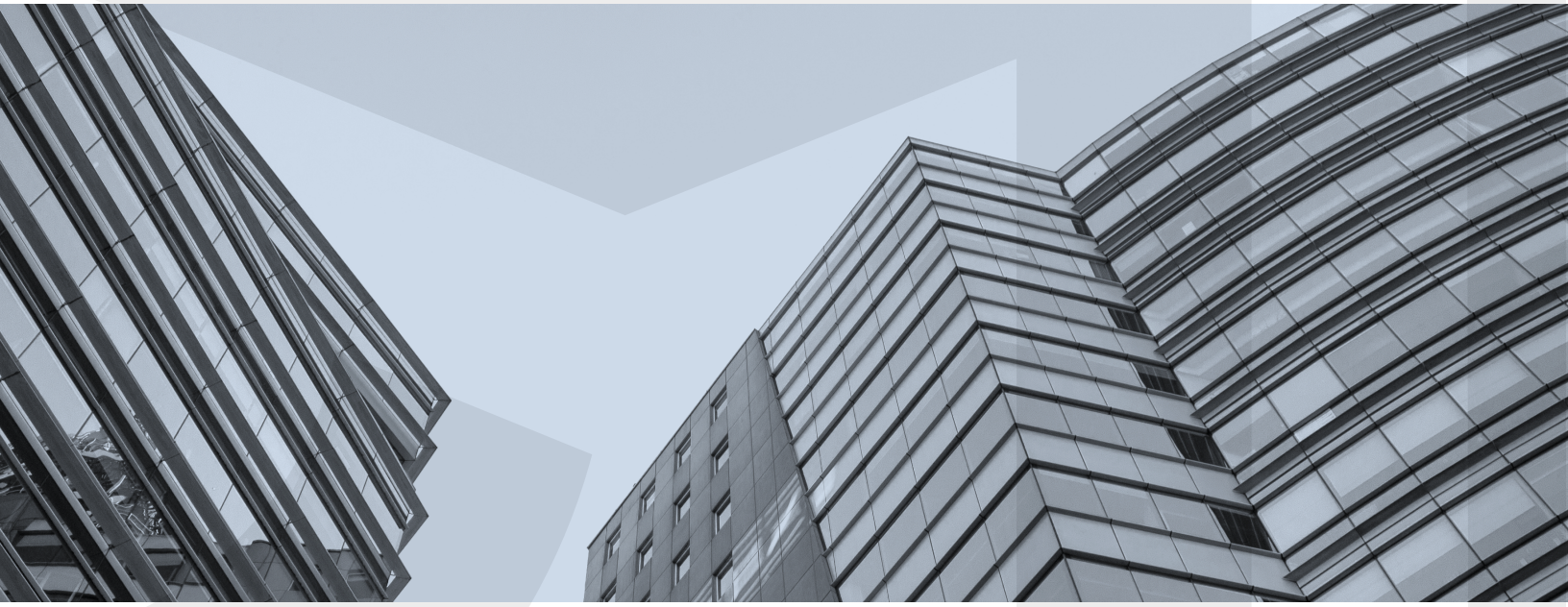
COMISIÓN
PARA EL MERCADO
FINANCIERO



Informe Normativo

Gestión de seguridad de la información y ciberseguridad

Noviembre 2019

Informe Normativo

Gestión de seguridad de la información y ciberseguridad

Noviembre 2019

Contenido

I. Introducción

Los lineamientos definidos en esta propuesta normativa tienen como objetivo establecer sanas prácticas para una adecuada gestión de los riesgos en seguridad de información y ciberseguridad. Al respecto, en los últimos años las instituciones financieras han migrado de manera creciente al mundo de las operaciones digitales, situación que, si bien ofrece una serie de oportunidades a las instituciones fiscalizadas y a sus clientes, también implica mayores riesgos operacionales que deben ser adecuadamente administrados, a fin de lograr un equilibrio entre el uso de las tecnologías de la información y el control de los riesgos subyacentes.

II. Objetivo de la Propuesta Normativa

El objetivo principal de la propuesta normativa es entregar a las empresas bancarias, así como a sus filiales y a las sociedades de apoyo al giro bancarias, y a los emisores y operadores de tarjetas de pago no bancarios, una serie de lineamientos y de mejores prácticas en esta materia, que deben ser consideradas por las entidades en su proceso de la gestión de la seguridad de la información y ciberseguridad, dando con ello cumplimiento a una iniciativa estratégica de este Organismo.

Con esta norma se busca, además, contar con lineamientos específicos para la gestión de esta materia, atendida la importancia que la seguridad de la información y ciberseguridad representan dentro del ámbito de la administración del riesgo operacional. Por ende, la implementación del nuevo marco normativo permitirá eliminar brechas en la materia, apoyando el avance del sistema bancario chileno y financiero, en lo aplicable, en la senda de adopción de las mejores prácticas internacionales.

III. Diagnóstico, Estudios, Principios y Recomendaciones Internacionales

El *World Economic Forum* en su Reporte Global de Riesgos 2019 señala que el fraude y robo de datos masivos se clasificó como el riesgo número cuatro a nivel mundial en un horizonte de 10 años, con los ataques cibernéticos en el número cinco, lo cual si bien es una baja respecto del año 2018 (3° lugar), sigue representando dos de los cinco principales riesgos con mayor probabilidad de materializarse y un alto impacto. Cabe señalar que durante los últimos cinco años los ataques se han duplicado, aumentado también su impacto, particularmente en industrias estratégicas con infraestructura crítica. Adicionalmente, el reporte menciona que los ciberataques o *malware* a gran escala causan graves daños, tensiones geopolíticas o pérdida generalizada de confianza en la Internet, además de los altos costos involucrados, en particular aquellos relacionados con *ransomware*. Un claro ejemplo de la vulnerabilidad de los sistemas en el mundo es que el ataque *WannaCry* afectó a más de 300.000 computadores en más de 150 países, impactando la infraestructura crítica gubernamental como ministerios y hospitales, como también la privada como ferrocarriles, proveedores de telecomunicaciones, empresas de energía y bancos. En nuestro país la industria financiera también se ha visto afectada por eventos de ciberataques, iniciados a través de un *malware* y vulnerando sistemas y/o aplicativos relevantes dentro de las instituciones, generando importantes pérdidas monetarias para las entidades involucradas. Asimismo, se han producido eventos de filtración de datos de tarjetas de pago.

Adicionalmente, el proveedor global de soluciones de seguridad de IT, *Check Point Research* emitió en noviembre del año 2018, un reporte sobre seguridad titulado "Bienvenidos al Futuro de la Ciberseguridad". En él destaca el análisis realizado a la industria financiera y el estado de vulnerabilidad en que se encuentra por su interconectividad de redes y la información financiera de miles de personas concentradas en las instituciones bancarias haciendo más atractivo un ataque a un banco en vez de miles de ataques a miles de personas.

En diciembre del año 2018, el Comité de Supervisión Bancaria de Basilea del BIS (*Bank for International Settlements*), emitió un reporte que identifica, describe y compara las prácticas observadas en las industrias bancarias y sus reguladores respecto de la *ciber-resiliencia* en distintas jurisdicciones. Dentro de las conclusiones se señalan los desafíos e iniciativas actuales para mejorar la resiliencia en esta materia, los que se resumen en 10 hallazgos claves: entorno; estrategia; gestión del riesgo cibernético; instancias de gobierno y organización; fuerza laboral; pruebas; respuesta ante incidentes; métricas; intercambio de información; y riesgos de subcontratación. Todos estos elementos que se consideran un insumo útil para identificar los ámbitos en los cuales se debe normar al respecto.

