estos: software de interfaz de usuario (SWP), core del SC: SAA y SAG-SNL en diferentes activos.

3.9.4 Mensajería electrónica. Intercambio de información

Intercambio de información con SWIFT Service Bureau.

Generadores de riesgo: Pérdida de confidencialidad de la información. Tiempo de respuesta ante eventos.

Tratamiento: Establecer claramente las políticas de seguridad de la información , los tiempos de respuesta ante eventos. Así como también, mecanismos criptográficos que identifiquen unívocamente al proveedor de servicios, a la entidad y la integridad de los datos intercambiados. Establecer los procedimientos de credenciales críticas en poder del proveedor que afecten a la institución. Generar un certificado de autenticación manejado por la entidad para ser instalado en el servidor remoto del proveedor con el fin de identificar fehacientemente donde se conecta la entidad enviando la mensajería SWIFT: Recordar que la firma digital de identidad de la entidad se realiza en el SAG del *service bureau*.

3.10 Relaciones con proveedores

Los proveedores de comunicaciones y soporte son críticos en el sistema instalado en la institución. Para aquellas instituciones que utilizan la modalidad de *service bureau* el control del proveedor es sumamente crítico ya que depositan en el SB credenciales críticas que pueden reconfigurar el sistema brindado mediante el servicio.

Generadores de riesgo: Procedimientos internos en el proveedor diferentes de lo estipulado. Pérdida de certificaciones de proveedor. Pérdida de RRHH certificados por parte del proveedor.

Tratamiento: Permisos de auditorías espontáneas de la institución al proveedor por contrato. Acceso a los logs de los equipos de servicio. Eventos de utilización de credenciales críticas del sistema on-line con el proveedor. Procedimientos internos del proveedor que requieran presencia de personal de la entidad. El proveedor debe otorgar credenciales y medios seguros de verificación del estado del sistema en su totalidad. analizar la posibilidad de un segundo proveedor de servicios como redundancia. Generación automática de eventos dirigida a repositorios de logs de la institución para su control.

3.11 Gestión de incidentes

Generadores de riesgo: Compromiso de equipamiento no detectado. Pérdida de conocimiento de la institución frente a la solución de eventos.

Tratamiento: Establecer la recopilación, delegación, tratamiento y solución de eventos en activos de SC. Generación de eventos con múltiples ingresos: automáticos y vía usuario. Posibilidad de consulta sobre eventos históricos, base de conocimiento y evolución de eventos. Correlacionar eventos en el tiempo y frente a otras áreas críticas. Definir índices de compromiso de SC en función de eventos reportados. Clasificar y priorizar

eventos de SC. Los elementos del SC SWIFT: SAW, SAA, SAG, etc. de deben configurar para alimentar la generación automática de eventos a ser tratados por los procedimientos correspondientes. Generar eventos para verificar el correcto funcionamiento de los elementos y procedimientos. En función de la clasificación de eventos. El refuerzo de configuraciones seguras produce alta probabilidad de eventos, alarmas, incidentes cuando hay intento de violentar alguna de las configuraciones y también en falsos positivos.En definitiva: son avisos a los que hay que analizar, llamemos como sea que los llamemos.

3.12 Continuidad del negocio

Generadores de riesgo: Entidad parcial o totalmente inoperable frente a eventos. Sanciones del ente regulador. Entidad y Directorio afectado por sanciones legales. Pérdida de negocios y clientes.

Tratamiento: Desarrollar y analizar el plan de continuidad de la institución frente a eventos. La dirección debe exigir a los responsables de áreas las pruebas de planes de continuidad en forma regular y coordinada. Clasificar la periodicidad de pruebas de la continuidad de negocio según la criticidad de los elementos del plan. La verificación del plan de continuidad de negocio durante simulacros no solo verifica el plan, sino que instruye y da confianza al personal en acciones a tomar frente a eventos, disminuye el riesgo operacional de la entidad y refuerza su imagen institucional.

3.12.1 Redundancias

Generadores de riesgo: Pérdida de servicio por desconocimiento de procedimiento del sistema alternativo. Procesamiento duplicado de órdenes. Procesamiento incompleto de órdenes solicitadas. Exposición a nuevos riesgos por fallas en los procedimientos y configuración de activos contingentes. Impedimento de operar sitios alternativos.

Tratamiento: Contar con procedimientos claros y verificados para la activación de redundancias. Definir y detectar eventos que disparan los procedimientos para activar las redundancias que se necesiten. Entrenamiento del personal en la activación de redundancias y vuelta a la normalidad. Permisos de personal con acceso a los sitios alternativos frente a una situación de emergencia en sitio primario. Testeos periódicos de canales de redundancia. Los datos de configuraciones resguardados adecuadamente y los backups ayudan a disminuir significativamente el tiempo de pérdida de servicio.

3.13 Cumplimiento

Este control se refiere al cumplimiento de las normas del mercado donde opera la entidad y cumplir los requisitos obligatorios de los proveedores de servicios evitando sanciones que pueden aumentar los costos de la entidad o bien derivar en pérdidas de licencias.

Generadores de riesgo: Sanciones del ente regulador. Entidad y Directorio afectado por sanciones legales. Pérdida de licencia de SWIFT. Comunicación de SWIFT al ente regulador, por falta de cumplimiento de temas referentes a la seguridad o mal comportamiento de la entidad en la red de servicios.

Tratamiento: Implementar los requisitos del ente regulador según corresponda a la institución, en caso de faltas de incumplimiento comunicar al ente regulador las mismas junto a un plan de mitigación y solución. Realizar las auditorías de los requisitos obligatorios mediante personal certificado según solicita SWIFT. Solucionar observaciones de auditorías de anteriores.

