ASBA
ASOCIACIÓN DE SUPERVISORES BANCARIOS DE LAS AMÉRICAS

Aspectos Destacados

Reunión de Discusión Técnica sobre Enfoques Regionales en **Ciberseguridad**

Abril 2019

COMITÉ TÉCNICO DE ASBA

LUIS FIGUEROA DE LA BARRA

INTENDENTE DE REGULACIÓN, SUPERINTENDENCIA DE BANCOS E INSTITUCIONES FINANCIERAS

JAVIER POGGI

SUPERINTENDENTE ADJUNTO DE ESTUDIOS ECONÓMICOS , SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP DEL PERÚ

JUAN SERRANO

DIRECTOR DEPARTAMENTO PLANIFICACIÓN Y ANÁLISIS , BANCO DE ESPAÑA

KERON BURRELL

DIRECTOR POLICY AND METHODS DEPARTMENT , BANK OF JAMAICA

KWAYNE JENNINGS

MANAGER, LARGE AND FOREIGN BANKING ORGANIZATIONS, BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

WILMA DE AQUINO

JEFE DE DEPARTAMENTO DE SUPERVISIÓN BANCARIA , BANCO CENTRAL DO BRASIL

GENERO SEGURA CALDERÓN

SERVICIOS TÉCNICOS, SUPERINTENDENCIA GENERAL DE ENTIDADES FINANCIERAS

ELABORADO POR:

MARCOS FABIÁN COVARRUBIAS

ANTONIO PINEDA ACOSTA

DARÍO TRUJANO OCHOA

ASBA agradece la participación de los miembros que formaron parte de las actividades de la Reunión de Discusión Técnica sobre Enfoques Regionales en **Ciberseguridad:**

Central Bank of Brazil	Jefferson Umebara Pelegrini. Coordinador de Gobernanza de Tecnologías de la Información. (Líder der Sesión 1)
Comisión Nacional Bancaria y de Valores. Mexico	María Elena Calatayud. Directora de Supervisión de Seguridad de la Información. (Líder de Sesión 2)
Bank of Spain	Jose Miguel del Rio Silvia Senabre (Líder de Sesión 3)
Superintendencia de Bancos, Seguros y AFP Perú.	Magno Condori Mollehuara. Intendente de Supervisión de Sistemas de Información y Tecnología (Líder de Sesión 4)
Central Bank of Paraguay	Carmelo Fretes. Intendente de Riesgo Operacional y Tecnológico
Superintendencia de Bancos de Guatemala	Daniel Augusto Monzón Pérez. Departamento de Supervisión de Riesgos Específicos Daniel Estuardo Tobar Torres. Departamento de Normativa.
Superintendencia de Bancos e Instituciones Financieras. Chile	Myriam Uribe. Directora de Riesgos
Central Bank of Uruguay	Gabriela Conde. Gerente de Supervisión de Riesgos. Gustavo Romano. Jefe de Supervisión de Riesgo Operativo y Tecnológico.
Superintendencia Financiera de Colombia	Miguel Angel Villalobos. Superintendente Delegado para Riesgos Operativos Francisco Espinosa. Director de Riesgos Operativos Joshsua González. Asesor Delegatura para Riesgos Operativos
Superintendencia General de Entidades Financieras. Costa Rica	Comisión de Ciber-seguridad (Laura Alpízar Chaves, Ronald González Víquez, Javier Céspedes Ballestero, Osvaldo Sánchez Chaves) Jorge Alvarez Ledezma, Servicios Financiero Digitales Christian Vega Céspedes, Inclusión Financiera, Innovación y Sostenibilidad

