Alianza del Pacífico

Presidencia Pro Tempore de Chile
2019 - 2020

GUÍA

MEJORES PRÁCTICAS EN EL REPORTE DE INCIDENTES, CIBER-COORDINACIÓN E INTERCAMBIO DE INFORMACIÓN PARA LOS PAÍSES DE LA ALIANZA DEL PACÍFICO

SUBGRUPO CIBERSEGURIDAD

CONSEJO DE MINISTROS DE FINANZAS

OCTUBRE 2020

> "La naturaleza del riesgo cibernético y la experiencia de la regulación financiera reciente permiten concluir que la coordinación y cooperación internacional son los pilares de una estrategia de seguridad cibernética basada en mejores prácticas domésticas y en una mayor cooperación interinstitucional que incluya, además, la participación de agencias gubernamentales relevantes, que van más allá del ámbito financiero" [1].

CONTENIDO

(1) OAS (2019). Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina.

Introducción

En esta guía se recogen algunas de las mejores prácticas a nivel internacional en términos de reporte de incidentes cibernéticos, ciber-coordinación y la comunicación e intercambio de información respecto a amenazas y ciber-incidentes en el sector financiero. Destacamos la importancia de la colaboración entre los múltiples stakeholders, tanto del sector público como privado, para enfrentar este riesgo creciente en el sector. La información recopilada proviene de fuentes publicadas y también del taller "Developing Cybersecurity Capabilities in the Pacific Alliance" que tuvo lugar los días 23 y 24 de junio 2020 a través de la plataforma virtual Gotowebinar. En este taller participaron expertos internacionales de ciberseguridad tanto del sector público como privado (ver agenda y biografías en Anexo).

Reporte de Ciber-incidentes

¿Que constituye un "incidente" de ciberseguridad?

La regulación de cada país generalmente define lo que constituye un "incidente cibernético" o un "incidente de seguridad de la información". Adicionalmente, las regulaciones de ciberseguridad muchas veces definen la confidencialidad con cual esta información tiene que ser tratada.

Según ISO/IEC 27001, un incidente de seguridad de la información es un "evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información."

En el sector financiero, las definiciones son más específicas y la regulación de cada país de la Alianza del Pacífico define lo que constituye un "incidente cibernético" o un "incidente de seguridad de la información".

Chile: "...Acción desarrollada a través del uso de redes de computadores u otros medios, que se traducen en un efecto real o potencialmente adverso sobre un sistema de información y/o la información que trata o los servicios que presta"[2]. Las instituciones financieras deberán reportar "los incidentes operacionales que afecten o pongan en riesgo la continuidad del negocio, los fondos o recursos de la entidad o de sus clientes, la calidad de los servicios o la imagen de la institución" [3].

Colombia: "Ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio" [4].

México: "Aquel evento que la Institución evalúe de acuerdo a sus procesos de gestión, que pueda: a) Poner en peligro la confidencialidad, integridad o disponibilidad de un componente o la totalidad de la infraestructura tecnológica utilizada por una Institución o de la información que dicha infraestructura procesa, almacena o transmite.

(2) Capítulo 20-10 de la RAN
(3) Capítulo 20-8 de la RAN. Resulta obligatorio el reporte del N°1 del Cap. 20-8 de la RAN a: entidades bancarias, empresas emisoras de tarjetas de pago no bancarias (circular N°2), empresas operadoras de tarjetas de pago (circular N°2), Cooperativas de Ahorro y Crédito bajo fiscalización de la CMF (circular N° 108), filiales bancarias (circular N°8), y Sociedades de Apoyo al Giro (Circular N°3).
(4) Superintendencia de Colombia. Circular externa 007 de 2018

b) Representar una pérdida, extracción, alteración o extravío de información.

c) Constituir una violación de las políticas y procedimientos de seguridad de la información.

d) Representar la materialización de una pérdida por daños, interrupción, alteración o fallas derivadas del uso del hardware, software, sistemas, aplicaciones, redes y cualquier otro canal de transmisión de información en la prestación de servicios, en infraestructuras tecnológicas interconectadas que permiten interacciones entre personas, procesos, datos y componentes de tecnologías de información y telecomunicaciones y que sean causados o deriven, entre otros, en accesos no autorizados, uso indebido de la información o de los sistemas, fraude, robo de información o en interrupción de los servicios, que ponga en riesgo la confidencialidad, integridad y disponibilidad de la información.

e) Vulnerar los sistemas o componentes de la infraestructura tecnológica con un efecto adverso para la Institución, sus clientes, terceros, proveedores o contrapartes, comúnmente conocidos como ciberataques [5].

Perú: Un incidente de seguridad de información es un "evento que se ha determinado que tiene un impacto sobre la organización y que requiere de acciones de respuesta y recuperación", y es "asociado a una posible falla en la política de seguridad, una falla en los controles, o una situación previamente desconocida relevante para la seguridad, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información"[6a].

Ciberseguridad: es un "conjunto de políticas, procesos, procedimientos y recursos utilizados por la organización para proteger los activos de información mediante la prevención, detección, respuesta y recuperación ante incidentes en el ciberespacio; el que consiste a su vez en un sistema complejo que no tiene existencia física, en el que interactúan personas, dispositivos y sistemas informáticos"[6b]. Además, es la "condición de estar protegido en contra de consecuencias físicas, sociales, financieras, emocionales, ocupacionales, psicológicas, educacionales o de otro tipo que resultan del fallo, daño, error, accidentes, perjuicios o cualquier otro evento en el Ciberespacio que se pueda considerar no deseable"[6a].

¿Cuándo reportar?

- Cuando hay una obligación regulatoria/legal.
- Cuando hay una duda si el evento constituye un "incidente".
- Cuando el evento pueda tener un impacto en otras entidades, sectores o un impacto sistémico.

Muchas jurisdicciones ocupan los principios de estándares internacionales de manejo de incidentes como ISO/IEC 27035 y/o NIST Publicación Especial 800-61 Revisión 2 para establecer los lineamientos para reportar incidentes de ciberseguridad tanto al regulador financiero, como al CSIRT nacional, CSIRT sectorial y otras entidades del gobierno.

(5) Artículo 1, fracción LXXVI de la Disposiciones de carácter general aplicables a las Instituciones de Crédito.
(6a) Reglamento de gestión del riesgo operacional de la Superintendencia de Mercado de Valores de Perú. Ver link: https://www.smv.gob.pe/sil/RSMV00001600027001.pdf
(6b) "Proyecto de Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad", prepublicación para comentarios, SBS Perú, agosto 2020

Por ejemplo, el gobierno federal de EEUU pide que las entidades privadas "reporten incidentes que resulten en: 1) una pérdida significativa de datos, disponibilidad del sistema o control de sistemas; 2) impacten a un gran número de víctimas; 3) indiquen acceso no autorizado o software malicioso presente en sistemas críticos de tecnología de la información; 4) afecten la infraestructura crítica o las funciones centrales del gobierno; o 5) impacten la seguridad nacional, la seguridad económica o la salud y seguridad públicas"[7].

Según las recomendaciones de las autoridades inglesas, si es que existe una duda respecto a si una institución financiera debiera reportar un incidente, es mejor reportar o, por lo menos, consultar[8]. Este consejo es pertinente para las instituciones financieras operando en los países de la Alianza del Pacífico.

Aunque las regulaciones de ciberseguridad en cada jurisdicción generalmente definen lo que constituye un "incidente" de ciberseguridad, de todas formas, puede existir una zona "gris" respecto a si el ataque cibernético llega al umbral necesario para reportarlo como un "incidente" e implementar todos los protocolos correspondientes. Por lo tanto, en algunas jurisdicciones también definen lo que no constituye un "incidente" y lo que no requiere evaluación o gestión por un CSIRT interno/externo ni un reporte a autoridades.

Por ejemplo, en Canadá, en la Guía de Planificación de Gestión de Incidentes Cibernéticos para Intermediarios de Inversiones de la Organización Reguladora de la Industria de Inversiones de Canadá (IIROC) recomiendan eventos que no necesitan estar escalados (o reportados): "Los siguientes son ejemplos de eventos que no tienen que ser reportados al Equipo de Respuesta a Incidentes (CSIRT), pero deben ser reportados a la mesa de ayuda: casos únicos de actividad de virus que se pueden remediar fácilmente y que no afectan los sistemas críticos de una organización, interrupciones a corto plazo de servicios no críticos, casos únicos de correos electrónicos no deseados estándar sin ningún enlace malicioso o archivos adjuntos, y usuarios que infringen las políticas o directrices específicas de la organización relacionadas con Internet."