4. Cuarta Parte: Ataques reportados

La información del siguiente análisis se basa en noticias de ataques presentados en diferentes medios de Internet y en los reportes de analistas de seguridad. Se pretende detectar situaciones que reflejen la falta de controles mencionados en el análisis realizado en capítulos anteriores del presente trabajo. Si bien los casos mencionados son fehacientes, el verdadero aporte son las hipótesis de trabajo que permiten la reflexión y el análisis. Veremos vulnerabilidades generadas por la implementación incorrecta de sistemas críticos, muchas veces basadas en el desconocimiento y otras pocas en la planificación de ataques futuros.

4.1 Banco Central de Bangladesh (Feb 2016) (101M)

Fraude: jueves 4 de feb. de 2016 (8:03 PM) El Banco Central de Bangladesh (BB) envía 35 pedidos de transferencias vía la Reserva Federal totalizando un valor cercano a mil millones de dólares. La Reserva Federal utiliza sus corresponsales para cumplir las órdenes recibidas: Deutsche Bank, Sri Lanka PABC y Filipinas RCBC. El sistema automático de la Reserva Federal direcciona las 35 órdenes irrevocables recibidas a los corresponsales correspondientes por la misma red, SWIFT.

Viernes 5 de feb.: Algunas transacciones llegan a destino, otras son bloqueadas por la coincidencia de la palabra “Júpiter”: sistemas automáticos de prevención de lavado detienen el pago por la palabra “Júpiter” que parte del nombre de una empresa sospechada de lavado de dinero. Los mensajes que llegan a destino (80M) son trasladados a otras cuentas en casinos locales y también retirados el mismo día en efectivo y de la sucursal del banco RCBC en la ciudad de Metro Manila, Filipinas, de la calle Júpiter. Otros pagos fueron detenidos en el Deutsche Bank advertidos por *Pan Asia Bank* basados en el monto inusual de la operación y en la imposibilidad de

identificar al destinatario por normas de lavado de dinero: *Shalika Foundation* estaba mal escrita “Shalika Fundation”.

El viernes a las 8:00 AM se detecta en Dhaka que la impresora no funciona y no hay impresiones de mensajes disponibles para ejecutar los procesos correspondientes. Se solicita su reparación. Ese viernes era feriado en Dhaka.

Sábado 6 de feb a las 8:00 AM. Se repara la impresora, y se detecta que no responden correctamente los servidores de SWIFT. El soporte de SWIFT soluciona el inconveniente remotamente [25]. Una vez que los empleados ingresan al sistema, se detecta que hay mensajes extraños y el operador trata de comunicarse con la Reserva Federal para clarificar el supuesto error de esta última. El sábado no hay respuesta alguna de la Reserva Federal, tampoco el domingo.

Lunes 8 de feb. de 2016, una vez contactada la Reserva Federal y detectado el ataque, el Banco de Bangladesh trata de hacer lo mismo con el banco RCBC de Filipinas para detener los pagos pero sin éxito. Así como el Jueves 4 y viernes 5 fue día no laborable en Bangladesh, el lunes fue feriado en Filipinas y el inicio de la temporada alta en los casinos de la zona por el Año Nuevo Lunar Chino. BB también envía mensajería de cancelación al banco en Filipinas sin éxito alguno.

Según análisis posteriores, se detectó que atacantes externos ingresaron al sistema SWIFT *Alliance Access* e instalaron malware para diferentes propósitos. Durante la etapa de reconocimiento y movimiento lateral se comprometieron 35 máquinas del BB, hasta obtener las credenciales de la cuenta de mayor privilegio en el sistema operativo donde estaba instalado el sistema SWIFT.

Uno de los propósitos del malware instalado fue detectar la operatoria del banco para conocer sus movimientos y evaluar la factibilidad del ataque

durante varios meses, segundo obtener las credenciales de acceso al sistema (usuario y *password*) y preparar el ataque. Para ello se modificó el sistema de impresión utilizado por SWIFT y, así se evitó mostrar las operaciones enviadas vía impresora y de las respuestas recibidas respecto de las confirmaciones de las operaciones. Pero el más sofisticado de los preparativos fue modificar la rutina de verificación de la integridad del sistema mediante el cambio de dos bytes que anularon la verificación de integridad dando siempre resultado exitoso durante los meses que duró la etapa de reconocimiento del ataque [26]. Generalmente los antivirus se configuran con excepciones en directorios y tal vez este fue el caso: El atacante trabajaba en los directorios exceptuados del control de malware, donde el control de integridad del SAA debería funcionar.

Las autoridades de Bangladesh que investigaron el incidente- el área de ciberseguridad de la policía nacional- detectaron que el sistema SWIFT estaba expuesto, no solo a las 5.000 estaciones de la red del banco, también tenía conectado un *router* inalámbrico, reutilizado de otra área, con acceso a internet. Si bien el *router* inalámbrico fue utilizado durante las configuraciones del sistema SWIFT, luego se apagó. Oficiales del banco no se explican cómo estaba encendido en los días del ataque ya que- algunos meses atrás- había finalizado la configuración del sistema y se habia desconectado. El sistema fue instalado en una sala cofre y el *router* inalámbrico facilitaba el acceso de los expertos del sistema SWIFT para su puesta a punto.

Es importante notar que el sistema había sido instalado pocos meses atrás y que el BB iniciaba una era tecnológica, dejando atrás el Télex.

Según el análisis de la policía de ciberseguridad, el personal técnico del banco sabía que estaba exponiendo el sistema a ataques externos en función de la baja protección del SC [27]. Otro dato importante es que el BB

enviaba un promedio de dos mensajes diarios y el día del ataque se emitieron 35 mensajes en cuestión de minutos.