I. INTRODUCCIÓN

Los incidentes cibernéticos son eventos que amenazan la ciberseguridad de los sistemas de información, la información misma y su procesamiento, o que violen las políticas y procedimientos de seguridad. Estos pueden ocurrir por ciberataques a través de malware o virus o amenazas internas maliciosas o no maliciosas.[1] Los incidentes cibernéticos aumentan los costos operativos y el riesgo reputacional de las instituciones pudiendo amenazar la estabilidad financiera. Así, para proteger la confianza, la rentabilidad y la estabilidad es necesario mantener el riesgo cibernético acotado. Por lo tanto, la seguridad cibernética concierne tanto a las Autoridades de Supervisión y Regulación (ASR) como a las Instituciones Financieras (IF), quienes enfrentan un entorno cambiante en el que terceras partes están jugando un papel cada vez más relevante. La rápida evolución tecnológica está obligando a las IF y a las ASR a incrementar su capacidad técnica y grado de especialización o bien, a contratar empresas para mantener su competitividad, credibilidad y enfrentar desafíos como la ciberseguridad y seguridad de la información.

El desafío para las autoridades financieras es comprender cómo contribuir a generar un entorno financiero más seguro y resiliente frente a ciberincidentes mediante un enfoque de política pública. Las ASR deben definir sus responsabilidades y alcance dentro del conjunto de autoridades y otras partes interesadas. El monitoreo de la gestión de riesgos es parte de los deberes de las autoridades, y deben determinar su papel en la evaluación de amenazas y vulnerabilidades, pruebas de penetración o en el establecimiento de pautas de gobernanza que incluyan estas cuestiones. Por otro lado, las autoridades tienen que evaluar la información que pueden compartir y que puede ser usada para la gestión de riesgos o para responder a incidentes.

El desarrollo de marcos regulatorios y de supervisión sobre ciberseguridad es heterogéneo entre países y depende de la complejidad de los sistemas financieros y el grado de adopción de nuevas tecnologías. El FSB señaló que sus miembros basaron sus marcos de regulación de ciberseguridad en un pequeño cuerpo de guías o normas nacionales o internacionales previamente desarrolladas por otras autoridades o entidades privadas.[2]

En la región de las Américas , las autoridades regionales son conscientes de la relevancia de la seguridad cibernética[3]. La mayoría de las economías grandes y medianas pertenecientes a la región han aprobado estrategias nacionales de ciberseguridad en los últimos dos años y, de acuerdo con la Encuesta de Expectativas de Regulación y Supervisión Bancaria 2019 realizada por ASBA, la discusión y el establecimiento de nuevas reglas de ciberseguridad se encuentran en el foco de atención de las autoridades. Por lo tanto, es importante comprender el problema, los actores involucrados, así como los enfoques y desafíos regionales para proponer e implementar estrategias que fomenten la resiliencia cibernética y protejan la estabilidad financiera.

El día 02 de abril de 2019 se llevó a cabo la Reunión de Discusión Técnica sobre Enfoques Regionales en Ciberseguridad organizada por ASBA. La reunión consistió de cuatro sesiones:

- Estrategia Nacional de Ciberseguridad y el rol del regulador
- Respuesta a ciberincidentes y compartición de datos
- Prevención y Auditorias
- Elementos clave para la regulación

El presente documento rescata los puntos relevantes de la discusión sostenida por expertos de las instituciones Miembro de ASBA, los cuales se espera sean de utilidad para las ASR de la región.

[1] FSB(2018), Cyber Lexicon https://www.fsb.org/wp-content/uploads/P121118-1.pdf

[2] BCBS (2018), Cyber-resilience: Range of practices. Available at: https://www.bis.org/bcbs/publ/d454.htm

[3] ASBA (2018), Banking Regulation and Supervision Expectations for 2018 in the Americas. Available at: http://www.asbasupervision.com/es/bibl/i-publicaciones-asba/i-2-otros-reportes/1768-banking-regulation-and-supervision-expectations-for-2018-in-the-americas