Por otra parte, durante julio del año 2018, el Fondo Monetario Internacional (FMI) realizó una evaluación en materia de ciberseguridad, la cual fue solicitada por el Ministerio de Hacienda, de manera de incorporar las recomendaciones en el proyecto de ciberseguridad para el sector financiero. Las principales conclusiones del informe emitido por esa entidad son las siguientes:

- Existe un marco legal y regulatorio desigual y fragmentado en materia de ciberseguridad en las distintas industrias del mercado financiero.
- Las regulaciones relevantes siguen un enfoque basado en principios, lo que hace que el marco regulatorio sea más estable y flexible. Sin embargo, la falta de detalles puede llevar a divergencias en el cumplimiento, dificultades en la aplicación y a insuficiente inversión en seguridad cibernética por parte de algunas de las instituciones reguladas.
- La evaluación anual obligatoria de cada institución da como resultado la dilución de los recursos de supervisión de la ciberseguridad, limitando la capacidad de supervisar en materia de ciberseguridad según el riesgo de cada institución en esta materia.
- Los recursos de supervisión específicos para riesgo cibernético son bajos en relación al número y la complejidad de las instituciones supervisadas.

Considerando este diagnóstico, el FMI recomienda cinco pasos clave para fortalecer la capacidad de regulación y supervisión en la gestión de estos riesgos:

1) Crear mandatos homogéneos y explícitos para que cada autoridad regule y supervise la gestión del riesgo cibernético en sus respectivas industrias;
2) Las autoridades deben emitir directrices detalladas sobre la gestión del riesgo cibernético según la exposición a este tipo de riesgo;
3) Las autoridades deben fortalecer su capacidad de supervisión del riesgo cibernético con equipos especializados en ciberseguridad y brindando oportunidades de capacitación;
4) Se debe poner más énfasis en la supervisión in situ de la ciberseguridad;
5) Se deben desarrollar manuales detallados de gestión de riesgos cibernéticos que indiquen la manera de implementar lo establecido en las regulaciones a nivel de principios.

Es en este contexto que esta Comisión considera relevante emitir una normativa específica al respecto, que permita eliminar ciertas brechas y fortalecer la supervisión de estos riesgos.

Además, esto permite ir en línea con lo establecido a nivel de gobierno, donde el año 2017 se crea la Política Nacional de Ciberseguridad, la cual busca orientar la acción del país en materia de ciberseguridad, junto con implementar y poner en marcha las medidas que sean necesarias para proteger la seguridad de los usuarios del ciberespacio, considerando estrategias educativas y de prevención en el ambiente digital.

IV. Jurisdicciones Extranjeras

A continuación, se resume una serie de iniciativas que se han estado adoptando y/o promoviendo, en diferentes jurisdicciones, tanto a nivel gubernamental como de Organismos Reguladores para lograr una adecuada gestión de la seguridad de la información y ciberseguridad. En este contexto, la norma propuesta por la Comisión para el Mercado Financiero ("Comisión" o "CMF") se encuentra, en el ámbito que le corresponde, plenamente en concordancia con las mejores practicas impulsadas por las diferentes organizaciones relacionadas con esta materia.

En este sentido, es importante señalar que para instaurar un adecuado gobierno de seguridad es relevante la existencia de leyes, reglamentos, y otros mecanismos de control que establezcan requisitos que las entidades deben cumplir, asignando responsabilidades a las diferentes instancias, como son por ejemplo el Directorio, los consejos directivos, y gerencias especializadas.

Es así como se pueden distinguir las siguientes formas en que ha abordado esta materia el supervisor financiero en otros países.

a. Singapur

Singapur es considerado el líder en temas de ciberseguridad en Asia y el mundo.

Con respecto al sector financiero, el *Monetary Authority of Singapore* (MAS) emitió en el año 2013 Directrices de Riesgo Tecnológicos. Mientras estas directrices no eran legalmente obligatorias, el cumplimiento de éstas sí fueron considerados en la clasificación de riesgo de las revisiones efectuadas por el MAS a las instituciones. Adicionalmente, el MAS emitió dos circulares en el año 2015 con instrucciones específicas para instituciones financieras del país en temas relacionados con ciberseguridad.

La primera circular "Detección temprana de intrusiones cibernéticas" requiere que las instituciones financieras no solo aseguren sus sistemas contra ataques sino también tengan capacidades robustas para detectar prontamente cualquier ataque y promulgar una rápida contención y recuperación. Enfatiza que la rapidez de la respuesta de la institución es crucial.

Por lo tanto, el MAS requiere que las instituciones financieras 1) tengan habilidades de detectar ciber-intrusiones no solo para sus redes externas sino también por sus redes internas 2) que monitorean la red de comunicaciones internas para detectar y bloquear comunicaciones no autorizados o atípicas entre servidores, sistemas, dispositivos, etc. 3) si llegan a tener una ciber-intrusión exitosa deben hacer una investigación exhaustiva para determinar el nivel de intrusión y los daños incurridos 4) deben contar con un plan de respuesta para ciberataques que ha sido previamente probado y que detalle acciones para recuperación del incidente y comunicación con todos los actores relevantes

(*stakeholders*) 5) finalmente las instituciones financieras tienen que hacer análisis de brechas y evaluación de riesgos en forma permanente para confirmar que sus controles son adecuados.

En la segunda circular emitida por el MAS, "Capacitación en riesgo tecnológico y ciberseguridad para el Directorio", se detallan las responsabilidades de las instituciones financieras en incorporar al Directorio en la toma de decisiones sobre los riesgos de ciberseguridad.

Específicamente, la circular señala que el Directorio y la alta gerencia son responsables de la supervisión de los riesgos tecnológicos y la ciberseguridad. En particular, el Directorio tiene que aprobar la estrategia de TI de la organización y la tolerancia al riesgo, y garantizar que el enfoque de la administración, su experiencia y los recursos disponibles son suficientes para abordar este tema.

MAS espera que el Directorio sea regularmente informado sobre la tecnología y la evolución del riesgo cibernético. Las instituciones financieras deben tener un programa integral de capacitación en riesgos tecnológicos y ciberseguridad para el Directorio. El objetivo es ayudar a equipar al Directorio con el conocimiento necesario para ejercer competentemente su función de supervisión y poder evaluar la adecuación y eficacia del programa de ciberseguridad.

b. Alemania

La regulación respecto a ciberseguridad se encuentra en la Ley de Bancos de Alemania, donde se establecen los requisitos mínimos para la gestión de este riesgo. También se dispone de una circular sobre el riesgo TI que fue publicada en noviembre del año 2017 que provee un marco para la gestión de recursos tecnológicos y riesgos TI. Adicionalmente las instituciones financieras tienen que seguir los estándares de los Manuales de Protección Base de la BSI y los estándares de la familia de las ISO/IEC 27000. Las normas están basadas en principios.

La ley de Seguridad de TI requirió que las instituciones compartan información de ataques cibernéticos. Este requisito entró en vigor el año 2018.

Las instituciones financieras tienen que reportar incidentes operacionales (incluyendo los de ciberseguridad) dentro de 4 horas. El primer reporte incluye información básica del incidente y después de 2-3 días tienen que entregar un reporte más detallado con información sobre el número de clientes afectados y los montos involucrados en el incidente. Finalmente, cuando está solucionado el problema tienen que entregar un reporte *post-mortem*.

El tema de ciberseguridad en Alemania está considerado en un contexto más amplio de riesgo TI, dado que también incluye temas como la seguridad del centro de datos. Los bancos tienen que tener una función de gestión de riesgo TI que está separada de su área de tecnología y que es una segunda línea de defensa con reporte al CRO (*Chief Risk Officer*).

El Directorio es responsable de cualquier eventualidad que enfrenta el banco y reciben reportes trimestrales de la administración sobre riesgos tecnológicos y ciberseguridad.

Si ocurre un ataque de ciberseguridad, no solo los reguladores bancarios se involucran sino también la policía[1], que tiene una unidad especializada en cibercrimen.

La regulación alemana faculta a los supervisores financieros Bafin/Bundesbank para tomar contacto directo y visitar proveedores de servicios críticos de las instituciones financieras.

c. Estados Unidos

En junio de 2015, el Consejo Federal de Evaluación de Instituciones Financieras (*Federal Financial Institutions Examination Council* o "FFIEC"[2]), emitió una Herramienta de Evaluación de Ciberseguridad, conocida como CAT (*Cibersecurity Assessment Tool*) que las instituciones financieras pueden usar para evaluar sus riesgos y su preparación para la ciberseguridad.