Principales dominios afectados

6-Organización interna. 8-Gestión de activos. 9-Control de accesos. 11-Protección física 12-Seguridad en las operaciones. 13-Seguridad de las comunicaciones. 15-Relaciones con los proveedores. 16-Gestión de incidentes.

4.2 Punjab National Bank (Feb 2018) (2000M)

Fraude: PNB es el segundo banco nacional en importancia en la India. El fraude se realiza utilizando garantías de comercio exterior para importar mercadería que nunca fueron canceladas. La operatoria del fraude funcionó desde 2011 hasta 2017.

Las garantías de crédito para comercio exterior se emiten por el servicio y el sistema SWIFT en el PNB. En ese período lo operaba una sola área sin conexión al resto del banco. Si el gerente del área no concurría a su puesto laboral, los mismos clientes solicitaban realizar la operación en otro momento “más adecuado”. No había otras personas que sepan operar el sistema SWIFT y el responsable no permitía que otras personas se involucraran [20]. Las órdenes de crédito (MT700) eran enviadas por carga manual.

El ente regulador del mercado financiero en India, el Banco de la Reserva de la India (RBI) realiza inspecciones con auditores certificados externos. En el período 2011-2017 el PNB tuvo contacto con 18 firmas de auditoría para cumplir con los requisitos de presentación de formularios al ente regulador. Ninguna de ellas detectó el inconveniente a pesar de constar reuniones con el responsable del área de SWIFT: “Shetty Sr”. También es llamativo que los principales beneficiarios de la estafa salieron del país días

antes de que el fraude se diera a conocer. El PNB implementó una oficina de autorización de transferencias para evitar futuros fraudes entre otras medidas [21]. Mencionamos esta para resaltar la importancia de los procedimientos y la desconcentración de credenciales en las tareas.

Principales dominios afectados: 6-Organización interna. 7-RRHH. 12-Seguridad en las operaciones. 18-Cumplimiento.

4.3 Banco de Chile (I) (Mayo 2018, 4M)

Fraude: Elías, un empleado del Banco de Chile, introduce órdenes de pagos mediante el conocimiento de credenciales de sus superiores (o connivencia, en investigación). Lo realizó durante 10 años (entre 2008 y 2018) trabajando desde la gerencia de pagos internacionales. Análisis posteriores determinaron que realizó un total de 300 transferencias desde la cuenta MB-Dólares-USA hacia la cuenta de extracción que manejaba para hacerlo físico. Durante un mes de aumento de estas transferencias por parte del atacante, otros operadores de la cuenta detectaron movimientos extrañas y se ordenó ejecutar un procedimiento interno en el área que detectó el fraude.

Según los procedimientos internos del banco de Chile y regulaciones bancarias, las órdenes de pagos necesitan un soporte físico de respaldo: no existe en los registros históricos soporte físico alguno. Posiblemente, el atacante destruyó los registros físicos una vez realizada la transferencia, o bien, nunca fueron realizados, como parte del plan para no ser detectado por los controles en ese momento, claramente incompletos, vistos ahora a la luz de los hechos.

Existen registros internos en algunos de los sistemas que permitieron evaluar el fraude realizado durante diez años. Lo más llamativo es que la cuenta origen no debía registrar operaciones hacia una cuenta en Chile [22].

Principales dominios afectados: 6-Organización interna. 7-RRHH. 9-Control de accesos. 12-Seguridad en las operaciones. 16-Gestión de incidentes. 18-Cumplimiento.

4.4 Banco de Chile (II) (Mayo 2018, 10M)

El incidente se inicia el jueves 24 [23] y se restablece el normal funcionamiento con los clientes el lunes 28 de mayo de 2018 según un comunicado oficial del Banco de Chile [24].

Al detectar el ataque el banco decidió ejecutar el protocolo de contingencia. Recibieron un ataque similar al *ransomware* pero que destruía el MBR (*master boot record*) al simular ser una encriptación del disco duro. Así inhabilitaron cerca de 500 servidores y 9000 computadoras de escritorio, ya sea por afectación directa o bien por apagado preventivo: El objetivo DoS se cumplió.

Este fue un ataque de interrupción de servicio para apartar la atención del ataque primario. Afectando 500 servidores y 9000 computadoras se aseguraban que todo el personal técnico estaba abocado a solucionar semejante inconveniente y el personal operativo aplicando los planes de contingencia.

La instalación SWIFT del banco funcionaba sin inconvenientes aunque ya estaba comprometida. Es así que los atacantes lograron emitir órdenes de pago hacia cuentas fraudulentas usando el sistema SWIFT del Banco de Chile. Según el CEO del banco de Chile se detecta el movimiento y varias transacciones son detenidas satisfactoriamente pero logran pasar las primeras cuatro por un monto de diez millones [28] [29].

Según varios portales no se utilizó ninguna vulnerabilidad específica del sistema SWIFT: Los mensajes se enviaron utilizando las credenciales de operadores capturadas en la etapa de preparación del ataque [30]. Es de

importancia la coincidencia entre las fechas de ambos fraudes: el primero sale a la luz el 14 de mayo del 2018, después de diez años de fraude continuo, y el segundo se ejecuta el 24 del mismo mes con éxito.

En una entrevista al Gerente del banco, éste menciona que deberán manejar nuevos procesos de negocios, más seguros [31]. El banco de Chile se contacta inmediatamente con el Banco Central de Chile al detectar el ataque, evitando otros ataques similares en el país y en la región.

Principales dominios afectados:

6-Organización interna. 9-Control de accesos. 12-Seguridad en las operaciones. 13- Seguridad de las comunicaciones. 16-Gestión de incidentes. 18-Cumplimiento.