Para el caso de Instituciones de Crédito en México[9], las disposiciones generales establecen que se deberá notificar a la Comisión Nacional Bancaria y de Valores (CNBV) con carácter inmediato cuando el incidente ocurra en la infraestructura tecnológica propia o de terceros o en los canales de atención al público y que, además: i) genere pérdidas económicas o de información o interrumpa los servicios, ii) se pueda replicar en otras Instituciones, iii) afecte a los clientes o a la estabilidad del sistema financiero o, iv) se considere grave a juicio de la institución. Para el caso de las Instituciones de Financiamiento Colectivo (IFC)[10], se deberá notificar de forma inmediata a la CNBV, cuando el incidente ocurra en la infraestructura tecnológica propia o de terceros o, en los canales de atención a los Clientes.

Tanto para Instituciones de Crédito como para las IFC, cuando el incidente de seguridad esté relacionado con la extracción, eliminación o alteración de información sensible de los clientes, bajo la custodia de la institución o de terceros, se deberá notificar a los mismos clientes.

(7) Cyber Incident Reporting A Unified Message for Reporting to the Federal Government
(8) UK Financial Services Cyber Incident Reporting Framework CMORG Cyber Coordination Group, 2019
(9) CNBV. Disposiciones de carácter general aplicables las instituciones de crédito https://www.cnbv.gob.mx/Normatividad/Disposiciones%20de%20car%C3%A1cter%20general%20aplicables%20a%20las%20instituciones%20de%20cr%C3%A9dito.pdf
(10) CNBV. Disposiciones de carácter general aplicables a las instituciones de tecnología financiera https://www.cnbv.gob.mx/Normatividad/Disposiciones%20de%20car%C3%A1cter%20general%20aplicables%20a%20las%20instituciones%20de%20tecnolog%C3%ADa%20financiera.pdf

En Perú, la regulación señala que en el "Reporte de incidentes de ciberseguridad, la empresa debe reportar a la Superintendencia, en cuanto advierta, la ocurrencia de un incidente de ciberseguridad que tenga un efecto verificado o presumible de:

a) Pérdida o hurto de información de la empresa o de clientes.
b) Fraudes internos o externos.
c) Impacto negativo en la imagen y reputación de la empresa.
d) Interrupción de operaciones.

La Superintendencia, mediante norma de carácter general, establece el contenido mínimo, formato y protocolos adicionales a utilizar en dicho reporte" [11].

¿A quién reportar?

- Idealmente, la institución financiera afectada tendría que reportar un incidente de ciberseguridad a una sola entidad gubernamental.
- Esta entidad idealmente funcionaría como un hub central: asistiendo a la institución afectada en gestionar el incidente, informando a otras entidades gubernamentales y stakeholders esenciales sobre el incidente, y coordinando a las entidades del gobierno en la respuesta al incidente.
- Al establecer al destinatario de los reportes se requiere de un protocolo de información para no generar sobrecarga de reportes. También es necesario establecer tiempos y plazos.
- Existen obligaciones legales de reporte de incidentes, pero también hay recomendaciones de reporte que pueden ser extremadamente importantes en la respuesta al incidente.

El reporte de un incidente de ciberseguridad al regulador financiero es un requisito legal en los países de la Alianza del Pacífico para las entidades bancarias y otras instituciones financieras, dependiendo de la regulación específica de cada jurisdicción [12]. Estos requisitos son parte de las normas que rigen en la industria financiera de cada país. En el caso de una institución multilateral afectada por un incidente de ciberseguridad, generalmente se le imponen requisitos de reportar al regulador del país donde el incidente ocurrió y también al regulador en el país de origen de la matriz. Adicionalmente, dentro de una jurisdicción, la institución financiera puede tener múltiples requisitos de reporte a múltiples entidades: por ejemplo, la obligación de reportar el incidente al regulador financiero y también a otras autoridades como la agencia nacional de protección de datos, el banco central, el CSIRT nacional o sectorial, entre otras.

Es recomendable tener un hub central de reporte o un regulador o entidad a cargo cuando hay un ciber-incidente. Otra posibilidad es tener una plataforma única de reporte, que pueda centralizar y transmitir la información a las entidades regulatorias necesarias.

(11) "Proyecto de Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad", pre publicación para comentarios, SBS Perú, agosto 2020

(12) En el caso de Chile, las entidades del mercado de valores y de la industria aseguradora no tienen la obligación legal explícita de reportar los incidentes de ciberseguridad a la CMF. Sin embargo, en la industria aseguradora, por ejemplo, a través de la Circular N°662 de 1986, referida a divulgación de información relevante, se pueda considerar un incidente de ciberseguridad como una de las situaciones. No obstante, lo anterior, está pronta a emitirse una normativa específica sobre el tema, que hará exigible el reporte de cualquier incidente de seguridad de información relevante al regulador.

La Federación Europea de Bancos (EBF), en su propuesta a las autoridades europeas[13] enfatizó la importancia de centralizar los requisitos de reporte de incidentes para reducir la cantidad de reportes que una institución financiera tiene que generar en caso de un incidente. La centralización de reportes con requisitos y una taxonomía común ayuda a reducir la probabilidad de exigir múltiples veces la misma información, a mejorar el nivel de cumplimiento con requerimientos de reporte y a liberar recursos de la institución afectada para poder concentrarse en responder al incidente (gastando menos tiempo en el proceso de reporte).

En el Reino Unido, por ejemplo, una institución financiera puede estar obligada a reportar un ciberataque a varios reguladores, pero después hay un regulador que se encarga de gestionar el incidente. Utilizan un marco de acción desarrollado para coordinar las autoridades en situaciones de ciberataques en el sector financiero y para "facilitar decisiones colectivas"[14]. Estas decisiones se toman en un grupo de coordinación que consiste en autoridades financieras, el National Cyber Security Centre y otras autoridades del gobierno central. La autoridad que será designada como la "encargada de gestionar el incidente" se escogerá de acuerdo con la naturaleza del evento y sus impactos. El encargado sirve como el único punto de contacto con la entidad afectada y recauda la información necesaria de la entidad para reportarla al grupo[15].

También la institución que sufrió el ataque debiera considerar la importancia de reportar este ataque a otras autoridades y organizaciones, con las cuales no tiene una obligación de reportar, pero se recomienda hacerlo (agencias policiales, y otras entidades y corredores de servicios donde el banco intercambia información, etc.)[16].

Aparte de las obligaciones legales que tiene una institución financiera en reportar un ciberataque al regulador financiero y otras entidades gubernamentales, hay razones prácticas y útiles para reportarlo tanto a las entidades que por ley lo exigen como otras entidades donde el reporte del incidente es recomendado, pero no obligatorio.

Primero, la firma afectada puede necesitar asistencia técnica en mitigar el incidente, especialmente si la entidad no tiene un CSIRT interno dentro de la organización. Segundo, puede recibir información pertinente que el gobierno ya tiene como parte del intercambio de información desde sus foros internacionales, de su trabajo de recaudación de inteligencia del CSIRT nacional/sectorial o desde otros incidentes que han ocurrido en el sector financiero o en otros sectores. Finalmente, el reporte de incidentes ayuda a todos los stakeholders a trabajar en fortalecer el sector financiero contra ciber crimen, además de vincular eventos, encontrar patrones, así como entender mejor los métodos de ataque.

En Israel, por ejemplo, todos los sectores de infraestructura crítica en el país, incluyendo el sector financiero, cuentan con un CSIRT sectorial que puede asistir en un evento de un ciberataque. El "Financial CERT", parte del Israeli National Cyber Directorate, se enfoca en el intercambio de información, conocimiento de la situación y respuesta a incidentes[17].

(13) EBF Position on Cyber Incident Reporting, Brussels, Oct. 16, 2019 "Proposals from the European banking sector for a harmonized reporting environment".
(14) UK Financial Services Cyber Incident Reporting Framework CMORG Cyber Coordination Group, 2019
(15) Authorities Response Framework, Incident Response Protocol, Reino Unido.
(16) Para mayor información, ver las secciones sobre intercambio de información.
(17) Presentación de Lavy Shtokhamer, Head of Israeli National CERT, Israeli National Cyber Directorate, en el taller de "Developing Cybersecurity Capabilities in the Pacific Alliance", Junio 2020

En Colombia, por ejemplo, la circular externa 007 de 2018, expedida por la Superintendencia Financiera de Colombia (SFC), determina en su numeral 3.7 la obligación que tienen las entidades vigiladas de informar a la SFC, a las entidades adscritas a la estrategia nacional de ciberseguridad y ciberdefensa y a los consumidores financieros afectados, la materialización de un incidente significativo.

En la estrategia Nacional de Ciberseguridad y Ciberdefensa del gobierno colombiano, mediante el documento Conpes 3701 de 2011, se define que colCERT (Equipo de Atención a Emergencias Cibernéticas de Colombia), será la entidad encargada de la recepción de los reportes y gestión de incidentes cibernéticos que afecten al país.

¿Cómo reportar?

- El CSIRT Nacional o el regulador financiero de cada país debiera establecer un sistema de umbrales para clasificar el nivel de severidad de incidentes cibernéticos y cómo responder en cada caso: cuáles entidades deben estar informadas e involucradas en la respuesta.

- Si la institución afectada necesita reportar un incidente de ciberseguridad a múltiples autoridades, el uso de una taxonomía y requisitos de reporte en común entre reguladores es recomendado.

- El regulador financiero debiera disponer de una plataforma, teléfono u otro método de comunicación segura disponible 24/7 para informar incidentes. La comunicación de esta información es extremadamente sensible y el tránsito de información debe ser a través de una conexión segura[18].

- El regulador debiera establecer el plazo para informar el incidente y la información que requiere en el reporte del incidente, tanto en el reporte inicial, durante la gestión del evento y en el reporte de cierre. La exigencia de completitud de la información a cada fase de reporte también debe ser especificado por el regulador[19].

El reporte de información sobre el incidente puede tomar dos formas: un reporte de información regulatoria e información técnica. Generalmente, el reporte de información regulatoria corresponde a una descripción general del evento: los sistemas afectados, cuándo el incidente fue descubierto, los activos críticos afectados (información, cuentas, fondos, servicios, etc.) y la respuesta o gestión que está siendo implementada por la institución para mitigar o controlar el impacto del incidente, entre otros. Esta información generalmente involucra equipos de supervisión, cumplimiento, etc.

El reporte de información técnica puede involucrar detalles como códigos maliciosos, reportes de log, otros reportes forenses, etc. Esta información puede involucrar a los equipos técnicos de seguridad de la información/ciberseguridad tanto de la institución afectada como del regulador. En algunos casos, el regulador no cuenta con un equipo interno técnico, por lo que esta información está gestionada por el CSIRT sectorial o nacional.

(17) Presentación de Lavy Shtokhamer, Head of Israeli National CERT, Israeli National Cyber Directorate, en el taller de "Developing Cybersecurity Capabilities in the Pacific Alliance", Junio 2020.
(18) UK Financial Services Cyber Incident Reporting Framework CMORG Cyber Coordination Group, 2019
(19) Suele pasar que la institución financiera afectado por un cíber incidente no cuenta con mucha información sobre el incidente en las horas inmediatamente después de enterarse del incidente. Por lo tanto, lo más común es que el regulador no exige completitud de la información reportada en la fase inicial.

Por ejemplo, en el caso de México, la regulación vigente establece que para el caso de Instituciones de Crédito e IFC, se deberá notificar mediante correo electrónico considerando, al menos, la fecha y hora de inicio del incidente, duración, descripción y una evaluación inicial del impacto o gravedad. Adicionalmente, el Oficial de Seguridad de la Información de las instituciones, deberá enviar mediante correo electrónico, dentro de los cinco días hábiles siguientes a la identificación del incidente, el reporte con la información detallada relacionada con el incidente y el reporte con la afectación ocasionada. En relación con la notificación a los clientes, se deberá realizar dentro de las 48 horas siguientes a la identificación del incidente, mediante los medios de notificación que el cliente haya señalado, cuando exista una posible pérdida, extracción, alteración, extravío o acceso no autorizado a su información.

Otra recomendación que hizo la Federación Europea de Bancos[20] para los supervisores fue "armonizar los umbrales de informes y crear una taxonomía común para incidentes de ciberseguridad". Si una institución financiera tiene que reportar a múltiples entidades y además la entidad tiene que manejar distintos umbrales de reporte según la autoridad y utilizar taxonomías distintas, llenar múltiples formularios y bases de datos, con distintos plazos de reporte, etc., este proceso puede ser muy engorroso y la entidad puede perder tiempo valioso en reportar, tiempo que necesitan para gestionar el incidente.

En esta línea, en julio del presente año en Colombia, se publicó una nueva normativa en consulta que complementa las normas existentes sobre la gestión de riesgo de ciberseguridad en el sistema financiero[21]. Uno de los tres elementos contemplados en esta norma es la definición de la taxonomía única de incidentes cibernéticos (TUIC) que se adoptará con el propósito facilitar la clasificación y la remisión de información, en particular a ColCERT y a la SFC. La TUIC es el resultado de mesas de trabajo realizadas en 2019 con la participación de algunas entidades vigiladas, la agremiación de bancos (Asobancaria), colCERT y SFC.

Cíber Coordinación, Comunicación e Intercambio de Información

"Ser notificado y mantenerse informado sobre los detalles y las actividades en curso en relación con un incidente de seguridad de la información es fundamental para todas las partes interesadas y las organizaciones involucradas" [22].

Coordinación de autoridades

- Hay múltiples entidades públicas que tienen un interés o un papel importante ante la ocurrencia de un ciberataque significativo en el sector financiero, tanto autoridades financieras como otras autoridades del gobierno central.

- Es importante tener un marco de coordinación entre las autoridades en el evento de un incidente de ciberseguridad. Este marco debiera incluir una estructura de gobernanza que defina los papeles y las responsabilidades de las distintas autoridades y cómo debieran organizarse y comunicarse.

(22) FIRST, Computer Security Incident Response Team (CSIRT) Services Framework Version 2.0 (Review Release), June 2019

- Existirán distintos umbrales de severidad ante un incidente, los que ameritan distintas respuestas desde las autoridades.

- Es necesario establecer si existen diferencias en la información a reportar e intercambiar entre las autoridades distinguiendo los mandatos legales de cada una. Ejemplo, distinguir al regulador financiero de un CSIRT.

La ciber-coordinación implica notificaciones oportunas y una distribución precisa de la información sobre un incidente de ciberseguridad. Para alinear la respuesta de los stakeholders involucrados de alguna manera en la gestión del incidente, es importante mantener el flujo de información y actualizar a todas las partes sobre el estado de las actividades de las entidades que participan en la respuesta[23].

La mayoría de los reguladores financieros exigen que las instituciones financieras tengan un protocolo para responder internamente a un incidente de ciberseguridad, además de un protocolo de comunicaciones (internas y externas). Esta misma necesidad de coordinar distintas partes, con papeles definidos, una estructura de gobernanza y lineamientos para las comunicaciones es importante en el sector público. Cuando ocurre un incidente, no es el momento de improvisar y comenzar a pensar en alguna forma de organizarse. La coordinación de entidades involucradas debiera estar ya establecida y cada entidad debiera actuar desde su mandato legal y regulatorio (por ejemplo: protección del consumidor, estabilidad financiera, etc.). El marco debiera incluir una definición de qué entidad gubernamental tomará el liderazgo de la situación y servir como el punto único de contacto con la institución financiera afectada. También el marco debiera incluir un mecanismo para llegar a acuerdos y determinar cómo resolver temas cuando no hay consenso entre las autoridades. Finalmente, debiera incluir una definición de cómo y cuándo el sector público tomaría un papel más activo en la gestión del incidente (por ejemplo: en casos que la empresa solicita ayuda técnica, en casos donde hay múltiples empresas o múltiples sectores afectados, cuando existen riesgos a la estabilidad financiera o sistema de pagos, cuando el incidente tiene impactos internacionales, etc.)[24].

Finalmente, es recomendable que el marco de coordinación de entidades del sector público cuente con un marco de comunicaciones, tanto entre autoridades, las autoridades con el sector financiero y con el público en general. Este marco o protocolo de comunicaciones debiera respetar restricciones legales en términos de la información que se puede compartir, etc.

Intercambio de información

1. Coordinación de Ciberseguridad en la Industria Financiera

"El intercambio de información sobre un incidente de ciberseguridad en el sector financiero es una medida clave para enfrentar los riesgos de ciberataques y fortalecer el sistema financiero contra ataques repetidos o ataques masivos"[25]

(23) FIRST, Computer Security Incident Response Team (CSIRT) Services Framework Version 2.0 (Review Release), June 2019.
(24) Authorities Response Framework, Incident Response Protocol, Reino Unido
(25) Cyber Incident Management Planning Guide for IIROC Dealer Members, Investment Industry Regulatory Organization of Canada

- Es importante tener un mecanismo o instancia para coordinar los stakeholders del sector privado en el evento de un ciberataque significativo en el sector financiero.

- El mecanismo debiera proveer un ambiente de confianza para consultar y tomar decisiones.

- Antes de solicitar asistencia o informar a terceros, es fundamental que las empresas comprendan tanto las obligaciones de informar como los requisitos para proteger la información confidencial [26].

- En algunas jurisdicciones, es una obligación legal informar a los demás actores del sector financiero sobre un incidente de ciberseguridad, mientras en otras jurisdicciones el intercambio de información con el resto del sector es recomendado, pero no obligatorio [27].

- El intercambio de información sobre incidentes de ciberseguridad puede aumentar significativamente la velocidad de preparación de la respuesta. La institución afectada no solo provee un aviso a otras instituciones sino también puede recibir información importante por parte de las otras instituciones sobre patrones de ataque, posibles medidas para mitigar el ataque, etc.

El intercambio de información de ciber-incidentes es una forma de "reducir riesgo operacional a través de la reducción de asimetrías de información[28]". Sin embargo, pueden existir "barreras legales, comerciales, culturales, y transfronterizas" que dificultan el intercambio de información. Adicionalmente el intercambio de información requiere que existan capacidades robustas (de ciberseguridad) en las firmas, reguladores financieros y autoridades de ciberseguridad. Si no hay capacidades robustas, existirán barreras estructurales a pesar de las otras barreras que pudieran existir[29].

Algunos otros desafíos con el intercambio de información tienen que ver con las necesidades diferentes de las contrapartes que intercambian información. Por ejemplo, un Chief Information Security Officer (CISO), un Security Operation Center (SOC), una agencia policial o un regulador financiero tienen distintas formas de procesar, reportar y utilizar información respecto a incidentes de ciberseguridad[30], ya que tienen distintos propósitos en su trabajo y pueden tener distintos niveles de madurez cibernética, lo que hace más complejo el intercambio de información entre distintos stakeholders.

Finalmente, existen temas relacionados con la confianza, la privacidad y el desafío de intercambiar información en tiempo real para que la información sea lo más útil posible, potencialmente contribuyendo a la prevención de un ataque parecido a otra entidad[31].

---

(26) Cyber Incident Management Planning Guide for IIROC Dealer Members, Investment Industry Regulatory Organization of Canada.
(27) Por ejemplo, en Chile, solo los bancos tienen la obligación de informar el resto del sector bancario en el evento de un ciberataque. En el caso de la industria aseguradora en Chile, está próximo a emitirse una normativa que contemplaría el reporte de incidentes de ciberseguridad hacia el regulador y a las demás compañías de seguros. Sin embargo, la Asociación de Aseguradores ha desarrollado una plataforma para comunicar incidentes de ciberseguridad. En el Reino Unido, el regulador sugiere que una institución financiera comparte información sobre un ciberataque con la industria, pero no es una obligación legal o normativa. En los demás países de la Alianza del Pacífico no es una obligación legal informar a la industria en caso de un ciberataque.
(28) Presentación de Paul Williams, Head of the Operational Risk and Resilience Division, Bank of England, en el taller de "Developing Cybersecurity Capabilities in the Pacific Alliance", Junio 2020
(29) Presentación de Paul Williams, Head of the Operational Risk and Resilience Division, Bank of England, en el taller de "Developing Cybersecurity Capabilities in the Pacific Alliance", Junio 2020.
(30) Presentación de Lavy Shtokhamer, Head of Israeli National CERT, Israeli National Cyber Directorate, en el taller de "Developing Cybersecurity Capabilities in the Pacific Alliance", Junio 2020
(31) Presentación de Lavy Shtokhamer, Head of Israeli National CERT, Israeli National Cyber Directorate, en el taller de "Developing Cybersecurity Capabilities in the Pacific Alliance", Junio 2020

La Organización Reguladora de la Industria de Inversiones de Canadá en su Guía de Planificación de Gestión de Incidentes Cibernéticos recomienda que, antes de intercambiar información sobre un incidente de ciberseguridad, la institución afectada considera las siguientes preguntas:

- Por qué - Comprender el propósito del intercambio previsto.
- Qué - Determinar específicamente qué información se compartirá y con qué nivel de detalle.
- Quién - Seleccionar con qué partes compartir información.
- Cuándo - Decidir en qué punto se iniciará un intercambio.
- Cómo - Seleccionar tanto el método de intercambio como las protecciones a seguir.

Estas mismas consideraciones aplican a todas las organizaciones tanto públicas como privadas informando un incidente y/o involucradas en la gestión del incidente. El establecimiento de un mecanismo para coordinar todos los actores de la industria es fundamental y el uso de este canal de comunicación debe ocurrir en forma habitual para que las partes se acostumbren a utilizar este canal. El canal de comunicación puede ser solo entre los partes del sector privado o puede ser un mecanismo de comunicación que incluya el sector privado y el CSIRT sectorial o nacional. Adicionalmente, pueden existir múltiples canales de comunicación dentro del sector privado, por ejemplo a nivel técnico, estratégico o gerencial. La otra posibilidad es que existan canales de comunicación para los subsectores de la industria, por ejemplo: bancos, administradoras de fondos, empresas de seguros, cooperativas, etc.

Por ejemplo, en Chile existe el Virtual Task Force (VTF), un grupo compuesto por los bancos y organizado por la Asociación de Bancos e Instituciones Financiera (ABIF). El VTF tiene distintos niveles de comités que comunican respecto a amenazas e incidentes de ciberseguridad en el sector financiero y la información respecto a un incidente o amenaza puede estar escalada a los distintos niveles de comités dependiendo del impacto o severidad implicada. En el caso de la industria bancaria en Chile, es una obligación normativa de informar a los demás bancos de un incidente de ciberataque. El VTF fue formado en parte para cumplir con esta norma.

En el caso de la industria aseguradora, existe a nivel de la Asociación de Aseguradores de Chile (AACh) un Equipo Asesor en Ciberseguridad, integrado por especialistas de las compañías asociadas y que sirve como instancia de coordinación en temas de ciberseguridad. Adicionalmente, en la AACh se ha desarrollado una plataforma para el reporte e intercambio de información de incidentes de ciberseguridad entre las compañías asociadas. Para esto, los gestores designados por cada compañía deben informar a la AACh todo incidente operacional relacionado con la ciberseguridad a la mayor brevedad, la que no podrá exceder a las 2 horas de detectado el incidente, usando para ello la plataforma operativa de la Asociación para estos efectos denominada SUAC (Sistema Unificado de Alertas de Ciberseguridad) o a través de los correos electrónicos definidos para estos efectos (en caso de falla del sistema).

La información de estos incidentes se transmite inmediatamente a las otras compañías, a través de mensajes SMS a los Gestores designados por cada una de ellas, los que pueden acceder a mayor detalle a través de su acceso al sistema SUAC. La comunicación a los otros gestores es realizada de manera genérica, sin identificación de la compañía afectada.

En el caso de la industria aseguradora en Chile, si bien es cierto, actualmente no es una obligación legal o normativa informar a los demás participantes en la industria sobre un ciberataque, sí ha sido una recomendación del Regulador hacia la industria en distintas reuniones. Además, está próxima a ser emitida una normativa que abordaría este aspecto.

En Reino Unido, existe un mecanismo de comunicación entre los actores del sector privado y el National Cyber Security Centre, llamado Cross Markets Operational Resilience Group. Este mecanismo de coordinación y comunicación incluye un marco de reglas establecidas para el intercambio de información entre los actores del sector privado y el NCSC[32].

Israel tiene un mecanismo parecido que se llama el "Interbank Cyber Defense Forum", que es un foro que incluye los CISOs y gerentes de riesgo operacional de todos los bancos y miembros del Israel National Cyber Directorate donde intercambian información respecto a incidentes y amenazas de ciberseguridad y también donde conversan respecto a los desafíos de seguridad de la información que traen nuevas tecnologías y modelos de negocios (por ejemplo: Open APIs) [33].

Ambos mecanismos de comunicación para el sector privado – un modelo netamente del sector privado (Chile) o el modelo público-privado (Reino Unido e Israel) – sirven para coordinar las acciones del sector financiero frente a distintos riesgos y amenazas cibernéticas en un ambiente de confianza.

Es importante notar que, dependiendo del marco legal y la cultura local en una cierta jurisdicción, puede ser necesario tener un decreto o ley que permita (u obligue) a una entidad afectada por un incidente de ciberseguridad, a compartir la información con los demás actores del sector financiero. Las entidades temen que el intercambio de información sobre ciberseguridad pudiese terminar en acusaciones de colusión o comportamiento anticompetitivo. Por lo tanto, en algunas jurisdicciones las instituciones financieras pueden requerir la protección de una ley para compartir información con el sector.

Por ejemplo, en EE. UU., la Ley de Intercambio de Información sobre Ciberseguridad entró en vigor en 2015, "permitiendo que entidades no federales compartan indicadores de amenazas cibernéticas y medidas defensivas con cualquier otra entidad (privada, federal, estatal, local, territorial o tribal) con un "propósito de seguridad cibernética""[34]. La Ley especifica exactamente el tipo de información que se puede compartir y bajo cuáles circunstancias, dando lineamientos claros para el sector privado en términos de cómo intercambiar información sobre incidentes de ciberseguridad.

En Canadá la nueva Ley de Privacidad Digital "contiene lenguaje que permite a las organizaciones compartir información entre ellas con el fin de detectar o suprimir fraude o para la investigación de una violación de un acuerdo o una violación de las leyes de Canadá, que es razonablemente esperable que sea comprometida". Este lenguaje da más libertad a las empresas canadienses a intercambiar información sobre incidentes de ciberseguridad que leyes anteriores que requerían la instancia de una investigación formal[35].

(32) UK Financial Services Cyber Incident Reporting Framework CMORG Cyber Coo rdination Group, 2019
(33) Presentación de Aya Gal-Ed, Head of Cyber Defense Unit, Bank of Israel, en el taller de "Building Cybersecurity Capacities in the Pacific Alliance", Junio 2020
(34) Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015, U.S. Department of Homeland Security.
(35) Cyber Incident Management Planning Guide for IIROC Dealer Members, Investment Industry Regulatory Organization of Canada

En otras jurisdicciones puede ocurrir que no sea necesario obligar o dar permiso a las instituciones financieras para intercambiar información de ciberseguridad. El marco legal puede ser más flexible y las empresas podrían no requerir permiso explícito para intercambiar información de esta naturaleza. Adicionalmente, hay reguladores que han decidido no obligar – solo recomendar – el intercambio de información de incidentes y amenazas entre actores del sector privado, privilegiando la libertad de acción de las empresas por sobre las obligaciones colectivas.

La otra pregunta que surge en el intercambio de información entre actores del mercado financiero en casos de ataques cibernéticos es el tema de cuáles stakeholders debieran ser informados. Por ejemplo, si un banco de importancia sistémica sufre un ataque de ciberseguridad y quiere compartir o está obligado a compartir información sobre el ataque con el sector, ¿a cuáles otras instituciones financieras necesitará informar? ¿Es suficiente que informe solo a los demás bancos de importancia sistémica? ¿A todos los bancos? ¿O también necesita informar a otras instituciones de crédito, o incluso a otras entidades del mercado de capitales, infraestructura del mercado, etc.?

Idealmente, el regulador podría definir recomendaciones u obligaciones respecto al nivel de intercambio de información que la institución afectada debiera realizar y bajo cuáles circunstancias. Lo más común es que una institución financiera comparta información sobre un ciberataque con otras instituciones del mismo rubro específico y, si les interesara participar en una comunicación con el sector ampliado, lo harán a través de un foro nacional del sector financiero o un foro internacional como FS-ISAC o FIRST.

Adicionalmente, en aquellos casos en que se contempla el intercambio de información con terceros, es importante establecer protecciones de la información antes de un incidente, como acuerdos mutuos de no divulgación[36] o Memorandum of Understanding (MoU) para establecer las reglas para el intercambio de información. En muchos casos, el uso del traffic light protocol, creado originalmente por el gobierno del Reino Unido[37], es especialmente útil para indicar el nivel de confidencialidad que debe ser utilizado en el manejo de la información compartida.

"El Traffic Light Protocol (TLP) se creó para facilitar un mayor intercambio de información. TLP es un conjunto de designaciones que se utilizan para garantizar que la información confidencial se comparta con la audiencia adecuada. Emplea cuatro colores para indicar los límites de intercambio de información que los destinatarios deben aplicar."[38] Según NIST, no es necesario compartir información sobre el impacto del incidente en el negocio (en términos de información como daños financieros, cantidad de clientes afectados, etc.) con otras empresas de la misma industria. Estos detalles solo se necesitan informar al regulador u otra entidad con un interés legítimo en la sustentabilidad y misión del negocio. Sin embargo, la información técnica o indicadores (como códigos maliciosos, logs de aplicaciones, direcciones IP de dispositivos infectados, URLs de sitios web con actividad maliciosas, vulnerabilidades, etc.) pueden ser de mucha utilidad para otras empresas del mismo sector, otros CSIRTS, foros internacionales etc. En algunos casos será necesario "limpiar" la información técnica de detalles identificadores antes de compartirla. Adicionalmente, NIST enfatiza que algunas veces hay información sobre vulnerabilidades del sistema de la institución financiera que no va a querer compartir con terceros pero que la información sobre la identidad del atacante y detalles generales del incidente generalmente se puede compartir y es información útil para otras instituciones.

(36) Non-disclosure agreement
(37) https://www.first.org/global/sigs/tlp/
(38) TRAFFIC LIGHT PROTOCOL (TLP); FIRST Standards Definitions and Usage Guidance – Version 1.0

También surge el tema de cómo compartir información entre instituciones, específicamente a través de qué tipo de canales de información. Según el NIST, "las organizaciones deberían intentar automatizar la mayor parte del proceso de intercambio de información posible para que la coordinación entre organizaciones sea eficiente y rentable". Existen distintos modelos para el intercambio automatizado de datos y también distintos mecanismos para comunicar dichos datos automatizados. Los miembros de un grupo o foro de colaboración de ciberseguridad debieran ponerse de acuerdo respecto a la información que quieren compartir en forma automatizada. Por ejemplo, en EEUU, el Departamento de Homeland Security (DHS) a través del National Cybersecurity and Communications Integration Center (NCCIC) tiene un servicio que permite el intercambio de indicadores de amenazas cibernéticas entre el Gobierno Federal y el sector privado en tiempo real en formato máquina-a-máquina[39].

NIST, en su Guía de Manejo de Incidentes de Seguridad Informática, reconoce que esta automatización de intercambio de información de incidentes y amenazas cibernéticas puede coexistir con un intercambio ad-hoc de información en forma de mensajes entre personas involucrados en la gestión (emails, WhatsApp, etc.) debido a temas de confianza y la confidencialidad de los detalles de los incidentes que están compartiendo.

Se sugiere considerar como referencia el Convenio sobre la Ciberdelincuencia[40] del Consejo de Europa (Convenio de Budapest), ya que este Convenio es un acuerdo internacional usado en el medio para armonizar y desarrollar legislación, de combate relativa al cibercrimen, mejorar las capacidades de investigación de ese tipo de delitos y para establecer un régimen más efectivo de cooperación y asistencia internacional, en materia.

2. Coordinación entre Autoridades y la Industria

- Adicional a un marco de coordinación de las autoridades del sector público y un marco o instancia de coordinación de los actores de la industria financiera, es importante que exista un grupo o instancia de coordinación entre el sector público y privado, y que incluya instituciones de infraestructura del mercado financiero.

Las Autoridades Financieras del Reino Unido tienen una instancia para coordinar el sector financiero con las autoridades. Este grupo se llama el Cross Markets Business Continuity Group. Este grupo no solo incluye los reguladores financieros y las instituciones sistémicamente importantes de la industria financiera, sino también a otros actores claves de infraestructura del mercado financiero como en temas de pagos, liquidaciones de transacciones, etc. El grupo trabaja en simulaciones de ciberataques y disrupciones importantes en el funcionamiento del mercado financiero para ver cómo pueden prepararse mejor para ser resilientes en situaciones futuras[41].

Adicionalmente, el NCSC del Reino Unido tiene una unidad que se llama el Finance Engagement Team, que sirve para conectar especialmente con el sector financiero y piden que empleados de instituciones financieras del sector privado participen en prácticas (secondments) en el NCSC por periodos de varios meses para aprender mejor las necesidades de las instituciones financieras en términos de asistencia en ciberseguridad.

(39) Automated Indicator Sharing (AIS)
(40) Consejo de Europa, Council of Europe (COE), "Convention on Cybercrime", 23 noviembre 2002, en URL: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
(41) https://www.bankofengland.co.uk/news/2019/september/boe-sector-resilience-exercise

Actualmente, UK Finance (asociación del sector financiero del Reino Unido) está en proceso de crear el Financial Services Cyber Collaboration Centre (FSCCC), una instancia pública-privada más extensiva para trabajar en la resiliencia cibernética del sector financiero. Esta organización estará compuesta por múltiples stakeholders, comenzando con:

- Empresas financieras de Nivel 1 que proveen servicios a minoristas, mayoristas, pagos, infraestructura del mercado financiero y seguros.
- Autoridades financieras: Bank of England, Financial Conduct Authority (FCA), Prudential Regulation Authority (PRA).
- Gobierno - HM Treasury, National Cyber Security Center (NCSC).
- Aplicación de la ley – National Crime Agency (NCA).
- Foros de intercambio existentes: Cyber Defense Alliance (CDA), FS-ISAC[42].

El FSCCC va a ser una instancia de colaboración a través de todo el sector financiero, comenzando con las empresas financieras más grandes y agregando instituciones medianas y pequeñas con el tiempo. "El FSCCC tiene como objetivo permitir la identificación, investigación y mitigación proactivas de ataques cibernéticos a gran escala con consecuencias sistémicas a través de la coordinación efectiva de actividades y operaciones enfocadas en organizaciones de servicios financieros, socios de la industria y autoridades del Reino Unido e internacionales [43]". Las actividades del FSCCC estarán enfocadas en inteligencia de amenazas y manejo de incidentes. La idea de la FSCCC es eventualmente proveer apoyo de seguridad cibernético a todo el sector y en muchos frentes. Algunos de estas formas de apoyo ya están implementadas y otros están esperando la aprobación oficial del Gobierno del Reino Unido respecto a la asociación con el FSCCC.

Algunos de los conceptos destacables del FSCCC son:
- La eventual inclusión de todos los actores del sistema financiero,
- La búsqueda de elementos sistémicos,
- El apoyo a todas las instituciones financieras independiente de su nivel de madurez cibernética y presupuesto,
- Un enfoque cooperativo que antepone la defensa a la regulación o la competencia,
- Una instancia que complemente estructuras existentes para evitar duplicaciones, y
- Apuntar a acciones operativas (entre otros)[44].

La CNBV de México, como organismo regulador y supervisor, ha implementado mecanismos para compartir con sus supervisados información técnica de ciber-amenazas, que ayuden a las entidades financieras a implementar controles que los ayuden a la protección en contra de ataques cibernéticos y, por ende, a la prevención de incidentes.

La SFC trabaja con colCERT, C4 (Centro de Capacidades para la Ciberseguridad de Colombia) y CCOCI (Comando Conjunto Cibernético) en la generación y comunicación de alertas tempranas y boletines informativos. Adicionalmente, la SFC consulta diversas fuentes abiertas y realiza monitoreo mediante herramientas OSSINT (Open Source Social Network Intelligence).

(42) Presentación de Ian Burgess, UK Finance, en el taller de "Building Cybersecurity Capacities in the Pacific Alliance", Junio 2020
(43) Presentación de Ian Burgess, UK Finance, en el taller de "Building Cybersecurity Capacities in the Pacific Alliance", Junio 2020
(44) Presentación de Ian Burgess, UK Finance, en el taller de "Building Cybersecurity Capacities in the Pacific Alliance", Junio 2020

3. "Forward looking approach"

Aunque el intercambio de información respecto a incidentes y amenazas existentes es extremadamente importante para mejorar la ciberseguridad de todo el sistema financiero, no es suficiente solo esperar para reaccionar a los peligros que surgen, también es necesario tomar acciones concretas buscar proactiva y colaborativamente debilidades en el sistema de ciberseguridad de las instituciones financieras y el sistema financiero en su conjunto. Por ejemplo, el Bank of Israel, en su Unidad de Ciberdefensa de la División de Supervisión, organizó una prueba de tensión relacionada a un evento sistémico de ciberseguridad (un ataque al ecosistema de Open Banking)[45]. Esta prueba la realizaron en 2019-2020 para medir la resiliencia de cada institución, del sistema en su conjunto y también del regulador. Evaluaron no solo la resiliencia de ciberseguridad en esta prueba sino también otros impactos que ocurrieron en la estabilidad financiera, en temas relacionados a protección al consumidor, tecnología y operaciones. El intercambio de información respecto a los resultados de la prueba de tensión ayudaba a que cada stakeholder pudiera mejorar su resiliencia cibernética y operacional en forma individual y como parte del sistema.

Este intercambio de aprendizajes en actividades proactivas de ciber-resiliencia es muy valioso e importante de considerar, además del intercambio de información relacionado a la gestión de incidentes y amenazas existentes.

Adicionalmente es importante considerar la ciberseguridad e intercambio de información sobre ciber amenazas en sectores de la industria financiera no tradicionales. Por ejemplo, a partir de marzo 2019 la CNBV de México introdujo regulación respecto a seguridad de la información para fintechs y en junio 2020 otorgaron lineamientos de seguridad de la información para el intercambio de datos abiertos a través de APIs (para proveedores y solicitantes de datos)[46].

4. Con agencias policiales

Aunque generalmente no es un requisito legal reportar incidentes de ciberseguridad a entidades policiales nacionales e internacionales, hay casos en donde es fundamental reportar a ellas. El primero es si la entidad afectada quiere iniciar una investigación criminal para poder eventualmente llevar el caso enfrente de una corte de justicia. Segundo, el intercambio de información con agencias policiales permite la vinculación de casos y también la búsqueda de patrones en métodos de ataque, lo cual es útil a nivel sectorial y nacional (para toda la infraestructura crítica) en el combate contra crimen organizado.

(45) Presentación de Aya Gal-Ed, Head of Cyber Defense Unit, Bank of Israel, en el taller de "Building Cybersecurity Capacities in the Pacific Alliance", Junio 2020
(46) Presentación Elena Calatayud CNBV México en el taller de "Building Cybersecurity Capacities in the Pacific Alliance", Junio 2020

5. A través de foros o acuerdos internacionales

Además del intercambio de información con los stakeholders primarios como los reguladores, clientes y otras empresas del mismo sector, hay un abanico de stakeholders adicionales para considerar que también se podrían beneficiar de la información sobre el incidente e incluso podrían aportar en la gestión del incidente con información sobre un caso relacionado u otra inteligencia que tienen sobre incidentes o amenazas. Por ejemplo, existen foros internacionales para el intercambio de información de incidentes para el sector financiero como FS-ISAC y la red de CSIRTS, FIRST.

FS-ISAC (El Centro de Análisis e Intercambio de Información de Servicios Financieros) es un consorcio para la industria financiera con más de 7.000 miembros[47], mayormente bancos y cooperativas de crédito. El consorcio tiene un foro online donde intercambian información sobre incidentes y amenazas de ciberseguridad con el uso del Traffic Light Protocol. Adicionalmente FS-ISAC tiene un equipo de analistas de ciberseguridad/personal de inteligencia que investigan amenazas específicas, buscan la relación entre eventos y organizan grupos de trabajo y llamadas informativas sobre distintos temas de ciberseguridad o alertas.

También existe un foro internacional de intercambio de información de ciberseguridad para reguladores del sector financiero y bancos centrales que se llama CERES[48]. Este foro es parte del consorcio FS-ISAC y provee la oportunidad para que los reguladores financieros de distintas jurisdicciones de "acceder a inteligencia crítica, estar preparado para una crisis y fortalecer relaciones de confianza con otros reguladores[49]". En CERES se comparte información para mantener alerta a sus miembros mediante sistemas seguros. Permite a estos actores clave mantenerse continuamente informados de qué está pasando en el mundo respecto a ciberseguridad.

Además, muchos países tienen acuerdos bilaterales o multilaterales de cooperación de ciberseguridad con otros países. Por ejemplo, en la Alianza del Pacífico existen los siguientes acuerdos:

Acuerdos Internacionales de Cooperación en Temas de Ciberseguridad [50]

País	Acuerdo con
Chile	España, Argentina, Colombia, Ecuador, Israel, Reino Unido y con la OEA
Colombia	Guatemala, Honduras, Costa Rica, Panamá, República Dominicana, Nicaragua, Brasil*, Chile, Perú
México	Banco Central do Brasil[51]
Perú	No tiene acuerdos firmados en la materia.

(47) Presentación de Brian Hansen, Executive Director Asia Pacific, FS-ISAC, en el taller de "Building Cybersecurity Capacities in the Pacific Alliance", Junio 2020
(48) Central Banks, Rrgulators and Supervisory entities
(49) Presentación de Brian Hansen, Executive Director Asia Pacific, FS-ISAC, en el taller de "Building Cybersecurity Capacities in the Pacific Alliance", Junio 2020
(50) Encuestas de Ciberseguridad del Grupo de Trabajo de Integración Financiera del Consejo de Ministros de Finanzas, Alianza del Pacífico.
(51) Firmado con el Banco Central do Brasil el 4 de octubre de 2019.Si bien es cierto, este es el único instrumento con que cuenta la CNBV en donde el intercambio de información se establece de manera específica, también es cierto que si la CNBV cuenta con un instrumento bilateral de cooperación en materia de supervisión de entidades financieras, al amparo de este, es factible compartir información de ciberseguridad, al ser una medida transversal para todos los sectores.

Adicionalmente, los países de la Alianza del Pacífico a través del Grupo Técnico de Agenda Digital del Consejo de Ministros (Comercio y Relaciones Exteriores) han trabajado en coordinación con los equipos CSIRT de Chile, Colombia, México y Perú[52], para fortalecer la coordinación cibernética y promover el intercambio de información en la Alianza del Pacífico. Este trabajo incluye la implementación de una plataforma tecnológica utilizada por la red hemisférica de CSIRTAmericas (miembros de la Organización de los Estados Americanos), conocido como MISP o Malware Information Sharing Platform and Threat Sharing.

La adopción de esta plataforma tiene ventajas, como: i) una armonización de taxonomías para la descripción de incidentes, ii) niveles de información, iii) el uso del protocolo de tráfico (Traffic Light Protocol) y iv) canales de comunicación[53]. Los CSIRTS de los cuatro países miembros han sido entrenados en el uso de MISP y los ejes del Protocolo de CSIRTAmericas.

Aparte de participar en el intercambio de información e inteligencia de ciberseguridad a través de foros y acuerdos internacionales, existen otros stakeholders que podrían tener un interés y aporte relevante en la información y gestión de un incidente, por ejemplo: las empresas que fabrican hardware o software de TI, empresas que prestan servicios de ciberseguridad, investigadores, empresas en otros sectores de infraestructura critica, etc.

6. Comunicación con el público

- El regulador gubernamental o entidad gubernamental a cargo de gestionar el incidente de ciberseguridad, debe asistir la gestión y monitorear el incidente [54].
- La misma entidad debe apoyar tanto las entidades afectadas como no afectadas, dándoles consejo en caso de ser necesario.
- Los lineamientos para comunicaciones sobre incidentes de ciberseguridad en el sector financiero desde las autoridades deben estar dentro de un marco de respuesta y coordinación del sector publico frente a estos eventos.
- Normalmente las instituciones financieras y entidades reguladoras deben establecer un único punto de contacto con la prensa para limitar las posibilidades de tener alguna confusión en el mensaje[55].

Tanto las instituciones financieras como las entidades gubernamentales involucradas en la gestión de incidentes de ciberseguridad debieran contar con un protocolo de comunicaciones para enfrentar estos eventos, para no tener que improvisar en el minuto.

El regulador u otra autoridad a cargo de gestionar los incidentes que sufren las empresas deberían estar también a cargo de las comunicaciones del mismo hacia el resto del sector privado; este rol debiese estar establecido en un marco de coordinación de autoridades para incidentes de ciberseguridad. En este mismo marco, debiera estar establecido un mecanismo para coordinar las oficinas de comunicaciones de todas las autoridades que participan en el manejo del incidente, para llegar a un consenso respecto a los mensajes aprobados para las comunicaciones y los formatos aprobados para comunicar (sitio web de la entidad, entrevistas, social media, etc.)[56].

(52) CSIRTgov.cl, ColCERT, CERT-Mx, y PeCERT
(53) Protocolo de Intercambio de Información entre los Equipos de Respuestas a Incidentes Cibernéticos miembros de CSIRTAmerica
(54) Authorities Response Framework, Reino Unido
(55) Authorities Response Framework, Reino Unido
(56) Authorities Response Framework, Reino Unido

Las comunicaciones de las agencias policiales son una excepción, la necesidad de mantener bajo reserva y forma independiente la información respecto a investigaciones, para no comprometer el proceso.

Las comunicaciones del sector público debieran tomar en cuenta las necesidades de clarificar el apoyo que brindan las autoridades a la entidad afectada y la importancia de la transparencia y la confianza del público en el sistema financiero (estabilidad financiera, sistema de pagos, protección de consumidores, etc.). También es importante que las comunicaciones tomen en cuenta la información ya disponible en el ámbito público (verdadera y falsa) para clarificar los hechos y abordar las preocupaciones de los actores del sistema y el público en general.

La autoridad a cargo de las comunicaciones también puede proveer consejo y apoyo no solo a la institución afectada sino a otras instituciones financieras que no hayan sido afectados directamente por el incidente de ciberseguridad pero que tengan temores de serlo y estén en proceso de tomar medidas proactivas para proteger los activos y sistemas de su institución.

Finalmente, el regulador o autoridad a cargo de las comunicaciones del incidente también debiera asegurar que las comunicaciones que surgen desde la institución financiera afectada sean transparentes, claras y con los detalles necesarios para los clientes de la institución. NIST[57] recomienda que el equipo que esté manejando un incidente de ciberseguridad tenga lineamientos respecto a la información que van a divulgar sobre un incidente específico (limitando la información sobre las medidas que están tomando para mitigar el incidente para no ayudar a los atacantes indirectamente), que tengan un discurso preparado y que practiquen las respuestas a posibles preguntas antes de hablar con la prensa. Este mismo consejo aplica tanto a la institución afectada como a la autoridad a cargo de manejar las comunicaciones sobre el incidente con el público.

Consideraciones especiales para incidentes de ciberseguridad a una entidad listada en bolsa

En el caso de un ciberataque a una entidad listada en la bolsa de valores, puede ser necesario comunicar públicamente que el incidente ocurrió y también divulgar información interna de la entidad[58] al mercado lo antes posible, porque esta información podría estar en las manos de los atacantes y potencialmente afectar movimientos y el precio de la acción de la entidad en bolsa.

En México, las disposiciones aplicables a casas de bolsa[59] establecen que estas entidades financieras deberán contar con procesos de reacción y manejo de incidentes de seguridad, como parte de su sistema de control interno. En el caso de incidentes de seguridad relacionados con información sensible, la institución deberá notificar a la CNBV, realizar una investigación exhaustiva e informar de sus resultados, incluyendo las medidas correctivas que se implementarán, además de informar a los clientes afectados y a los comités de auditoría y de riesgos de la institución.

(57) Guía de Manejo de Incidentes de Seguridad Informática (Publicación Especial 800-61 Revisión 2).
(58) Insider information; UK Financial Services Cyber Incident Reporting Framework CMORG Cyber Coordination Group, 2019
(59) CNBV. Disposiciones de carácter general aplicables a las casas de bolsa https://www.cnbv.gob.mx/Normatividad/Disposiciones%20de%20car%C3%A1cter%20general%20aplicables%20a%20las%20casas%20de%20bolsa.pdf

Conclusiones

La experiencia internacional, tanto en los países de la Alianza del Pacífico como en otras jurisdicciones del mundo, ha demostrado la importancia de tener protocolos claros para el reporte de incidentes y la coordinación en el evento de un ciberataque. Existe una necesidad de tener protocolos de coordinación no solo adentro de cada institución financiera, sino también entre el sector público y privado, y también dentro del sector público entre autoridades del sector financiero y del gobierno central. Definición de roles y responsabilidades, una taxonomía única entre autoridades nacionales y un hub central para reportar incidentes también facilitan la rápida respuesta del sector financiero en el caso de un ataque. Finalmente, para mejorar la ciberseguridad del sector, el trabajo en conjunto y el intercambio de información con stakeholders nacionales e internacionales es un parte clave del fortalecimiento de la ciber-resiliencia del sector financiero nacional y las instituciones que se lo componen.

WORKSHOP

Developing cybersecurity capabilities in the Pacific Alliance

JUNE 23 | Information Sharing and Cyber Coordination

10:00 - 10:10 am	**Francisco Moreno,** Chilean Deputy Minister of Finance.
10:10 - 10:35 am	Information Sharing by Financial Sector Authorities and the Development of CERES: **Brian Hansen**, Executive Director Asia Pacific at FS-ISAC.
10:35 - 11:20 am	Information Sharing and Cybersecurity Coordination in the UK Financial Sector and the Role of the Public and Private Sectors: • **Paul Williams**, Head of the Operational Risk and Resilience Division, Bank of England. • **Ian Burgess,** Director, Cyber and Third-Party Risk, UK Finance.
11:20 - 11:45 am	The Role of the Financial CSIRT in the Event of a Cybersecurity Attack on the Financial Sector: • **Lavy Shtokhamer,** Executive Director, Head of Israel National CERT.

JUNE 24 | Developments in Cybersecurity Regulation/Supervision

10:00 - 10:10 am	**Ariel Nowersztern**, Cybersecurity Specialist, Interamerican Development Bank.
10:10 - 10:35 am	Cybersecurity Supervision of the Israeli Banking System • **Aya Gal-Ed**, Head of Cyber Defense Unit, Banking Supervision Department, Bank of Israel.
10:35 - 11:00 am	New Models for Cybersecurity Supervision in the Financial Sector: • **Ian Glover**, President, CREST.
11:00 - 12:00 pm	New developments in Cybersecurity Regulation in the Pacific Alliance, Pacific Alliance Regulators (in Spanish): **Elena Calatayud, CNVB, México**: 11:00 - 11:15 am **Alejandro Rabanal, SMV, Perú**: 11:15 - 11:30 am **Magno Condori, SBS, Perú**: 11:30 - 11:45 am **Maurice Frayssinet, Presidencia del Consejo de Ministros, Perú**: 11:45 am - 12:00pm

CO ORGANIZAN:

WORKSHOP

Developing cybersecurity capabilities in the Pacific Alliance

Brian Hansen

Executive Director Asia Pacific at FS-ISAC.

Brian serves as the Executive Director Asia Pacific for the Financial Services Information Sharing and Analysis Center (FS-ISAC) based in Singapore. He joined FS-ISAC in 2017 as the Intelligence Officer for Asia Pacific leading the regional effort for intelligence collection and sharing. Prior to joining FS-ISAC, Brian worked for the Pharmaceutical Security Institute as the Senior Intelligence Analyst directly coordinating production of intelligence analysis for executive leadership on criminal involvement with global counterfeit pharmaceutical networks, including cyber-based networks. Earlier, he served in the U.S. Department of Defense in intelligence and foreign affairs for twenty-six years culminating as the Principal Intelligence Officer for the Deputy Assistant Secretary of Defense, East Asia. Brian received his Master of Arts degree in Global Affairs from George Mason University focusing on global conflict and security.

Paul Williams

Head of the Operational Risk and Resilience Division, Bank of England.

Paul has over 25 years of experience in bank technology infrastructure and operational resilience, gained mainly in international investment banking. Paul has leveraged this formative experience to drive the Bank of England sectorfacing cybersecurity and operational resilience program. In his current role as Head of the Operational Risk and Resilience Division, he is responsible for supporting the development of the Bank's supervisory approach to Operational Resilience, working closely with other domestic and international authorities. Paul is chair of the European Central Bank's Systemic Cyber Group and represents the Bank of England on the G7 Cyber Experts Group.

Ian Burgess

Director, Cyber and Third-Party Risk, UK Finance.

Ian leads UK Finance's operational and policy work in the areas of cybersecurity and third-party risk management. In this role he engages with key industry stakeholders to determine the applicability of collective action on behalf of the financial sector, which has included developing the Financial Sector Cyber Collaboration Centre (FSCCC), an industry utility designed to promote cyber intelligence sharing amongst financial institutions.

Lavy Shtokhamer

Head of Israel National CERT, Israel National Cyber Directorate

Lavy is the Head of Israel National CERT at INCD - Prime Minister's Office. Prior to his current role, Lavy was the head of FC3 – the Financial Cyber & Continuity Center. Lavy spent the majority of his career in the cyber financial sector at FIBI – The First International Bank of Israel and in the financial cyber division at NISA – National Cyber Security Authority. Lavy is a senior cybersecurity expert and manager, with vast field experience and deep understanding of the cyber warfare ecosystem at corporate and national levels. On top of the cybersecurity field, Lavy is specialized in identification of new emerging FinTech technologies as a mentor at Barclay's accelerator.

Lavy holds a B.A. in Information Technology and Business Administration from the Inter-Disciplinary Center (IDC) in Herzliya and is an alumnus of the Cybersecurity Risk Management program of Harvard University.

CO ORGANIZAN:

BID Mejorando vidas

Aya Gal-Ed

Head of Cyber Defense Unit, Technology & Innovation Division Banking Supervision Department, Bank of Israel

Aya joined the Central Bank of Israel in 2004. Since then she has occupied a few positions, including System Analyst at the IT department and Operational Risk Auditor at the Banking Supervision Department. In 2012, when the Cyber Defense Unit was established at the Banking Supervision Department, Aya became the first employee of the unit, and played an integral role in all the activities carried out by the unit.

In September 2019, Aya was appointed to head of the unit, which role is to supervise all the aspects related to cyber risk management within the Israeli Banking System. Aya has a B.Sc. in computer sciences and a M.B.A from the Hebrew University, which provides her with the academic background and knowledge to combine cyber defense requirements with the complexity of the banking system

Ian Glover

President, CREST

Ian has worked in the IT industry for over 40 years. As President of CREST, he has taken it to a position of influence in the technical security industry and has been instrumental in major industry initiatives. These include the CREST, Bank of England and Government project to develop the STAR and CBEST Schemes, designed to provide higher levels of assurance for UK financial services and other critical national infrastructure.

Internationally he is working with governments and regulators to develop CREST chapters in Singapore, Hong Kong, Malaysia, Australia and the USA. Previously, Ian was one of the founders of Insight Consulting, a leading specialist information security consultancy which was purchased by Siemens. He then sat on the Board of Siemens Communications. Before establishing Insight Consulting, he worked for the MoD, Treasury (CCTA) and Ernst and Young.

CO ORGANIZAN:


Alianza del
Pacífico