La herramienta de evaluación incluye dos partes: un perfil de riesgo inherente y la madurez de la seguridad cibernética.

Para completar la evaluación, la administración primero evalúa el perfil de riesgo inherente de la institución en 5 categorías: 1) Tecnologías y tipos de conexión 2) Canales de entrega 3) Productos en línea / móviles y servicios de tecnología 4) Características organizacionales 5) Amenazas externas.

Luego, la administración evalúa el nivel de madurez en ciberseguridad de la institución para cada uno de los 5 temas: 1) gestión y supervisión del riesgo cibernético, 2) inteligencia y colaboración en amenazas, 3) controles de seguridad cibernética, 4) gestión de la dependencia externa 5) y manejo y resiliencia de incidentes cibernéticos. Por cada aspecto evaluado, hay cinco niveles de madurez: línea base, evolución, intermedio, avanzado e innovador.

Aunque actualmente el uso de la herramienta CAT es opcional, la OCC ocupa la herramienta de evaluación para apoyar sus auditorías de riesgo inherente de los bancos, las prácticas de gestión de riesgos y los controles relacionados con la ciberseguridad.

La primera revisión de los bancos usando esta herramienta de evaluación fue finalizada en el año 2017 y se continúa utilizando. Se evalúa el ciclo de vida del desarrollo de los sistemas, derechos de acceso de los usuarios, capacidad de recuperación del sistema y programas de concientización del usuario, entre otros.

d. México

En octubre de 2017 se firmó la declaración de los 5 Principios para el Fortalecimiento de la Ciberseguridad para la Estabilidad del Sistema Financiero Mexicano a manos de la Secretaría de Hacienda y Crédito Público, la Comisión Nacional Bancaria y de Valores (CNBV). Se adhirieron a estos principios, la Asociación de Bancos de México, la Asociación

[1] German Competence Center Against Cybercrime and the Federal Criminal Police Office

[2] *The FFIEC comprises the principals of the following: The Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee.*

Mexicana de Intermediarios Bursátiles, la Asociación Mexicana de Sociedades Financieras Populares, el Consejo Mexicano de Uniones de Crédito, la Confederación de Cooperativas de Ahorro y Préstamo de México, y la Asociación Fintech de México. Durante la jornada se destacaron la importancia de la colaboración, el rol del regulador, la confianza en el sector financiero, el reconocimiento del cibercrimen como un riesgo latente y la educación de la población tanto desde la sensibilización como la información y capacitación.

Principios para el Fortalecimiento de la Ciberseguridad para la Estabilidad del Sistema Financiero Mexicano:

1) Adoptar y mantener actualizadas las políticas, métodos y controles para identificar, evaluar, prevenir y mitigar los riesgos de ciberseguridad, que se autoricen por los órganos de gobierno de mayor decisión y permeen a todos los niveles de la organización.
2) Establecer mecanismos seguros para el intercambio de información entre los integrantes del sistema financiero y las autoridades, sobre ataques ocurridos en tiempo real y su modo de operación, estrategias de respuesta, nuevas amenazas, así como del resultado de investigaciones y estudios, que permitan a las entidades anticipar acciones para mitigar los riesgos de ciberataques; lo anterior, protegiendo la confidencialidad de la información.
3) Impulsar iniciativas para actualizar los marcos regulatorios y legales que den soporte y hagan converger las acciones y esfuerzos de las partes, considerando las mejores prácticas y acuerdos internacionales.
4) Colaborar en proyectos para fortalecer los controles de seguridad de los distintos componentes de las infraestructuras y plataformas operativas que soportan los servicios financieros del país, promoviendo el aprovechamiento de las tecnologías de información para prevenir, identificar, reaccionar, comunicar, tipificar y hacer un frente común ante las amenazas presentes y futuras.
5) Fomentar la educación y cultura de ciberseguridad entre los usuarios finales, y el personal de las propias instituciones que, a través de una capacitación continua, redunde en una participación activa para mitigar los riesgos actuales de ciberataques.

e. Colombia

La Superintendencia Financiera de Colombia emitió el año 2018 la Circular Externa 007, que impartió instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad que complementa las medidas sobre administración de riesgo operativo y de seguridad de la información, para la gestión de los riesgos de las entidades vigiladas por la Superintendencia.

Dentro de los aspectos más relevantes de dicha normativa, se encuentran los siguientes:

- Se establece la definición de Seguridad de la Información, Ciberseguridad, Ciberespacio, Ciberamenaza o amenaza cibernética, Ciberataque o ataque cibernético, Ciberiesgo o riesgo cibernético, Evento de ciberseguridad, *Security*

Information and Event Management (SIEM), *Security Operation Center* (SOC), Vulnerabilidad, entre otros.

- Obligación para las Entidades de contar con políticas, procedimientos y recursos técnicos y humanos necesarios para gestionar efectivamente el riesgo de ciberseguridad.
- Adopción, por parte de las entidades vigiladas, de medidas mínimas sobre ciberseguridad como:

  a) Políticas y procedimientos

  b) Unidad especializada que gestione los riesgos

  c) Sistema de Gestión para el riesgo de ciberseguridad

  d) Empleo de mecanismos fuertes de autenticación

  e) Establecimiento de estrategias de comunicación sobre ciberseguridad y reportes oportunos a autoridades y clientes

  f) Evaluaciones periódicas sobre gestión de ciberseguridad y establecimiento de indicadores que midan la eficiencia y eficacia de la gestión de seguridad de la información y ciberseguridad

  g) Etapas mínimas de gestión del riesgo de ciberseguridad (Prevención, Protección y Detección, Respuesta y Comunicación, y Recuperación y Aprendizaje)

Adicionalmente, a nivel nacional existe el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT), a quien reportan todos los incidentes relacionados con ciberseguridad y seguridad de la información, la que luego gestiona dichos incidentes y coordina las acciones necesarias para fortalecer las medidas de control y mitigación a nivel país. Complementariamente, existe una obligación de reporte inmediato a la Superintendencia de aquellos incidentes (intentos o ataques) relevantes para las instituciones financieras supervisadas.

f. Brasil

En abril de 2018, el Banco Central de Brasil emitió una resolución que obliga a las organizaciones financieras reguladas por el Banco Central a desarrollar políticas internas de ciberseguridad, un plan de acción para responder ante incidentes y cumplir con ciertos estándares a la hora de contratar servicios de nube. Provisiones especiales ordenan a las instituciones a adoptar las capacidades necesarias para prevenir, detectar y reducir las debilidades para implementar programas de construcción de capacidades para los equipos internos de seguridad.

V. Marco Regulatorio Vigente

La propuesta normativa viene a complementar la regulación vigente de la Comisión señalada en distintas normas, como son aquellas establecidas en la letra c) del numeral 3.2 del Título II del Capítulo 1-13 de la Recopilación Actualizada de Normas (RAN) sobre la evaluación de gestión del riesgo operacional para bancos; el Capítulo 8-41 relativo a las tarjetas de pago; el Capítulo 20-7

en lo que se refiere a los riesgos que las entidades asumen en la externalización de servicios; el Capítulo 20-8 sobre información de incidentes operacionales; y el Capítulo 20-9 sobre gestión de la continuidad del negocio; así como distintas circulares que aplican en la materia.

El detalle del marco normativo en el ámbito de seguridad de la información y ciberseguridad es el siguiente:

- **Capítulo 1-13 de la RAN "Clasificación de gestión y solvencia"**: se refiere a la clasificación de gestión y solvencia de los bancos, de acuerdo con lo señalado en el Título V de la Ley General de Bancos, la que es asignada por este Organismo, a lo menos una vez en cada año calendario, en base a la evaluación practicada sobre las materias que se relacionan directamente con el seguimiento oportuno de los riesgos.

  En ese contexto, en cuanto a los riesgos operacionales la normativa exige de los bancos un monitoreo permanente del riesgo operacional; inversiones en tecnología de procesamiento y seguridad de la información que mitiguen dichos riesgos y que sean concordantes con el volumen y complejidad de las actividades y operaciones que realiza; una adecuada planificación a largo plazo de la infraestructura tecnológica; una estructura dedicada que permita administrar la seguridad de la información en general y de ciberseguridad en particular, planes de continuidad del negocio y contingencia ante diversos escenarios y supuestos que pudieran impedir que la entidad cumpla toda o parte de sus obligaciones, entre otros elementos.

  En enero del año 2018, se introdujo el Anexo 3, que incorpora algunos elementos generales para una adecuada gestión en materia de ciberseguridad. En particular, señala que se debe contar con un marco de acción establecido por el Directorio, el que debe contemplar la estrategia de administración específica de este riesgo, el nivel de tolerancia admitido, roles y responsabilidades de los participantes, los procesos y las metodologías a utilizar para su gestión en consideración a las mejores prácticas, al volumen y complejidad de sus actividades de negocio y a los estándares internacionales existentes para este efecto.

  En agosto del año 2018, se incorporó la obligación del Directorio de pronunciarse sobre la gestión de la ciberseguridad al menos una vez al año y la necesidad contar con una base de incidentes de Ciberseguridad, entre otros aspectos.

- **Capítulo 8-41 de la RAN "Tarjetas de pago":** define las características que deben tener las tarjetas de pago bancarias y establece medidas de resguardo que deben considerar para su operación. Entre otros elementos, se señala que los bancos deben instruir a los tarjetahabientes acerca de las precauciones que deben tener en el manejo de sus tarjetas físicas y de los medios en que ellas pueden ser utilizadas, especialmente para mantener en resguardo las claves personales, así como de las principales normas que rigen su uso. Respecto de los sistemas de autorización y registros de transacciones, los bancos (emisores) operadores y marcas de tarjetas deben contar con una tecnología de seguridad que permita proteger apropiadamente la información contenida en las tarjetas de pago, implementar mecanismos robustos de autentificación y prevención de fraudes, entre otros elementos.

- **Capítulo 20-7 de la RAN "Externalización de servicios"**: contiene pautas de carácter general relativas a servicios externalizados y en forma particular, a la externalización de servicios de procesamiento de datos y resguardos adicionales en el caso de servicios en la nube. La norma señala las condiciones que debe cumplir una entidad ante la decisión de externalizar un servicio, contempla requisitos esenciales respecto a los sitios de procesamiento; los aspectos de continuidad del negocio, seguridad de la información propia y de sus clientes; entre otros. En cuanto a este último aspecto, la entidad bancaria debe exigir al proveedor asegurar la confidencialidad, integridad, trazabilidad y disponibilidad de sus activos de información y la de sus clientes.

- **Capítulo 20-8 de la RAN "Información de incidentes operacionales"**: establece lineamientos para la información que las entidades supervisadas a las que la misma aplica, deben remitir ante la ocurrencia de incidentes operacionales relevantes que afecten la continuidad del negocio, la seguridad de la información o la imagen de la institución, y además, señala las condiciones mínimas que se deben considerar para el desarrollo y mantención de bases de información respecto de incidentes de Ciberseguridad. El 31/08/2018 se introdujeron cambios que perfeccionan el sistema de reporte de incidentes, creando una plataforma digital especialmente establecida por la CMF para reportar los incidentes al regulador en un plazo máximo de 30 minutos. Adicionalmente, se definió la obligación de designar un encargado de nivel ejecutivo para comunicarse con la CMF en todo momento.

- **Capítulo 20-9 de la RAN "Gestión de continuidad del negocio":** contempla una serie de lineamientos para la adecuada gestión de los riesgos de continuidad del negocio, teniendo en cuenta el volumen y la complejidad de las operaciones de las entidades supervisadas a las que la misma aplica. De esta manera, indica la debida existencia de una estrategia aprobada por la máxima instancia de la entidad, de una función de riesgos que se encargue de este ámbito en conjunto con instancias colegiadas de alto nivel, de una estructura para el manejo de situaciones de crisis, de la evaluación de escenarios mínimos de contingencia, entre otros. Dentro de los escenarios de contingencia para los cuales se deben definir y probar planes se encuentran los "ataques maliciosos que afecten la ciberseguridad". Incluye la operatoria de los sitios de procesamiento de datos como parte de los aspectos relevantes que contribuyen a fortalecer la resiliencia operacional de las entidades.

- **Circular N°2 "Normas comunes sobre resguardos operacionales y de seguridad para la emisión y operación de tarjetas de pago":** establece el conjunto de resguardos operacionales y de seguridad que son propios de los sistemas de pago a través de tarjetas y otros medios electrónicos, junto a otras materias y elementos específicos que complementan la gestión del riesgo operacional aplicables tanto a las empresas emisoras de tarjetas de pago no bancarias, como a las empresas operadores de tarjetas de pago. Parte importante de estas normas también son aplicables a los bancos, las que están contenidas en los Capítulos de la RAN que esta Circular referencia. En agosto 2018 se introdujeron actualizaciones al reporte de incidentes operacionales para emisores y operadores de tarjetas de pago.

- **Circular N°3 "Normas generales para empresas de apoyo al giro":** establece el conjunto de disposiciones que deben aplicar las sociedades de apoyo al giro bancario, desde normas de carácter general como su dirección, administración y funcionamiento, sus

operaciones con partes relacionadas, la información que deben enviar a esta Comisión, normas contables y otros elementos de diferente índole.

- **Circular N°8 "Normas generales para sociedades filiales de bancos sujetas a la fiscalización de esta Comisión":** establece el conjunto de normas generales para sociedades filiales de bancos sujetas a la fiscalización de esta Comisión.

- **Carta Circular N° 06/2018 que "Introduce nuevo archivo I12 sobre Incidentes de Ciberseguridad"**: Mediante este archivo los bancos informan todos los incidentes y alertas en materia de ciberseguridad ocurridos en el mes en curso, incluida la información actualizada o complementaria de incidentes reportados en periodos anteriores.

VI. Propuesta Normativa

La siguiente propuesta de norma establece lineamientos y mejores prácticas a ser consideradas por los bancos, y que se harán extensivos a filiales y sociedades de apoyo al giro bancario, y emisores y operadores de tarjetas de pago no bancarios, quienes deberán dar cumplimiento a ésta en su proceso de la gestión de la seguridad de la información y ciberseguridad dentro del ámbito de la administración del riesgo operacional, atendiendo al volumen y complejidad de sus operaciones.

La propuesta en cuestión se describe a continuación:

La norma se divide en 4 secciones. La primera trata de aspectos generales de gestión para las materias de seguridad de la información y ciberseguridad. La segunda define lineamientos que deben considerar las instituciones en la implementación de un proceso de gestión de los riesgos para apoyar el sistema de seguridad de la información y ciberseguridad. La tercera, atendiendo la relevancia de los riesgos cibernéticos, señala una especial diligencia para gestionarlos. La última sección, establece consideraciones que deben tener las instituciones al formar parte relevante de la infraestructura crítica del país.

Los principales elementos que se abordan con las nuevas directrices en consulta se resumen a continuación:

- Se otorgan lineamientos específicos respecto del rol que debe tener el Directorio para la adecuada gestión, tanto de seguridad de la información como de ciberseguridad, otorgándole como responsabilidad la aprobación de la estrategia institucional en esta materia, así como asegurar que la entidad mantenga un sistema de gestión de la seguridad de la información y ciberseguridad, que contemple la administración específica de estos riesgos en consideración a las mejores prácticas internacionales existentes, entre otros aspectos.

- Definición de las etapas mínimas de un proceso de gestión de riesgos de seguridad de la información y ciberseguridad, considerando al menos, la identificación, el análisis, la valoración, el tratamiento y la aceptación de los riesgos a que están expuestos los activos de información de la entidad, así como su monitoreo y revisión permanente.

- Considerando la relevancia de los riesgos cibernéticos, se establece que las entidades deben realizar una especial diligencia para gestionarlos. Para esto se indica la necesidad

de definir los activos críticos, así como las funciones de protección de éstos, la detección de las amenazas y vulnerabilidades, la respuesta ante incidentes y la recuperación de la operación normal de la entidad.

- Se indica que las entidades como parte de la industria financiera deben contar con políticas y procedimientos para el intercambio de información en esta materia de alertas e incidentes de ciberseguridad, identifiquen los activos que componen la infraestructura critica de la industria financiera y del sistema de pago y avancen en la realización de pruebas conjuntas para detectar y gestionar las amenazas y vulnerabilidades que pudieran afectarla.

Contenido de la Propuesta

Texto Propuesto:

CAPÍTULO RAN 20-10

Gestión de seguridad de la información y ciberseguridad

El presente Capítulo contiene disposiciones, basadas en buenas prácticas, que deben ser consideradas como lineamientos mínimos a cumplir por las entidades para la gestión de la seguridad de la información y ciberseguridad. Se entenderá por seguridad de la información, el conjunto de acciones para la preservación de la confidencialidad, integridad y disponibilidad de la información de la entidad. A su vez, la ciberseguridad comprende el conjunto de acciones para la protección de la información presente en el ciberespacio y de la infraestructura que la soporta, que tiene por objeto evitar o mitigar los efectos adversos de sus riesgos y amenazas inherentes, que puedan afectar la seguridad de la información y la continuidad del negocio de la institución.

Especial importancia toman los riesgos que amenazan la ciberseguridad, en un entorno creciente de conectividad y dependencias de los servicios otorgados a clientes a través de plataformas tecnológicas, lo que conlleva a las entidades por una parte a que deban asegurar la adecuada calidad y disponibilidad de los sistemas utilizados para la prestación de dichos servicios y por otra a enfrentar una progresiva exposición a los riesgos especialmente cuando estos se asumen en el ciberespacio.

La debida adhesión a los lineamientos dispuestos en esta norma será parte de la evaluación de gestión que realiza este Organismo a las entidades fiscalizadas en el ámbito de los riesgos operacionales, atendiendo al volumen y complejidad de sus operaciones. Cabe señalar además, que este Capítulo complementa lo señalado en distintas normativas, como son aquellas establecidas en la letra c) del numeral 3.2 del Título II del Capítulo 1-13 de la Recopilación Actualizada de Normas (en adelante RAN) sobre la evaluación de gestión del riesgo operacional; el Capítulo 20-7 en lo que se refiere a los riesgos que las entidades asumen en la externalización de servicios; el Capítulo 20-8 sobre información de incidentes operacionales; y el Capítulo 20-9 sobre gestión de la continuidad del negocio.

En Anexo adjunto se incluyen definiciones de los conceptos utilizados en la presente normativa.

Elementos generales de gestión

En la evaluación de la gestión de la seguridad de la información y ciberseguridad que realiza este Organismo, un elemento fundamental corresponde al rol del Directorio en lo relativo a la aprobación de la estrategia institucional en esta materia y la aprobación de los recursos presupuestarios suficientes para mitigar los riesgos asociados. Es responsabilidad de esta instancia asegurar que la entidad mantenga un sistema de gestión de la seguridad de la información y ciberseguridad, que contemple la administración específica de estos riesgos en consideración a las mejores prácticas internacionales existentes, el que debe ser concordante con el volumen y complejidad de las operaciones de la entidad.

En ese sentido, serán considerados como elementos necesarios para un adecuado sistema de gestión aspectos tales como:

El Directorio, o quien haga sus veces, ha definido una estructura organizacional con personal especializado y dedicado e instancias colegiadas de alto nivel jerárquico, con atribuciones y competencias necesarias para gestionar la seguridad de la información y ciberseguridad, procurando una adecuada segregación funcional entre las diferentes áreas e instancias encargadas de estas materias, con roles y responsabilidades claramente establecidos para cada una de ellas.

Dentro de la estructura organizacional definida se ha dispuesto una función de riesgo, independiente de las áreas generadoras de riesgos, encargada del diseño y mantención de un adecuado sistema de identificación, seguimiento, control y mitigación de los riesgos de seguridad de la información y ciberseguridad. Además, debe ser parte de esta estructura organizacional, la función de un oficial de seguridad de la información y ciberseguridad a cargo de estas materias.

El Directorio ha dispuesto una estructura de alto nivel para la administración de crisis, con atribuciones técnicas y del negocio para conocer y administrar los incidentes de seguridad y ciberseguridad de alto impacto que afecten o pudieran afectar los activos de información, propios o de sus clientes. Como parte de sus funciones, esta estructura debe definir un plan de actuación frente a este tipo de eventos y mantener canales de comunicación adecuados para informar oportunamente de estos incidentes a las autoridades y a las partes interesadas, ya sean internas o externas a la institución.

El Directorio ha aprobado políticas para la gestión de los riesgos de seguridad de la información y ciberseguridad que definan al menos, el alcance y los objetivos de la entidad respecto de estas materias; el nivel de tolerancia al riesgo en específico para cada una de ellas; una clara definición de los activos de información a resguardar; criterios para clasificar la información y la existencia de un inventario de activos de información permanentemente actualizado, consistente con el mapa de procesos de la entidad. Estas políticas deben ser ampliamente difundidas al interior de la organización, revisadas y aprobadas al menos anualmente por esta instancia.

El Directorio como parte del nivel de tolerancia definido ha establecido los niveles de disponibilidad mínimos que espera asegurar en los servicios otorgados a través de plataformas tecnológicas, a fin de otorgar una adecuada prestación de servicios a los clientes.

El Directorio se asegura de informarse periódica y adecuadamente respecto de los riesgos a que está expuesta la entidad en términos de seguridad de la información y ciberseguridad, así como del cumplimiento de sus políticas e incidentes de seguridad de la información y ciberseguridad,

pronunciándose sobre ellos al menos semestralmente, con el fin de mejorar su gestión y prevención.

El Directorio ha aprobado políticas de conducta interna, de manera que todos los empleados y/o personas externas que presten servicios a la entidad utilicen de manera responsable las tecnologías de la información y comunicación puestas a su disposición.

La entidad promueve una cultura de riesgos en materia de seguridad de la información y ciberseguridad. Esto a través de planes formales de difusión, capacitación y concientización a todos los empleados y personal externo que preste servicios a la entidad, los que deben estar en concordancia con las funciones desempeñadas, considerando una periodicidad establecida y oportuna.

Los activos de información de la entidad cuentan con un adecuado resguardo en términos de la seguridad física y ambiental, como, por ejemplo: la protección de las áreas sensibles de negocios, operativas y dependencias técnicas dentro de las que se encuentran los centros de datos, fuentes de energía alterna (UPS por su sigla en inglés) y respaldos de datos y aplicativos.

La entidad como parte de la gestión de sus servicios externalizados, ha implantado un proceso de verificación permanente de la aplicación y cumplimiento de sus políticas de seguridad de la información y ciberseguridad, de manera de garantizar la adecuada protección de los activos de información que son utilizados o administrados por proveedores externos. Asimismo, monitorea permanentemente la infraestructura conectada con proveedores externos, y analiza e implementa medidas para detectar y mitigar potenciales amenazas a la ciberseguridad de la entidad.

La entidad se asegura de evaluar oportunamente los riesgos asociados a la seguridad de la información y ciberseguridad que se podrían estar asumiendo al introducir nuevos productos, sistemas, emprender nuevas actividades y/o definir nuevos procesos.

La entidad realiza inversiones en tecnologías de procesamiento y seguridad de la información y ciberseguridad, que responden a una estrategia definida para estos efectos, que permiten mitigar los riesgos operacionales y tecnológicos y que son concordantes con el volumen y complejidad de las actividades y operaciones que realiza.

La entidad gestiona sus incidentes de seguridad de la información y ciberseguridad, con el fin de detectar, investigar y generar acciones de mitigación de impacto de estos eventos, y resguardar la confidencialidad, disponibilidad e integridad de sus activos de información.

El proceso de gestión de la seguridad de la información y ciberseguridad implementado por la entidad asegura el cumplimiento de las leyes y normativas vigentes, entre las que se encuentran, por ejemplo, la protección de los datos de carácter personal y los derechos de propiedad intelectual.

La entidad realiza auditorías al proceso de gestión de la seguridad de la información y ciberseguridad, con la profundidad y alcance necesario, que considere aspectos tales como el cumplimiento de las políticas y la eficacia de los procedimientos y controles definidos en estas materias.

Proceso de gestión de riesgos de seguridad de la información y ciberseguridad

La implementación de un apropiado proceso de gestión de los riesgos es fundamental para apoyar el sistema de seguridad de la información y ciberseguridad instaurado por la entidad. Para ello este proceso debe considerar, al menos, la identificación, el análisis, la valoración, el tratamiento y la aceptación o tolerancia de los riesgos a que están expuestos los activos de información de la entidad, así como su monitoreo y revisión permanente.

En línea con lo anterior, se deben considerar al menos los siguientes aspectos:

Identificación de sus activos de información de acuerdo con la definición y alcance contenido en la política de seguridad de la información y ciberseguridad. El nivel de detalle utilizado en la identificación del activo de información debe ser suficiente para la adecuada evaluación del riesgo, considerando, por ejemplo, su ubicación física y función, entre otros aspectos.

Identificación de las amenazas que puedan dañar los activos de información, así como de sus vulnerabilidades con relación a las amenazas conocidas y los controles existentes. La identificación de amenazas y vulnerabilidades se refuerza con información obtenida de diferentes fuentes, tanto internas como externas.

Evaluación de los controles existentes de manera de conocer su efectividad y suficiencia.

Identificación de las consecuencias que puedan tener en los activos de información las pérdidas de confidencialidad, integridad y disponibilidad.

La entidad realiza un proceso de análisis de riesgo, que considera elementos como la evaluación de la probabilidad de ocurrencia de incidentes y su consecuencia o impacto en los activos de información, en base al grado de daño o costos causados por un evento de seguridad de la información y de ciberseguridad, determinando así su nivel de riesgo.

La entidad efectúa un proceso de valoración del riesgo, entendido como una actividad donde se compara el nivel de riesgo determinado previamente contra los criterios de valoración y de tolerancia, previamente definidos.

La entidad elabora un plan de tratamiento del riesgo, entendido como una actividad donde los riesgos priorizados en la etapa de valoración, permiten establecer los controles para reducir, aceptar, evitar o transferir los riesgos.

La entidad lleva a cabo un proceso formal tendiente a asegurar que los riesgos resultantes sean concordantes con la tolerancia a los riesgos definida.

La entidad monitorea y revisa regularmente su proceso de gestión de riesgos de seguridad de la información y ciberseguridad, de manera de identificar oportunamente la necesidad de efectuar ajustes en las metodologías y/o herramientas utilizadas.

Elementos particulares a considerar para la gestión de la ciberseguridad

Si bien el diseño, implementación y mantención del proceso de gestión de riesgos de seguridad de la información y ciberseguridad establecido en el Título II de este Capítulo proporciona directrices para la gestión de los riesgos, dada la relevancia de los riesgos cibernéticos, las entidades deben realizar una especial diligencia para gestionarlos.

Un elemento esencial de este proceso de diligencia es la determinación de los activos críticos de ciberseguridad, esto es, aquellos activos de información lógicos que son considerados críticos para el funcionamiento del negocio, incluidos los componentes físicos tales como *hardware* y sistemas tecnológicos que almacenan, administran y soportan estos activos, los que de no operar adecuadamente, exponen a la entidad a riesgos que afecten la confidencialidad, integridad y disponibilidad de la información.

Un segundo elemento, se refiere a las funciones de protección de estos activos, la detección de las amenazas y vulnerabilidades, la respuesta ante incidentes y la recuperación de la operación normal de la entidad. Para gestionar estas etapas se deben considerar aspectos tales como:

Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades

La institución cuenta con un inventario de activos ciberseguridad críticos clasificados desde una perspectiva de confidencialidad, integridad y disponibilidad, considerando sus diferentes estados de su ciclo de vida como son el almacenamiento, la transmisión y procesamiento.

La entidad cuenta con un proceso de gestión del cambio que permite que las modificaciones realizadas a la infraestructura de tecnologías de la información (TI) sean efectuadas de manera segura y controlada, y que los cambios realizados son controlados y monitoreados.

La entidad cuenta con un apropiado proceso de gestión de capacidades, que le permite asegurar que la infraestructura TI cubre las necesidades presentes y futuras, considerando el volumen y complejidad de las operaciones de la entidad.

La entidad cuenta con un proceso de gestión de la obsolescencia tecnológica que le permite mantener una infraestructura TI con estándares de seguridad adecuados.

La entidad cuenta con un proceso de gestión de configuraciones que permite asegurar adecuados controles a los elementos configurables de la infraestructura TI; y su acceso es controlado y monitoreado.

La entidad ha implementado un programa de gestión de parches para asegurar que éstos sean aplicados tanto al *software* como al *firmware* de manera oportuna.

Las redes informáticas se encuentran adecuadamente protegidas de ataques provenientes de Internet o de otras redes externas, a través de la implementación de herramientas que se complementan, tales como: *firewalls*, *firewalls* de aplicaciones *web* (WAF), sistemas de prevención de intrusos (IPS), sistemas de prevención de pérdida de datos (DLP), sistemas anti-denegación de servicios, filtrado de mail, antivirus y anti-*malware*.

Las redes informáticas se encuentran segmentadas de manera de implementar controles diferenciados, considerando aspectos como grupos de usuarios, tráfico de datos encriptado, tipo de servicios y sistemas de información, a fin de proteger las comunicaciones y los activos críticos de ciberseguridad, así como aislar la propagación de los efectos adversos que podrían derivarse de ciberataques a la infraestructura tecnológica.

La segmentación de redes alcanza los diferentes ambientes dispuestos por la entidad, entre los que se encuentran aquellos de desarrollo, de pruebas y de producción.

Los controles establecidos permiten proteger y detectar en forma proactiva ataques a la infraestructura TI realizados a través del uso de códigos maliciosos.

Los controles establecidos permiten mitigar los riesgos derivados del uso de dispositivos móviles y del trabajo a distancia realizado por personal interno o externo.

Los controles establecidos mitigan los riesgos derivados de la adquisición o desarrollo de aplicativos y sistemas, así como su puesta en producción.

La gestión de identidades y de acceso físico y lógico contempla adecuados controles para resguardar las áreas de acceso restringido, los privilegios otorgados a los usuarios de los sistemas, los derechos de accesos a los servicios de red, a los sistemas operativos, a las bases de datos y a las aplicaciones de negocios, entre otros aspectos.

La entidad cuenta con adecuadas herramientas para controlar, registrar y monitorear las actividades realizadas por los usuarios en general, así como de aquellos con privilegios especiales.

Los canales electrónicos dispuestos por la entidad, con los que interactúan los clientes y usuarios, cuentan con apropiados mecanismos de control de accesos, de manera de mitigar, entre otros, los riesgos de suplantación o uso indebido por parte de terceros, de los productos y servicios puestos a su disposición.

La entidad ha dispuesto normas y procedimientos que establecen el tipo de información que requiere ser protegida a través de técnicas de cifrado, así como los algoritmos criptográficos permitidos o autorizados, controles que se utilizan tanto para la transmisión como para el almacenamiento de la información, en orden de proteger su confidencialidad e integridad.

La entidad ha implementado adecuados resguardos para la conservación, transmisión y eliminación de la información, en conformidad con lo establecido en las políticas internas y la legislación vigente.

La entidad ha dispuesto herramientas de monitoreo permanente que le permitan en forma proactiva identificar, recolectar y analizar información interna y externa respecto de nuevas amenazas y vulnerabilidades que puedan afectar sus activos de ciberseguridad.

La entidad cuenta con un proceso de administración de respaldos que le permite asegurar la integridad y la disponibilidad de su información y de sus medios de procesamiento, ante la ocurrencia de un incidente o desastre. A su vez, la entidad realiza al menos anualmente pruebas de restauración de sus respaldos, con el fin de verificar que la información crítica puede ser recuperada en caso que los datos originales se pierdan o se dañen.

La entidad evalúa mecanismos de cobertura destinados a cubrir los costos asociados a eventuales ataques cibernéticos.

La entidad cuenta con un *Security Operation Center* (SOC), propio o a través de un servicio externo, que opera las 24 horas del día, con instalaciones, herramientas tecnológicas y personal dedicado, a fin de prevenir, detectar, evaluar y responder a amenazas e incidentes de ciberseguridad.

La entidad identifica y evalúa regularmente los vectores de ataque a los cuales pudiera estar expuesta, como por ejemplo la manipulación o interceptación de las comunicaciones; *phishing*;

malware; elevación de privilegios; inyección de código; denegación de servicios; ingeniería social; etc., distinguiendo claramente entre aquellos que pueden afectar la infraestructura física; la infraestructura lógica; o los equipos finales (*endpoint*).

La entidad realiza en forma regular, con el suficiente alcance y profundidad, pruebas a la infraestructura critica de ciberseguridad para detectar las amenazas y vulnerabilidades que pudieran existir sobre su sistema de gestión de seguridad de la información en el ciberespacio, tales como *pentesting* y/o *ethical hacking*. Sus resultados son gestionados por las áreas de tecnología y seguridad de la información, monitoreados y controlados por el oficial de seguridad, y comunicados al Directorio, al menos semestralmente, quedando evidencia en las actas de los análisis y acuerdos adoptados.

Respuesta y recuperación de las actividades ante incidentes

La entidad prueba, al menos anualmente, los planes necesarios para enfrentar adecuadamente los escenarios que puedan afectar la ciberseguridad, así como los equipos para dar respuesta a los ciberincidentes que se pudieran materializar, conforme a los escenarios que amenacen la ciberseguridad, definidos de acuerdo al Capítulo 20-9 de la RAN. Estos planes son actualizados cada vez que se registran cambios relevantes, o se materialicen eventos que amenacen la ciberseguridad.

La entidad cuenta con un plan definido de actuación, que dependiendo de la severidad de un incidente de ciberseguridad permite escalar la situación a la alta administración para la toma de decisiones.

La entidad cuenta con un plan de comunicaciones, liderado por la alta administración, que opera ante incidentes de ciberseguridad de alto impacto, el cual alcanza a todas las partes interesadas, ya sea internas o externas, a fin de mantenerlas adecuadamente informadas.

La entidad efectúa un proceso de análisis forense para los ciberincidentes relevantes, que incluya al menos las etapas de investigación y recolección de evidencias, junto con la generación de documentación con el análisis y las conclusiones del trabajo realizado; además de los requerimientos necesarios para custodiar adecuadamente las evidencias generadas.

La entidad cuenta con una base comprensiva de incidentes de ciberseguridad que ponen en riesgo la seguridad de los activos de información presentes en el ciberespacio, identificados de manera individual.

La entidad considera la base de incidentes como un insumo para la realización de pruebas que permitan detectar las amenazas y vulnerabilidades que pudieran existir sobre su sistema de gestión de seguridad de la información y ciberseguridad.

La entidad cuenta con una base de conocimientos y lecciones aprendidas, con el objeto de disminuir los tiempos de respuesta cuando se repita un incidente igual o similar; identificar posibles mejoras en los procesos; facilitar el intercambio de conocimientos; y disponer de información que permita apoyar la toma de decisiones en caso de materializarse nuevos incidentes.

La entidad realiza autoevaluaciones en esta materia, al menos anualmente, para determinar el grado de cumplimiento con las políticas internas, normativa regulatoria y la adherencia a las

mejores prácticas en ciberseguridad, de manera de determinar las vulnerabilidades de su infraestructura y tomar las acciones para su mitigación, así como para prever la adopción oportuna de medidas ante escenarios de amenazas de ciberseguridad.

Gestión de la infraestructura crítica de ciberseguridad del país

La entidad como componente de la industria financiera y del sistema de pagos, se convierte en un actor relevante de la infraestructura critica del país, la que de acuerdo con la definición establecida por la Política Nacional de Ciberseguridad[3] "comprende las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, interrupción o destrucción pueden tener una repercusión importante en la seguridad, la salud, el bienestar de los ciudadanos y el efectivo funcionamiento del Estado y del sector privado".

En este sentido resulta importante que las entidades cuenten con políticas y procedimientos para la identificación de aquellos activos que componen la infraestructura critica de la industria financiera y del sistema de pago, así como para el adecuado intercambio de información de incidentes, con otros integrantes que son parte de esta infraestructura crítica. Además, debe participar en la realización de pruebas conjuntas para detectar y gestionar las amenazas y vulnerabilidades que pudieran afectarla.

Anexo

Definiciones

Activo de información: Componente, recurso o bien económico que sustenta uno o más procesos de negocio de una entidad. Los activos de las entidades varían de acuerdo con la naturaleza de la actividad desarrollada, los que pueden ser primarios como la información (física y lógica) y los procesos y actividades de negocio, o de soporte como *hardware*; *software*; redes de comunicación; personal; entre otros.

Amenaza: Cualquier circunstancia o evento que puede explotar, intencionadamente o no, una vulnerabilidad específica en un sistema u otro tipo de activo, resultando en una pérdida de confidencialidad, integridad o disponibilidad de la información manejada o de la integridad o disponibilidad del propio sistema o activo.

Ciberespacio: Entorno virtual donde se agrupan y relacionan usuarios, líneas de comunicación, páginas *web*, foros, servicios de Internet y otras redes.

Ciberincidentes: 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.

Criterios de impacto del riesgo: Se refiere al perjuicio o costos a la entidad causados por un evento de seguridad de la información, considerando aspectos tales como el nivel de clasificación del activo afectado; los incumplimientos de seguridad de la información (pérdida de confidencialidad, integridad y disponibilidad); o incumplimientos de requisitos legales, regulatorios o contractuales.

Criterios de valoración del riesgo: Valor que tienen para la entidad, los activos de información, considerando aspectos tales como el valor estratégico del proceso de información del negocio; la

[3] https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

criticidad de los activos; la importancia operacional del negocio en términos de su disponibilidad, confidencialidad e integridad; y el cumplimiento de requisitos legales y regulatorios.

Denegación de servicios (DoS): Un ataque de denegación de servicio (*Denial of Service*) se basa en provocar la saturación del objetivo, en la red y/o en los sistemas (servidor, sitio *web*, entre otros), impidiendo el acceso a los usuarios; normalmente, de forma temporal, hasta que se consigue restablecer el servicio.

Elevación de privilegios: Acto de explotación de un error, fallo de diseño o configuración de una aplicación, dentro de un sistema operativo o aplicación, para conseguir acceso a recursos del sistema que normalmente están protegidos frente a una aplicación o usuario.

Ethical hacking: Utilización de técnicas de ataque para encontrar fallas de seguridad, con el permiso de la organización que es objeto de estos ataques, con el propósito de mejorar la seguridad.

Información: Cualquier forma de registro o dato físico, electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesado, distribuido y almacenado.

Incidente de seguridad de la información: Acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la política de seguridad de la información de la entidad.

Manipulación de las comunicaciones: Se basa principalmente en la captura de tráfico, inyección de paquetes, tramas, modificación de la información, entre otros.

Pentesting: Acción constituida por un conjunto de pruebas que se basan en ataques hacia los sistemas informáticos con la intención de encontrar sus debilidades o vulnerabilidades.

Security Operation Center (SOC): Área de seguridad informática, interna o externa, que es responsable de prevenir, monitorear y controlar la seguridad en las diferentes redes y en Internet, con el objetivo de contar con una capacidad de respuesta proactiva, efectiva y eficiente a incidentes de seguridad.

Sistema de Gestión de Seguridad de la Información: Se refiere a la estructura organizacional, políticas, responsabilidades, procedimientos, recursos y procesos dispuestos por la entidad para establecer, implementar, operar, monitorear, revisar y mejorar la seguridad de la información.

Vector de ataque: Ruta o camino que utiliza un atacante para tener acceso al activo objetivo de ataque, incluyendo las actividades y herramientas que el atacante emplea para materializar la amenaza.

Vulnerabilidad: Cualquier debilidad de un activo o control que puede ser explotada por una o más amenazas.

Vigencia

Las instrucciones establecidas en la presente Norma de Carácter General regirán a contar del 1 de marzo del 2020.

CAPÍTULO RAN 1-13 – Clasificación de Gestión y Solvencia

Se eliminan los siguientes párrafos del Título II, numeral 3.2, Letra C) del Capítulo 1-13 de la RAN:

- "La institución gestiona sus incidentes de Ciberseguridad, con el fin de detectar, investigar y generar acciones de mitigación del impacto de estos eventos, y resguardar la confidencialidad, disponibilidad e integridad de sus activos de información. El Directorio de la institución toma conocimiento regularmente de estos incidentes, sean estos materializados o no, y se pronuncia sobre ellos al menos una vez al año, con el fin de mejorar su gestión y prevención."

- "La institución considera la base de incidentes como un insumo para la realización de pruebas que permitan detectar las amenazas y vulnerabilidades que pudieran existir sobre su sistema de gestión de seguridad de la información, las cuales están indicadas en la letra g del Anexo N° 3 de este Capítulo."

- "El banco cuenta con una estructura dedicada que permite administrar la seguridad de la información en general y de Ciberseguridad en particular, en términos de resguardar su confidencialidad, integridad y disponibilidad. Respecto a la gestión de la Ciberseguridad, la entidad al menos contempla los aspectos descritos en el Anexo N° 3 de este Capítulo."

Por otra parte, se agrega el siguiente párrafo al final del Título II, numeral 3.2, Letra C) del Capítulo 1-13 de la RAN:

"Adicionalmente, para una adecuada gestión de la seguridad de información y ciberseguridad, la evaluación de esta Comisión considerará lo dispuesto en el Capítulo 20-10 de esta Recopilación."

Se elimina el Anexo N°3 – Gestión de la Ciberseguridad del Capítulo 1-13 de la RAN.

CIRCULAR N° 2 - Empresas emisoras de tarjetas de pago no bancarias / Empresas operadoras de tarjetas de pago

Se incorpora, a continuación del numeral 5 de esta Circular, un nuevo numeral 6 sobre:

6. Gestión de seguridad de la información y ciberseguridad.

"Las disposiciones del BCCH establecen que como parte de los elementos que deben ser considerados para el desarrollo e implementación de las políticas de gestión y control de riesgos de los emisores y operadores de tarjetas de pago, se incluyan las medidas necesarias para resguardar la Ciberseguridad y de otra índole adoptadas para prevenir y mitigar los riesgos de fraude, así como los demás aspectos que pueda instruir esta Comisión.

En atención a lo indicado, se dispone que las entidades de que trata la presente Circular cumplan con las instrucciones contenidas en el Capítulo 20-10 de la Recopilación Actualizada de Normas para bancos, que contiene el conjunto de lineamientos y buenas prácticas para una adecuada gestión de la seguridad de información y ciberseguridad, las que en todo caso deben ser observadas considerando la naturaleza, volumen y complejidad de las operaciones de cada institución."

CIRCULAR N° 3 - Sociedades de apoyo al giro

Se incorpora, a continuación del numeral 5 del Título V de esta Circular, un nuevo numeral 6 sobre:

6. Gestión de seguridad de la información y ciberseguridad.

"Para una adecuada gestión de la seguridad de información y ciberseguridad, las sociedades de apoyo al giro deberán atenerse a lo dispuesto en el Capítulo 20-10 de la Recopilación Actualizada de Normas para bancos."

CIRCULAR N° 8 - Filiales

Se incorpora, a continuación del numeral 5 en el Título V de esta Circular, un nuevo numeral 6 sobre:

6. Gestión de seguridad de la información y ciberseguridad.

"Para una adecuada gestión de la seguridad de información y ciberseguridad, las filiales deberán atenerse a lo dispuesto en el Capítulo 20-10 de la Recopilación Actualizada de Normas para bancos."

VII. Análisis de Impacto Regulatorio

a. Principales Costos de la Aplicación de la Norma

i. Principales Costos para las Entidades Fiscalizadas a quiénes esta norma les aplica

La propuesta normativa busca establecer buenas prácticas para una adecuada gestión de los riesgos en seguridad de la información y ciberseguridad, basado en estándares internacionales y complementado con algunos lineamientos particulares que ayudan a fortalecer la gestión de las entidades reguladas en esta materia. Lo anterior, podría implicar a las entidades fiscalizadas a quiénes aplica esta propuesta normativa, un aumento en los costos asociados a su implementación, generando un mayor gasto en el diseño y operación de actividades que deben desarrollar para identificar, controlar y monitorear los riesgos.

No obstante, en la práctica, existe un número importante de las entidades financieras que ya cuenta con parte de las exigencias establecidas en la propuesta normativa, debido a que ésta ha sido una materia de preocupación de las entidades y de este Organismo durante los últimos años. Lo anterior, implicaría que, para dichas entidades los costos de la ampliación regulatoria podrían ser acotados.

Se espera que los fiscalizados a quiénes aplica esta propuesta normativa entreguen mayores antecedentes respecto a los posibles costos asociados a la implementación de la norma, en el proceso de consulta pública que se lleve a cabo para estimar el impacto cuando la norma sea emitida.

ii. Principales Costos para la CMF

Si bien en la actualidad durante la fiscalización en terreno se validan aspectos de seguridad de la información y ciberseguridad, la existencia de una normativa específica que norme los distintos aspectos que componen estas temáticas, podrían derivar en nuevas acciones de supervisión, lo que también representa un potencial incremento en los recursos destinados a los procesos de fiscalización de la CMF.

b. Principales Beneficios

i. Principales Beneficios para las Entidades Fiscalizadas

Con la modificación normativa, las entidades financieras a quiénes les aplica tendrán un marco de referencia que contempla las buenas prácticas en materias de seguridad de la información y ciberseguridad, lo que deriva en mejoras para contar con una adecuada gestión de su negocio, así como anticiparse de manera apropiada frente a posibles escenarios adversos, lo que podría implicar ahorro por concepto de disminución de la probabilidad en ciberataques y sus impactos por la materialización de éstos. Adicionalmente, les otorga claridad de los elementos que resultan esenciales para esta Comisión en estos ámbitos, no solo para efectos del cumplimiento normativo, sino que también para su adecuada gestión.

ii. Principales Beneficios para la CMF

La nueva normativa permitiría un fortalecimiento de la supervisión y su alcance por parte de la CMF, otorgando un estándar comparable para la evaluación de gestión de las distintas entidades sujetas a su fiscalización a las cuales les aplica la propuesta, permitiendo perfeccionar y fortalecer el proceso de supervisión que se realiza actualmente. Lo anterior, se podría traducir en una mejor focalización de los recursos del Supervisor, así como también un proceso de supervisión continuo en el tiempo.

c. Principales Riesgos

En caso de que la normativa no se emitiera, dificultaría la labor del Supervisor para exigir requisitos relevantes para la gestión de este riesgo en los términos dispuestos en la propuesta, al no disponer con una base normativa local específica sobre el particular, que permita a su vez, la exigencia de soluciones para las debilidades de control identificadas en el proceso de supervisión. Adicionalmente, generaría un retraso en el ámbito normativo respecto de otras jurisdicciones que ya han dictado instrucciones más detalladas al respecto.

La emisión de la normativa en materia de seguridad de la información y ciberseguridad no presenta riesgos relevantes para los objetivos de la CMF, considerando que se trata de una nueva normativa que permitirá complementar y apoyar el marco normativo

actual, así como fortalecer el modelo de supervisión basada en riesgo, que esta Comisión considera clave para sus procesos de supervisión.

COMISIÓN
PARA EL MERCADO
FINANCIERO

www.cmfchile.cl