4.5 Bancomext

Bancomext- enero de 2018 primer ataque fallido [32] (100M) Bancomext: Mensajes vía SWIFT enviados a una iglesia en Corea como donación, son detectados y anulados por un operador del sistema SWIFT del banco. Feriado en Corea, lo cual le da tiempo al banco para detener la operación.

Principales dominios afectados:

6-Organización interna. 8-Gestión de activos. 9-Control de accesos. 12-Seguridad en las operaciones. 13-Seguridad de las comunicaciones. 18-Cumplimiento.

4.6 Banxico en México

Ataque a Banxico - abril de 2018, el día 17 el Banco Central detecta irregularidades en una entidad. Fines de abril hasta el 17 de mayo de 2018, con éxito (20M): No se trasladó el dinero vía SWIFT, se la extrajo en el mismo México. El ataque utilizó vulnerabilidades del protocolo SPEI

(Banxico). El principal banco afectado fue el segundo más grande de México, Banorte. El ataque se basó en la interacción entre los bancos y el sistema de pagos SPEI, su protocolo. Cinco instituciones detectaron transferencias no autorizadas.

El Sistema de Pagos Electrónicos Interbancario de México (SPEI), llamado también Banxico, se inició en el 2004. El sistema utiliza un protocolo propietario y abierto, diseñado en México. Cada entidad lo implementa según sus requisitos internos operativos y productos de servicios ofrecidos a los clientes. Aparentemente los atacantes tuvieron acceso al código del protocolo [33] disponible para todas las entidades en México y detectaron vulnerabilidades que podrían explotar. Las transacciones son firmadas electrónicamente con un esquema PKI de certificados emitidos por el Banco Central de México [34], [35].

Principales dominios afectados:

8-Gestión de activos. 9-Control de accesos. 11-Protección física 12-Seguridad en las operaciones. 13-Seguridad de las comunicaciones. 14-Desarrollo de sistemas. 15-Relaciones con los proveedores. 16-Gestión de incidentes. 17-Gestión de Continuidad del negocio.

4.7 Cronología de ataques registrados durante los últimos años:

- Enero de 2015 : Banco del Austro, Ecuador (10 días, 12 órdenes de ataque vía Wells Fargo y Citibank /SWIFT. Reutilización de mensajes) [36]
- Noviembre de 2015 : *Vietnam's Tien Phong Bank* (se detectó y anuló. *PDF reader*, *top Internet Bank*, Parte de un grupo tecnológico) [37] y [38]
- Febrero de 2016 : Banco Central de Bangladesh
- Mayo de 2016 : Noticia de SWIFT alertando [39]

- ➢ Abril de 2017 : Ingreso al Service Bureau EastNet SB (NSA) [40]
- ➢ Octubre de 2017 : NIC *Asia Bank* [41] [42] (Destino US, LON, Feriado, 31 ms.)
- ➢ Octubre de 2017 : *Taiwan's Far Eastern International Bank* (Multa de Ente regulador local FCS por incumplimiento de protecciones) [43]
- ➢ Diciembre de 2017 : *Russian State Bank Globex* [44]
- ➢ Enero de 2018 : Bancomext
- ➢ Febrero de 2018 : *India's City Union Bank* [45]
- ➢ Abril de 2018 : SPEI México (Red nacional de pagos)
- ➢ Mayo de 2018 : Banco de Chile

5. Quinta parte, detección de ataques.

Los ataques al SC tienen como primer objetivo ingresar a la institución, moverse lateralmente hasta obtener información de la operación del sistema para luego llevar adelante el segundo objetivo, el retiro de dinero, según el plan más pertinente. Al ajustarse el SC a los puntos tratados anteriormente, por ejemplo, segregados los roles y la red, etc., uno de los principales indicadores de compromiso en las máquinas es la existencia de tráfico inusual y la utilización de credenciales fuera del horario normal de tareas: El funcionamiento del ataque debe ser verificado con anterioridad al mismo y esto va a producir fallas, o comportamientos inusuales, en el SC comprometido. La primera etapa de preparación del ataque es donde se detectan comportamientos anormales que parecen inofensivos. En esta etapa la víctima soluciona inocentemente estos “problemas” mediante justificaciones simples: “siempre pasa a esta hora, la prendo y la apago y listo” o “debe ser la actualización, después lo reporto”. Sumado a esto, la falta de análisis de eventos recopilados o su calidad. La ventaja del atacante es que para la víctima - cuyas credenciales está intentando obtener, y opera en el sistema ya comprometido- este es su ambiente normal de trabajo y necesita llevarlo adelante ya que son tareas que deben ejecutarse con cierta atención y en el tiempo determinado porque “cierran los mercados y quedamos afuera”. Esta característica de la tarea en el sistema SWIFT juega a favor del atacante y la decisión de cómo actuar frente a la detección de estos indicios extraños durante el horario productivo debe analizar la institución. No es menor la decisión de instituciones atacadas que decidieron agregar áreas de análisis de mensajes antes de su envío.

Para detectar ataques, es importante analizar los comportamientos extraños por simples que parezcan: cuanto más sofisticado sea el ataque más simples serán los indicios. También nos puede ayudar la recolección de

información del comportamiento del SC respecto de la carga de trabajo para luego verificar si hay o no desvíos en métricas aplicadas a esta información. Por ejemplo midiendo tiempo de proceso, uso del CPU, de la memoria, tráfico y tipo de tráfico de red, *handshake*[4], etc.

El ataque de Bangladesh nos propone la alternativa de verificar controles: con la periodicidad adecuada y los recaudos pertinentes, modificar parámetros de las verificaciones para detectar si los controles implementados funcionan realmente. Cómo también repasar las configuraciones y verificar que estén según lo establecido.