II. Panorama General

Las Instituciones Financieras (IF) y las Autoridades de Supervisión y Regulación (ASR) han intensificado el uso de medios digitales. Es responsabilidad de ambas partes conocer los riesgos asociados a estas operaciones así como establecer formas de mitigarlos. El aumento en el uso de herramientas digitales para llevar a cabo procesos como almacenamiento de información, procesamiento y análisis de datos, provisión de servicios, entre otros, muchas veces no coincide con la madurez de las instituciones para gestionar y mitigar los riesgos que estos conllevan. De manera paralela, el premio por ataques cibernéticos exitosos se ha incrementado. Esto da lugar a vulnerabilidades que ponen en riesgo a los usuarios y al sistema. Actualmente, en la mayoría de los países las IF no cuentan con guías o lineamientos sólidos por parte de las ASR, y basan la gestión de estos riesgos en estándares internacionales de tecnología que muchas veces las autoridades financieras no comprenden completamente o no responden a la realidad local de economías más pequeñas y de menor complejidad.

Los acercamientos regulatorios a la ciberseguridad en la región han sido limitados, y más reactivos que proactivos. Las jurisdicciones que más han avanzado son las que mayor cantidad de ataques relevantes han recibido. Además, de acuerdo con la Encuesta de Expectativas de 2019 de ASBA, menos de la mitad de las autoridades encuestadas cuentan con una definición de ciberseguridad y poco más de la mitad requieren a las IF reportar ataques cibernéticos relevantes. Sin embargo, en la práctica, muchas veces no existen incentivos ni canales adecuados para hacerlo. Por último, sólo un país mencionó estar considerando requerimientos de capital especiales por ciber riesgo.

Para 2019, diversas autoridades de la región han manifestado que tendrán algún tipo de propuesta regulatoria al tema de ciberseguridad en el sector financiero. En algunas jurisdicciones ya se planea emitir normativa relacionada exclusivamente con el riesgo de ciberseguridad, mientras que otras autoridades han optado por incluir este tema dentro de un marco de gestión de riesgos más amplio que comprende seguridad de la información y otros riesgos operacionales.

Las autoridades financieras están de acuerdo en que es adecuado avanzar en la regulación a través de un marco de principios en lugar de reglas prescriptivas. En un entorno donde los desarrollos en tecnología y la sofisticación de los ataques ocurren de manera acelerada, una regulación prescriptiva corre el riesgo de tornarse obsoleta rápidamente o puede generar complacencia en las IF con la prescripción definida por las autoridades, por lo que las autoridades reconocen la conveniencia de un marco basado en principios.

III. Estrategia Nacional y Organización: Rol y Responsabilidades del Supervisor Bancario

Es necesaria la existencia de una Estrategia Nacional de Ciberseguridad que incluya a la ASR y otras autoridades con experiencia y atribuciones relevantes en el tema. Estas estrategias son necesarias dado el impacto que tiene el sistema financiero sobre cada país y debe incluir diversos actores del sector público tal como incluye varios actores del privado: sectores financieros, tecnología, energía, o seguridad nacional. Esta vinculación es de mucha ayuda dado que las ASR pueden no contar con las capacidades suficientes para asegurar el buen comportamiento de las IF para asegurar la seguridad del sistema. La ciberseguridad se fortalece en la medida en la que un mayor número de instituciones se compromete a hacer frente a este problema.

El rol de las ASR dentro de una Estrategia Nacional de Ciberseguridad es el de establecer los principios mínimos aceptables de ciberseguridad que se esperan de los participantes del sistema financiero. A muchos sectores les preocupa la ciberseguridad, pero las IF son un objetivo frecuente de ciberincidentes. Entonces, éstas deben cumplir con requerimientos operacionales específicos que aseguren la continuidad del plan de negocio y la protección de la privacidad de datos financieros. Las IF deben asegurar dentro de sus procedimientos el buen funcionamiento de sus sistemas de seguridad, que muchas veces están en manos de terceros. Por su parte, las ASR deben verificar y asegurar la implementación de los requerimientos y principios estipulados.