Como vimos los ataques, al Banco Central de Bangladesh y al sistema de pagos local de México, son muy sofisticados y específicos. Como se mencionó en párrafos anteriores, esto requiere una contramedida de igual naturaleza: Tareas de reconocimiento específicas ya que el ataque tendrá similitudes a otros pero cada institución es diferente y el atacante deberá adecuar las técnicas cada vez más sigilosas y efectivas.

De lo que no puede prescindir el atacante es de recolectar información y datos, por esto la detección de comunicaciones anormales es muy importante, como también controlar todos los accesos físicos y/o lógicos a los activos del SC.

Todo intento de comprometer las credenciales del banco debe generar alertas en los procesos de seguridad de los sistemas críticos. Hasta ahora no se observaron ataques efectivos del tipo de Banxico a la red SWIFT, vulnerando sus capacidades criptográficas y de protocolo, es posible en el futuro observar este tipo de intentos en función de la escalada tecnológica y sofisticacion en los ataques. Para reducir este tipo de ataques

[4] Sin importar el contenido ni el motivo de paquetes de tráfico, registrar cómo dialogan entre sí los activos del SC en una situación normal y segura. Se debe contemplar cambios de patrones mediante actualizaciones en los *drivers* de red, versiones de SO o elementos de red reemplazados, etc.

es altamente recomendable que siempre una institución se conecte a SWIFT mediante los productos Alliance Connect propios o vía un SB, evitando conectividades que no involucren un SAC o saltos de conectividad evitables. En todas las conectividades se debe activar la autenticación y encriptación de la información intercambiada en todas sus capas posibles. También es altamente recomendable llevar un control, y su histórico, respecto de eventos de conectividad con SWIFT para detectar cambios en los patrones y así analizar qué implica el cambio de patrón detectado.

Siempre debe estar presente que las configuraciones de seguridad complican al atacante introduciendo complejidades, no garantizan la seguridad absoluta. Permiten que el atacante desestime el objetivo en función de su complejidad y también que el atacante sea detectado en función de los errores cometidos en función de las protecciones configuradas.

Las herramientas disponibles como los sistemas de detección de intrusiones (IDS), los sistemas de prevención de intrusiones (IPS), tratamiento automático de eventos (SIEM), los antivirus, junto a los procedimientos adecuados, ayudan a mantenernos alerta. En las búsquedas automáticas puede haber muchos falsos positivos pero todos deben ser analizados y catalogados. Aquí también podemos analizar el cambio de comportamiento y obtener datos importantes para detectar ataques. El desvío en el comportamiento de los errores conocidos será una fuente importante a tener presente.

Cada entidad deberá generar su patrón de comportamiento y en función de las alteraciones encender las alarmas que correspondan para su análisis por parte de los expertos en seguridad informática asignados.

Como mencionamos, SWIFT provee a las instituciones reportes de investigaciones realizadas en servidores comprometidos por ataques

detectados en las entidades. La base de información disponible también se nutre de información de agencias de inteligencia y organismos de seguridad que aportan información a la cooperativa. Esta información es muy valiosa para orientar el análisis y realizar verificaciones específicas según lo recomendado por SWIFT.

Los ataques reportados a las entidades financieras que implementan el sistema SWIFT tienen como particularidad que se extienden en el tiempo para lograr su objetivo. También involucran una cantidad importante de activos comprometidos en la institución. Este tipo de ataques está catalogado con el nombre *Advanced Persistent Threats* (APT).

Según el NCCIC del gobierno de EEUU [46] la alerta comunicada TA18-276B sobre los ataques del tipo APT [47] propone aumentar la robustez del sistema a defender para poder detectar la intrusión ya que el atacante deberá emplear métodos que pueden exponerlo a los sistemas y procedimientos de detección. Muchas de las recomendaciones coinciden con lo analizado en el presente trabajo: Segregar la red del SC del resto de la red de la institución financiera, protecciones perimetrales, roles, análisis de eventos, etc. Las bases para permitir la detección temprana está en los pilares:

- Segregacion de la red
- Segregacion de roles
- Protecciones perimetrales y de configuración
- Análisis de eventos

Conclusiones

Según el responsable del Banco Central de Bangladesh, en 2016, no solo el banco no estaba preparado para responder al ataque, tampoco lo estaba la comunidad internacional al momento del incidente para detectar y detener semejante ataque, que solo por una coincidencia fortuita no tuvo el éxito pretendido por los atacantes.

Analizando la reacción de la comunidad podemos ser optimistas respecto del futuro de la robustez y seguridad del SC SWIFT. La primera reacción positiva de la comunidad fue la discusión de la amenaza planteando una estrategia inicial para mitigar la situación involucrando a toda la comunidad en acciones a tomar. Una de las lecciones transmitidas a la comunidad internacional, no solo financiera, es que tratar los ataques de manera individual, aumenta el riesgo de ataques al sistema en su totalidad. Hoy SWIFT brinda un canal donde se comparte información sobre eventos y ataques ocurridos a la comunidad. También varios entes reguladores establecen la obligatoriedad de informar los eventos ocurridos en la institución detallando las medidas implementadas al respecto.

Los ataques efectuados al sistema de transferencias de las entidades financieras ayudaron a mejorar la madurez en seguridad del SC y de la comunidad. Sí bien todo el sistema está bajo análisis permanente, SWIFT no sumó nuevas características tecnológicas críticas de seguridad al producto utilizado en las instituciones, pero sí debió transformar parámetros de configuración opcionales de los productos en obligatorias para las entidades mediante el contrato de servicio que tienen con la cooperativa. Los parámetros como doble factor de autenticación, segregación de red, encriptación, autenticación de datos, etc. se tornaron requisitos obligatorios. Además entre los puntos que SWIFT hace énfasis se encuentran la gestión

de incidentes y la segregación de roles entre muchos más. La gestión de los incidentes se presenta en el trabajo cómo sumamente crítica. Las protecciones configuradas tienen por finalidad primaria blindar el servicio transformándolo en seguro tecnológicamente mediante métodos criptográficos cómo autenticación, encriptación, etc. El segundo objetivo de la configuración de protecciones, de todo sistema, es la alta probabilidad de generación de eventos en una institución comprometida. Por esto se debe tener especial cuidado en el proceso de tratamiento de eventos: sí no hay atención a la detección de eventos, sí no hay adaptación a la defensa en función de los eventos y sus métricas, solo es cuestión de tiempo para el atacante obtener éxito.

Por otro lado, los ataques que vimos hasta este momento, salvo una excepción, buscan obtener credenciales válidas para efectuar los fraudes. El modus operandi actual es el de obtener las credenciales de los operadores validos para generar las órdenes fraudulentas armando una infraestructura que permita esconder las operaciones del fraude y otros eventos capaces de alertar a la institución comprometida. Vemos que el eslabón más débil del sistema descripto en el trabajo es el mapeo de un operador con sus credenciales electrónicas que lo representan digitalmente: El doble factor, los datos biométricos y la geolocalización son herramientas para acercar estos dos universos, la identidad real versus la identidad virtual, y a la vez para robustecer la utilización de credenciales válidas. Las herramientas listadas mitigan el problema de identidad, no lo solucionan. Con más certezas que antes seguimos expuestos a la incertidumbre del actor real.

Cómo vimos en el análisis realizado oportunamente sobre los roles y su segregación: la cadena tecnológica productiva se ve reforzada frente la posibilidad de procesar datos incorrectos con la distribución adecuada de los roles en función de la creación del autocontrol en la cadena productiva.

Además de la segregación, se puede plantear en las instituciones la creación de roles de monitoreo permanente de los datos productivos con el objetivo de detectar datos erróneos o bien fraudulentos. Este tipo de roles no pueden ser detectados desde el relevamiento realizado por el atacante ya que solo detectara los roles que intervienen en el proceso activamente.

Con respecto al protocolo de servicios de la red, seguramente en un futuro cercano veremos cambios importantes en los protocolos de ejecución de órdenes entre instituciones financieras; por ejemplo, no sería extraño, ni tecnológicamente imposible, agregar métodos de autenticación del estilo de doble factor de autenticación a las órdenes irrevocables más allá del robusto esquema de certificación que hoy existe pero que no fue diseñado para detectar órdenes fraudulentas. Esta funcionalidad puede implementarse simplemente si las instituciones origen y destino lo coordinasen. Por supuesto será mucho más robusta una solución planteada por la comunidad en su conjunto.

El rastreo de las transferencias también es un tema importante en el momento de ejecutar la vuelta atrás de las órdenes fraudulentas y como control de órdenes enviadas. SWIFT estableció los instrumentos necesarios para la trazabilidad de las órdenes irrevocables, ahora le toca a las instituciones respetar las reglas de juego y ponerlas en funcionamiento dentro de la comunidad financiera.

Respecto a los entes reguladores, Bancos Centrales y otras entidades no comerciales en el sistema financiero es recomendable deshabilitar las órdenes a entidades no financieras innecesarias contenidas en los RMA (MT1xx, por ejemplo en el actual ISO 16022), canalizando estas necesidades mediante bancos comerciales y no exponer a un fraude importante las reservas que manejan los entes no comerciales pero con funciones críticas dentro del sistema financiero.

La criticidad del tema planteado en este trabajo es alta: Claramente una institución comprometida afecta a sus clientes, y a sus socios de negocios, pero también a su comunidad financiera, a la confianza del mercado afectado y a su ente regulador.

Las acciones llevadas adelante por SWIFT y su comunidad frente a los ataques están dirigidas al eslabón más débil del sistema de transferencias: la entidad financiera. El presente trabajo intenta aportar a los profesionales de seguridad y a las instituciones un poco de claridad sobre el críptico mundo de SWIFT para que se pueda discutir el tema de su seguridad con una base como punto de partida.

Anexo I

Tabla de asignación de funciones contemplando incompatibilidades detectadas. Dentro de cada área, (I ,N , S, A) aplicar la segregación correspondiente para evitar incompatibilidades mencionadas en el documento y generar el autocontrol en el flujo de tareas.

ID	Tareas	I	N	S	A
1.1	Administrador de Redes - Protecciones perimetrales	**X**	**IN**	**IN**	**MO**
1.2	Administradores de sistema operativo de servidores de aplicaciones, clientes y servicios.	**X**	**IN**	**IN**	**MO**
1.3	Owners de los elementos de software de servicios complementarios (Nota 1)	**X**	**IN**	**X**	**MO**
1.4	Owners de los elementos de software de infraestructura: SWP, SAA, SAG y SNL.	**X**	**IN**	**IN**	**MO**
2.1	Administradores de los elementos de software de infraestructura: SWP, SAA, SAG.	**X**	**IN**	**X**	**MO**
2.2	SAA Security Officers LSO y RSO (Nota 2)	**IN**	**X**	**X**	**MA**
2.3	SAA LSO y RSO Master Key	**IN**	**X**	**X**	**MA**
2.4	SAA LSO y RSo Installation Key	**IN**	**X**	**X**	**MA**
2.5	SAG LSO y RSO Installation	**IN**	**X**	**X**	**MA**
2.6	PKI Security Officers (Nota 3)	**X**	**IN**	**X**	**MA**
2.7	Administradores de HSM SWIFT	**IN**	**IN**	**X**	**MA**
2.8	Usuarios HSM	**X**	**IN**	**IN**	**MA**
3.1	Usuarios de mensajería SAA	**IN**	**X**	**IN**	**MO**
3.2	Carga y Modificación	**IN**	**X**	**IN**	**MO**
3.3	Verificacion	**IN**	**X**	**IN**	**MO**
3.4	Autorizacion	**IN**	**X**	**IN**	**MO**
3.5	RMA	**IN**	**X**	**IN**	**MO**
4.1	Monitoreo de eventos	**X**	**X**	**X**	**MO**
5.1	Administradores de swift.com	**IN**	**X**	**X**	**MA**
5.2	Usuarios de swift.com	**X**	**X**	**X**	**MO**

I : área dedicada a la infraestructura de sistemas, redes, etc.