Las ASR deben apoyar la coordinación con otras autoridades relevantes. Existen autoridades relevantes en otros sectores con quienes es necesario realizar un trabajo de coordinación para asegurar una regulación eficaz de la ciberseguridad en el sector financiero. Esta coordinación intersectorial es vital para la prevención de ciberincidentes que ocasionan ataques y la mitigación de daños cuando estos ocurran.

Para integrar a las autoridades de sectores clave, como telecomunicaciones y seguridad, se pueden implementar Ejercicios de Seguridad Cibernética, donde la ASR puede participar coordinando a los actores del sector financiero. Los participantes de este tipo de ejercicios provienen de diferentes sectores como: legales, TI, relaciones públicas y comunicación, así como de seguridad y defensa, manejo de riesgos, energía, telecomunicaciones y supervisión bancaria. Para incluir al sistema financiero, la convocatoria a los Ejercicios de Seguridad Cibernética se haría a través de la ASR, quien debe ser responsable de coordinar las acciones con bancos y otros proveedores de servicios financieros. En Brasil, por ejemplo, estos ejercicios (*Exercício Guardião Cibernético*), son coordinados por el ministerio de defensa, pero es el Banco Central do Brasil quien representa al sector financiero.

Las autoridades deben realizar simulaciones de escenarios frente a incidentes que amenacen el sistema financiero aún cuando la fuente de estos escape del perímetro regulatorio. Estas simulaciones les ayudan a desarrollar planes de contingencia, estrategias de prevención y a identificar áreas de oportunidad. Por un lado, se pueden seleccionar para simulación escenarios que afecten directamente la operación del sistema como crisis severas del sistema financiero por disrupciones críticas de los servicios de telecomunicación o intrusiones en las operaciones como el ataque a cajeros automáticos. Por otro lado, se pueden analizar escenarios que afecten al comportamiento de los agentes en el sistema financiero y que pueden crear problemas de liquidez bancaria debido a noticias falsas que pueden provocar retiros masivos, o por manipulación de la información sobre el precio de activos. Estos ejercicios permiten mejorar la comunicación y reconocer brechas en la regulación y los marcos de gestión de riesgos. Finalmente, el éxito de estos ejercicios de análisis de escenarios se basa en la participación de diferentes actores.

Se requiere que las ASR analicen y compartan rápidamente la información de los incidentes con autoridades de otros sectores, e incluso, de otros países. Los instrumentos de intercambio de información tradicionales como el Memorándum de Entendimiento (*memorandum of understanding*, MoU), son importantes, pero no suficientes; se necesitan canales más eficientes para responder a futuros incidentes y recibir información proveniente de otros países. Las preguntas que deben hacerse las autoridades son: ¿Cómo deberían ser estos nuevos mecanismos? ¿Debería ser a través de otro instrumento legal, medios informales, cambios en la normas, o nuevas construcciones institucionales? ¿Qué poder legal o de autoridad tendrían estas redes?

La necesidad de compartir la información sobre incidentes con otros actores relevantes de manera oportuna implica que no se puede esperar por un análisis completo del incidente. Esto representa un reto para las ASR quienes deben ponderar la exigencia de compartir la información de manera oportuna y la necesidad de realizar una evaluación previa que provea mayor información relevante de la situación. Cómo las ASR deben enfrentar esta disyuntiva sigue siendo una pregunta abierta. En el caso de Brasil, uno de los resultados esperados de los *Exercício Guardião Cibernético* es la creación de protocolos de comunicación que permita la creación de una red de cooperación entre las autoridades para el intercambio de información inmediata y relevante. Así mismo, una red de respuesta por parte de las IFs también es imprescindible.

Los retos más importantes para el Supervisor Bancario son:

- **Lograr establecer una cultura generalizada de ciberseguridad e integrarla con el marco de gestión de riesgos.** En general, los directivos de los bancos, acostumbrados a lidiar con riesgos tradicionales como crédito o liquidez, deben poner mayor atención al riesgo operacional de los ciberincidentes. En un ciberincidente ocurrido en un banco de Brasil, por ejemplo, se encontró que la causa principal fue la falta de cultura en ciberseguridad (lo que ha resultado ser un factor habitual en este tipo de incidentes).

- **Establecer lineamientos sobre la información que se comparte.** Las autoridades deben ponderar la velocidad con que se comparte la información contra la profundidad del análisis del incidente antes de ser compartido.
- **Analizar el posible impacto de la provisión de servicios por terceros, facilitar la adopción de nuevas tecnologías y fortalecer la resiliencia operacional.** Las ASR deben prestar especial atención a los servicios provistos por terceros a las IF, pues si le ocurre un incidente al proveedor de varios bancos, representaría una grave amenaza a la estabilidad del sistema financiero. Así, aunque las ASR no puedan regular directamente a los proveedores, sí pueden realizar requerimientos sobre los contratos con las entidades reguladas, donde pueden mediar este riesgo indirectamente.

IV. Respuesta a Ciberincidentes e Intercambio de Información

Los ciberincidentes "significativos" deben ser reportados inmediatamente y, la autoridad establecerá un lapso razonable para solicitar los planes de acción y mitigación. En el caso de México, los reportes inmediatos pueden ser realizados incluso vía telefónica antes de hacer el análisis correspondiente. El lapso establecido debería permitir a otras instituciones preparar un plan de contingencia en caso de propagación de *malware* o virus, u otro tipo de incidente de manera oportuna. Asimismo, las ASR deberían contar con facultades punitivas en caso de que una institución no reporte un evento significativo de manera inmediata.

Establecer criterios para determinar el tipo de incidentes que se consideran significativos y que deben ser reportados a las autoridades es una buena práctica, en la medida en que no todos los ciberincidentes son relevantes para el correcto funcionamiento del sistema financiero. La autoridad deberá definir claramente los eventos considerados como relevantes. Pueden existir criterios generales, pero cambiarán entre jurisdicciones dependiendo de las características inherentes a sus sistemas financieros. Algunos criterios que se pueden considerar son: el modo de operación replicable, la generación de pérdidas económicas o de información, la interrupción de servicios financieros, la afectación a la estabilidad financiera, a los clientes, o a los sistemas de pagos y compensaciones, y el grado de interconectividad del proceso en cuestión con otras instituciones o el sistema en general.

El intercambio de información y la colaboración entre ASR e IFs es indispensable para la respuesta y gestión ágil de incidentes. Los mecanismos de este intercambio de información deben crear incentivos de colaboración con IFs para obtener información relevante y oportuna para la prevención de incidentes. La información compartida debería concentrarse en el tipo de incidente y no en la identidad u otra información reservada de la institución afectada.

Es conveniente contar con un entorno habilitado exclusivamente para el análisis y divulgación de información entre autoridades sobre incidentes, que contribuya a que la información fluya más rápido, y mitigue la propagación de amenazas. En el caso de México, por ejemplo, la CNBV cuenta con un laboratorio que tiene a cargo las funciones de análisis y comunicación. Luego de analizar un incidente, se envía un comunicado a los actores relevantes con la descripción éste y un conjunto de recomendaciones y acciones inmediatas para mitigar la propagación de la amenaza. Por ejemplo, bloqueo de direcciones IP, *urls*, puertos en los *firewalls*; la actualización de firmas; inclusión de *hashes* particulares en antivirus; actualización de software con posibles vulnerabilidades descubiertas, entre otros.

Es necesario contar con funcionarios expertos dentro de la ASR y las IF. Un reto para las autoridades es atraer y retener talento especializado. No basta solo con compartir información cruda sobre el tipo de incidente, se debe contar con capacidad para entender y utilizar esta información. El análisis interno de las características específicas del malware o virus, previo a la divulgación de información, puede ser de utilidad para facilitar la respuesta de otras instituciones ante incidentes similares. Esto hace que los recursos humanos capacitados en ciberseguridad sean cada vez más importantes.