N : area de negocios.

S : seguridad informática.

A : auditoría interna de sistemas.

IN : incompatibilidad de funciones

X : area asignada a la tarea descripta.

MO : tarea de monitoreo, control y contraste de información realizada por el área de auditoría.

MA : monitoreo activo, procedimiento de documentación de la utilización de credenciales críticas en el momento de la tarea.

Nota 1 : Autenticación, Middleware, Fileserver, etc.Owner es el usuario que ejecuta el servicio, y lo mantiene, con los menores privilegios necesarios.

Nota 2 : LSO y RSO son los dos roles que definen las configuraciones , perfiles, etc. y trabajan con el principio cuatro-ojos. Incompatible con tareas de mensajería y mantenimiento de rutina.Tienen privilegios de configuración, instalación y mantenimiento. Es recomendable delegar los roles de LSO y RSO en cuentas identificadas.

Nota 3 : Security Officers definen los certificados de conectividad que representan a la institución. Pueden trabajar con el principio cuatro-ojos. Existen dos tipos de SO que la institución debe tener presente: Online y Offline.

Referencias

[1] SWIFT: Sobre Nosotros

https://www.swift.com/about-us

Consultado 2 diciembre 2018

[2] SWIFT: Historia

https://www.swift.com/about-us/history

Consultado 2 diciembre 2018

[3] Banco Central de la Rep. Argentina. Carta Orgánica

https://www.bcra.gob.ar/Institucional/Carta_Organica.asp

Consultado 2 diciembre 2018

[4] Alliance Connect. Bronze, Silver y Gold.

https://www.swift.com/our-solutions/interfaces-and-integration/alliance-connect/packages#gold

Consultado 10 enero 2019

[5] Alliance Connect. Conectividad vía Internet. Bronze

https://www.swift.com/our-solutions/interfaces-and-integration/alliance-connect/packages#bronze

Consultado 10 enero 2019

[6] Alliance Connect. Conectividad directa, GOLD

https://www.swift.com/our-solutions/interfaces-and-integration/alliance-connect/packages#gold

Consultado 10 enero 2019

[7] Conectividad mediante terceros: Service Bureau

https://www.swift.com/about-us/partner-programme/shared-infrastructure-programme#topic-tabs-menu

Consultado 10 de enero 2019

[8] Plan de Service Bureau.

https://www.swift.com/about-us/partner-programme/shared-infrastructure-programme/programme-description?tl=en#topic-tabs-menu

Consultado enero 2019

[9] Directorio de Service Bureau

https://www.swift.com/about-us/partner-programme/shared-infrastructure-programme/service-bureau-directory?tl=en#topic-tabs-menu

Consultado enero 2019

[10] Producto Swift Alliance Access: Interfaz de mensajería.

https://www.swift.com/our-solutions/interfaces-and-integration/alliance-access

Consultado 10 enero 2019

[11] Producto Swift, Alliance Messaging Hub: Interfaz de mensajería.

https://www.swift.com/our-solutions/interfaces-and-integration/alliance-messaging-hub-amh_

Consultado 10 enero 2019

[12] Swift Alliance Entry. Interfaz de mensajería de SWIFT

https://www.swift.com/our-solutions/interfaces-and-integration/alliance-entry

Consultado 10 de enero 2019

[13] Conectividad. SWIFT Alliance Gateway

https://www.swift.com/our-solutions/interfaces-and-integration/alliance-gateway

Consultado 15 enero 2019

[14] Conectividad a SWIFT. SWIFT Net Link.

https://www.swift.com/our-solutions/interfaces-and-integration/swiftnet-link#topic-tabs-menu

Consultado 15 enero 2019

[15] Hardware Security Module de SWIFT, modelos por cantidad de certificados.

https://www.swift.com/our-solutions/interfaces-and-integration/hardware-security-module-hsm_

Consultado 15 enero 2019

[16] Secure IP Network (SIPN)

https://www2.swift.com/knowledgecentre/publications/udic/4.0?topic=leme690.htm

Consultado 15 enero 2019

[16] IRAM Instituto Argentino de Normalización y Certificación.

https://catalogo.iram.org.ar/home

Consultado 10 de diciembre 2018

[17] NIST: Framework for Improving Critical Infrastructure Cybersecurity

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Consultado 10 de diciembre 2018

[18] BCRA : Texto Ordenado Requisitos Mínimos de Gestión, Implementación y Control de los Riesgos Relacionados con la Tecnología Informática, sistemas de Información y Recursos Asociados para las Entidades Financieras.

https://www.bcra.gob.ar/Pdfs/Texord/t-rmsist.pdf

Consultado 10 de diciembre 2018

[19] Política de Seguridad de la Información Modelo, ONTI

http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/242859/norma.htm

Consultado 10 de enero 2019

[20] Punjab National Bank: PNB SCAM

https://www.news18.com/news/business/pnb-scam-loopholes-in-indian-banks-systems-were-flagged-but-not-fixed-1679749.html

7/10/2019

[21] Punjab National Bank

https://www.reuters.com/article/us-punjab-natl-bank-fraud-swift-exclusiv/exclusive-indias-pnb-adopts-strict-swift-controls-after-mega-fraud-case-idUSKCN1G52LQ

7/10/2019

[22] Hackeo interno en el Banco de Chile: informático robó 475 M

https://www.biobiochile.cl/especial/noticias/reportajes/reportajes-reportajes/2018/07/18/hackeo-interno-en-el-banco-de-chile-informatico-robo-475-millones-de-pesos-usando-su-pc.shtml

Consultado 7/10/2019

[23] Robaron US$10 millones en ataque informático al Banco de Chile

https://www.biobiochile.cl/noticias/nacional/chile/2018/06/09/robaron-us10-millones-en-ataque-informatico-al-banco-de-chile-virus-fue-un-distractor.shtml

7/10/2019

[24] Comunicado Oficial del Banco de Chile

https://ww3.bancochile.cl/wps/wcm/connect/nuestro-banco/portal/sala-de-prensa/noticias-y-comunicados/declaracion-publica2

Consultado 7/10/2019

[25]How the New York Fed fumbled over the Bangladesh Bank cyber-heist

https://www.reuters.com/investigates/special-report/cyber-heist-federal/

Consultado 7/10/2019

[26] TWO BYTES TO $951M

https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html

Consultado 7/10/2019

[27] Exclusive: Some Bangladesh Bank officials involved in heist

https://de.reuters.com/article/us-cyber-heist-bangladesh-exclusive/exclusive-some-bangladesh-bank-officials-involved-in-heist-investigator-idUSKBN1411ST

Consultado 7/10/2019

[28] Robaron US$10 millones en ataque informático: virus fue un distractor

https://www.biobiochile.cl/noticias/nacional/chile/2018/06/09/robaron-us10-millones-en-ataque-informatico-al-banco-de-chile-virus-fue-un-distractor.shtml

Consultado 7/10/2019

[29] Banco de Chile Loses $10 Million in SWIFT-Related Attack

https://www.bankinfosecurity.com/banco-de-chile-loses-10-million-in-swift-related-attack-a-11075

Consulado 7/10/2019

[30] BANCO DE CHILE PIERDE 10 MILLONES EN ATAQUE https://noticiasseguridad.com/hacking-incidentes/banco-de-chile-pierde-10-millones-en-ataque-relacionado-con-la-red-swift/

Consultado 7/10/2019

[31] Gerente general de Banco de Chile, Eduardo Ebensperger por ciberataque: “El evento fue destinado a dañar al banco, no a los clientes”

https://www.latercera.com/pulso/noticia/gerente-general-banco-chile-eduardo-ebensperger-ciberataque-evento-fue-destinado-danar-al-banco-no-los-clientes/198912/

7/10/2019

[32] Mexican Bank Foils $110 Million Cyber Robbery

https://www.zerohedge.com/news/2018-05-29/mexican-bank-foils-110-million-cyberheist

Consultado 7/10/2019

[33] B. de Chile: “El evento fue destinado a dañar al banco, no a los clientes”

https://www.wired.com/story/mexico-bank-hack/

Consultado 7/10/2019

[34] Descripción de funcionamiento Banxico

http://www.anterior.banxico.org.mx/sistemas-de-pago/informacion-general/sistemas-de-pago-de-alto-valor/sistema-pagos-electronicos-in.html

Consultado 7/10/2019

[35] Interbank Electronic Payment System (SPEI, Banxico)

https://www.banxico.org.mx/payment-systems/d/%7B90965A55-8F44-7DD2-45CF-2BF1D7C0B75B%7D.pdf

Consultado 9/10/2019

[36] Special Report: Cyber thieves exploit banks' faith in transfer network

https://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD

Consultado 9/10/2019

[37] Vietnam’s Tien Phong Bank says it was second bank hit by cyberattack

https://www.cnbc.com/2016/05/15/vietnams-tien-phong-bank-says-it-was-second-bank-hit-by-swift-cyber-attack.html

Consultado 9/10/2019

[38] Vietnamese bank foils $1m cyber heist

https://www.theguardian.com/technology/2016/may/16/vietnamese-bank-foils-1m-cyber-heist

Consultado 9/10/2019

[39] Customer security issues

https://www.swift.com/insights/press-releases/swift-customer-communication_customer-security-issues

Consultado 9/10/2019

[40] Documents show NSA tools for breaching

https://www.reuters.com/article/us-usa-cyber-swift-idUSKBN17H0NX

Consultado 9/10/2019

[41] Attackers Hacked Nepalese Bank

https://www.bankinfosecurity.com/report-attackers-hacked-nepalese-banks-swift-server-a-10437

Consultado 9/10/2019

[42] NIC Asia cyber heist

https://www.nationthailand.com/asean-plus/30329996

Consultado 9/10/2019

[43] Taiwan's Far Eastern International fined

https://www.reuters.com/article/us-far-eastern-fine/taiwans-far-eastern-international-fined-t8-million-over-swift-hacking-incident-idUSKBN1E60Y3

Consultado 9/10/2019

[44] Russia's Globex bank says hackers targeted its computers

https://www.reuters.com/article/us-russia-cyber-globex/russias-globex-bank-says-hackers-targeted-its-swift-computers-idUSKBN1EF294

Consultado 9/10/2019

[45] India bank hack 'similar' to $81 million Bangladesh central bank heist

https://www.reuters.com/article/us-city-union-bank-swift/india-bank-hack-similar-to-81-million-bangladesh-central-bank-heist-idUSKCN1G319K

Consultado 9/10/2019

[46] National Cybersecurity and Communications Integration Center

https://www.dhs.gov/cisa/national-cybersecurity-communications-integration-center

Consultado 9/10/2019

[47] Advanced Persistent Threat Activity

https://www.us-cert.gov/ncas/alerts/TA18-276B

Consultado 9/10/2019