Uno de los retos más importantes que han encontrado algunos países es la dificultad para generar un ambiente de colaboración para intercambio de información sobre incidentes. El diseño de mecanismos que incentiven la colaboración es fundamental para cualquier marco de gestión de riesgos cibernéticos. En este aspecto, las jurisdicciones más avanzadas en este tema coinciden con los países afectados de manera relevante por ciber ataques. Sin embargo,a pesar de los avances, aún existen reticencias de algunas instituciones para compartir información.

En términos de Gobierno Corporativo, el posicionamiento del Oficial de seguridad de la información (CISO, por sus siglas en inglés) en la estructura de la institución es fundamental. En muchos casos, el CISO se encuentra en áreas de tecnología, lo que demora la respuesta al tener que solicitar autorización a las áreas de cumplimiento, de negocio o jurídicas. Una tendencia es requerir a las instituciones que el CISO se encuentre inmediatamente abajo del CEO en jerarquía. Este enfoque puede permitir una respuesta más ágil al tomar acciones y decisiones sin tener que enfrentar toda la carga burocrática.

V. Prevención y Auditoria

Existe heterogeneidad en la capacidad técnica y en el nivel de involucramiento tanto de las autoridades como de las IFs para evaluar el entorno de ciberseguridad bancario. En la actualidad, la aplicación de un marco regulatorio de ciberseguridad "universal" puede no ser apropiado debido al alto grado de heterogeneidad en la madurez cibernética de las entidades. Se debe alcanzar un nivel de madurez previo a la adopción de marcos de ciberseguridad que pueden resultar sofisticados. Los marcos propuestos podrían escalar de manera gradual, ajustándose a los arreglos institucionales y mercados de cada jurisdicción.

Para que las pruebas de penetración y evaluaciones de gestión de riesgos cibernéticos sean efectivas, se requiere que tanto las instituciones financieras (IF) como las ASR en la región alcancen cierto grado de madurez tecnológica. Existen distintos niveles de madurez en ciberseguridad tanto entre países como entre instituciones financieras dentro de cada país. No todas las instituciones financieras tienen la capacidad técnica y financiera para desarrollar y soportar los costos de pruebas de ciberseguridad sofisticadas. Es así que las ASR tienen como desafío lograr consolidar un nivel mínimo de madurez que permita la comparabilidad entre instituciones al realizar evaluaciones o inspecciones. Para lograr este cometido las autoridades deberán contar con suficientes recursos financieros y capacidad técnica, esto último relacionado con el problema de atracción y retención de talento.

La supervisión de la tercerización de servicios debe ser un tema de alta relevancia en la agenda de las autoridades supervisoras, en especial los relacionados a proveedores de *cloud computing*. Aunque estos proveedores no responden directamente a las ASR, debido a que se encuentran fuera del perímetro regulatorio, representan riesgos relevantes (operacionales y sistémicos) para el sistema financiero. Aunque estos proveedores realizan inversiones importantes en sus sistemas de seguridad, estos no son infalibles. Así, en el caso de un ataque cibernético o filtración de información, se comprometería el funcionamiento del sistema financiero debido a la extensa y sensible información bancaria que poseen. Se ha observado que las IFs están mudando gradualmente ciertos servicios e información a la nube. Aunado a lo anterior, la experiencia de algunos expertos sugiere que los servicios de cloud estarán concentrados en alrededor de 10 proveedores.

Las autoridades han diseñado mecanismos para gestionar de manera indirecta los riesgos que plantean la tercerización de servicios a la estabilidad financiera. Los mecanismos diseñados por las autoridades son dos: la primera es a través de la revisión de cláusulas en los contratos entre los proveedores de servicios de cloud y las IF. En este aspecto, algunas autoridades tienen la facultad de autorizar o rechazar ciertas cláusulas, así como proponer otras que aseguren cierto grado de prudencia. El segundo mecanismo identificado es requerir un listado de auditores internos certificados para vigilar a sus proveedores de *cloud*. Se ha observado que algunos bancos pequeños han hecho alianzas para poder absorber los costos derivados de este tipo de auditorías.

VI. Elementos Clave para la Regulación

La amenaza y vulnerabilidad que podría ocasionar la materialización de un riesgo en ciberseguridad se debe a la creciente dependencia de activos digitales en las organizaciones. El entorno actual del análisis de riesgo de seguridad de la información es distinto a cualquier contexto anterior porque las organizaciones cada vez más poseen activos digitales. Para atender temas de ciberseguridad, anteriormente bastaba con establecer controles de acceso, de cambio o respaldo de información. Sin embargo, en la actualidad, no sólo el nivel de complejidad es distinto, sino que el tiempo de respuesta ante un incidente demanda una configuración de organización diferente. Para saber cuál es la amenaza o la vulnerabilidad existente en el entorno tecnológico se requiere de la identificación precisa de cuáles son los riesgos que plantean esos activos digitales, es decir, un análisis a mayor detalle.

Existen dos posturas sobre el tratamiento regulatorio de la ciberseguridad en el sector financiero: A través de una regulación específica o como una extensión de los lineamientos para riesgo operacional. En 2017 el Consejo de Estabilidad Financiera levantó un cuestionario[4] acerca del enfoque del sector bancario ante riesgos de ciberseguridad. En la encuesta se observa que un 70% de los países sugiere que la ciberseguridad requiere de un desarrollo regulatorio individual y el restante 30%, que ésta puede tratarse como una extensión sobre riesgos operacionales y de información. La evaluación de riesgo, reporte regulatorio, y la interconexión con terceras partes son los temas que los reguladores consideran de mayor prioridad para atender a través de una regulación específica de ciberseguridad. Es decir, estos tres temas requieren de un análisis mucho más detallado y de un análisis de riesgo individual que no podrían ser atendidos con lineamientos existentes de riesgo operacional.

IOSCO, NIST e ISO/IEC 27000 son los marcos regulatorios más frecuentes usados en el desarrollo de la regulación para tratar con la ciberseguridad. Existe una amplia similitud entre estos marcos regulatorios. Los estándares desarrollan medidas de prevención, detección y de respuesta ante distintos escenarios de ciber-riesgos. En general, existe un conjunto de ocho elementos fundamentales de ciberseguridad para el sector financiero: el marco y estrategia de ciberseguridad empleados; la respuesta del gobierno corporativo; la evaluación de control y riesgo; el monitoreo constante; el nivel de respuesta de las autoridades; la etapa de recuperación y experiencias; el compartir información entre los sectores privados y públicos y; finalmente, el aprendizaje continuo por parte de las jurisdicciones.

No es claro si los temas de ciberseguridad y de seguridad de la información deben atenderse como asuntos independientes o dentro de un mismo marco de gestión de riesgo tecnológico. En este aspecto, el marco que se establece en el estándar ISO 27032 hace una distinción entre seguridad de la información y ciberseguridad, donde ciberseguridad contempla eventos que suceden exclusivamente en el ciberespacio y seguridad de la información contempla cualquier otro tipo de evento. Bajo esta perspectiva, algunos enfoques proponen establecer un marco general de seguridad de la información, imponiendo requisitos adicionales a eventos que sucedan en el ciberespacio ya que la ciberseguridad no solo implica proteger información, sino también otras infraestructuras críticas.

Los principales desafíos que tiene el sector público para enfrentar asuntos de ciberseguridad están relacionados con cooperación, coordinación, y asignación efectiva de recursos. La autoridad financiera debería lograr establecer un marco de cooperación efectiva entre autoridades de otros sectores, crear confianza para intercambio de datos con el sector privado, asegurar que los recursos son adecuados y utilizarlos de manera eficiente y la creación e implementación de marcos de análisis de vulnerabilidades y riesgos.

[4] Financial Stability Board, "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices",