



COMISIÓN
PARA EL MERCADO
FINANCIERO

PROYECTO NORMATIVO

Gestión de Riesgo Operacional y Ciberseguridad

Enero 2021



Proyecto Normativo

Gestión de Riesgo Operacional
y Ciberseguridad

Enero 2021

Contenido

I.	INTRODUCCIÓN	4
II.	OBJETIVO DE LA PROPUESTA NORMATIVA.....	5
III.	DIAGNÓSTICO.....	6
IV.	ESTUDIOS, PRINCIPIOS Y RECOMENDACIONES INTERNACIONALES.....	8
V.	PROPUESTA NORMATIVA PUESTA EN CONSULTA	12
VI.	EVALUACIÓN DE IMPACTO REGULATORIO	77
ANEXO A: PRINCIPIOS Y RECOMENDACIONES INTERNACIONALES		80
1.	IAIS: INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS.....	80
2.	OCDE: ORGANIZACIÓN PARA LA COOPERACIÓN Y DESARROLLO ECONÓMICO	87
ANEXO B: MARCO NORMATIVO EXTRANJERO		91
1.	AUSTRALIA, AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY (APRA)	91
2.	REINO UNIDO, FINANCIAL CONDUCT AUTHORITY (FCA)	99
3.	EIOPA: EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY.....	107
4.	USA: NAIC (NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS)	111
5.	OSFI: OFFICE OF THE SUPERINTENDENT OF FINANCIAL INSTITUTIONS.....	119
ANEXO C: MARCO NORMATIVO LOCAL		121
1.	COMISIÓN PARA EL MERCADO FINANCIERO, CMF, ÁREA SEGUROS:.....	121
2.	COMISIÓN PARA EL MERCADO FINANCIERO, CMF, ÁREA BANCOS:.....	122
3.	POLITICA NACIONAL DE CIBERSEGURIDAD (PNCS).....	129

I. INTRODUCCIÓN

En el marco de la implementación de un sistema de Supervisión Basado en Riesgo, la Comisión para el Mercado Financiero (CMF) ha estado impulsando en los últimos años el fortalecimiento del marco de supervisión para el mercado de seguros en Chile.

Es así, como a partir del análisis de la experiencia en otras jurisdicciones y las recomendaciones internacionales, la CMF ha decidido emitir una normativa cuyo objetivo es establecer los principios y mejores prácticas para un sistema de gestión del riesgo operacional y ciberseguridad en la industria de seguros. Estos principios y prácticas servirán, a su vez, a la CMF como parte de la evaluación que realizará de los niveles de solvencia de las compañías (NCG N°325).

Adicionalmente, la normativa establece una autoevaluación, cada 2 años en lo relativo al riesgo operacional y anual en lo referente a ciberseguridad, respecto del grado de cumplimiento de dichos principios y los planes de acción implementados para cerrar las brechas detectadas por las aseguradoras. Asimismo, la norma establece la obligación de entregar información a esta Comisión sobre los incidentes operacionales que las entidades enfrenten.

Los principios y conceptos de gestión del riesgo operacional y ciberseguridad, señalados en la normativa, serán considerados en la evaluación de la CMF de acuerdo a la realidad de cada compañía, reconociendo diferentes prácticas en función de su tamaño, naturaleza, alcance y complejidad de sus operaciones, estrategia corporativa y perfil de riesgo.

La efectividad del sistema de gestión del riesgo operacional y de ciberseguridad como herramienta de mitigación de los riesgos operacionales, dependerá de una participación activa del directorio y la alta gerencia en la definición de la estrategia de gestión de riesgo operacional y de sus políticas, y en la supervisión de su correcta aplicación. Por lo anterior, la presente norma se enmarca en el contexto de la aplicación de adecuados principios de gobierno corporativo en las compañías, considerando para ello las definiciones y principios establecidos en la NCG N°309.

II. OBJETIVO DE LA PROPUESTA NORMATIVA

El objetivo principal de la propuesta normativa es establecer los principios y conceptos de gestión del riesgo operacional y ciberseguridad, que las compañías de seguros deben considerar en la gestión de los riesgos ya señalados.

De igual forma, se busca contar con una autoevaluación de las compañías como herramienta de diagnóstico, que determine el grado de cumplimiento de estos principios, conjuntamente con el establecimiento de planes de acción de las aseguradoras tendientes a cerrar las brechas que éstas identifiquen en la materia.

Asimismo, las compañías deberán reportar a esta Comisión los incidentes operacionales oportunamente, de manera que ésta tome conocimiento y lleve a cabo las acciones pertinentes, en el uso de sus facultades. Deberán además compartir con la industria los incidentes de ciberseguridad, con el objetivo de que los participantes de ésta tengan una mayor capacidad de respuesta y tomen los resguardos necesarios en forma oportuna frente a las amenazas de ciberseguridad.

Finalmente, la normativa permite el fortalecimiento de la supervisión en esta materia por parte de la CMF, estableciendo un marco para la evaluación de gestión de riesgos asociada al riesgo operacional y ciberseguridad, permitiendo complementar y fortalecer el proceso de supervisión que se realiza actualmente.

III. DIAGNÓSTICO

En el marco de la adopción, planificación y desarrollo del modelo de Supervisión Basado en Riesgo en el mercado de seguros, la CMF publicó en 2011 la NCG N°325. Dicha norma establece instrucciones sobre el sistema de gestión de riesgos de las compañías de seguros, basado en principios y buenas prácticas. En particular, para la gestión de riesgo operacional, establece una serie de aspectos que debería contemplar dicha gestión.

Es así como, en el contexto del Sistema de Gestión de Riesgos (SGR) de las aseguradoras, uno de los aspectos que se debe contemplar se refiere a los “Procedimientos y metodologías explícitas para la administración del **riesgo operacional y tecnológico**, incluyendo los riesgos asociados con sus **sistemas informáticos, ...**”.

No obstante lo anterior, es necesario abordar aspectos adicionales incluidos en los principios y recomendaciones internacionales en materia de gestión de riesgo operacional, que permitan:

- Guiar a las compañías en la implementación de los sistemas de gestión de riesgos operacionales, tales como establecimientos de estructuras robustas y apropiadas que sirvan para delinear las prácticas claves de la gestión del riesgo operacional,
- Generar mecanismos de diagnóstico del grado de madurez en la implementación de los principios y mejores prácticas a través de ejercicios de autoevaluación, e
- Implementar herramientas de comunicación de incidentes operacionales significativos, que afecten o pongan en riesgo la continuidad del negocio, los fondos o recursos de la entidad o de sus clientes, la calidad de los servicios o la imagen de la compañía.

En forma similar, es necesario profundizar en aspectos derivados de las amenazas emergentes, específicamente en materia de Ciber Riesgos. Las aseguradoras están buscando constantemente aumentar la eficiencia de sus procesos, así como incorporar nuevos productos para satisfacer y atraer a nuevos clientes. Para ello, las compañías incorporan innovaciones tecnológicas y nuevos modelos de negocios, que conllevan la automatización de sus procesos y el uso creciente de información. En este contexto, las amenazas de ciberataques representan un riesgo para los participantes del mercado de seguros, tanto para la continuidad operacional como para la seguridad de la información. Cabe considerar que las compañías recopilan, almacenan y administran volúmenes sustanciales de información personal y comercial confidencial, lo que, en términos proporcionales, sitúa al Ciber Riesgo como un riesgo crítico.

Más aún, un evento de ciberataque podría poner en riesgo la integridad y estabilidad del sistema financiero en su conjunto. En esta línea, la Comisión, como parte de la Supervisión Basada en Riesgo para el sector bancario, ha emitido normativa relacionada a la información de incidentes operacionales¹ y a la gestión de la seguridad de la información y ciberseguridad², que buscan fortalecer la gestión de dichos riesgos e impulsar a las instituciones a mantener un equilibrio entre el uso de tecnologías de información y mitigación de los riesgos subyacentes.

¹<https://www.sbif.cl/sbifweb/servlet/LeyNorma?indice=C.D.A&idContenido=14321>

²http://www.cmfchile.cl/normativa/cir_2261_2020.pdf

Organismos internacionales, como la IAIS (Asociación Internacional de Supervisores de Seguros), reconocen que los incidentes de ciberseguridad pueden minar la confianza en el sector, dañar a las aseguradoras en su capacidad de realizar negocios y comprometer la protección de los datos comerciales y personales³. Este último punto es de especial relevancia, por cuanto todas las aseguradoras, independientemente de su tamaño, complejidad o líneas de negocio, recopilan, almacenan, procesan y comparten con terceros⁴ cantidades sustanciales de información personal no pública del titular de la póliza, incluida, en algunos casos, información sensible relacionada con la salud. Por lo tanto, la protección de la confidencialidad, integridad y disponibilidad de los datos de las aseguradoras es de fundamental importancia.

El Reporte de Riesgos Globales para 2019⁵, publicado por el *World Economic Forum*, sitúa los ciberataques entre los principales 5 riesgos en crecimiento, e IBM señala en su informe anual de costo de brechas de datos 2019⁶, que el daño económico producido por dichas brechas se ha incrementado en un 12% en el último quinquenio.

Por su parte, el informe anual elaborado conjuntamente por *The Economist Intelligence Unit* y el BID, “El Microscopio global de 2019 - El entorno propicio para la inclusión financiera”⁷ identifica como áreas de mejora en Chile la protección de la privacidad de datos y contra el Ciberdelincuencia.

Por lo anterior, la Comisión ha decidido emitir una norma de riesgo operacional que establezca los principios y conceptos de gestión del riesgo operacional y ciberseguridad, que las compañías de seguros deben considerar en la gestión de dichos riesgos.

³ <https://www.iaisweb.org/file/61857/issues-paper-on-cyber-risk-to-the-insurance-sector>

⁴ Por ejemplo, proveedores de servicios, intermediarios y reaseguradores.

⁵ <https://es.weforum.org/reports/the-global-risks-report-2019>

⁶ <https://www.ibm.com/cl-es/security>

⁷ <https://digital-iadb.lpages.co/bid-invest-microscopio-global-2019/>

IV. ESTUDIOS, PRINCIPIOS Y RECOMENDACIONES INTERNACIONALES

IV.1 Gestión de Riesgo Operacional

En el plano internacional, existen organismos y jurisdicciones que imparten lineamientos relacionados a la gestión del riesgo operacional a través de guías y normativas en la materia. Entre ellos se encuentran la CPS 220 del APRA⁸, la Directriz N°19 de EIOPA⁹, la Guía E-21 de la OSFI¹⁰, la Guía SYSC 13 del FCA¹¹ y el ICP 8 de la IAIS¹².

En todos estos documentos se señala en la necesidad de establecer por parte de las compañías de un sistema efectivo de administración de riesgos y control interno. Dicho sistema debe permitir el desarrollo e implementación apropiado de estrategias, políticas, procedimientos y controles para gestionar diferentes tipos de riesgos materiales, entre los cuales se incluye el riesgo operacional. A su vez, debe proveer al directorio de una amplia y completa visión de los riesgos materiales a los que las compañías están expuestas.

Algunos aspectos que debe incluir el marco de gestión de riesgo dice relación con:

- Estrategia de gestión de riesgo documentada y aprobada por el directorio, que describa los riesgos materiales declarados por la compañía, y la relación entre el directorio y la administración en relación al Marco de Gestión de Riesgo.
- Declaración de apetito de riesgo aprobada por el directorio que sea apropiada, clara, concisa, que incluya todos los riesgos materiales de la compañía y que contenga un componente medible.
- Políticas, procedimientos y mecanismos formales para la identificación y gestión de riesgos materiales.
- Procesos de revisión que garanticen la efectividad del Marco de Gestión de Riesgos

Asimismo, tanto el APRA como la OSFI a través de las guías CPG 220 y E-21, respectivamente, establecen la adopción del modelo de tres líneas de defensa para la gestión del riesgo operacional. Este modelo define responsabilidades de propiedad del riesgo, con supervisión y aseguramiento funcionalmente independientes, proporcionando una visión objetiva adecuada, delineando las prácticas claves de la gestión del riesgo operacional y garantizando su validez.

Al respecto, la primera línea de defensa comprende las actividades propietarias del riesgo y es responsable de planificar, dirigir y controlar las operaciones de las actividades significativas de

⁸ APRA: Australian Prudential Regulation Authority
<https://www.legislation.gov.au/Details/F2019L00669>

⁹ EIOPA: European Insurance and Occupational Pensions Authority
<https://eiopa.europa.eu/publications/eiopa-guidelines>

¹⁰ OSFI: Office of the Superintendent of Financial Institutions (Canadá)
https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/e21_gias.aspx

¹¹ FCA: Financial Conduct Authority (Reino Unido)
<https://www.handbook.fca.org.uk/handbook/SYSC/13.pdf>

¹² IAIS: International Association of Insurance Supervisors
<https://www.iaisweb.org/page/supervisory-material/insurance-core-principles-and-comframe/file/91154/iais-icps-and-comframe-adopted-in-november-2019>

la compañía y, consecuentemente, de identificar y gestionar los riesgos propios de dichas actividades. Por su parte, la segunda línea de defensa corresponde a aquellas actividades que proporcionan asistencia en la gestión del riesgo a través del monitoreo y reporte objetivo del riesgo operacional. Finalmente, la tercera línea de defensa corresponde a la función de auditoría interna responsable de proporcionar una revisión objetiva independiente de controles, procesos y sistemas de gestión de riesgo operacional.

En el plano local, la CMF, en lo relativo a Bancos e Instituciones Financieras, en sus normativas RAN 1-13, 20-7, 20-8 y 20-9, y el documento “**Modelo Chileno de Supervisión Basada en Riesgos**”, ha establecido lineamientos y principios consistentes con la experiencia y principios internacionales en la gestión y evaluación del riesgo operacional. Lo anterior, describiendo, por una parte, ejemplos de buena gestión de riesgo operacional. Y, por otra parte, que dicha gestión se basa en la existencia de una adecuada estructura de gobierno corporativo, un marco con políticas, normas y procedimientos, así como un entorno que permita identificar, evaluar, controlar, mitigar, monitorear y reportar los riesgos más relevantes asociados al outsourcing de actividades.

Tanto la experiencia internacional como la normativa local ya señaladas, se encuentran recogidas e incorporadas en la normativa propuesta.

IV.2 Gestión de Riesgo de Ciberseguridad

En el plano internacional, el documento sobre Supervisión de la Ciberseguridad de las Aseguradoras publicado por la IAIS el año 2018, considera marcos y guías de distintas fuentes, incluidos los Elementos Fundamentales de Ciberseguridad para el Sector Financiero del G7 (G7FE)¹³, los Elementos fundamentales del G7 para una evaluación eficaz de la ciberseguridad para el sector financiero (G7FEA), y la Guía CPMI-IOSCO sobre resiliencia cibernética para las infraestructuras del mercado financiero (CPMI-IOSCO).

Estos elementos constituyen una base sobre los cuales una entidad financiera puede diseñar e implementar su estrategia de ciberseguridad y su marco operativo.

Los 8 elementos fundamentales del G7FE, y que están contenidos en la normativa propuesta, son:

1. Estrategia y marco de seguridad cibernética: su propósito es especificar cómo identificar, gestionar y reducir los riesgos cibernéticos de forma eficaz, de manera integral y comprensiva.
2. Gobierno: su propósito es definir las funciones y responsabilidades del personal necesario para implementar, gestionar y supervisar la implementación de la estrategia de ciberseguridad, proporcionando los recursos necesarios su implementación.
3. Evaluación de riesgos y control: su propósito es identificar las funciones, actividades y servicios (incluidos los servicios subcontratados) sujetos a riesgos cibernéticos,

¹³ https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

- entendiendo y evaluando los riesgos e implementando los controles correspondientes. Estos últimos deben estar alineados con el apetito por el riesgo de la aseguradora.
4. Monitoreo: su propósito es adherirse a las tolerancias de riesgo establecidas y a mejorar o remediar oportunamente las debilidades en los controles existentes.
 5. Respuesta: su propósito es la implementación de políticas de respuesta a incidentes y otros controles para facilitar una respuesta efectiva a incidentes. Entre otras cosas, estos controles deben abordar claramente las responsabilidades de toma de decisiones, definir procedimientos de escalamiento y establecer procesos de comunicación con las partes interesadas internas y externas.
 6. Recuperación: su propósito es asegurar la estabilidad e integridad operativa de la aseguradora una vez ocurrido un incidente de ciberseguridad.
 7. Intercambio de información: su propósito es fomentar el compartir información técnica, como indicadores de amenazas o detalles sobre cómo se explotaron las vulnerabilidades, ayudando a las entidades mantenerse al día en sus defensas y aprender sobre los métodos emergentes utilizados por los atacantes, y
 8. Aprendizaje continuo: las amenazas cibernéticas evolucionan rápidamente, por lo tanto, las estrategias y los marcos de ciberseguridad específicos de la entidad necesitan revisiones y actualizaciones periódicas para adaptarse a los cambios en el entorno de control y amenazas, mejorar la conciencia del usuario y desplegar recursos de manera eficaz.

Por su parte, tanto el APRA en su estándar prudencial CPS 234¹⁴ sobre Seguridad de la información, la NAIC a través de la Ley Modelo de Seguridad de Datos de Seguros, el FCA en su guía Buena Ciberseguridad - los cimientos¹⁵, incorporan en gran medida los 8 elementos anteriormente señalados.

IV.3 Ejercicio de Autoevaluación de Riesgo Operacional y Ciberseguridad

El ejercicio de autoevaluación, a nivel internacional, en el ámbito de seguros, es abordado por la OSFI. El objetivo es la autoevaluación por parte de las compañías de los principios sobre riesgo operacional, de manera que éstas evalúen sus prácticas de gestión de riesgo contra los principios establecidos en la Guía de gestión de riesgo operacional E-21.

De igual forma, dado que la ciberseguridad está adquiriendo una importancia cada vez mayor debido a factores como la dependencia continua y creciente de la tecnología, la interconexión del sector financiero y el papel fundamental que desempeñan las instituciones financieras reguladas en la economía en general, la OSFI dentro de sus procesos de supervisión, incentiva a las entidades a realizar una autoevaluación en esta materia.

Por su parte la CMF, en el ámbito de seguros, a través de la NCG N°309, de 2011, estableció una autoevaluación, cada 2 años, del grado de cumplimiento de las estructuras y principios de

¹⁴ https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf

¹⁵ <https://www.fca.org.uk/publication/documents/cyber-security-infographic.pdf>

gobierno corporativo establecidos en la dicha norma. Estos principios son los que deberían guiar a la compañía en materia de gestión de riesgo y sistemas de control.

Estas directrices de autoevaluación son consistentes con lo establecido en la presente norma en lo relacionado al riesgo operacional y ciberseguridad.

IV.4 Comunicación Incidentes Operacionales

En el ámbito internacional, en lo relativo a la comunicación de incidentes o eventos de riesgo operacional, la FCA a través del principio N°11, establece que las compañías deberán notificar, entre otros eventos, cualquier evento de riesgo operacional significativo identificado por la compañía. En particular, en el SUP 15.3.9 del FCA, establece que el periodo de notificación al regulador dependerá del evento, aunque se espera que las compañías notifiquen eventos relevantes en una etapa temprana.

En el marco normativo local, la CMF, para el caso de los Bancos e Instituciones Financieras, a través de la RAN 20-8, refuerza la relevancia de que las entidades dispongan de sistemas, procedimientos y mecanismos de gestión que permitan identificar, registrar, evaluar, controlar, mitigar, monitorear y reportar incidentes operacionales. Dicha norma, en consistencia con la experiencia internacional, establece que las entidades deberán comunicar los incidentes operacionales que afecten o pongan en riesgo la continuidad del negocio, los fondos o recursos de la entidad o de sus clientes, la calidad de los servicios o la imagen de la institución, en un plazo máximo de 30 minutos luego de su ocurrencia.

V. PROPUESTA NORMATIVA PUESTA EN CONSULTA

REF.: Imparte instrucciones en materia de gestión de Riesgo Operacional y Ciberseguridad, así como de la realización periódica de autoevaluaciones en ambas materias en entidades aseguradoras y reaseguradoras.

NORMA DE CARACTER GENERAL N° BORRADOR

A todas las entidades aseguradoras y reaseguradoras

Esta CMF, en uso de sus facultades legales, en especial lo dispuesto en el número 1 del artículo 5 y el número 3 del artículo 20 del DL N°3.538, de 1980, y la letra b) del artículo 3° del D.F.L N°251, de 1931, y lo acordado por el Consejo de la Comisión para el Mercado Financiero en Sesión Ordinaria N° XX del XX de diciembre de 2020, ha resuelto impartir las siguientes instrucciones relativas al sistema de gestión del riesgo operacional por parte de las entidades aseguradoras y reaseguradoras, de ciberseguridad y a la información sobre sus eventos de seguridad de la información y ciberseguridad que dichas entidades deben proporcionar a este Servicio.

I. OBJETIVO Y ALCANCE DE LA NORMA.

En el marco de la implementación del sistema de Supervisión Basado en Riesgo que la Comisión para el Mercado Financiero (CMF) ha estado impulsando en los últimos años con el propósito de fortalecer el sistema de supervisión del mercado de seguros en Chile, y a partir del análisis de la experiencia en otras jurisdicciones y las recomendaciones internacionales en materia del sistema de gestión de riesgo operacional, en especial de la Asociación Internacional de Supervisores de Seguros (IAIS, por siglas en inglés), la CMF ha decidido emitir la presente norma. Su objetivo es establecer principios de un adecuado sistema de gestión del riesgo operacional y ciberseguridad que servirán de base para la evaluación de las compañías en esta materia por parte de esta Comisión. Lo anterior, en el contexto de la evaluación del nivel de solvencia de las compañías que este Servicio realiza, de acuerdo a lo dispuesto en la NCG N°325. Asimismo, la presente norma establece la información sobre los eventos operacionales que las entidades deberán comunicar a esta Comisión.

Los principios y conceptos de gestión del riesgo operacional señalados en la presente norma, serán considerados en la evaluación de la CMF, de acuerdo a la realidad de cada compañía, reconociendo la existencia de diferentes prácticas de gestión de riesgo operacional dependiendo del tamaño, naturaleza, alcance y complejidad de sus operaciones, estrategia y perfil de riesgo de la compañía. De esta manera, la aplicación de estos principios o conceptos

pueden adoptar modalidades distintas en cada aseguradora, lo que será tomado en cuenta por la Comisión en su evaluación.

El directorio y la alta gerencia son los responsables del cumplimiento de los principios establecidos en esta norma. De esta forma, el directorio deberá aprobar las políticas que implementan los principios detallados en esta norma en la compañía, y monitorear el cumplimiento de estos principios. Por su parte, la administración deberá establecer los procedimientos para una correcta implementación de dichos principios. De la misma forma, el directorio de la compañía deberá aprobar los informes de autoevaluación en materia de riesgo operacional y ciberseguridad requeridos en esta norma, previo a su envío a la CMF en el caso de riesgo operacional.

La efectividad del sistema de gestión del riesgo operacional, como herramienta de mitigación de los riesgos operacionales que enfrentan las compañías, dependerá en gran medida de una participación activa del directorio y alta gerencia en la definición de dicho sistema, de la estrategia de gestión de riesgo operacional y de sus políticas, y en la supervisión de su adecuada aplicación. Por lo anterior, la presente norma se enmarca en el contexto de la aplicación de los principios de un adecuado gobierno corporativo en las compañías, considerando para ello las definiciones y principios establecidos en la NCG N°309.

II. DEFINICIÓN DE RIESGO OPERACIONAL.

Para los fines de esta norma, el riesgo operacional se definirá como el riesgo de pérdida resultante de fallas humanas, procesos y sistemas internos inadecuados o fallidos, o de eventos externos. Esta definición excluye el riesgo estratégico y reputacional. Se excluye la exposición al riesgo que se deriva de la cobertura vendida por las compañías a terceros; mientras que el riesgo en las operaciones propias de una compañía se considera incorporado dentro del alcance de la definición de riesgo operacional.

III. PRINCIPIOS DE UNA ADECUADA GESTIÓN DE RIESGO OPERACIONAL

A continuación, se detallan los principios asociados a una adecuada gestión del riesgo operacional.

1) MARCO DE GESTIÓN DE RIESGO OPERACIONAL

Principio 1: La gestión del riesgo operacional debe integrarse completamente en el sistema de gestión de riesgos de las compañías y documentarse adecuadamente.

El riesgo operacional es inherente a todos los productos, actividades, procesos y sistemas. Como tal, la gestión efectiva del riesgo operacional debe ser un elemento fundamental del sistema de gestión de riesgos de una compañía. La CMF espera que las compañías tengan un marco para la gestión del riesgo operacional que establezca mecanismos para gestionar el riesgo operacional.

Además, un marco sólido para la gestión del riesgo operacional proporciona un mecanismo para el debate y la escalada efectiva de los problemas que conducen a una mejor gestión del riesgo a lo largo del tiempo y una mayor capacidad de recuperación institucional. La completa recopilación de datos, que soporta el marco, permite el análisis de problemas complejos a nivel corporativo y facilita las acciones de mitigación de riesgos en la medida de las necesidades de la compañía. Las herramientas adicionales, como el análisis de eventos externos y el análisis de escenarios, pueden aportar valor al proceso de gestión de riesgos y desalentar la complacencia en la gestión de riesgos operacionales.

2) DECLARACIÓN DE APETITO DE RIESGO OPERACIONAL

Principio 2: La gestión del riesgo operacional debe servir para respaldar la estructura general de gobierno corporativo de las compañías. Como parte de esto, las compañías deben desarrollar y utilizar una declaración de apetito de riesgo operacional.

Las compañías de seguros deben desarrollar y mantener una declaración de riesgo operacional, como parte del Marco de Apetito de Riesgo general de las compañías, según lo define la NCG N° 309 de 2011. La declaración de apetito de riesgo operacional debe comprender la naturaleza y los tipos de riesgo operacional que la compañía está dispuesta o espera asumir. La declaración de apetito de riesgo operacional debe ser sucinta, clara e incluir un componente medible (límites o umbrales). El propósito de tener un componente medible es indicar el nivel de riesgo operacional que se considera aceptable dentro de la compañía. Los límites o umbrales también pueden servir para indicar el nivel en el cual los eventos de riesgo operacional, los casi fallos o los patrones acumulativos, se consideran necesarios para la escalada a la alta gerencia (en algunos casos, se pueden establecer umbrales de reporte separados).

Al formular su declaración de apetito de riesgo para el riesgo operacional, las compañías pueden considerar elementos tales como: cambios en el entorno externo; aumentos o disminuciones importantes en los volúmenes de negocios o actividades; la calidad del ambiente de control; la efectividad de la gestión de riesgos o estrategias de mitigación; la experiencia de eventos de riesgo operacional de la compañía; y la frecuencia, el volumen o la naturaleza de las violaciones del límite y/o umbral del apetito de riesgo autoimpuesto.

La declaración de apetito de riesgo operacional y / o el umbral de reporte para eventos de riesgo operacional materiales deben revisarse periódicamente para asegurar que siga siendo apropiado. Deben implementarse procesos de escalamiento e informe de violaciones, o posibles violaciones.

3) TRES LINEAS DE DEFENSA

Principio 3: Las compañías deben garantizar la rendición de cuentas efectiva para la gestión del riesgo operacional. Un enfoque de “tres líneas de defensa”, o una estructura apropiadamente robusta, debe servir para delinear las prácticas clave de la gestión del riesgo operacional y proporcionar una visión objetiva adecuada y que trate de desafiar su validez. La forma en que esto se haga operativo en la práctica, en términos de la estructura organizacional de la compañía, dependerá de su modelo de negocio y perfil de riesgo.

La adecuada rendición de cuentas para la gestión del riesgo operacional es esencial. Una estructura de “tres líneas de defensa” es una forma de lograr ese objetivo. Para propósitos ilustrativos, los roles y responsabilidades de cada una de las tres líneas se describen a continuación. Al determinar qué se considera una estructura apropiadamente robusta, tanto las compañías como la CMF considerarán el tamaño, la estructura de propiedad, la naturaleza, el alcance y la complejidad de las operaciones, la estrategia corporativa y el perfil de riesgo.

Primera línea de defensa

La línea de negocios, la primera línea de defensa, tiene la propiedad del riesgo, por lo que reconoce y gestiona el riesgo operacional en el que incurre al realizar sus actividades. La primera línea de defensa es responsable de planificar, dirigir y controlar las operaciones diarias de una actividad significativa y/o proceso de toda la empresa y de identificar y gestionar los riesgos operacionales inherentes en los productos, actividades, procesos y sistemas asociados a dichas líneas de negocio.

Segunda línea de defensa

La segunda línea de defensa son las actividades de supervisión que identifican, miden, monitorean y reportan objetivamente el riesgo operacional. Representan una recopilación de actividades y procesos de gestión de riesgos operacionales, incluido el diseño y la implementación del marco para la gestión de riesgos operacionales. La segunda línea de defensa es la mejor situada para proporcionar revisiones especializadas relacionadas con la gestión del riesgo operacional de la compañía. Además, se debe tener en cuenta que otras áreas del personal de la compañía también pueden considerarse parte de la segunda línea de defensa.

Una función clave requerida de la segunda línea de defensa es proporcionar una evaluación objetiva de los aportes y salidas de las líneas de negocios de la gestión de riesgos de la compañía (incluida la medición y/o estimación de riesgos), y establecer herramientas de informes para proporcionar una seguridad razonable de que son adecuadamente completos y bien informados.

Las aseguradoras deberán contar formalmente con una función de gestión de riesgos en su estructura organizacional. Dicha función deberá contar con los recursos e independencia adecuados, y debe estar contemplada en la estrategia de gestión de riesgos de la compañía.

Tercera Línea de Defensa

La función de auditoría interna se encarga de la tercera línea de defensa. La tercera línea de defensa debe estar separada tanto de la primera como de la segunda línea de defensa, y proporcionar una revisión y pruebas objetivas de los controles, procesos y sistemas de gestión de riesgo operacional de la compañía y de la efectividad de las funciones de primera y segunda línea de defensa. La tercera línea de defensa se encuentra en la mejor posición para observar y revisar la administración de riesgos operacionales de manera más general dentro del contexto de las funciones de administración de riesgos generales y de gobierno corporativo de la compañía. La revisión objetiva y la cobertura de las pruebas deben tener un alcance suficiente para verificar que el marco de gestión del riesgo operacional se haya implementado según lo previsto y funcione de manera efectiva.

4) IDENTIFICACIÓN Y EVALUACIÓN DEL RIESGO OPERACIONAL.

Principio 4: Las compañías deben garantizar una identificación y evaluación integrales del riesgo operacional mediante el uso de herramientas de gestión adecuadas. El mantenimiento de un conjunto de herramientas de gestión de riesgos operacionales proporciona un mecanismo para recopilar y comunicar información relevante sobre riesgos operacionales, tanto dentro de la compañía, como a las autoridades de supervisión relevantes.

La CMF reconoce que el uso de herramientas bien implementadas agrega un mayor valor a la gestión de riesgos y que las compañías deberían tener implementadas herramientas para recopilar y analizar información relevante para la gestión de riesgos operacionales, adecuadas a su estructura organizacional y complejidad de sus operaciones.

Es por lo anterior, que la CMF solicita a las compañías que deban continuar desarrollando y mejorando las herramientas que utilizan para administrar su riesgo operacional y para monitorear y adoptar las mejores prácticas en esta área. Las herramientas específicas utilizadas para identificar, evaluar y analizar el riesgo operacional dependerán de una serie de factores relevantes, en particular la naturaleza (incluido el modelo de negocio), el tamaño, la complejidad y el perfil de riesgo de la compañía.

A continuación, se resumen un conjunto de mejores prácticas emergentes en materia de gestión de riesgo operacional (PGRO) que la CMF tendrá en consideración en la evaluación de la calidad de la gestión de riesgo operacional de las aseguradoras.

5) PRÁCTICAS EMERGENTES DE GESTIÓN DE RIESGO OPERACIONAL

Las siguientes mejores prácticas en materia de gestión de riesgo operacional pueden ser útiles como ejemplos concretos de las prácticas de la industria aseguradora internacional. En su lectura debe estar presente el principio de proporcionalidad, que dependerá de la naturaleza, el tamaño, la complejidad y el perfil de riesgo de las diferentes compañías, así como de la complejidad de sus operaciones, lo que va asociado a la naturaleza de los productos que vende.

Los ejemplos de dichas prácticas que se presentan a continuación no son exhaustivos y no representan una lista de verificación o un punto final para la revisión de supervisión o auditoría interna. Las discusiones en estas áreas deben centrarse en las mejoras en la gestión del riesgo operacional, en lugar de centrarse en el cumplimiento.

Un marco de gestión de riesgo operacional debe proporcionar un mecanismo único para solicitudes de datos específicos por parte de la alta gerencia, lo que lleva a una recopilación de información más completa relacionada con problemas organizativos complejos. Por ejemplo, si la alta gerencia de una compañía está observando un tipo particular de evento de riesgo operacional en un área de la organización, puede ser útil recopilar información sobre si eventos o patrones similares están ocurriendo en otras áreas, es decir, hay indicios de riesgos operacionales más ampliamente difundidos dentro de la compañía.

La toma de decisiones en los niveles más altos de una organización se beneficia de una información más completa. Los marcos de gestión de riesgo operacional están diseñados para permitir la recopilación de información en áreas específicas a través de las líneas de negocios en toda la empresa. Esto puede ser particularmente útil en áreas de riesgo operacional como el fraude externo en todas las líneas de productos o las infracciones y deficiencias del sistema organizacional, ya sea indicativo de casos aislados de comportamiento deshonesto o problemas sistémicos más amplios. En organizaciones con segundas líneas de defensa bien establecidas, las capacidades de recopilación y agregación de información de estos grupos de profesionales pueden conducir a una mejor identificación de problemas y, por lo tanto, a soluciones más amplias y de más largo plazo para los problemas de organización de toda la empresa.

A continuación, se procede a exponer las mejores prácticas en materia de gestión de riesgo operacional como ejemplos concretos de las prácticas de la industria aseguradora internacional en la materia:

1. Dentro de las compañías, el marco documentado para la gestión del riesgo operacional debería considerar al menos los siguientes elementos:
 - a) Una descripción del enfoque de gestión del riesgo operacional de la compañía, incluida una referencia a las políticas y procedimientos relevantes de gestión del riesgo operacional;
 - b) Clara rendición de cuentas, transparencia y responsabilidad sobre la gestión del riesgo operacional entre las tres líneas de defensa;
 - c) Las herramientas de evaluación de riesgos e informes utilizadas por la compañía y cómo se utilizan dentro de la institución;

- d) El enfoque de la compañía para establecer y monitorear el apetito de riesgo y los límites relacionados al riesgo operacional;
 - e) Las estructuras de gobierno utilizadas para gestionar el riesgo operacional, incluidas las líneas de reporte y rendición de cuentas. Esto incluye asegurar que la gestión del riesgo operacional tenga suficiente jerarquía dentro de la organización para ser eficaz;
 - f) El marco debe ser aplicado a nivel de toda la organización;
 - g) Las políticas sobre riesgo operacional debieran ser revisadas regular y apropiadamente;
 - h) La documentación sobre riesgo operacional debe ser eficiente, y proporcionar un valor de administración de riesgo proporcional y ser adecuada para el usuario y/o la audiencia a la que va dirigida.
2. Dentro de las compañías, la primera línea de defensa debe ser responsable de desarrollar capacidades en las siguientes áreas:
- a) Adherencia al marco de gestión del riesgo operacional y políticas establecidas;
 - b) Identificación y evaluación del riesgo operacional inherente dentro de su unidad de negocios respectiva y de su materialidad;
 - c) Establecimiento de controles de mitigación apropiados y evaluación del diseño y la eficacia de estos controles;
 - d) Supervisar y generar informes sobre los perfiles de riesgo operacional de las líneas de negocios y su coherencia con la declaración de apetito de riesgo operacional establecida;
 - e) Generar y analizar el informe del riesgo operacional residual que no está siendo mitigado por los controles, incluidos los eventos de riesgo operacional, las deficiencias de control, los recursos humanos, los procesos y las deficiencias del sistema;
 - f) Promoción de una fuerte cultura de gestión del riesgo operacional en la primera línea de defensa;
 - g) Confirmación de la escalada oportuna y precisa, dentro de la compañía, de cuestiones materiales sobre riesgo operacional;
 - h) Capacitación del personal en sus roles respecto de la gestión del riesgo operacional.

Dentro de la primera línea de defensa las compañías pueden optar por establecer grupos de control que puedan tener una responsabilidad específica por las actividades de riesgo operativo, que incluyen:

- i. Identificar, medir, administrar, monitorear y reportar el riesgo operacional que surge de las actividades e iniciativas operativas de acuerdo con los estándares corporativos.
- ii. Establecer una estructura de control interno adecuada para gestionar los riesgos operativos en su área específica.
- iii. Escalar, de manera oportuna, los riesgos operativos hacia la alta gerencia o hacia las áreas encargadas la de realizar la gestión de riesgos dentro de la compañía.

- iv. Desarrollar e implementar, de manera oportuna, acciones correctivas para los problemas de riesgo operacional que se han identificado.
3. La CMF reconoce que el tamaño y el grado de independencia de la segunda línea de defensa diferirán entre las compañías. La segunda línea de defensa debe tener un nivel adecuado de recursos y encontrarse lo suficientemente calificados para cumplir efectivamente con sus responsabilidades.

Dentro de las compañías, los ejemplos de responsabilidades comúnmente asociadas con la segunda línea de defensa incluyen:

- a) Proporcionar una evaluación efectiva y objetiva, que debe evidenciarse y documentarse donde sea material (por ejemplo, proporcionando ejemplos de las pruebas a los sistemas de gestión de riesgo y sus resultados) para que luego sea observable a la primera línea de defensa;
- b) Verificar el desarrollo continuo de estrategias apropiadas para identificar, evaluar, medir, monitorear y controlar y/o mitigar el riesgo operacional;
- c) Verificar el establecimiento y la documentación continuos de las políticas y procedimientos apropiados de la compañía relacionados con el marco de gestión de riesgo operacional;
- d) Verificar el desarrollo continuo, la implementación y el uso de herramientas apropiadas de gestión de riesgo operacional en toda la empresa;
- e) Verificar que existen procesos y procedimientos adecuados para proporcionar una supervisión adecuada de las prácticas de gestión de riesgos operacionales de la compañía;
- f) Verificar que los procesos de medición del riesgo operacional se integran adecuadamente en la gestión general del riesgo de la compañía;
- g) Revisar y contribuir al monitoreo y reporte del perfil de riesgo operacional de la compañía (esto también puede incluir la agregación y el reporte);
- h) Promover una fuerte cultura de gestión del riesgo operacional en toda la compañía;
- y
- i) Verificar la escalada oportuna y precisa, dentro de la compañía, de los problemas materiales.

4. La evaluación objetiva es el proceso de desarrollar una visión objetiva con respecto a la calidad y la suficiencia de las actividades de gestión de riesgos operacionales de la unidad de negocios, incluida la identificación y evaluación de los riesgos operacionales; Identificación y evaluación de controles; suposiciones y decisión de riesgo (por ejemplo, aceptación, transferencia, rechazo, plan de acción). Esto incluye proporcionar las pruebas a los sistemas de gestión de riesgo cuando sea apropiado.

La evaluación objetiva debe realizarse basada en un proceso estructurado y repetible que se adapta a la mejora continua, permitiendo la flexibilidad cuando sea apropiado). El proceso de evaluación objetiva debe ser:

- aplicado a través de las diversas herramientas de gestión de riesgos operacionales, informes y otros procesos de gobierno;
- realizado por personal capacitado y competente;
- compartido con el negocio de manera constructiva;
- realizado de manera oportuna;
- medido por los resultados (Ej; ha influido en una decisión y/o acción de gestión);
- evidenciado y/o documentado.

La evidencia observable de las pruebas a los sistemas de gestión de riesgo puede incluir evidencia de pruebas integrales a un proceso o evidencia de pruebas con documentación de respaldo en varias etapas del proceso, cuando sea apropiado. Consistente con otras áreas de gestión de riesgo operacional, y la gestión de riesgo en general, el nivel de documentación requerido debería agregar valor al proceso de gestión del riesgo y no convertirse en una distracción de los objetivos generales de gestión de riesgo.

5. En la tercera línea de defensa para el riesgo operacional de la compañía: la revisión objetiva y las actividades de prueba generalmente implican pruebas para el cumplimiento de las políticas y procedimientos establecidos, así como evaluar si el marco para la gestión del riesgo operativo es apropiado dado el tamaño, la complejidad y el perfil de riesgo. La revisión objetiva y las pruebas generalmente consideran el diseño y el uso de herramientas de gestión de riesgos operacionales tanto en la primera como en la segunda línea de defensa, la idoneidad de la evaluación objetiva aplicada por la segunda línea de defensa y los procesos de monitoreo, reportes y de gobernanza.
6. Los siguientes son ejemplos de herramientas de gestión de riesgos operacionales que pueden ser útiles:
 - a) Taxonomía de riesgo operacional;
 - b) Evaluaciones de riesgo y control;
 - c) Cambios en la gestión de riesgos y evaluaciones de control;
 - d) Recopilación y análisis interno de eventos de riesgo operacional;
 - e) Recopilación y análisis externo de eventos de riesgo operacional;
 - f) Indicadores de riesgo y desempeño;
 - g) Mapeo de procesos de negocios materiales;
 - h) Análisis de escenarios;

- i) Cuantificación y/o estimación de la exposición al riesgo operacional
- j) Análisis comparativo

Cada herramienta de gestión de riesgos se describe con más detalle a continuación:

a) Taxonomía de riesgo operacional

Una taxonomía común de fuentes de tipos de riesgos operacionales contribuye a la consistencia de las actividades de identificación y evaluación de riesgos, a la articulación de la naturaleza y el tipo de riesgo operacional al que la compañía está potencialmente expuesta. Una taxonomía inconsistente de los términos de riesgo operacional puede aumentar la probabilidad de no identificar, categorizar y asignar adecuadamente la responsabilidad de la evaluación, monitoreo y mitigación de riesgos.

b) Evaluaciones de riesgo y control

Las evaluaciones de riesgo y control son una de las herramientas principales utilizadas en la evaluación de los riesgos operacionales inherentes y en el diseño y la efectividad de los controles de mitigación dentro de las compañías. Las evaluaciones de riesgo y control proporcionan valor a través de:

- inclusión de una evaluación del entorno empresarial, los riesgos inherentes, los controles y los riesgos residuales, haciendo referencia a la taxonomía de riesgo operacional de la compañía;
- fomentando la alineación adecuada entre el riesgo y sus controles de mitigación;
- desarrollándose periódicamente (para respaldar información precisa y oportuna); y
- manteniendo actividades de apoyo apropiadas y con la frecuencia de mantenimiento necesarias para mantenerse actualizadas y relevantes en la gestión del riesgo operacional

Las evaluaciones de riesgo y control generalmente se completan con la primera línea de defensa en toda la compañía, incluidos los diversos grupos de control, y deben reflejar el entorno actual, pero también deben ser de naturaleza prospectiva. Los planes de acción resultantes que surgen de la finalización de las evaluaciones de riesgo y control deben ser rastreados y monitoreados para facilitar que las mejoras requeridas se implementen adecuadamente. Además, la segunda línea de defensa debe revisar y proporcionar pruebas al sistema de gestión de riesgo operacional y al control, y a los planes de acción resultantes de la primera línea de defensa.

c) Gestión del cambio de riesgos y evaluaciones de control

Las evaluaciones de control y riesgo de gestión de cambios establecen un proceso formalizado para evaluar el riesgo operacional inherente y la conveniencia de mitigar los controles cuando la compañía realiza cambios significativos. Las evaluaciones de riesgo operacional realizadas como parte del proceso de gestión del cambio generalmente deben ser realizadas por la primera línea de defensa. Este proceso de evaluación de riesgos debe considerar al menos:

- riesgos inherentes en el nuevo producto, servicio o actividad;
- cambios en el perfil de riesgo operacional y el apetito de riesgo de la compañía;
- el conjunto requerido de controles, procesos de gestión de riesgos y estrategias de mitigación de riesgos que se implementarán;
- el riesgo residual (riesgo no mitigado); y
- cambios al límite y/o umbral de riesgo relevante.

d) Recopilación y análisis interno de eventos de riesgo operacional

La recopilación y el análisis interno de eventos de riesgo operacional robustos incluyen contar con sistemas y procesos que capturen y analicen eventos de riesgo operacional internos importantes (por ejemplo, aquellos que exceden un umbral interno predeterminado). Un evento de riesgo operacional, que se define como un resultado no intencionado de riesgo operacional, incluye pérdidas y ganancias operacionales reales y potenciales, así como cuasi pérdidas (cuando la compañía no experimentó una pérdida o ganancia explícita como resultado de un evento de riesgo operacional).

La recopilación y el análisis interno de eventos de riesgo operacional brindan información significativa para evaluar 1) la exposición de una compañía al riesgo operacional mediante la agregación y el monitoreo de eventos de riesgo operacional a lo largo del tiempo, y 2) la efectividad general del entorno de controles operacionales. La recopilación de datos internos de riesgo operacional debe ser administrada principalmente por la primera línea de defensa y deben existir controles apropiados (segregación de funciones, verificación) para mantener la integridad de los datos a un nivel aceptable.

Para los eventos de riesgo operacional determinados como materiales, se espera que las compañías identifiquen la causa, así como cualquier acción correctiva requerida, de modo que eventos similares en el futuro no ocurran o se mitiguen adecuadamente. Los estándares establecidos de informes y análisis también deben abordar las expectativas mínimas sobre el análisis de eventos, que incluyen:

- si la exposición es un evento real, potencial o muy cercano a la falta;
- la exposición subyacente a la categoría de riesgo operacional como se define dentro de la taxonomía de riesgo;
- deficiencias y fallas de control que pueden ser mitigadas;
- las acciones correctivas que se tomarán para abordar las deficiencias y fallas de control;
- y
- autorizaciones requeridas

Para los eventos de riesgo operacional materiales, la primera línea de defensa generalmente realiza un análisis apropiado de la causa y se escala de manera adecuada en función del impacto potencial u observado del evento. La segunda línea de defensa revisa y aplica sistema de pruebas al análisis realizado por la primera línea de defensa.

e) Recopilación y análisis externo de eventos de riesgo operacional

Los eventos de riesgo operacional externos son eventos relacionados con el riesgo operacional que ocurren en organizaciones distintas a las compañías de seguros. Las actividades externas de recopilación y análisis de eventos de riesgo operacional pueden incluir la suscripción a una base de datos de informes de pérdidas externas, monitorear la experiencia del evento de riesgo operacional de la compañía a lo largo del tiempo en relación con sus pares, evaluar las exposiciones generales y la efectividad general del entorno de controles operativos.

f) Indicadores de riesgo y desempeño

Los indicadores de riesgo y desempeño son métricas de riesgo que se utilizan para monitorear los principales factores de exposición asociados con los riesgos operacionales clave, los que también pueden proporcionar información sobre las debilidades de control y ayudar a determinar el riesgo residual de una compañía. Los indicadores de riesgo y desempeño, junto con los factores desencadenantes de escalamiento y monitoreo, actúan para identificar tendencias de riesgo, advierten cuando los niveles de riesgo se acercan o exceden los umbrales o límites, y la adopción oportuna de acciones y planes de mitigación. Estas métricas de riesgo podrían contener indicadores internos y externos relevantes para la toma de decisiones.

g) Mapeo de Procesos de Negocios

El mapeo de procesos de negocios es una herramienta utilizada para identificar y administrar riesgos operacionales en procesos significativos o transversales a toda la empresa. Implica identificar los pasos dentro del proceso y evaluar los riesgos operacionales inherentes, las interdependencias de riesgos y la efectividad de los controles, así como las acciones de gestión posteriores necesarias cuando se identifican las debilidades de control.

h) Análisis de escenarios

El análisis de escenarios es un proceso para identificar posibles eventos de riesgo operacional y evaluar su posible resultado e impacto en la compañía. El análisis de escenarios puede ser una herramienta eficaz para considerar posibles fuentes de riesgo operacional y la necesidad de mejoras en los controles de gestión de riesgos o soluciones de mitigación. Para utilizar eficazmente el análisis de escenarios como parte de un programa de gestión de riesgos, los escenarios de riesgos operacionales deben considerar tanto la respuesta organizacional esperada como la inesperada en relación con un evento de riesgo operacional. Si el análisis de escenarios se utiliza como una entrada en la cuantificación / estimación de la exposición al riesgo operacional, la segunda línea de defensa revisa si los escenarios elegidos son apropiados y consistentes con el programa de análisis de escenarios de la compañía.

i) Cuantificación y/o Estimación de la exposición al riesgo operacional

La cuantificación y/o estimación de la exposición al riesgo operacional se debiera discutir a través de los procesos existentes de la evaluación de la solvencia de riesgo propio (ORSA). Independientemente del enfoque de cuantificación del riesgo operacional adoptado, se deben documentar los supuestos clave y se deben realizar las actividades apropiadas de validación y verificación de las exposiciones estimadas en riesgo operacional versus los incidentes operacionales que efectivamente se hayan materializado en la compañía, bajo el período de estimación.

j) Análisis comparativo

El análisis comparativo implica que la primera línea de defensa revisa las evaluaciones de riesgo y los resultados de cada una de las herramientas de gestión del riesgo operacional, de manera de confirmar la evaluación general del riesgo operacional. El análisis comparativo puede ayudar a facilitar que las evaluaciones de riesgos se realicen de manera consistente, y que los aprendizajes de los eventos ocurridos se compartan adecuadamente dentro de la organización. El análisis comparativo también puede identificar áreas en las que una mayor coherencia dentro de las herramientas utilizadas, a nivel de toda la empresa, puede generar valor en la gestión de riesgos mediante el apoyo a la recopilación, agregación y análisis resultante de información más consistente. El análisis comparativo también puede ayudar a identificar herramientas de gestión de riesgos operacionales que pueden no ser efectivas o estar bien implementadas.

Con el fin de evaluar el nivel actual de preparación, y desarrollar y mantener prácticas efectivas de gestión de riesgo operacional, la CMF solicita a las compañías que completen el cuestionario de autoevaluación contenido en el Anexo N° 1 de esta norma, la cual está enfocada en las mejores prácticas de gestión de riesgo operacional.

IV. MARCO DE GESTIÓN DE RIESGO DE CIBERSEGURIDAD

La llegada de las nuevas tecnologías, que se han incorporado a los modelos de negocios de las compañías de seguros, se han traducido principalmente en la obtención de una mayor eficiencia en los procesos asociados a los ciclos de negocio de éstas.

Pero la tecnología también ha ocasionado la aparición de nuevos riesgos que las compañías tienen que enfrentar. Dentro del riesgo operacional existe el riesgo asociado al uso de la tecnología en las operaciones de las compañías de seguros, y como uno de los riesgos tecnológicos importantes se encuentra el de ciberseguridad. La IAIS reconoce que los incidentes de ciberseguridad pueden dañar a las aseguradoras en su capacidad de realizar negocios, comprometer la protección de los datos comerciales y personales y minar la confianza en el sector.

Todas las aseguradoras, independientemente de su tamaño, complejidad o líneas de negocio, recopilan, almacenan y comparten con terceros (por ejemplo, proveedores de servicios, intermediarios y reaseguradores) cantidades sustanciales de información privada y confidencial del titular de la póliza, incluida, en algunos casos, información sensible relacionada con la salud. Por lo tanto, la protección de la confidencialidad, integridad y disponibilidad de los datos de las aseguradoras es de fundamental importancia.

Tomando en cuenta esta situación, y en respuesta a la creciente amenaza y sofisticación de los crímenes y riesgos de ciberseguridad, en 2015, la IAIS realizó una encuesta a sus miembros respecto a sus percepciones sobre el riesgo de ciberseguridad en la industria de seguros, su participación como reguladores en la lucha contra las amenazas cibernéticas y sus enfoques de supervisión de la ciberseguridad que están en uso o en desarrollo. En base a las conclusiones obtenidas de esta encuesta, realizada en agosto de 2016, la Financial Crime Task Force (FCTF) de la IAIS publicó un documento temático sobre riesgo de ciberseguridad para el sector asegurador¹⁶, enfocado en sensibilizar a las aseguradoras y supervisores sobre los desafíos que presenta el riesgo de ciberseguridad, incluidos los enfoques de supervisión actuales y aquellos contemplados para abordar estos riesgos. Una de las principales conclusiones de este documento se centró en que *“El riesgo de ciberseguridad presenta un desafío cada vez mayor para el sector de seguros, y uno que, bajo los Principios Básicos de Seguros, los supervisores están obligados a abordar.”*

En 2018, reconociendo la constante evolución de la amenaza y los potenciales beneficios de la convergencia regulatoria, y tomando en consideración las indicaciones y conclusiones contenidas en el documento emitido el año 2016, la Financial Crime Task Force (FCTF), en consulta con los miembros de la IAIS, emitió un documento basado en principios y marcos de referencia de diversas fuentes tales como: el *NIST Cybersecurity Framework*¹⁷, publicado por el Instituto Nacional de Estándares y Tecnología (NIST); el *G7 Fundamental Elements of Cyber Security for the Financial Sector (G7FE)*¹⁸; el *G7 Fundamental Elements for Effective Assessment*

¹⁶ <https://www.iaisweb.org/file/61857/issues-paper-on-cyber-risk-to-the-insurance-sector>

¹⁷ <https://www.nist.gov/cyberframework>

¹⁸ https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

of *Cybersecurity for the Financial Sector (G7FEA)*¹⁹ y en la *Guidance on Cyber Resilience for Financial Market Infrastructures (CPMI-IOSCO Guidance)*²⁰. El documento proporciona orientación para los supervisores de seguros, pudiendo ser útil también para las aseguradoras.

Por lo tanto, ante la naturaleza evolutiva de los riesgos en ciberseguridad y el alcance que puede presentar tal amenaza en el sector asegurador chileno, la CMF decidió elaborar la siguiente norma basada en las mejores prácticas reconocidas internacionalmente respecto de la prevención de los riesgos en materia de ciberseguridad. En particular, el marco de referencia estará basado en los ocho elementos fundamentales de "alto nivel" de la ciberseguridad establecido por el G7FE.

1. **Estrategia y Marco de Ciberseguridad;** referente al ICP 8 (Administración de riesgos y Controles Internos), "Establecer y mantener una estrategia y un marco de ciberseguridad adaptados a los riesgos cibernéticos específicos y debidamente informados por las normas y directrices internacionales, nacionales y de la industria".

En cuanto a la Estrategia y Marco de Ciberseguridad, se recomienda la implementación de las siguientes mejores prácticas, de manera proporcional y con un enfoque basado en riesgo:

- La estrategia sobre ciberseguridad debe estar alineada con el marco de gestión del riesgo de ciberseguridad.
 - El marco de ciberseguridad de la aseguradora debe respaldar y promover tanto su seguridad operativa como la protección de los datos de los asegurados.
 - El marco de ciberseguridad debe definir claramente sus objetivos y horizontes de ciberseguridad, así como los requerimientos necesarios para gestionar los riesgos cibernéticos y las comunicaciones oportunas con las áreas interesadas.
 - El marco de ciberseguridad debe definir claramente las funciones y responsabilidades del directorio de la aseguradora y la alta gerencia.
 - El marco de ciberseguridad debe estar alineado con el marco de gestión de riesgo operacional.
 - La documentación, relacionada al marco de ciberseguridad, debe articular claramente cómo la aseguradora planea identificar de manera efectiva los riesgos cibernéticos a los que se enfrenta, determinar sus objetivos de ciberseguridad y su tolerancia al riesgo, y mitigar y gestionar sus riesgos cibernéticos.
 - Debe considerar cómo la aseguradora revisaría y mitigaría de manera activa los riesgos cibernéticos que asume y tomará a sus accionistas, como los asegurados, otras aseguradoras, proveedores de servicios de terceros y otros terceros.
 - La estrategia y el marco de ciberseguridad de la aseguradora deben revisarse y actualizarse con la frecuencia suficiente para garantizar que sigan siendo efectivos.
2. **Gobierno;** referente al ICP 7 (Gobierno Corporativo) e ICP 8 (Administración de riesgos y Controles Internos), "Definir y facilitar el desempeño de roles y responsabilidades para el personal que implementa, administra y supervisa la efectividad de la estrategia y el marco de ciberseguridad para garantizar la responsabilidad; y/para proporcionar los recursos adecuados, la autoridad apropiada y el acceso a la autoridad de gobierno (por ejemplo, la junta directiva o los funcionarios superiores de las autoridades públicas)".

¹⁹ http://www.mef.gov.it/inevidenza/documenti/PRA_BCV_4728453_v_1_G7_Fundamental.pdf

²⁰ <https://www.bis.org/cpmi/publ/d146.pdf>

En cuanto a Gobierno, se recomienda la implementación de las siguientes mejores prácticas, de manera proporcional y con un enfoque basado en riesgo:

- El directorio de la aseguradora junto con la alta gerencia, serán los responsables últimos en establecer una estrategia la cual debe administrarse de manera efectiva. A su vez, deberá supervisar el marco de ciberseguridad de la aseguradora y la tolerancia de la aseguradora al riesgo cibernético.
 - El directorio deberá evaluar regularmente el perfil de riesgo de la aseguradora para garantizar que se mantenga consistente con la tolerancia al riesgo y con los objetivos comerciales generales de la aseguradora. La alta gerencia debe considerar los cambios en sus productos, servicios, políticas y prácticas, y el panorama de amenazas en su perfil de riesgo cibernético.
 - La alta gerencia debe estar estrechamente involucrada en la implementación de su marco de ciberseguridad y las políticas y procedimientos que respaldan el marco.
 - El directorio de la aseguradora y la alta gerencia deberán fomentar el conocimiento y el compromiso con la ciberseguridad. El directorio y la alta gerencia deben incluir miembros con las habilidades adecuadas para supervisar y administrar los roles con respecto a los riesgos planteados por las amenazas cibernéticas. Además, el directorio y la alta gerencia deben promover una cultura que reconozca que el personal de todos los niveles es responsable de garantizar la ciberseguridad de la aseguradora y dar el ejemplo.
 - Las aseguradoras deben tener implementadas políticas, procedimientos y procesos de seguridad de la información que incluyan definiciones de roles y responsabilidades en toda la organización. Estas políticas, procedimientos y procesos deben incluir la supervisión de proveedores de servicios de terceros, así como los procesos de administración de riesgos cibernéticos y la determinación de prioridades, restricciones, suposiciones y niveles de tolerancia al riesgo.
 - Cada aseguradora debe designar un ejecutivo senior para que sea responsable del marco de ciberseguridad dentro de la organización. Esta función debe tener autoridad, independencia, recursos y acceso suficientes a la Junta. El ejecutivo senior que desempeña este rol debe poseer la experiencia y el conocimiento necesarios para planificar y ejecutar de manera competente las iniciativas de ciberseguridad a nivel de gestión.
 - Las aseguradoras deberán implementar programas de evaluación para ayudar al directorio y la alta gerencia a evaluar y medir la idoneidad del marco de ciberseguridad, incluyendo, cuando sea apropiado y en línea con el principio de proporcionalidad, a través de un programa independiente de cumplimiento y auditoría, llevado a cabo por personas calificadas, para evaluar el marco de ciberseguridad y la implementación de medidas.
3. **Evaluación de Riesgo y Control;** referente al ICP 8 (Administración de riesgos y Controles Internos) e ICP 19 (Conducta de mercado), “Identificar funciones, actividades, productos y servicios, incluyendo las interconexiones, dependencias y terceros, priorizando su

importancia relativa, y evaluando sus respectivos riesgos cibernéticos” e “identificar e implementar controles, incluidos sistemas, políticas, procedimientos, y entrenamiento, para proteger y administrar a aquellos riesgos dentro de la tolerancia establecida por la autoridad de gobierno”.

En cuanto a Evaluación de riesgo y control, se recomienda la implementación de las siguientes mejores prácticas, de manera proporcional y con un enfoque basado en riesgo:

Identificación y clasificación de funciones.

- La aseguradora debe tener en cuenta adecuadamente los riesgos cibernéticos en su sistema general de gestión de riesgos, identificando las funciones y procesos de soporte del negocio y realizando una evaluación de riesgos para asegurarse de que comprende completamente la importancia de cada función y los procesos de soporte, y sus interdependencias, en el desempeño de sus funciones. Las aseguradoras deben clasificar las funciones y los procesos de negocios identificados en términos de criticidad, lo que debería guiar la priorización de los esfuerzos de protección, detección, respuesta y recuperación de la aseguradora.
- La aseguradora debe identificar y mantener un inventario actual o un mapeo de sus recursos/activos informáticos y configuraciones de sistema, incluidas las interconexiones con otros sistemas internos y externos, para poder saber en todo momento los recursos/activos que respaldan las funciones y procesos del negocio. La aseguradora debe realizar una evaluación de riesgo de esos recursos/activos y clasificarlos en términos de criticidad.
- En cuanto al criterio de calificación de activos críticos, estos deberán ser clasificados desde una perspectiva de confidencialidad, integridad y disponibilidad. La aseguradora deberá tener especial consideración en la clasificación de aquellos activos cuya seguridad se relacione con la “garantía de protección de la privacidad y el resguardo de los datos personales y sensibles”, identificándolos en su inventario y detallando las medidas asociadas al cumplimiento de la legislación vigente en esta materia.
- Como parte de este proceso de mapeo, la aseguradora también deberá identificar las dependencias en sus recursos informáticos y configuraciones del sistema, por ejemplo, de proveedores de servicios de terceros.
- El inventario debe abarcar hardware, plataformas de software y aplicaciones, dispositivos, sistemas, datos, personal, sistemas de información externos, procesos críticos y documentación sobre los flujos de datos esperados.
- Las aseguradoras deben identificar y mantener un registro actual de los derechos de acceso individuales y del sistema para saber quién tiene acceso a los activos de información y sus sistemas de respaldo, y utilizar esta información tanto para garantizar que los derechos de acceso no sean más amplios de lo necesario, como para facilitar la identificación e investigación de actividades anómalas.
- Las aseguradoras deben coordinar los esfuerzos de identificación con otros procesos relevantes, como la gestión de adquisiciones y cambios, a fin de facilitar una revisión periódica de su lista de procesos críticos del negocio, funciones, credenciales

individuales y del sistema, así como su inventario de recursos informáticos para garantizar que estos permanecen actualizados, precisos y completos.

- De manera similar, las aseguradoras deben realizar un análisis de impacto (BIA por sus siglas en Inglés) al negocio para los riesgos cibernéticos.

Inclusión del riesgo cibernético en el perfil de riesgo

- Los perfiles de riesgo de las aseguradoras deben identificar las áreas operativas clave expuestas al riesgo cibernético, derivadas de fuentes internas y externas.
- Utilizando los mismos preceptos que en el desarrollo de un perfil de riesgo para toda la empresa, la aseguradora apuntaría a describir el riesgo cibernético general al que está expuesta la empresa. El perfil de riesgo puede beneficiarse de la inclusión de procesos de evaluación que abarcan evaluaciones de probabilidad e impacto de daño.
- Las perspectivas de ambos procesos, enunciados en los puntos anteriores (identificar y describir), pueden organizarse, por ejemplo, dentro de las siguientes categorías: (1) tecnologías y tipos de conexión; (2) canales de entrega; (3) características organizacionales; y (4) amenazas externas.
 - Tecnologías y tipos de conexión; Ciertas tecnologías y tipos de conexión pueden presentar un mayor riesgo cibernético en función de la complejidad y la madurez, las conexiones y la naturaleza de los productos o servicios tecnológicos específicos de la aseguradora.
 - Canales de entrega; Las aseguradoras deben tener en cuenta que algunos canales de entrega de productos y servicios pueden suponer un riesgo cibernético mayor en función de la naturaleza del producto o servicio específico que se ofrece. El riesgo cibernético aumenta a medida que aumenta la variedad y el número de canales de entrega.
 - Características organizacionales; Las características a considerar incluyen fusiones, escisiones, adquisiciones y ventas pasadas y planificadas, el número de empleados directos y contratistas de ciberseguridad, cambios en la dotación de personal de seguridad, el número de usuarios con acceso privilegiado, cambios en el entorno de tecnología de la información (TI), ubicaciones de presencia comercial, ubicaciones de operaciones y centros de datos (incluidos los sistemas heredados), y dependencia de proveedores de servicios de terceros, incluidos proveedores de servicios en la nube.
 - Amenazas externas; en particular el volumen y el tipo de ataques (intentados o exitosos) reflejan y afectan la exposición al riesgo cibernético de una aseguradora. Una aseguradora debe considerar el volumen y la sofisticación de los ataques dirigidos a ella y a otras organizaciones similares.

Implementación de tecnología y procesos proactivos.

- Las aseguradoras deben proteger los datos, incluidos los sistemas de respaldo y los almacenes de datos fuera de línea, cuando están en reposo, en tránsito y en almacenamiento²¹ de acuerdo con la criticidad y clasificación de la información que se tiene.

Gestión de Dependencias Externas.

- Los sistemas y procesos de muchas aseguradoras están directa o indirectamente interconectados con numerosos terceros, incluidos los proveedores de servicios en la nube y los proveedores de funciones subcontratadas. La ciberseguridad de esas entidades puede afectar significativamente el riesgo cibernético que enfrenta una aseguradora. Las aseguradoras deben gestionar activamente los riesgos cibernéticos presentados por terceros, incluso a través de revisiones realizadas con regularidad y según lo ameriten los cambios en las circunstancias.
- Las aseguradoras deben verificar que los proveedores de servicios externos hayan implementado medidas administrativas, técnicas y físicas adecuadas para proteger y asegurar los datos de la aseguradora y sus clientes en el mismo grado que se espera de la aseguradora.
- Las aseguradoras deben ser conscientes de que la importancia de los riesgos que los terceros pueden suponer para ellas no es necesariamente proporcional a la importancia de su relación comercial.

Mejorar la conciencia situacional

- Una aseguradora debe tener un conocimiento adecuado de la situación de los riesgos cibernéticos que enfrenta. Una aseguradora debe tratar de identificar proactivamente las amenazas cibernéticas que podrían afectar materialmente su capacidad para realizar o prestar servicios según lo esperado, o que podría tener un impacto significativo en su capacidad para cumplir con sus propias obligaciones, incluida la protección de datos confidenciales. La aseguradora debe revisar y actualizar regularmente este análisis.
- Las amenazas cibernéticas a considerar deben incluir a aquellas que podrían desencadenar eventos cibernéticos extremos pero plausibles, incluso si se considera que es poco probable que ocurran o que nunca hayan ocurrido en el pasado.

²¹ Los datos en tránsito, o datos en movimiento, son datos que se mueven activamente de una ubicación a otra, como a través de Internet o a través de una red privada. La protección de datos en tránsito es la protección de estos datos mientras viaja de una red a otra, o se transfiere de un dispositivo de almacenamiento local a un dispositivo de almacenamiento en la nube, donde sea que se muevan los datos, las medidas efectivas de protección de datos para los datos en tránsito son fundamentales, ya que los datos son a menudo considerados menos seguros mientras están en movimiento.

Los datos en reposo, son datos que no se mueven activamente de un dispositivo a otro o de una red a otra, como los datos almacenados en un disco duro, computadora portátil, unidad flash o archivados y/o almacenados de alguna otra manera. La protección de datos en reposo tiene como objetivo proteger los datos inactivos almacenados en cualquier dispositivo o red. Mientras que los datos en reposo a veces se consideran menos vulnerables que los datos en tránsito, los atacantes a menudo consideran que los datos en reposo son un objetivo más valioso que los datos en movimiento. El perfil de riesgo para los datos en tránsito o los datos en reposo depende de las medidas de seguridad establecidas para proteger los datos en cualquier estado.

Además de la reputación, una aseguradora debe considerar amenazas a la confidencialidad, integridad y disponibilidad de los procesos de sus negocios y los datos de los asegurados. Las amenazas que surgen de fuentes internas y externas, como empleados o proveedores de servicios de terceros, respectivamente, deben considerarse.

4. **Monitoreo;** referente al ICP 8 (Administración de riesgos y Controles Internos), “Establecer procesos de monitoreo sistemático para detectar rápidamente incidentes cibernéticos y evaluar periódicamente la efectividad de los controles identificados, incluyendo los mediante el monitoreo de red, pruebas, auditorías y ejercicios”. En cuanto a Monitoreo, se recomienda la implementación de las siguientes mejores prácticas, de manera proporcional y con un enfoque basado en riesgo:

Monitoreo continuo

- Las aseguradoras deben proteger la integridad de la red (hardware, firmware y componentes de software), incluido el control del flujo de información, la protección de límites y la segregación de la red, si es necesario.
- Una aseguradora debe considerar establecer capacidades de monitoreo continuo en tiempo real o casi en tiempo real, con el fin de detectar actividades y eventos anómalos.
- Las aseguradoras deben poder reconocer los signos de un posible incidente cibernético o detectar que una violación real ha tenido lugar, lo cual es esencial para una fuerte ciberseguridad.
- Dada la naturaleza sigilosa y sofisticada de los incidentes de ciberseguridad y los múltiples puntos de entrada a través de los cuales podría tener lugar un compromiso, una aseguradora debe mantener capacidades efectivas para monitorear ampliamente las actividades anómalas.
- Las aseguradoras deben monitorear las actividades y eventos internos y externos relevantes, buscando detectar vulnerabilidades a través de una combinación de monitoreo de firmas digitales (ejemplo el uso hash) para detectar vulnerabilidades conocidas y mecanismos de detección basados en el comportamiento.
- Las capacidades de detección de los aseguradores también deben abordar el uso indebido del acceso por parte de proveedores de servicios de terceros, asegurados, posibles amenazas internas y otras actividades avanzadas de amenazas.
- Como parte del proceso de monitoreo, las aseguradoras deben administrar las identidades y credenciales para el acceso físico, lógico y remoto a los activos de información, basados en principios tales como el mínimo privilegio y la separación de funciones.

- Una aseguradora debe implementar, dentro de los límites legales pertinentes, medidas para capturar y analizar el comportamiento anómalo de las personas con acceso a la red corporativa.
- Las aseguradoras deben tener la capacidad de detectar una intrusión en etapa temprana, ya que esta capacidad es crítica para una rápida contención y recuperación. Además, una capacidad efectiva de detección de intrusiones podría ayudar a las aseguradoras a identificar deficiencias en sus medidas de protección para una remediación temprana.
- La aseguradora debe emplear sus capacidades de monitoreo y detección para facilitar su proceso de respuesta a incidentes y apoyar la recopilación de información para el proceso de investigación forense.

Testeo

- Las aseguradoras deben testear rigurosamente todos los elementos de su marco de ciber seguridad para determinar su efectividad general, antes implementadas y regularmente después de su implementación.
- Las aseguradoras deben testear su marco de ciber seguridad y comunicar los resultados dentro de su organización.
- Los resultados del programa de testeo deben ser utilizados por la aseguradora para respaldar la mejora continua de su ciberseguridad.
- Los aseguradores deben considerar el uso de una combinación de las metodologías y prácticas de testeo de vanguardia disponibles. Actualmente, dichas metodologías y prácticas de testeo de vanguardia incluyen los siguientes elementos (que en parte se superponen y se pueden combinar):
 - Evaluación de vulnerabilidades (EV); Las aseguradoras deberán realizar de manera regular con el fin de identificar y evaluar las vulnerabilidades de seguridad en sus sistemas y procesos.
 - Pruebas basadas en escenarios; Los planes de respuesta, reanudación y recuperación de una aseguradora deben estar sujetos a revisiones y pruebas periódicas. Las pruebas deben abordar un amplio abanico de escenarios, incluida la simulación de incidentes de ciberseguridad extremos pero plausibles, y deben diseñarse para desafiar los supuestos de las prácticas de respuesta, reanudación y recuperación, incluidos los acuerdos de gobierno y los planes de comunicación.
 - Pruebas de penetración; Las aseguradoras deben realizar pruebas de penetración para identificar las vulnerabilidades que pueden afectar sus sistemas, redes, personas o procesos. Para proporcionar una evaluación en

profundidad de la seguridad de los sistemas de las aseguradoras, estas pruebas deben simular ataques reales en los sistemas.

- Pruebas de Red Team; Las aseguradoras deben considerar desafiar a sus propias organizaciones y dependencias externas mediante el uso de los llamados Red Team para introducir una perspectiva adversa en un entorno controlado. Los Red Team sirven para probar posibles vulnerabilidades y la efectividad de los controles de mitigación de una aseguradora. Un Red Team puede estar formado por los propios empleados de la aseguradora y/o expertos externos, que en ambos casos son independientes de la función que se está probando.
 - Una aseguradora debe, en la medida de lo posible, promover, diseñar, organizar y administrar ejercicios diseñados para testear sus planes y procesos de respuesta, reanudación y recuperación.
 - Los escenarios de pruebas asumen que los demás participantes se encuentran operando de manera normal, lo que es poco realista. Es por esto mismo que las pruebas deben incluir escenarios que cubran las infracciones que afectan las dependencias externas.
5. **Respuesta;** referente al ICP 8 (Administración de riesgos y Controles Internos), "Oportunamente (a) evaluar la naturaleza, el alcance y el impacto de un incidente cibernético; (b) contener el incidente y mitigar su impacto; (c) notificar a las partes interesadas internas y externas, como Agentes de cumplimiento legal, los reguladores y otras autoridades públicas, así como los accionistas, proveedores de servicios de terceros y clientes, según corresponda); y (d) coordinar las actividades de respuesta conjunta según sea necesario".

En cuanto a Respuesta, se recomienda la implementación de las siguientes mejores prácticas, de manera proporcional y con un enfoque basado en riesgo:

- Previo a un incidente de ciberseguridad, las aseguradoras deben crear conciencia entre todos los interesados mediante la capacitación de los empleados y otras personas con acceso a sus sistemas. La capacitación personalizada puede ser apropiada para empleados con acceso a datos críticos o confidenciales o privilegios mejorados del sistema. Las aseguradoras también deben desarrollar planes de respuesta (Respuesta a incidentes y continuidad del negocio) y planes de comunicación sobre incidentes cibernéticos. Estos planes deben estar sujetos a revisión y mejora según corresponda.
- Tras la detección de un incidente de ciberseguridad (o un intento), una aseguradora debe realizar una investigación exhaustiva para determinar su naturaleza y extensión, así como el daño infligido. Mientras la investigación está en curso, la aseguradora también debe tomar medidas inmediatas para contener la situación para evitar más daños y comenzar los esfuerzos de recuperación para restablecer las operaciones según la planificación de respuesta (a incidentes).

- Las aseguradoras también deben ser conscientes de no volver a activar los sistemas demasiado rápido y arriesgarse a otro ataque o expansión del incidente de ciberseguridad.
- Previo a la reanudación de operaciones, y tan pronto como estas sean posibles después de un incidente, se debe analizar funciones críticas, transacciones e interdependencias para priorizar las acciones de reanudación y recuperación mientras continúan los esfuerzos de remediación. Las aseguradoras también deben planificar situaciones en las que personas, procesos o sistemas críticos pueden no estar disponibles por períodos significativos, por ejemplo, al revertir, cuando sea factible y practicable, procesar manualmente si los sistemas automáticos no están disponibles.
- Las aseguradoras deben planear tener acceso a expertos externos, reconociendo que un evento a gran escala o en toda la industria puede reducir la disponibilidad de dichos recursos clave en un corto plazo.
- Las aseguradoras deben desarrollar y probar los planes de respuesta, reanudación y recuperación. Estos planes deben respaldar los objetivos para proteger la confidencialidad, integridad y disponibilidad de sus activos, incluidos los datos de los asegurados.
- Las aseguradoras deben diseñar sistemas y procesos para limitar el impacto de cualquier incidente cibernético y proteger la privacidad de los datos de los asegurados.
- Las aseguradoras deben considerar la posibilidad de contar con un equipo específico para todas las comunicaciones de los interesados, para garantizar una preparación adecuada y la coherencia del mensaje.
- Como parte de su marco de gobierno general y de conformidad con las leyes pertinentes, las aseguradoras deben tener una política y un procedimiento para permitir la divulgación responsable de las vulnerabilidades potenciales siguiendo un enfoque basado en el riesgo. En particular, las aseguradoras deben priorizar las divulgaciones que podrían facilitar la respuesta temprana y la mitigación de riesgos por parte de las partes interesadas en beneficio del ecosistema cibernético y la estabilidad financiera más amplia.
- En el caso de una exposición de los datos de los asegurados, una aseguradora debe tener una política y un procedimiento para cumplir con las obligaciones de divulgación establecidas en las leyes y regulaciones de todas las jurisdicciones relevantes.
- Las aseguradoras deben tener la capacidad de asistir o realizar investigaciones forenses de incidentes cibernéticos y diseñar controles de protección y detección para facilitar el proceso de investigación.

6. **Recuperación;** referente al ICP 8 (Administración de riesgos y Controles Internos), “Reanudar las operaciones de manera responsable, al tiempo que permite la remediación continua, incluso mediante (a) la eliminación de los restos dañinos del incidente; (b) restaurar los sistemas y los datos a su estado normal y confirmar el estado normal; (c) identificar y mitigar todas las vulnerabilidades que fueron explotadas; (d) remediar las vulnerabilidades para prevenir incidentes similares; y (e) comunicarse apropiadamente interna y externamente ”.

En cuanto a Recuperación, se recomienda la implementación de las siguientes mejores prácticas, de manera proporcional y con un enfoque basado en riesgo:

- Las aseguradoras deben contar con planes y procedimientos para recuperarse de un incidente de ciberseguridad. Los acuerdos de recuperación de incidentes cibernéticos deben diseñarse para permitir a los aseguradores reanudar las operaciones de manera segura con un mínimo de interrupciones a los asegurados y las operaciones comerciales.
 - Las aseguradoras deben diseñar y probar sus sistemas y procesos para permitir la recuperación oportuna de datos precisos luego de una violación. Teniendo en cuenta la criticidad y la clasificación de la información contenida, los datos deben protegerse mediante estrictos controles de detección y protección. Además, el marco de ciberseguridad de la aseguradora debe incluir medidas de recuperación de datos, como mantener una copia de seguridad de todos los datos de los asegurados en caso de que dichos datos se corrompan.
 - Los planes de recuperación de las aseguradoras (Recuperación de incidentes y Recuperación de desastres) deben estar sujetos a revisión y mejoras, según corresponda.
 - Dada la interconexión de sistemas y procesos entre la aseguradora y terceros, en el caso de un incidente cibernético a gran escala, es posible que la aseguradora plantee un riesgo de contagio al estar expuesto a este tipo de riesgo dado el nivel de interconexión. Una aseguradora debe trabajar con estos terceros para reanudar las operaciones de manera segura.
 - Las aseguradoras deben tener planes formales para comunicarse con los asegurados, partes interesadas internas y externas que puedan sufrir daños debido a un incidente importante de ciberseguridad.
7. **Intercambio de información;** referente al ICP 8 (Administración de riesgos y Controles Internos) e ICP 16 (Gestión de riesgos empresariales con fines de solvencia), “Participar en el intercambio oportuno de información de ciberseguridad confiable y accionable con partes interesadas internas y externas (incluidas entidades y autoridades públicas dentro y fuera del sector financiero) sobre amenazas, vulnerabilidades, incidentes y respuestas para

mejorar las defensas, limitar los daños, aumentar la conciencia de la situación, y ampliar el aprendizaje ".

En cuanto a Intercambio de Información, se recomienda la implementación de las siguientes mejores prácticas, de manera proporcional y con un enfoque basado en riesgo:

- Las aseguradoras deben establecer un proceso para recopilar y analizar información relevante sobre amenazas cibernéticas. Las aseguradoras deben considerar la posibilidad de participar activamente en grupos y colectivos de intercambio de información, incluidos los grupos de la industria, el gobierno y los grupos transfronterizos para recopilar, distribuir y evaluar información sobre prácticas cibernéticas, amenazas cibernéticas e indicadores de alerta temprana relacionados con las amenazas cibernéticas. Las aseguradoras pueden participar en iniciativas de todo el sistema, como los Equipos de Respuesta a Incidentes (IRT por sus siglas en inglés), si se establecen en las jurisdicciones pertinentes.

A su vez puede ser apropiado que los aseguradores se comprometan con el Centro de Análisis e Intercambio de Información de Servicios Financieros (FS-ISAC), un recurso mundial reconocido para el sector financiero para el análisis e intercambio de inteligencia de amenazas físicas y cibernéticas.

- El análisis de una aseguradora sobre la información de amenazas cibernéticas debe realizarse junto con otras fuentes de información, internas y externas, del negocio y del sistema para proporcionar un contexto específico para el negocio, convirtiendo la información en inteligencia de amenazas cibernéticas que proporcione información oportuna e informe la toma de decisiones mejorada, permitiendo a la aseguradora anticipar las capacidades, intenciones y modus operandi de un atacante cibernético.
- Si es posible, las operaciones de inteligencia de amenazas cibernéticas de una aseguradora deberían incluir la capacidad de recopilar e interpretar información sobre las amenazas cibernéticas relevantes planteadas por los proveedores de servicios externos de la aseguradora, así como los proveedores de servicios públicos y otros recursos de infraestructura críticos. Además, las operaciones de inteligencia de amenazas cibernéticas deben interpretar esta información de manera que el asegurador pueda identificar, evaluar y gestionar las amenazas y vulnerabilidades de seguridad con el fin de implementar salvaguardas adecuadas en sus sistemas. En este contexto, la información relevante sobre amenazas cibernéticas podría incluir información sobre desarrollos geopolíticos que puedan desencadenar ataques cibernéticos a la aseguradora o cualquiera de sus dependencias externas.
- Cuando está correctamente contextualizada, la información sobre amenazas cibernéticas permite a una aseguradora validar e informar la priorización de los recursos, las estrategias de mitigación de riesgos y los programas de capacitación. Por lo tanto, una aseguradora debe poner la información sobre amenazas cibernéticas a disposición del personal apropiado dentro de la aseguradora con la responsabilidad de mitigar los riesgos cibernéticos en los niveles estratégico, táctico y operativo. La inteligencia sobre amenazas cibernéticas se debe utilizar para garantizar que la implementación de cualquier medida de ciberseguridad esté informada sobre amenazas.

- Para facilitar la respuesta de todo el sector a los incidentes de ciberseguridad a gran escala, las aseguradoras deben planificar el intercambio de información a través de canales confiables, recolectando e intercambiando información oportuna que pueda facilitar la detección, respuesta, reanudación y recuperación de sus propios sistemas y los de otros participantes del sector durante y después de un incidente de ciberseguridad. Las aseguradoras deben, como parte de sus programas de respuesta, determinar de antemano qué tipos de información se compartirán con quién y cómo se actuará sobre la información proporcionada a la aseguradora. Los requisitos y las capacidades de los informes deben estar alineados con las leyes y regulaciones pertinentes, así como con los acuerdos de intercambio de información dentro de las comunidades de seguros y el sector financiero.
 - Una aseguradora debe considerar intercambiar información sobre su marco de ciberseguridad bilateralmente con sus proveedores de servicios externos para promover el entendimiento mutuo de los enfoques de los demás para asegurar los sistemas que están vinculados o interconectados. Dicho intercambio de información podría facilitar los esfuerzos de una aseguradora y de sus partes interesadas para combinar sus respectivas medidas de seguridad para lograr una mayor ciberseguridad.
8. **Aprendizaje Continuo;** referente al ICP 16 (Gestión de riesgos empresariales con fines de solvencia), "Revisar la estrategia y el marco de ciberseguridad periódicamente y cuando los eventos lo justifiquen, incluidos su gobierno, evaluación de riesgos y controles, monitoreo, respuesta, recuperación e intercambio de información, para abordar los cambios en los riesgos cibernéticos, asignar recursos, identificar y remediar las brechas, e incorporar las lecciones aprendidas".

En cuanto a Intercambio de Aprendizaje Continuo, la recomendación para los supervisores es que es apropiado que las prácticas de supervisión estimulen o reflejen, en síntesis, lo siguiente de manera proporcional y basada en el riesgo:

- Las aseguradoras deben adoptar un marco de ciberseguridad basado en garantizar la ciberseguridad continua en un entorno de amenaza cambiante.
- Las aseguradoras deben implementar prácticas de administración de riesgos cibernéticos que vayan más allá de los controles reactivos e incluyan protección proactiva contra futuros eventos cibernéticos.
- Las capacidades predictivas y la anticipación de futuros eventos cibernéticos se basan en el análisis de las actividades que se desvían de la línea de base. Las aseguradoras deben trabajar para lograr o adquirir capacidades predictivas, capturar datos de múltiples fuentes, internas y externas, y definir una línea de base para las actividades tanto del comportamiento y como del sistema, incluso a través de la subcontratación de dicha experiencia.
- Para ser eficaz en mantener el ritmo de la rápida evolución de las amenazas cibernéticas, una aseguradora debe implementar un marco de ciberseguridad adaptable que evolucione con la naturaleza dinámica de los riesgos cibernéticos y

le permita identificar, evaluar y gestionar amenazas y vulnerabilidades de seguridad con el propósito de implementar salvaguardias apropiadas en sus sistemas. Una aseguradora debe tratar de inculcar una cultura de concientización sobre el riesgo cibernético mediante la cual su postura de resiliencia, en todos los niveles, sea reevaluada con regularidad y frecuencia.

- Una aseguradora debe identificar y extraer de forma sistemática las lecciones clave de los eventos cibernéticos que se han producido dentro y fuera de la organización para mejorar sus capacidades de resiliencia. Los puntos de aprendizaje útiles a menudo se pueden deducir de las intrusiones cibernéticas exitosas y los casi fallos en términos de los métodos utilizados y las vulnerabilidades explotadas por los atacantes cibernéticos.
- Una aseguradora debe monitorear activamente los desarrollos tecnológicos y mantenerse al tanto de los nuevos procesos de administración de riesgos cibernéticos que pueden contrarrestar de manera más efectiva las formas de ciberataques existentes y recientemente desarrolladas. Una aseguradora debe considerar adquirir dicha tecnología y conocimientos para mantener su ciberseguridad, incluso a través de la externalización de dicha experiencia.
- A medida que los métodos para la cuantificación del riesgo cibernético continúan desarrollándose, las aseguradoras pueden considerar el uso de métricas para evaluar la madurez de la ciberseguridad frente a un conjunto de criterios predefinidos, como los objetivos de confiabilidad operacional. La evaluación comparativa permite a una aseguradora analizar y correlacionar hallazgos de auditorías, revisiones de gestión, incidentes, casi fallas, pruebas y ejercicios, así como inteligencia externa e interna

Con el fin de evaluar el nivel actual de preparación, y desarrollar y mantener prácticas efectivas de ciberseguridad, la CMF solicita a las compañías que completen el cuestionario de autoevaluación contenido en el Anexo N° 2 de esta norma, la cual está enfocada en las mejores prácticas de gestión del riesgo de ciberseguridad.

V. AUTOEVALUACIÓN DE LOS PRINCIPIOS DE RIESGO OPERACIONAL Y CIBERSEGURIDAD.

Las compañías de seguros deberán realizar, cada 2 años, una autoevaluación del grado de cumplimiento de sus prácticas de gestión de riesgo operacional y en forma anual en lo relativo a ciberseguridad, respecto de los principios establecidos en esta norma. Adicionalmente, deberán comunicar a la CMF, en el caso del riesgo operacional, sus resultados y el plan de acción que hayan definido, para cerrar las brechas que en relación a estos principios hayan detectado.

Los informes con los resultados de la autoevaluación y el plan de acción deberán, tanto en el caso de gestión de riesgos operacionales como de ciberseguridad, ser aprobados por el directorio de la compañía de seguros y, en el caso de la autoevaluación de riesgo operacional, enviarse a este Servicio a más tardar el 30 de septiembre de cada año, referida a la situación de la compañía al 30 de junio del mismo año. En lo relativo a la autoevaluación de ciberseguridad, ésta deberá quedar a disposición de la CMF en la compañía, pudiendo ser requerida dentro de los procesos de supervisión de la Comisión.

Los informes señalados deberán contener al menos la siguiente información:

- a) Una explicación del trabajo de autoevaluación realizado, indicando personas involucradas, apoyo de asesores externos, en caso de haberlos, horas aproximadas de trabajo, metodología, etc.
- b) El plan de acción definido, indicando las acciones concretas que la compañía de seguros adoptará respecto de cada brecha identificada. En caso que la compañía considere que una determinada brecha es justificada en su entidad, por su modelo de negocio u otra razón, y por lo tanto no requiere una acción de cierre o mitigación de la brecha, deberá explicarlo detalladamente en este informe.

Las compañías de seguros deberán mantener a disposición de la CMF, toda la información de respaldo de los informes de autoevaluación del cumplimiento de los principios y buenas prácticas de gestión de riesgo operacional y de ciberseguridad, señalados en la presente norma.

Para realizar los mencionados informes de autoevaluación de los principios de riesgo operacional y ciberseguridad establecidos en esta norma, las compañías de seguros tendrán que utilizar los formatos descritos en Anexos adjuntos.

Las compañías deberán informar en forma reservada a la CMF el resultado de de la autoevaluación de riesgo operacional que será en formato Excel, a través del Módulo SEIL, disponible en el sitio Web de esta Comisión, www.cmfchile.cl, de acuerdo a las instrucciones establecidas para tal efecto.

VI. COMUNICACIÓN DE INCIDENTES OPERACIONALES

Las compañías de seguros deberán comunicar a esta Comisión los incidentes operacionales que afecten o pongan en riesgo la continuidad del negocio, los fondos o recursos de la entidad o de sus asegurados, la calidad de los servicios o la imagen de la institución. Las compañías, en caso de incidentes, serán responsables de mantener informada a esta Comisión de la situación en desarrollo y de las medidas o acciones de detección, respuesta y recuperación del incidente. A modo de ejemplo, deberán ser reportadas las fallas en el servicio de proveedores críticos, problemas tecnológicos que afecten la seguridad de la información; la indisponibilidad o interrupción de algún servicio o producto que afecte a los asegurados, en cualquier canal; pérdidas o fugas de información de la compañía de seguros o de asegurados; los incidentes que afecten el patrimonio de la compañía producto de fraudes internos o externos, o los eventos que gatillen planes de contingencia, entre otros.

Asimismo, deben ser informados los incidentes que afecten a un grupo de asegurados que puedan impactar la imagen y reputación de la compañía en forma inmediata, o con posterioridad a ocurrido un determinado evento, como por ejemplo sería el caso de los pensionados de Rentas Vitalicias.

Una vez comunicado el evento, la institución es responsable por establecer un canal permanente de comunicación con la Comisión.

1.1 Envío de la información a la Comisión

El envío de la comunicación de incidentes operacionales requerida en esta norma, deberá comenzar a informarse a la CMF, por parte las compañías de seguros, a contar del 30 de septiembre de 2021.

La información deberá ser enviada a través de la plataforma dispuesta especialmente para estos efectos por esta Comisión, en cualquier horario, tanto en días hábiles como no hábiles, en el plazo máximo de 30 minutos luego de su ocurrencia.

Para estos efectos, la entidad deberá definir un funcionario encargado, quien realizará los reportes y enviará la información según lo indicado en este numeral, y su designación y/o reemplazo deberá ser comunicado mediante carta a la CMF. Esta persona o quien la reemplace deberán tener un nivel ejecutivo y ser designados por la compañía tanto para este efecto, como para responder eventuales consultas por parte de este Servicio.

La información deberá ser reportada de acuerdo al siguiente esquema:

a) Al momento de inicio del incidente. El reporte deberá incluir, al menos, los siguientes aspectos:

- Número único identificador del incidente (asignado por la CMF)
- Nombre de la entidad informante
- Descripción del incidente
- Fecha y hora de inicio del incidente
- Causas posibles o identificadas
- Productos o servicios afectados
- Tipo y nombre de proveedor o tercero involucrado (si corresponde)

- Tipo y número estimado de clientes afectados
- Dependencias y/o activos afectados (si corresponde)
- Medidas adoptadas y en curso
- Otros antecedentes

El no contar con toda la información de los campos mencionados previamente no debe ser impedimento para el envío de la comunicación dentro del plazo definido en este numeral. En los casos que este Servicio lo estime necesario, se podrá requerir a las compañías un plan de recuperación.

b) Al momento de cierre del incidente. Una vez cerrado el incidente, se deberá informar esta situación a través de la plataforma ya mencionada previamente. Dicho reporte deberá incluir, al menos, los siguientes aspectos:

- Número único identificador del incidente
- Nombre de la entidad informante
- Descripción del incidente
- Causas identificadas
- Fecha y hora de inicio del incidente
- Fecha de cierre del incidente
- Productos o servicios afectados
- Tipo y nombre de proveedor involucrado (si corresponde)
- Tipo y número de clientes afectados
- Dependencias y/o activos afectados (si corresponde)
- Medidas adoptadas
- Otros antecedentes

1.2 Información a clientes o usuarios

Al tratarse de incidentes que afecten la calidad o continuidad de los servicios a los clientes o se trate de un hecho de público conocimiento, la compañía será responsable de informar oportunamente a los usuarios sobre la ocurrencia de dicho evento, debiendo actualizar la información disponible hasta el momento en que el incidente sea superado.

1.3 Información a la industria

Sin perjuicio de la información que debe ser reportada a la Comisión, los incidentes asociados a ciberseguridad deben ser compartidos por las compañías de seguros con el resto de la industria, a modo de proteger a los usuarios y al sistema en su conjunto. El principal objetivo de este mecanismo para compartir información es prevenir a los participantes de la industria aseguradora sobre las amenazas de ciberseguridad, con el fin de que las demás entidades puedan tomar los resguardos pertinentes, facilitando la detección, respuesta y recuperación, y así disminuir la probabilidad de que impactos negativos se propaguen en el sistema.

Para ello, las compañías de seguros deberán mantener un sistema de alertas de incidentes, en el cual deberán reportar como mínimo, una breve descripción del tipo de amenaza, indicando los canales o servicios afectados y, cuando la información se encuentre disponible, la caracterización o identificación del software malicioso y de cualquier mecanismo de protección que se haya identificado. La información debe ser comunicada en el más breve plazo posible.

El sistema implementado además deberá considerar el acceso por parte de esta Comisión a la información compartida.

1.4 Envío de Información a la CMF

En lo relacionado al envío de la comunicación de incidentes operacionales requerida en esta norma, las compañías de seguros deberán enviar a la CMF, a través del Módulo SEIL, en formato disponible en el sitio Web de esta Comisión, www.cmfchile.cl, de acuerdo a las instrucciones establecidas para tal efecto.

VII. VIGENCIA Y APLICACIÓN

La presente norma entra en vigencia a contar del 31 de mayo de 2021.

Disposición Transitoria.

La autoevaluación del cumplimiento de los principios de riesgo operacional y de ciberseguridad establecidos en esta norma, deberá efectuarse e informarse, en el caso de riesgo operacional, por primera vez a más tardar al 30 de septiembre de 2021. Dichas autoevaluaciones se deberán realizar en régimen con una periodicidad cada dos años, para el caso de riesgo operacional y anual en lo relativo a ciberseguridad, debiendo ser informadas, en el caso de riesgo operacional, al 30 de septiembre de cada año.

COMISIÓN PARA EL MERCADO FINANCIERO

ANEXO 1

EJERCICIO AUTOEVALUACIÓN DE RIESGO OPERACIONAL

Se solicita a cada compañía calificar su grado actual de cumplimiento de cada principio y criterios que lo integran, y proporcionar una justificación y/o los fundamentos de cada calificación dentro de la sección de comentarios.

La CMF solicita que las compañías califiquen su grado actual de madurez, respecto a los principios y criterios, en una escala de 1 a 4 y brinden suficiente justificación en todas las circunstancias relacionadas a dicha calificación. Para la evaluación de cada principio y sub principio, los criterios deberán ponderarse de igual forma en la nota asignada. A continuación, se establece una definición de cada una de las evaluaciones de cumplimiento por parte de la compañía.

- 1. Totalmente implementado:** La compañía ha implementado plenamente los principios en toda su compañía. Hay evidencia para fundamentar la evaluación. No se han identificado temas pendientes (por ejemplo, temas planteados a través de la autoevaluación o por personas que desempeñan funciones tales como la de gestión de riesgo operacional, auditoría interna o supervisores, entre otros).
- 2. Largamente implementado:** La compañía ha implementado los principios en gran medida, pero no los ha implementado en su totalidad, pudiendo haber algunos temas de menor importancia identificados.
- 3. Parcialmente implementado:** La compañía ha implementado parcialmente el principio, los aspectos principales de la implementación permanecen, pudiendo haber algunos temas significativos identificados que se encuentran pendientes.
- 4. No implementado:** La compañía aún no ha implementado esta práctica.
- 5. N/A:** Si la compañía determina que la calificación de 1 a 4 no es aplicable, se solicita que proporcione una justificación suficiente para esta selección.

Los elementos incluidos en el título “VII. PRÁCTICAS EMERGENTES DE GESTIÓN DE RIESGO OPERACIONAL” (PGRO) no son exhaustivos y se incluyen como ejemplos de las mejores prácticas líderes para mejorar la gestión del riesgo operacional. Estas mejores prácticas se calificarán bajo la misma métrica aplicable a los cuatro principios definidos.

Las compañías pueden tener otras prácticas que deseen resaltar además de las incluidas en el documento; por lo tanto, se ha incluido un apartado de "Prácticas adicionales" para su descripción.

Aspectos generales a considerar en la evaluación:

1. Para cada principio y/o práctica deberá adjuntarse una explicación de las razones que justifican la calificación otorgada. Cuando la calificación sea distinta de “Totalmente implementado” se deberá informar un plan de acción definido para superar la brecha detectada, o la justificación detallada de por qué, a su juicio, la brecha es justificada en su entidad. El plan de acción definido, deberá indicar las acciones concretas que la compañía adoptará respecto de cada brecha identificada, adjuntando plazos y responsables asociados a cada plan de acción orientado a cerrar dicha brecha.
2. En caso que la compañía considere que una determinada brecha es justificada en su entidad, por su modelo de negocio u otra razón, y por lo tanto no requiere una acción de cierre o mitigación de la brecha, deberá explicarlo detalladamente en este informe.
3. En cuanto a la evaluación se deberá adjuntar la calificación correspondiente a cada principio la cual consistirá en el promedio de los ítems correspondientes a cada uno de ellos. Cabe señalar, que para el cálculo de la nota no se considerarán las evaluaciones de las Prácticas Emergentes de Gestión de Riesgo Operacional (PGRO) de cada principio.
4. En el caso que la compañía de seguros considere que alguno de los principios y/o criterios tengan una ponderación distinta, dadas las condiciones particulares de la compañía, estas deberán ser justificadas argumentado la ponderación propuesta.
5. Para finalizar, las aseguradoras deberán mantener a disposición de la CMF, toda la información de respaldo del informe de autoevaluación del cumplimiento de los principios y buenas prácticas señaladas en la presente norma.

Autoevaluación de Riesgo Operacional

Principio 1: La gestión del riesgo operacional debe integrarse completamente en el programa general de gestión de riesgos de las compañías y documentarse adecuadamente.

Item	Criterio	Evaluación de Cumplimiento	Fundamento de la Evaluación	Plan de acción y plazo(s) para su plena implementación
1-1.01	La compañía cuenta con un marco para la gestión del riesgo operacional que establezca mecanismos para identificar y gestionar el riesgo operacional.			
1-1.02	La compañía tiene un proceso definido para la discusión y el escalamiento efectivo de los problemas.			
1-1.03	La compañía tiene un proceso definido para la completa recopilación de datos.			
1-1.04	La compañía tiene un proceso definido a nivel corporativo para el análisis de problemas complejos.			
1-1.05	La compañía tiene un proceso definido para documentar, monitorear y administrar acciones de mitigación de riesgos operacionales.			

PGRO

El documento del marco para la gestión del riesgo operacional debe incluir al menos los siguientes elementos:				
1-2.01	Una descripción del enfoque de la compañía para gestionar el riesgo operacional, incluida la referencia a las políticas y procedimientos relevantes de gestión del riesgo operacional.			
1-2.02	Clara rendición de cuentas, transparencia y responsabilidad sobre la gestión del riesgo operacional entre las tres líneas de defensa .			
1-2.03	Las herramientas de evaluación de riesgos como reportes e informes utilizadas por la compañía.			
1-2.04	El enfoque de la compañía para establecer y monitorear el apetito por riesgo y los límites relacionados al riesgo operacional.			
1-2.05	Las estructuras de gobierno utilizadas para gestionar el riesgo operacional, incluidas las líneas de reporte y las responsabilidades.			
1-2.06	Las estructuras de gobierno utilizadas para garantizar que la gestión del riesgo operacional tengan un estatus suficiente dentro de la organización para ser eficaces.			
1-2.07	Aplicación transversal en la compañía.			
1-2.08	Es necesario que las políticas relevantes sean revisadas periódicamente y cuando corresponda.			

1-2.09	Documentación eficiente, que debe proporcionar un valor para la gestión de riesgos proporcional y ser adecuada para el usuario.			
--------	---	--	--	--

Prácticas Adicionales

1-3.01	Cualquier otra práctica implementada relacionada al Marco de Gestión de Riesgo Operacional.			
--------	---	--	--	--

Declaración de apetito de riesgo operacional

Principio 2: La gestión del riesgo operacional debe servir para respaldar la estructura general de gobierno corporativo de las compañías. Como parte de esto, las compañías deben desarrollar y utilizar una declaración de apetito de riesgo operacional, o en el caso de las compañías pequeñas y menos complejas con perfiles de riesgo operacional más bajos, el uso de los umbrales de informe y/o escalamiento para eventos de riesgo operacional materiales.

Item	Criterio	Evaluación de Cumplimiento	Fundamento de la Evaluación	Plan de acción y plazo(s) para su plena implementación
2-1.01	La compañía ha desarrollado y mantiene una declaración de apetito de riesgo integral para riesgos operacionales o ha evaluado su perfil de riesgo operacional como bajo y ha desarrollado umbrales de escalamiento y/o reporte para eventos de riesgo operacional materiales.			
2-1.02	La declaración del apetito de riesgo de la Compañía por los riesgos operacionales o los umbrales de generación de informes y/o escalamiento para eventos de riesgo operacional materiales se encuentran integrados dentro del Marco de Apetito de Riesgo general de la Compañía.			
2-1.03	La declaración de apetito de riesgo operacional considera la naturaleza y los tipos de riesgo operacional que la compañía está dispuesta o espera asumir.			
2-1.04	La declaración de apetito de riesgo operacional es concisa, clara e incluye un componente medible (límites y/o umbrales).			

2-1.05	La declaración de apetito de riesgo operacional y/o el umbral de reporte para eventos de riesgo operacional materiales se revisan regularmente para asegurar que sean apropiados.			
2-1.06	Se han implementado procesos de escalamiento e informes para los incumplimientos del apetito por el riesgo operacional.			

PGRO

La declaración de apetito de riesgo operacional debe considerar al menos elementos tales como:				
2-2.01	Cambios en el entorno externo.			
2-2.02	Aumentos y/o disminuciones significativos en los volúmenes de negocios o actividad.			
2-2.03	Calidad en el ámbito de control.			
2-2.04	Efectividad de la gestión de riesgos o estrategias de mitigación.			
2-2.05	Experiencia en eventos de riesgo operacional de la compañía.			
2-2.06	Frecuencia, volumen o naturaleza del límite de apetito por riesgo y/o umbral de incumplimientos.			

Prácticas Adicionales

2-3.01	Cualquier otra práctica implementada relacionada a la declaración de apetito de riesgo operacional.			
--------	---	--	--	--

Las Tres Líneas de Defensa

Principio 3:

Las compañías deben garantizar la rendición de cuentas efectiva para la gestión del riesgo operacional. Un enfoque de “tres líneas de defensa”, o una estructura apropiadamente robusta, debe servir para delinear las prácticas clave de la gestión del riesgo operacional y proporcionar una visión objetiva adecuada y un desafío. La forma en que esto se haga operativo en la práctica, en términos de la estructura organizacional de la compañía, dependerá de su modelo de negocio y perfil de riesgo.

Item	Criterio	Evaluación de Cumplimiento	Fundamento de la Evaluación	Plan de acción y plazo(s) para su plena implementación
Áreas tomadoras de Riesgo, primera línea de defensa				
3-1.01	La propiedad (responsabilidad) del riesgo se ha definido y los propietarios del riesgo reconocen y administran el riesgo operacional en el que se incurre al realizar las actividades.			
3-1.02	Los propietarios de riesgos son responsables de planificar, dirigir y controlar las operaciones diarias de una actividad y/o proceso, y de identificar y gestionar los riesgos operacionales inherentes en los productos, actividades, procesos y sistemas de los que son responsables.			
Supervisión del Riesgo, segunda línea de defensa				
3-2.01	La supervisión del riesgo es realizada por partes calificadas independientes de los propietarios del riesgo. Realizan una evaluación objetiva de las entradas y salidas de las líneas de negocios de la gestión de riesgos de la compañía (incluida la			

	medición y/o estimación de riesgos).			
3-2.02	La supervisión de riesgos ha establecido herramientas de informes para proporcionar una seguridad razonable de que las entradas y salidas de las líneas de negocios de la gestión de riesgos de la compañía están adecuadamente completas y bien informadas.			

Auditoría Interna, tercera línea de defensa

3-3.01	La revisión y pruebas objetivas son independientes tanto de la propiedad del riesgo como de la supervisión del riesgo.			
3-3.02	La revisión y pruebas objetivas son completadas por los controles, procesos y sistemas de gestión de riesgos operacionales de la compañía y la efectividad de las actividades realizadas por los propietarios de riesgos y la supervisión de riesgos.			
3-3.03	La revisión y pruebas objetivas tienen un alcance suficiente para verificar que el marco de gestión del riesgo operacional se haya implementado según lo previsto y esté funcionando de manera efectiva.			

PGRO

Áreas tomadoras de Riesgo, primera línea de defensa				
La primera línea de defensa debe ser responsable de desarrollar capacidades en las siguientes áreas:				
3-4.01	Adhesión al marco de gestión del riesgo operacional y políticas relacionadas.			
3-4.02	Identificación y evaluación del riesgo operacional inherente dentro de su unidad de negocios respectiva y evaluación de la importancia de los riesgos para las unidades de negocios respectivas.			
3-4.03	Establecimiento de controles de mitigación apropiados y evaluación del diseño y la efectividad de estos controles.			
3-4.04	Supervisar e informar sobre los perfiles de riesgo operacional de las líneas de negocios y la operación de respaldo dentro de la declaración de apetito de riesgo operacional establecida.			
3-4.05	Análisis y reporte del riesgo operacional residual que no es mitigado por los controles, incluidos los eventos de riesgo operacional, las deficiencias de control, los recursos humanos, los procesos y las deficiencias del sistema de gestión de riesgo.			
3-4.06	Promoción de una fuerte cultura de gestión del riesgo operacional a lo largo de la primera línea de defensa.			
3-4.07	Confirmación de la escalada oportuna y precisa, dentro de la compañía, de cuestiones materiales.			
3-4.08	Capacitación del personal en sus roles en la gestión del riesgo operacional, si es requerido			
3-4.09	Identificar, medir, gestionar, monitorear y reportar el riesgo operacional que surja de las actividades operativas e			

	iniciativas en línea con los estándares corporativos.			
3-4.10	Establecer una estructura de control interno adecuada para gestionar los riesgos operacionales en su área específica.			
3-4.11	Escalar de manera oportuna, los riesgos operativos a la alta administración.			
3-4.12	Desarrollar e implementar, de manera oportuna, acciones correctivas para los problemas de riesgo operacional que se han identificado.			
Supervisión del Riesgo,segunda línea de defensa				
La evaluación objetiva proporcionada por la supervisión de riesgos es:				
3-5.01	Basado en un proceso estructurado y repetible que se adapta a la mejora continua (al tiempo que permite una flexibilidad ad hoc donde sea apropiado).			
3-5.02	Se aplica a través de las diversas herramientas de gestión de riesgo operacional, informes y otros procesos de gobierno.			
3-5.03	Realizado por personal experto y competente.			
3-5.04	Comunicado y compartido en la compañía de manera constructiva.			
3-5.05	Realizado en forma oportuna.			
3-5.06	Medido por resultados (Ej, ha influido en una decisión y/o acción de gerencia).			
3-5.07	Evidenciada / Documentada.			
3-5.08	Respaldado con un nivel adecuado de recursos suficientemente calificados para cumplir efectivamente con sus responsabilidades.			
La segunda línea de defensa puede contribuir al rol desempeñado por la primera línea de defensa de la siguiente manera:				

3-5.09	Contribuye a la notificación de los perfiles de riesgo operacional, en particular con respecto a la agregación de información a nivel de toda la compañía.			
3-5.10	Contribuye al análisis y reporte del riesgo operacional residual, particularmente con respecto a la agregación de información a nivel de toda la compañía.			
La segunda línea de defensa puede ser responsable de:				
3-5.11	Proporcionar una evaluación objetiva efectiva, que debe ser evidenciada y documentada donde el material (por ejemplo, proporcionando ejemplos de los desafíos y resultados) para que luego sea observable para la primera línea de defensa.			
3-5.12	Confirmar el desarrollo continuo de estrategias apropiadas para identificar, evaluar, medir, monitorear y controlar, y mitigar el riesgo operacional.			
3-5.13	Confirmar el establecimiento continuo y la documentación de políticas y procedimientos apropiados de la compañía relacionados con el marco de gestión de riesgo operacional.			
3-5.14	Confirmar el desarrollo continuo, la implementación y el uso de herramientas apropiadas de gestión de riesgo operacional en toda la compañía.			
3-5.15	La confirmación de que existen procesos y procedimientos adecuados para proporcionar una supervisión adecuada de las prácticas de gestión de riesgos operacionales de la compañía.			
3-5.16	Confirmar que los procesos de medición del riesgo operacional se integran adecuadamente en la gestión			

	general del riesgo de la compañía.			
3-5.17	Revisar y contribuir al monitoreo y reporte del perfil de riesgo operacional de la compañía (esto también puede incluir la agregación y el reporte).			
3-5.18	Promover una sólida cultura de gestión del riesgo operacional en toda la compañía.			
3-5.19	Confirmar la escalada oportuna y precisa, dentro de la compañía, de los problemas materiales.			
Auditoría Interna, tercera línea de defensa				
La revisión objetiva y las actividades de prueba involucran:				
3-6.01	Pruebas de cumplimiento de las políticas y procedimientos establecidos.			
3-6.02	Evaluar si el marco para la gestión del riesgo operacional es apropiado dado el tamaño, la complejidad y el perfil de riesgo de la compañía.			
3-6.03	Consideración del diseño y uso de las herramientas de gestión de riesgo operacional utilizadas por las áreas tomadoras de riesgo y la supervisión de riesgos.			
3-6.04	Consideración de la adecuación de la evaluación objetiva aplicada por la supervisión del riesgo.			
3-6.05	Consideración de los procesos de seguimiento, reporte y gobierno.			

Prácticas Adicionales

3-7.01	Cualquier otra práctica implementada por la compañía con respecto a un enfoque de "tres líneas de defensa".			
--------	---	--	--	--

Identificación y Evaluación de Riesgo Operacional.

Principio 4: Las compañías deben garantizar una identificación y evaluación integrales del riesgo operacional mediante el uso de herramientas de gestión adecuadas. El mantenimiento de un conjunto de herramientas de gestión de riesgos operacionales proporciona un mecanismo para recopilar y comunicar información relevante sobre riesgos operacionales, tanto dentro de la compañía como a las autoridades de supervisión relevantes.

Item	Criterio	Evaluación de Cumplimiento	Fundamento de la Evaluación	Plan de acción y plazo(s) para su plena implementación
4-1.01	La compañía ha establecido herramientas para lograr un nivel robusto de gestión de riesgo operacional, adecuado a su naturaleza, tamaño, complejidad y perfil de riesgo.			
4-1.02	La compañía desarrolla y mejora sus herramientas, y supervisa y adopta las mejores prácticas según corresponda, para gestionar sus riesgos operativos.			

PGRO

La compañía puede implementar herramientas de gestión de riesgo operacional tales como:				
Taxonomía de Riesgo Operacional				
4-2.01	Taxonomía de riesgo operacional que articule la naturaleza y el tipo de riesgo operacional al que la compañía está potencialmente expuesta.			
Evaluación y Control				
4-3.01	Evaluaciones de riesgo y control de los riesgos operacionales inherentes y el diseño y la efectividad de los controles de mitigación dentro de la compañía.			
Las Evaluaciones y Control de Riesgos				
4-3.01a	Son realizadas por las áreas tomadoras de riesgo, primera línea de defensa, incluye grupos de control.			
4-3.01b	Refleja el entorno actual, pero con foco prospectivo.			

4-3.01c	Resultado gatilla planes de acción que son seguidos y monitoreados.			
4-3.01d	Son revisados y testeados objetivamente por la Supervisión del Riesgo (segunda línea de defensa).			
4-3.01e	Se realizan periódicamente para respaldar información precisa y oportuna.			

Evaluaciones y Control de Riesgos en la Gestión del Cambio

4-4.01	Proceso formal para evaluar el riesgo operacional inherente y los controles cuando la compañía realiza cambios significativos.			
Las Evaluaciones y Control de Riesgos en la Gestión del Cambio deberían:				
4-4.01a	Ser realizado por las áreas tomadoras de riesgos (primera línea de defensa).			
4-4.01b	Considerar los riesgos inherentes en el nuevo producto, servicio o actividad.			
4-4.01c	Considerar los cambios en el perfil de riesgo operacional de la compañía y el apetito de riesgo.			
4-4.01d	Considerar el conjunto requerido de controles, procesos de administración de riesgos y estrategias de mitigación de riesgos que se implementarán.			
4-4.01e	Considerar el riesgo residual (riesgo no mitigado).			
4-4.01f	Considerar los cambios en los límites y/o umbrales de riesgo relevante.			
Recopilación y análisis de eventos de riesgo operacional interno				
4-5.01	Recopilación y análisis robusto de eventos de riesgo operacional interno, incluidos los sistemas y procesos implementados que capturan y analizan eventos de riesgo			

	operacional importantes.	internos		
La recopilación y análisis de eventos de riesgo operacional interno:				
4-5.01a	Es administrado por las áreas tomadoras de riesgo (primera línea de defensa) con controles apropiados implementados (es decir, segregación de tareas, verificación) para mantener la integridad de los datos a un nivel aceptable.			
4-5.01b	Para eventos materiales, identifique la causa, así como cualquier acción correctiva requerida.			
4-5.01c	Han establecido estándares de informes y análisis que describen las expectativas mínimas sobre el análisis de eventos.			
4-5.01d	Los eventos Operacionales materiales tienen un análisis apropiado de la causa, realizado por los tomadores de Riesgo (primera línea de defensa), revisado y testeado por la Supervisión del Riesgo (segunda línea de defensa) y escalado adecuadamente.			
Recopilación y análisis de eventos de riesgo operacional externo				
4-6.01	Proceso de recopilación y análisis eventos externos de riesgo operacional.			
Indicadores de riesgo y desempeño				
4-7.01	Indicadores de riesgo y desempeño que monitorean los principales factores de exposición asociados con los riesgos operacionales claves.			
Mapeo de procesos de negocio materiales				
4-8.01	Mapeo de procesos de negocio de materiales que identifica y administra los riesgos operativos para procesos importantes la compañía.			

Análisis de Escenarios de Riesgo Operacional				
4-9.01	Análisis de escenarios de riesgo operacional que consideren respuestas organizacionales esperadas e inesperadas a un evento de riesgo operacional.			

Si se utiliza como entrada en la determinación y/o estimación de la exposición al riesgo operacional, el análisis de escenarios debe:

4-9.01a	Ser revisado por la función de Supervisión de Riesgos (segunda línea de defensa) para garantizar que sea apropiado y coherente con el programa de análisis de escenarios de la Compañía.			
---------	--	--	--	--

Determinación y/o estimación de la exposición al riesgo operacional

4-10.01	La determinación y/o estimación de la exposición al riesgo operacional se compara con el capital requerido para el riesgo operacional.			
4-10.01a	Los supuestos clave para la determinación del riesgo operacional están documentados y se realizan las actividades apropiadas de validación, investigación y verificación.			

Análisis comparativo

4-11.01	El análisis comparativo se utiliza para confirmar la evaluación general del riesgo operacional.			
---------	---	--	--	--

Prácticas Adicionales

4-12.01	Cualquier otra herramienta específica utilizada para identificar y evaluar y/o analizar el riesgo operacional.			
---------	--	--	--	--

ANEXO 2

EJERCICIO AUTOEVALUACIÓN DE CIBERSEGURIDAD

La creciente frecuencia y sofisticación de los ciberataques recientes ha elevado el perfil de riesgo para muchas organizaciones de todo el mundo. Como resultado de lo señalado, recientemente se ha prestado gran atención al nivel de preparación general contra tales ataques por parte de estas organizaciones, incluidas las instituciones financieras, los proveedores de infraestructura crítica, los organismos reguladores, los medios de comunicación y el público en general.

La ciberseguridad está adquiriendo cada vez más importancia debido a factores tales como la continua y creciente dependencia tecnológica, la interconexión del sector financiero y, en particular, el rol fundamental que tienen las compañías de seguro reguladas en la economía en general. Es así como la Comisión para el Mercado Financiero espera que la alta gerencia de las compañías revise las políticas y prácticas de la gestión de riesgo cibernético, para garantizar que estas sigan siendo apropiadas y efectivas a la luz de las circunstancias y los riesgos cambiantes.

La CMF reconoce que muchas compañías pueden haber realizado ya, o pueden estar en el proceso de realizar, una evaluación de su nivel actual de preparación. Teniendo esto en cuenta, la CMF cree que podrían beneficiarse de la orientación relacionada con dichas actividades de autoevaluación. En consecuencia, se comparte la guía adjunta de autoevaluación de ciberseguridad para ayudar a las compañías en sus actividades de autoevaluación.

Guía de autoevaluación de ciberseguridad

Esta plantilla de autoevaluación establece propiedades y características deseables sobre prácticas de ciberseguridad que podrían ser consideradas por una compañía al evaluar la idoneidad de su marco de ciberseguridad y al planificar mejoras en su estructura. Se recomienda a las compañías reflejar el estado actual de las prácticas de ciberseguridad en sus evaluaciones y no en su estado objetivo, y a que consideren las prácticas de ciberseguridad en toda la organización. Si una compañía emplea prácticas relevantes no descritas en la plantilla, se solicita enumerarlas junto con sus respectivas evaluaciones.

La CMF solicita que las compañías califiquen su grado actual de madurez en una escala de 1 a 4 y brinden suficiente justificación en todas las circunstancias. A continuación, se establece una definición de cada una de las evaluaciones de cumplimiento:

1. **Totalmente implementado:** La compañía ha implementado plenamente los principios en toda su empresa. Hay evidencia para fundamentar la evaluación. No se han identificado temas pendientes (por ejemplo, temas planteados a través de la autoevaluación o por grupos tales como el de gestión de riesgo operacional, auditoría interna, supervisores o de terceros).
2. **Largamente implementado:** La compañía ha implementado los principios en gran medida, pero no los ha implementado en su totalidad, o puede haber algunos temas de menor importancia identificados.
3. **Parcialmente implementado:** La compañía ha implementado parcialmente el principio, los aspectos principales de la implementación permanecen, y puede haber algunos temas significativos pendientes.
4. **No implementado:** La compañía aún no ha implementado esta práctica.
5. **N/A:** Si la compañía determina que la calificación de 1 a 4 no es aplicable, se recomienda que proporcione una justificación suficiente para esta selección.

1. Organización y Recursos

Item	Criterio	Evaluación de Cumplimiento	Fundamento de la Evaluación (Diseño de Control y Eficacia)	Plan de acción y plazo(s) para su plena implementación
1.01	La compañía ha establecido claramente la responsabilidad y propiedad de, y los recursos financieros para, el marco de ciberseguridad ²² .			
1.02	La compañía ha asignado roles y responsabilidades específicas para la gestión de la ciberseguridad, y estas personas tienen suficientes autoridades operativas delegadas.			
1.03	La compañía cuenta con un grupo de especialistas en ciberseguridad, gestionado de manera centralizada, que se encarga de la inteligencia de amenazas, la gestión de amenazas y la respuesta a incidentes.			
1.04	La compañía proporciona 24/7 capacidades de identificación y respuesta para la gestión de la ciberseguridad.			
1.05	La compañía cuenta con suficiente personal calificado para la gestión de la ciberseguridad.			
1.06	Los especialistas en ciberseguridad están sujetos a una mejor control de antecedentes y seguridad.			
1.07	La compañía tiene un plan formalizado para proporcionar capacitación técnica continua a los especialistas en ciberseguridad.			
1.08	Se proporciona capacitación en ciberseguridad a empleados nuevos y existentes.			
1.09	Se proporciona concientización sobre ciberseguridad a todos los empleados.			

2. Control y Evaluación de Riesgo de Ciberseguridad

Item	Criterio	Evaluación de Cumplimiento	Fundamento de la Evaluación (Diseño de Control y Eficacia)	Plan de acción y plazo(s) para su plena implementación
2.01	La compañía tiene un proceso para realizar evaluaciones integrales y regulares de riesgos de ciberseguridad que consideran a las personas (es decir, empleados, clientes y otras partes externas), procesos, datos, tecnología en todas sus líneas de negocios y geografías.			
2.02	La compañía evalúa y toma medidas para mitigar el potencial riesgo de ciberseguridad			

²² Marco de ciberseguridad: Un conjunto completo de recursos organizativos que incluye políticas, personal, procesos, prácticas y tecnologías utilizadas para evaluar y mitigar los riesgos y ataques cibernéticos.

	que surge de sus acuerdos de subcontratación que se consideran materiales.			
2.03	La compañía evalúa y toma medidas para mitigar el potencial riesgo de ciberseguridad derivado de sus proveedores de servicios de TI críticos.			
2.04	La evaluación de riesgos de la gestión del cambio y el proceso de diligencia debida de la compañía consideran el riesgo de ciberseguridad.			
2.05	La compañía realiza regularmente escaneos y pruebas de vulnerabilidad de hardware y software para clientes, servidores y la infraestructura de red para identificar brechas de control de seguridad.			
2.06	La compañía realiza pruebas regulares de penetración de los límites de la red (p. ej., puntos de entrada y salida de la red abierta) para identificar brechas de control de seguridad.			
2.07	La compañía realiza pruebas regulares con sus proveedores de servicios de mitigación de riesgos de ciberseguridad.			
2.08	La compañía realiza ejercicios regulares de ataque cibernético (incluyendo el ataque de denegación de servicio distribuido -DDoS por sus siglas en inglés-) y de simulación de recuperación.			
2.09	La compañía considera en su evaluación del riesgo el impacto de una interrupción de Internet en todo Chile durante un período de tiempo prolongado.			

3. Conocimiento de la Situación

Item	Criterio	Evaluación de Cumplimiento	Fundamento de la Evaluación (Diseño de Control y Eficacia)	Plan de acción y plazo(s) para su plena implementación
3.01	La compañía mantiene una base de conocimiento actual en toda la empresa de sus usuarios, dispositivos, aplicaciones y relaciones, incluyendo pero no limitado a: <ul style="list-style-type: none"> · inventario de activos de software y hardware; · mapas de red (incluidos los límites, el tráfico y el flujo de datos); y · utilización de la red y datos de rendimiento. 			

3.02	La compañía almacena centralmente un historial de información de eventos de ciberseguridad.			
3.03	La compañía normaliza, agrega y correlaciona información de eventos de ciberseguridad.			
3.04	La compañía realiza un análisis automatizado de los eventos de ciberseguridad para identificar posibles ataques cibernéticos, incluidos los ataques DDoS.			
3.05	La compañía complementa el análisis automatizado de eventos de ciberseguridad mediante la realización de análisis adicionales expertos sobre eventos de ciberseguridad para identificar posibles ataques cibernéticos.			
3.06	La compañía monitorea y rastrea los incidentes de ciberseguridad en la industria de seguros y, de manera más amplia, según sea relevante, a través de la participación en programas de la industria.			
3.07	La compañía se suscribe a la investigación de la industria sobre ciberseguridad.			

4. Gestión de Riesgos de Amenazas y Vulnerabilidades

Item	Criterio	Evaluación de Cumplimiento	Fundamento de la Evaluación de Control y Eficacia)	Plan de acción y plazo(s) para su plena implementación
<u>Detección de Pérdida de Datos / Prevención</u>				
4.01	La compañía ha implementado herramientas para: <ul style="list-style-type: none"> · impedir la salida de datos no autorizados de la empresa; · monitorear el tráfico saliente de alto riesgo para detectar datos no autorizados que salen de la compañía (por ejemplo, por geografía, tamaño, volumen, tipo de información); · salvaguardar los datos en tiendas online y offline (p. ej., ordenadores de escritorio, ordenadores portátiles, dispositivos móviles, dispositivos extraíbles y medios extraíbles); y · salvaguardar los datos en reposo y en movimiento. 			
4.02	La compañía ha implementado los controles previos en toda la empresa.			

<u>Detección y mitigación de incidentes de ciberseguridad</u>			
4.03	La compañía ha implementado las siguientes herramientas de ciberseguridad, actualizaciones automatizadas, y aplicación para toda la empresa: · sistemas de detección / protección de intrusos; · firewalls de aplicaciones Web; · anti-virus; · anti-spyware; · anti-spam; · Protección DDoS; y · otro (por favor describa).		
4.04	La compañía ha implementado las herramientas de ciberseguridad anteriores utilizando técnicas de detección mejoradas (por ejemplo, basadas en la reputación y/o basadas en el comportamiento).		
<u>Seguridad del Software</u>			
4.05	La compañía tiene un proceso para obtener, probar y desplegar automáticamente los parches y actualizaciones de seguridad de manera oportuna según la criticidad.		
4.06	La compañía considera y mitiga el riesgo de ciberseguridad derivado del uso de cualquier software sin soporte.		
4.07	La compañía tiene un proceso para confirmar la implementación exitosa de parches de seguridad y resolver fallas de actualización.		
4.08	El software desarrollado internamente o externamente por la compañía está sujeto a estándares seguros de diseño, codificación y prueba de sistemas que incorporan controles de ciberseguridad apropiados.		
4.09	La compañía implementa los controles anteriores en toda la empresa.		
<u>Infraestructura de Red</u>			
4.10	La compañía ha implementado monitoreo y protección de límites de red.		
4.11	La compañía segmenta la red de la empresa en múltiples zonas de confianza separadas.		
4.12	La infraestructura de red de la compañía tiene múltiples capas de defensa (por		

	ejemplo, basada en la nube, ISP, in situ) para mitigar los ataques DDoS.			
4.13	La compañía puede aislar, contener o cerrar de forma rápida y remota las operaciones comprometidas.			
4.14	La compañía ha implementado procesos y herramientas para proteger dispositivos móviles y redes inalámbricas.			
4.15	La compañía implementa los controles anteriores en toda la empresa.			
Configuración y Gestión de Seguridad Estándar				
4.16	La compañía utiliza imágenes estándar seguras del sistema operativo para clientes, servidores y dispositivos de red.			
4.17	La compañía sigue un proceso formal de gestión de cambios para la administración de la configuración de seguridad para todos los activos de hardware y software de la red en sus redes.			
4.18	La compañía documenta, implementa y aplica los estándares de configuración de seguridad a todos los activos de hardware y software en la red.			
4.19	La compañía restringe el uso de software y hardware no autorizado y/o no registrado mediante políticas y herramientas automatizadas, incluyendo los dispositivos móviles.			
4.20	La compañía implementa los controles anteriores en toda la empresa.			
Control de Acceso a Redes y Administración				
4.21	La compañía tiene la capacidad de detectar y bloquear automáticamente el acceso no autorizado a la red (por ejemplo, incluyendo el acceso por cable, inalámbrico y remoto).			
4.22	La compañía aplica fuertes mecanismos de autenticación para administrar el acceso y las identidades de los usuarios.			
4.23	La compañía controla y administra de manera estricta el uso de privilegios administrativos.			

4.24	La compañía implementa los controles anteriores en toda la empresa.		
Administración de terceros			
4.25	La compañía considera el riesgo de ciberseguridad como parte de su proceso de diligencia debida para acuerdos de subcontratación de materiales y proveedores de servicios de TI críticos, incluidos los acuerdos de subcontratación relacionados.		
4.26	Los contratos para todos los acuerdos de subcontratación de materiales y proveedores de servicios de TI críticos incluyen disposiciones para salvaguardar la información de la compañía.		
4.27	La compañía dispone de un proceso establecido para monitorear el nivel de preparación de riesgos de ciberseguridad para acuerdos de subcontratación de materiales y proveedores de servicios de TI críticos.		
4.28	La compañía tiene procesos establecidos para garantizar la notificación oportuna de un incidente de ciberseguridad de los proveedores de servicios con los que la compañía tiene uno o más acuerdos de subcontratación de materiales, o proveedores de servicios de TI críticos.		
Asegurados			
4.29	Se proporciona información y concientización sobre ciberseguridad a asegurados.		
4.30	La compañía ha tomado medidas adicionales para proteger a sus asegurados.		

5. Administración de Incidentes de Ciberseguridad

Item	Criterio	Evaluación de Cumplimiento	Fundamento de la Evaluación (Diseño de Control y Eficacia)	Plan de acción y plazo(s) para su plena implementación
5.01	El Marco de Gestión de Incidentes de la compañía está diseñado para responder rápidamente a incidentes de ciberseguridad materiales.			

5.02	Se ha establecido una estructura apropiada de 'comando y control' con la autoridad de gastos delegada requerida dentro del Marco de Gestión de Incidentes para brindar una respuesta rápida a todos los niveles de incidentes de ciberseguridad.			
5.03	La compañía tiene procedimientos documentados para monitorear, analizar y responder a incidentes de ciberseguridad.			
5.04	El proceso de gestión de cambios de la compañía se ha diseñado para permitir una respuesta y mitigación rápida de incidentes materiales de ciberseguridad.			
5.05	El Marco de Gestión de Incidentes de la compañía incluye criterios de escalamiento alineados con su taxonomía de ciberseguridad.			
5.06	La compañía tiene un plan de comunicación interno para abordar incidentes de ciberseguridad que incluye protocolos de comunicación para las principales partes internas interesadas (por ejemplo, unidades de negocios relevantes y/o centros de llamadas, alta gerencia, gestión de riesgos, Junta Directiva, etc.).			
5.07	La compañía tiene un plan de comunicación externo para abordar incidentes de ciberseguridad que incluye protocolos de comunicación y propuestas de comunicaciones predefinidas para interesados externos clave (es decir, clientes, medios de comunicación, proveedores de servicios críticos, etc.).			
5.08	El proceso de gestión de incidentes de la compañía está diseñado para garantizar que las siguientes tareas se completen de manera íntegra antes de que se pueda cerrar formalmente un incidente: <ul style="list-style-type: none"> · Recuperación de la interrupción de los servicios del incidente de ciberseguridad; · Garantía de la integridad de los sistemas luego del incidente de ciberseguridad y · Recuperación de datos perdidos o dañados debido al incidente de ciberseguridad. 			
5.09	La compañía tiene un proceso establecido de revisión posterior al incidente que: <ul style="list-style-type: none"> · se completa por incidentes materiales de ciberseguridad; · incluye investigaciones forenses de cibernéticas apropiadas; · narra los eventos que llevaron a, durante y después del incidente de ciberseguridad; · identifica la causa raíz y resalta las deficiencias de control; 			

- evalúa cualquier imperfección en el proceso de gestión de incidentes; y
- establece un plan de acción para abordar las deficiencias identificadas.

6. Gobernanza de Ciberseguridad

Item	Criterio	Evaluación de Cumplimiento	Fundamento de la Evaluación (Diseño de Control y Eficacia)	Plan de acción y plazo(s) para su plena implementación
Política y estrategia de ciberseguridad				
6.01	La compañía ha establecido una política de ciberseguridad para toda la empresa ²³ , con procedimientos de soporte que establecen cómo la compañía identificará y administrará sus riesgos de ciberseguridad.			
6.02	Las funciones y responsabilidades de cada una de las tres líneas de defensa y otras partes interesadas están descritas claramente dentro de la política de ciberseguridad.			
6.03	La política de ciberseguridad se aplica a todos los grupos y entidades operativas de la compañía, incluidas filiales nacionales (administradora de mutuo hipotecario endosable) y las subsidiarias en el extranjero.			
6.04	La compañía tiene definida una taxonomía común y consistente para el riesgo de seguridad cibernético.			
6.05	La política de ciberseguridad de la compañía está vinculada a otras políticas relevantes de gestión de riesgos, incluida la seguridad de la información, la gestión de la continuidad del negocio, la subcontratación, las nuevas iniciativas y la gestión del cambio, etc.			
6.06	La compañía ha establecido una estrategia de ciberseguridad que está alineada con la estrategia comercial de la compañía.			
6.07	La compañía tiene un plan estratégico y táctico de implementación de ciberseguridad que describe iniciativas clave y líneas de tiempo.			
Segunda Línea de Defensa (por ejemplo, gestión de riesgos)				
6.08	Las evaluaciones relevantes de riesgo y control (RCAs por sus siglas en inglés) abordan el riesgo de ciberseguridad y los controles de mitigación.			

²³ Política de ciberseguridad: un conjunto de principios documentados y autorizados que establecen cómo se debe gobernar y ejecutar el Programa de ciberseguridad.

6.09	Se han establecido indicadores clave de riesgo y rendimiento, así como umbrales para los riesgos y controles clave de ciberseguridad inherentes a la compañía.			
6.10	La compañía ha utilizado el análisis de escenarios para considerar un ataque cibernético material, mitigar acciones e identificar posibles brechas de control.			
6.11	La segunda línea de defensa evalúa adecuadamente el riesgo de ciberseguridad dentro del proceso de gestión de cambios de la compañía.			
6.12	Las responsabilidades de la segunda línea de defensa relacionadas con las evaluaciones de ciberseguridad se han asignado a un grupo de control independiente con experiencia en riesgo cibernético.			
6.13	La segunda línea de defensa proporciona regularmente un desafío independiente a las diversas evaluaciones de riesgos de ciberseguridad realizadas por la primera línea de defensa (por ejemplo, evaluaciones de riesgos dentro de las autoevaluaciones de riesgo y control (RCSAs por sus siglas en inglés), análisis de escenarios, procesos de gestión de cambios, indicadores claves de riesgo (KRIs por sus siglas en inglés), evaluaciones de riesgos de amenazas, etc.).			
6.14	La segunda línea de defensa supervisa y cuestiona la identificación, adecuación y remediación de las acciones, como resultado de incidentes de ciberseguridad y evaluaciones de riesgo.			
6.15	El apetito y la tolerancia del riesgo operacional de la compañía considera el riesgo de ciberseguridad.			
6.16	La compañía ha considerado la cobertura de seguro de riesgo cibernético que proporciona mitigación financiera a los incidentes e impactos del riesgo cibernético.			
Auditoría Interna - Tercera Línea de Defensa				
6.17	La cobertura de auditoría interna incluye, pero no se limita a, todos los aspectos de la ciberseguridad dentro de este cuestionario.			
6.18	La frecuencia de las auditorías de ciberseguridad está determinada y es consistente con el riesgo de un ataque cibernético.			
6.19	La auditoría interna ha evaluado o está planeando evaluar tanto el diseño como la efectividad del marco de ciberseguridad.			
6.20	La auditoría interna tiene recursos y experiencia suficientes para auditar la implementación del marco de ciberseguridad.			
Supervisión de la Alta Dirección				

6.21	Se ha establecido un comité de Alta Gerencia que se dedica al tema del riesgo cibernético, o un comité de Alta Gerencia alternativo tiene tiempo suficiente dedicado a la discusión de la implementación del marco de ciberseguridad.			
6.22	La alta gerencia proporciona fondos adecuados y recursos suficientes para respaldar la implementación del marco de ciberseguridad de la compañía.			
6.23	Existen procesos para escalar las infracciones de límites y umbrales a la Alta Dirección por incidentes de ciberseguridad importantes o críticos.			
6.24	El Marco de Control Interno de la compañía comprende su marco de ciberseguridad y su plan de implementación, incluida la adecuación de los controles de mitigación existentes.			
Benchmarking Externo				
6.25	La compañía ha realizado una revisión externa de su marco de ciberseguridad.			

VI. EVALUACIÓN DE IMPACTO REGULATORIO

1.- Beneficios

1.1 Beneficios para las compañías

La implementación de una adecuada política de gestión del riesgo operacional y cibernético, basado en los principios contenidos en la propuesta normativa, debiese permitir una mejor gestión y mitigación de dichos riesgos, reduciendo las vulnerabilidades que enfrentan las compañías en esta materia, fortaleciendo en última instancia su solvencia, con un beneficio directo para sus accionistas y para sus asegurados. Lo anterior se ve reforzado con la implementación de un registro de incidentes operacionales a ser reportados a la CMF, que les permitirá a las compañías poder contabilizar y sistematizar dichos eventos, apoyando por lo tanto los procesos de gestión.

Por otra parte, la construcción de un registro común de incidentes cibernéticos permitirá compartir información relevante entre compañías, favoreciendo la pronta implementación de medidas que permitan contener el riesgo en aquellos casos en que la amenaza cibernética puede afectar a la industria como un todo. De esta forma, se logran mayores niveles de protección y resguardo frente a estos riesgos.

1.2 Beneficios para la CMF

La nueva normativa permitirá un fortalecimiento de la supervisión en esta materia por parte de la CMF, estableciendo un marco comparable para la evaluación de gestión de riesgos asociada a riesgo operacional y ciberseguridad, permitiendo complementar 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. Una mejor gestión del riesgo operacional y de la ciberseguridad, a partir de un marco de supervisión más robusto, le permiten al regulador cumplir de mejor forma con su rol de procurar la estabilidad del sistema financiero.

2.- Costos

2.1 Costos para las compañías

Es de esperar que las entidades aseguradoras ejecuten inversiones en recursos humanos, operacionales y tecnológicos para poder cumplir con las mejores prácticas en materia de gestión del riesgo operacional y ciberseguridad. Lo anterior, también considera los costos asociados al mayor involucramiento del directorio y la alta gerencia en la implementación y supervisión de una política de gestión del riesgo operacional y cibernético, que permita identificar, monitorear, controlar y mitigar efectivamente dichos riesgos. Es importante destacar que todos los costos antes descritos dependerán del grado de avance que tenga en la actualidad cada compañía y de su voluntad por cumplir con las mejores prácticas en la materia, tanto para efectos de la evaluación de Solvencia que hace la CMF, como para efectos de gestión interna.

Cabe destacar, tal como lo señala la normativa, que se debe aplicar un enfoque de proporcionalidad, en función del tamaño, naturaleza, alcance y complejidad de las operaciones,

estrategia de la compañía y perfil de riesgo, por lo que el costo de cumplir con el nuevo marco de principios podría variar significativamente entre una compañía y otra.

Por otra parte, se deben considerar también los costos, que se incurren cada dos y un año, asociados al cumplimiento normativo respecto a las autoevaluaciones de riesgo operacional y ciberseguridad, respectivamente, que deben efectuarse, así como el diseño, implementación y monitoreo de un plan que permita reducir las brechas detectadas.

Por último, es relevante destacar los recursos tecnológicos y humanos que deberán destinar las entidades aseguradoras para poder implementar y poner en marcha un sistema de alerta de incidentes operacionales con la CMF, además de uno enfocado a ciberseguridad, para ser compartido con la industria.

Se espera que la industria pueda entregar antecedentes cuantitativos asociados a los costos de implementación de la normativa puesta en consulta durante el proceso de consulta pública.

2.2 Costos para la CMF

Considerando el nuevo marco de principios para la adecuada gestión del riesgo operacional y cibernético, la CMF deberá destinar recursos adicionales para fortalecer sus procesos de supervisión en relación a estos temas, considerando especialmente el análisis de los resultados de la autoevaluación, el monitoreo del cumplimiento de los planes de acción comprometidos por las compañías para el cierre de brechas, así como una integración de estos aspectos dentro de la matriz de evaluación de riesgos que sirve para determinar la evaluación de solvencia por parte de la CMF.

Por otra parte, la CMF deberá incurrir en costos, principalmente asociados a horas hombres informáticas, para el diseño, implementación y puesta en marcha de un sistema que permita recepcionar las respuestas de las autoevaluaciones, que serán realizadas cada dos años.

Adicionalmente, la CMF deberá destinar recursos para poder diseñar e implementar el sistema que permita que las entidades aseguradoras puedan reportar sus incidentes operacionales, así como procurar los recursos correspondientes para poder acceder a la base de incidentes cibernéticos que mantendrá la industria, en caso de así definirse. Una alternativa, sería adoptar el Módulo RIO actualmente existente para el reporte de incidentes operacionales de los Bancos, el cual podría hacerse extensivo a las compañías de seguros.

3.- Riesgos

3.1 Riesgos de Emitir la Norma

No se prevén riesgos relevantes asociados a la implementación de la norma, ya que fortalece y complementa el esquema de supervisión de la CMF a favor de la estabilidad financiera y conducta de mercado, sin poner en riesgo el resto de los objetivos de la Comisión.

3.2. Riesgos de No Emitir la Norma

En caso de no emitirse la norma, se corre el riesgo de que tanto las entidades aseguradoras, como la CMF, no tengan acceso a un marco conceptual formal sobre buenas prácticas de gestión

de riesgo operacional y cibernético, ni a las herramientas regulatorias suficientes como para poder gestionar y supervisar, respectivamente, dichos riesgos, con implicancias potencialmente relevantes para la solvencia y estabilidad del mercado asegurador.

Cabe destacar que el riesgo operacional, y particularmente el riesgo cibernético, son cada vez más relevantes para la industria financiera, considerando el uso cada vez más intensivo de la tecnología dentro de los distintos procesos que aplican las compañías para la gestión diaria de su negocio, así como la creciente interconexión digital. En este contexto, aspectos tales como la protección de datos, resultan ser fundamentales para poder garantizar la confianza y solvencia de la industria de seguros.

ANEXO A: PRINCIPIOS Y RECOMENDACIONES INTERNACIONALES

1. IAIS: INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

La Asociación Internacional de Supervisores de Seguros (IAIS) es una organización voluntaria de supervisores y reguladores de seguros de más de 200 jurisdicciones en casi 140 países. La misión de la IAIS es promover una supervisión eficaz y coherente a nivel mundial de la industria de seguros con el fin de desarrollar y mantener mercados aseguradores justos, seguros y estables para el beneficio y protección de los asegurados y contribuir a la estabilidad financiera global.

Establecida en 1994, la IAIS es el órgano responsable del desarrollo de principios y normas internacionales, y otros materiales de apoyo para la supervisión del sector de seguros y la asistencia en su aplicación. La IAIS también proporciona un foro para que los miembros compartan sus experiencias y conocimiento en relación al mercado de seguros.

La IAIS coordina su trabajo con otros responsables de políticas financieras internacionales y asociaciones de supervisores o reguladores, y ayuda en la organización de los sistemas financieros a nivel mundial. En particular, la IAIS es un miembro del Consejo de Estabilidad Financiera (FSB), miembro del Consejo Asesor de la Junta de Normas de las Normas Internacionales de Contabilidad (IASB) y socio de la Iniciativa de Acceso a Seguros (A2ii).

En reconocimiento a su experiencia colectiva, la IAIS también es invocada por los líderes del G-20 y otros organismos que establecen estándares internacionales para asesorar en temas de seguros, así como en temas relacionados con la regulación y supervisión del sector financiero mundial. En noviembre de 2015, la IAIS publicó un documento actualizado de sus Principios Básicos de Seguros (PBS o ICP por sus siglas en inglés), que establece un conjunto de 25 principios cuyo objetivo es proporcionar un marco globalmente aceptado para la supervisión del sector asegurador.

En agosto de 2016 la IAIS publicó un **“Documento Temático sobre Riesgo Cibernético para el Sector de Seguros”**²⁴. En este documento temático, de carácter descriptivo, se destaca la importancia y preocupación por la ciberseguridad en todos los sectores de la economía mundial, en especial en el sector asegurador. Se resalta como los incidentes relacionados a la Ciberseguridad pueden perjudicar la capacidad para emprender negocios, comprometer la protección de datos comerciales y personales, así como socavar la confianza en el sector. El objetivo del documento es el de sensibilizar a los aseguradores y supervisores frente a los desafíos presentados por estos riesgos, incluyendo los enfoques de supervisión actuales y futuros para abordar estos riesgos.

El sector de los seguros se enfrenta al Ciber riesgo tanto por fuentes internas como externas, incluso a través de terceros. Las aseguradoras recopilan, procesan y almacenan volúmenes

²⁴ <https://www.iaisweb.org/file/61857/issues-paper-on-cyber-risk-to-the-insurance-sector>

sustanciales de datos, incluyendo datos personales. De igual forma, están conectadas a otras instituciones financieras a través de múltiples canales, incluyendo inversiones, captación de capital y emisión de deuda. Las aseguradoras realizan fusiones y adquisiciones y otros cambios en la estructura corporativa que pueden afectar a la ciberseguridad. Los aseguradores también externalizan una variedad de servicios, que pueden aumentar, o en algunos casos disminuir, la exposición al Ciberriesgo. Algunos ejemplos de debilidades en relación a la Ciberseguridad en la industria de seguros recientemente observadas por los miembros de la IAIS son las siguientes:

- Falta o incompleta visión general del paisaje informático: falta de percepción de la magnitud de flujo de datos y si los niveles de seguridad son acordes a este flujo.
- Proceso de control inadecuado en relación con los privilegios del usuario; usuarios con privilegios mayores a los permitidos y la falta de actualización cuando una cuenta deja de necesitar ciertos privilegios del sistema.
- Acceso incorrecto a cuentas de súper-usuario: acceso directo cuentas de “súper-usuario” (cuentas con privilegios mayores a un usuario normal) constituye un riesgo tanto por el uso inadecuado de estas cuentas, voluntario o involuntario, por parte del usuario, y su consiguiente impacto en todo el sistema, así como el riesgo que alguna de estas cuentas pudiese caer en manos de un hacker.

En cuanto a las consecuencias potencialmente adversas derivadas de los incidentes de ciberseguridad en el sector de seguros, se pueden incluir, por ejemplo: pérdida o corrupción de datos confidenciales de empresas, consumidores o terceros; interrupción del negocio; pérdida física (por ejemplo, daño al hardware); pérdidas financieras y daños a la reputación.

i. Pérdida de datos personales: la información almacenada por las aseguradoras incluye información personal de los asegurados, incluyendo datos sensibles de salud. Los registros privados de salud pueden ser particularmente valiosos en los mercados negros, como herramientas para la extorsión, el fraude y el robo de identidad, lo que hace que los aseguradores que tratan este tipo de información representen objetivos de alto valor para los criminales.

Desde la perspectiva de los titulares de pólizas comerciales, las aseguradoras pueden recopilar información confidencial de negocios que podría ser valiosa para espías corporativos y extranjeros. En el caso de los productos de ciberseguridad, por ejemplo, los aseguradores pueden poseer información sobre los controles de seguridad de la red de un asegurado y otra información de resistencia cibernética que podría ser valiosa para hackers y otros ciber delincuentes. Además, la pérdida de información confidencial podría perjudicar los derechos de propiedad intelectual de un asegurado.

ii. Interrupción del negocio: algunos ciberataques pueden provocar interrupciones en las operaciones comerciales normales, resultando en un daño significativo a la empresa con sustanciales costos de recuperación.

iii. Daños a la reputación: el negocio de seguros se basa en la confianza de los asegurados. Ellos confían que la información recolectada por los aseguradores estará protegida y que las reclamaciones se pagarán de manera oportuna. Si un asegurador sufre una

violación de sus datos, por la que su información confidencial se expone, esa confianza puede ser puesta en duda. De manera similar, si un asegurador sufriera un incidente de ciberseguridad que lo hiciera incapaz de hacer pagos puntuales de reclamaciones o que de otra manera interrumpiera sus operaciones, también se mina la confianza. El riesgo de reputación podría extenderse al sector de los seguros en su conjunto y afectar negativamente la confianza de los consumidores, asegurados, inversionistas, agencias clasificadoras y socios comerciales.

Contar con un gobierno corporativo eficaz y establecer un programa de gestión de riesgos, que incluya mejoras continuas, es una de los principales desafíos en cuanto al riesgo cibernético. Este desafío es parte de las mejores prácticas en cuanto a la ciber resiliencia en consistencia con los principios básicos de seguros (PBS).

Para ser eficaz, es necesario abordar la ciberseguridad a todos los niveles de una institución y, en lo que respecta, a acuerdos relevantes con terceros. Un programa eficaz de gestión del ciber riesgo incluye mejoras continuas de procesos y control; procedimientos de gestión de incidentes tales como respuesta y recuperación de desastres; políticas y procedimientos de red apropiados; administración y control riguroso de privilegios de usuario; guía de configuración segura; monitoreo de los procedimientos de trabajo en el hogar y las iniciativas continuas de concientización y educación para todo el personal.

Generalmente las mejores prácticas para la resistencia cibernética incluyen:

- Gobierno

Junto con el compromiso de la Junta Directiva y la Alta Dirección, un marco adecuado de resistencia cibernética contribuye a la mitigación del riesgo cibernético. Por ejemplo, la Alta Dirección debería incluir a un funcionario con acceso a la Junta, que fuera responsable de desarrollar e implementar el marco de la ciber resistencia (CISO).

- Identificación

Detectar aquellas funciones y procesos empresariales que deben protegerse contra ciberataques. Los activos de información, incluida la información personal sensible, y el acceso al sistema conexo deben ser parte del proceso de identificación. Las revisiones regulares y las actualizaciones son factores clave, ya que el riesgo cibernético está en constante evolución y pueden surgir "riesgos ocultos". Las entidades conectadas forman parte del cuadro completo. La importancia de los riesgos que plantean no es necesariamente proporcional a la importancia del servicio en particular. Por ejemplo, el bien conocido ataque cibernético contra el minorista Target²⁵ (USA) implicaba la entrada a través de un proveedor de servicios de ventilación.

²⁵ Robo de información de datos personales de más de 70 millones de clientes incluida cuentas bancarias y tarjetas de crédito.

- Protección

La resistencia puede ser proporcionada por el diseño. La protección integral implica la protección de las interconexiones y otros medios de acceso a las amenazas internas y externas a la institución.

Al diseñar la protección, se debe tener en cuenta el "factor humano". Por lo tanto, la formación también es una parte esencial de la red de seguridad contra el riesgo cibernético. Los controles deben estar en línea con las principales normas técnicas, ya que los sólidos controles de TI contribuyen a la protección.

- Detección

El monitoreo continuo y completo de la Ciberseguridad es esencial para detectar posibles incidentes cibernéticos. Llevar a cabo análisis de seguridad también ayuda a detectar y mitigar incidentes cibernéticos.

- Respuesta y recuperación

No siempre es posible detectar o prevenir incidentes cibernéticos antes de que sucedan, incluso con los mejores procesos instalados. Por esta razón, la planificación de respuesta a incidentes es de gran importancia. La reanudación de los servicios, si se interrumpen, se debe lograr dentro de un plazo razonable, dependiendo del impacto de los incidentes y de la importancia del servicio. La planificación de contingencia, el diseño y la integración empresarial, así como la integridad de los datos, también en el caso de los acuerdos de intercambio de datos, son factores clave para una rápida reanudación. Para que la planificación de contingencia sea efectiva, debe someterse a pruebas periódicas. Los pasos para prevenir el contagio pueden mitigar otros riesgos. Debería establecerse una política de divulgación para mejorar la comunicación en caso de crisis. Por último, pero no menos importante, la preparación forense es esencial para las investigaciones de inmersión profunda. Estos elementos deben ser considerados en la planificación de la continuidad del negocio.

- Pruebas

Los programas de pruebas, las evaluaciones de vulnerabilidad, las pruebas basadas en escenarios, las pruebas de penetración y las pruebas en equipo rojo²⁶ son las piedras angulares en la fase de pruebas. Las pruebas de Ciberseguridad deben incluirse cuando los sistemas se especifican, desarrollan e integran.

- Conciencia de la situación

La conciencia contribuye a la identificación de amenazas cibernéticas. En consecuencia, el establecimiento de un proceso de inteligencia de amenazas ayuda a mitigar el riesgo

²⁶ Grupo de personas autorizadas y organizadas para emular un potencial ataque de adversarios o capacidades de explotación contra la postura de seguridad de una empresa.

cibernético. En este sentido, los aseguradores deberían considerar participar en iniciativas establecidas de intercambio de información.

- Aprendiendo y evolucionando

Los aseguradores deben reevaluar continuamente la eficacia de la gestión de la Ciberseguridad. Las lecciones aprendidas de los eventos e incidentes cibernéticos contribuyen a mejorar la planificación. Los nuevos desarrollos en tecnología deben ser monitoreados. Aunque los PBS no abordan específicamente el riesgo cibernético y la resistencia cibernética, proporcionan una base general para que los supervisores aborden el sector de seguros con respecto a estos riesgos, exigiendo el manejo de riesgos significativos y controles internos relacionados.

Por otra parte, en 2018, reconociendo la constante evolución de las amenazas cibernéticas y los potenciales beneficios de la convergencia regulatoria, y tomando en consideración las indicaciones y conclusiones contenidas en el documento emitido el año 2016, la IAIS Financial Crime Task Force (FCTF), en consulta con los miembros de la IAIS, emitió un documento basado en principios y marcos de referencia para orientar a los supervisores en su tarea de supervisión de la gestión de riesgos de ciberseguridad en la industria de seguros. Para ellos consideró de diversas fuentes tales como: el NIST Cybersecurity Framework²⁷, publicado por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST); el G7 Fundamental Elements of Cyber Security for the Financial Sector (G7FE)²⁸; el G7²⁹ Fundamental Elements for Effective Assessment of Cybersecurity for the Financial Sector (G7FEA)³⁰ y en la Guidance on Cyber Resilience for Financial Market Infrastructures (CPMI-IOSCO Guidance)³¹. Los ocho elementos fundamentales de la función supervisora identificados por el G7son: Estrategia y marco de seguridad cibernética, Gobernanza, Evaluación de riesgos y control, Supervisión, Respuesta, Recuperación, Intercambio de información y Aprendizaje continuo.

G7FE 1 - Estrategia y marco de Ciberseguridad

- Las aseguradoras debe especificar como identifica, gestiona y reduce sus ciberriesgos en modo integrado y exhaustivo.
- El PBS 8.1 exige al supervisor que requiera a las aseguradoras que establezcan sistemas efectivos de gestión de riesgos y de controles internos, y que funcione dentro de ese marco.
- Dos riesgos se encuentran asociados a este principio, riesgos asociados a la capacidad de la aseguradora de operar sin problemas y el riesgo de pérdida asociado a la información sobre los asegurados que se encuentra en poder de la aseguradora.

²⁷ <https://www.nist.gov/cyberframework>

²⁸ https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf.

²⁹ El Grupo de los Siete (G7) es el foro de siete economías muy industrializadas: Canadá, Francia, Alemania, Italia, Japón, Reino Unido y Estados Unidos. Su objetivo es coordinar las finanzas, la economía, el empleo, la seguridad, la política comercial y muchas otras áreas.

³⁰ <http://www.g7.utoronto.ca/finance/171013-fundamentals.html>

³¹ <https://www.bis.org/cpmi/publ/d146.htm>

G7FE 2 - Gobernanza

- Las aseguradoras debe definir roles y responsabilidades del personal encargado de implementar, gestionar y supervisar la ejecución de la estrategia de ciberseguridad. Las aseguradoras deben proveer los recursos necesarios para la ejecución de la estrategia de ciberseguridad.
- El PBS 7 exige al supervisor que requiera a las aseguradoras que establezcan e implementen un marco de gobierno corporativo que brinde una administración y supervisión de la actividad de la aseguradora estable y prudente, y que reconozca y proteja de manera adecuada los intereses de los asegurados

G7FE 3 - Evaluación de riesgos y control

- Las aseguradoras deben identificar funciones, actividades y servicios (incluidos servicios tercerizados) sujetos a ciberriesgos, entender y evaluar los riesgos, e implementar los controles correspondientes. Estos últimos deben ser consistentes con el apetito de riesgo de la aseguradora.
- El PBS 8 exige al supervisor que requiera a las aseguradoras que cuenten con sistemas efectivos de gestión de riesgos y controles internos, incluyendo funciones eficaces en materia de gestión de riesgos.
- El PBS 19.12 exige al supervisor que requiera a las aseguradoras y a los intermediarios que tengan políticas y procedimientos para la protección y uso de información de los asegurados.

G7FE 4 - Monitoreo

- Las aseguradoras deben tener sistemas de monitoreo que permitan detectar ciberataques rápidamente. Las aseguradoras deben permanentemente evaluar la efectividad de los controles en existencia sobre los ciberriesgos, incluidos simulacros de ciberataques.
- El PBS 8.1 exige al supervisor que requiera a las aseguradoras que establezcan sistemas efectivos de gestión de riesgos, incluidos sistemas de alerta temprana y respuesta a la materialización de riesgos.
- El PBS 8.2 exige al supervisor que requiera a las aseguradoras que los sistemas de monitoreo estén sujetos periódicamente a pruebas de efectividad.

G7FEs 5 y 6 – Respuesta y recuperación

- Las aseguradoras deben responder a ciberataques oportunamente, entendiendo la seriedad del ataque, conteniendo sus efectos, notificando apropiadamente a quien corresponda, y coordinando y ejecutando una respuesta que les permita volver a operar normalmente.
- El PBS 8.1.2 establece los elementos necesarios que las aseguradoras deben considerar para poder responder a la materialización de riesgos en modo efectivo y proporcional al riesgo que se ha materializado.

G7FEs 7 – Intercambio de información

- Las aseguradoras deben informar sobre amenazas, vulnerabilidades, ataques, y respuestas a ataques con el objetivo de mejorar respuestas a ataques, limitar daños, concientizar y promover aprendizaje. Las aseguradoras deben informar internamente y externamente, incluyendo a autoridades públicas.
- El PBS 8.1.2 y el PBS 16.10 proveen el sustento normativo a los supervisores para exigir a las aseguradoras que informen sobre sus sistemas de gestión de ciberriesgos, así como también sobre la materialización de riesgos.
- Los PBS 3 y PBS 25 tratan el tema de intercambio de información entre supervisores, así como también la cooperación entre supervisores, incluyendo cooperación en la gestión de crisis internacionales.

G7FEs 8 – Aprendizaje continuo

- Las aseguradoras deben mantener sus sistemas de gestión de riesgos constantemente bajo revisión con el objetivo de mantenerlos actualizados con respecto a nuevos ciber riesgos y también con el objetivo de brindarles los recursos adecuados.
- El **PBS 16.10** exige al supervisor que requiera a las aseguradoras incorporen un circuito de retroalimentación que permita tomar medidas necesarias en forma oportuna como respuesta a los cambios surgidos en el propio perfil de riesgo.

2. OCDE: ORGANIZACIÓN PARA LA COOPERACIÓN Y DESARROLLO ECONÓMICO

La Organización para la Cooperación y Desarrollo Económico (OCDE) es una Organización intergubernamental que reúne a 34 países, que en su conjunto representan el 80% del PIB mundial, comprometidos con la economía de mercado y con sistemas políticos democráticos.

La OCDE permite a los países comparar, intercambiar experiencias en políticas públicas, identificar mejores prácticas, promover decisiones y recomendaciones. Mediante estas acciones y otros instrumentos legales, los países miembros acuerdan y se comprometen con estándares de alto nivel técnico y avanzada voluntad política. Para ello, el diálogo, el consenso, las evaluaciones y las revisiones entre pares conforman el núcleo del trabajo de la OCDE, la que constituye una de las fuentes más grandes y confiables a nivel internacional en los ámbitos de las estadísticas y de la información económica y social.

En septiembre de 2015 la OCDE publicó el documento *Recommendation on Digital Security Risk Management for Economic and Social Prosperity*³² con el fin de brindar una guía en cuanto a estrategias nacionales sobre la gestión del riesgo de seguridad digital, con el objetivo de optimizar los beneficios económicos y sociales que se esperan del proceso de digitalización.

Dentro de las principales consecuencias de una inadecuada gestión de riesgos en entornos digitales, la OCDE destaca:

- Interrupción de las operaciones.
- Pérdidas financieras directas.
- Daño reputacional.
- Pérdida de competitividad.
- Pérdida de la confianza de los clientes.

La recomendación para los países, miembros y no miembros, es implementar los principios a todos los niveles de gobierno y organizaciones públicas, así como adoptar una estrategia nacional para el manejo de riesgos de seguridad digital descrita en el documento. En cuanto a los principios relacionados al manejo de riesgos de seguridad, estos son:

Principios Generales

1. **Conciencia, habilidades y empoderamiento:** todas las partes interesadas deben comprender el riesgo de seguridad digital y cómo gestionarlo. Es fundamental tomar conciencia sobre las amenazas y vulnerabilidades digitales y su impacto sobre el cumplimiento de los objetivos económicos y sociales.
2. **Responsabilidad:** todas las partes interesadas deben asumir la responsabilidad de la gestión del riesgo de seguridad digital. Es necesario actuar responsablemente y asumir las consecuencias de acuerdo con los roles, el contexto y la capacidad otorgada para responder ante los riesgos digitales.

³² <https://www.oecd.org/governance/digital-security-risk-management-for-economic-and-social-prosperity-9789264245471-en.htm>

3. **Derechos humanos y valores fundamentales:** todas las partes interesadas deben gestionar el riesgo de seguridad digital de manera transparente y coherente con los derechos humanos y los valores fundamentales. Se deben respetar los derechos a la libre expresión, el libre flujo de la información, la confidencialidad de la información y las comunicaciones, así como la protección de la privacidad de las personas.
4. **Cooperación:** todas las partes interesadas deben cooperar, incluida la cooperación transfronteriza. La interconectividad digital crea interdependencia entre gobiernos, organizaciones e individuos.

Principios Operacionales

5. **Evaluación de riesgos y ciclo de tratamiento:** los líderes y los responsables de la toma de decisiones deben garantizar que el riesgo a la seguridad digital se trata sobre la base de una evaluación de riesgos continua. Es necesario evaluar tanto las amenazas como las vulnerabilidades que afectan el cumplimiento de los objetivos económicos y sociales.
6. **Medidas de seguridad:** los líderes y los responsables de la toma de decisiones deben garantizar que las medidas de seguridad sean adecuadas y estén en consonancia con el riesgo. Dentro de los procesos de selección de controles, es necesario considerar diferentes tipos de medidas incluidas las físicas, las digitales, las relativas a las personas, los procesos o la tecnología.
7. **Innovación:** los líderes y los tomadores de decisiones deben garantizar que se considere la innovación. La innovación debe estar presente en el diseño operacional y económico de las organizaciones
8. **Preparación y continuidad:** los líderes y los tomadores de decisiones deben garantizar que se adopte un plan de preparación y continuidad para garantizar la continuidad y efectiva respuesta ante la ocurrencia de riesgos a la seguridad digital. Los planes deben contemplar los niveles de escalamiento necesarios de acuerdo con la magnitud de los eventos.

Adicionalmente, la recomendación de la OCDE adjunta un documento complementario, en anexo, el cual describe un proceso de gestión de riesgo digital en las organizaciones.

El año 2017, la OCDE emitió dos documentos relacionados con el papel de las coberturas de los seguros contra incidentes cibernéticos. El primero, en mayo de 2017, titulado **Supporting an effective cyber insurance market**³³, es un reporte realizado para la presidencia del G7 en el cual se describe el entorno del mercado de seguros Ciber y los principales desafíos en cuanto a su desarrollo.

En base al reporte anterior, la OCDE publicó un nuevo reporte **Enhancing the Role of Insurance in Cyber Risk Management**³⁴, el cual ofrece una serie de recomendaciones de políticas destinadas a mejorar la contribución del mercado de los seguros cibernéticos a la gestión de

³³ <http://www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf>

³⁴ https://www.oecd-ilibrary.org/finance-and-investment/enhancing-the-role-of-insurance-in-cyber-risk-management_9789264282148-en

este riesgo cada vez más frecuente. El informe examina el estado actual del mercado, en función de los aportes sustanciales de las compañías de seguros, corredores y reguladores que participan directamente en su desarrollo, y los obstáculos que impiden que el mercado alcance su máximo potencial.

En febrero 2019, la OCDE publicó el documento **Policies for the protection of critical information infrastructure: Ten years later**³⁵, el cual hace una revisión del documento del 2008 **Recommendation on the Protection of Critical Information Infrastructures**³⁶ (“**CIIP Recommendation**”). El documento incorpora los resultados y análisis del cuestionario que circuló entre los miembros de la OCDE y los participantes en el Comité de Política de Economía Digital. El cuestionario fue respondido por dieciocho países, representando una variedad de regiones, culturas, tamaños y madurez digital. Este documento proporciona un análisis de estas respuestas y sugerencias para guiar la actualización del documento de recomendaciones publicado en 2008.

En paralelo al documento anterior, en diciembre de 2019, la OCDE emitió el documento **Recommendation on Digital Security of Critical Activities**³⁷ el cual reemplazó el documento del año 2008. Este documento toma como base el documento del 2008, y además se basa en el reporte descriptivo **Recommendation on Digital Security Risk Management for Economic and Social Prosperity (2015)** y el documento **Policies for the protection of critical information infrastructure: Ten years later (2019)**. Entre las principales recomendaciones contenidas se encuentran:

- Reforzar la coordinación internacional.
- Establecer ciclos de supervisión y monitoreo basados en la evidencia.
- **Gobernanza** - establecer un marco de tratamiento y evaluación de riesgos de seguridad digital.
- **Protección** - implementación de medidas de seguridad adecuadas para reducir los riesgos de seguridad digital a funciones críticas.
- **Defensa** - implementar procesos y medidas para defenderse y responder a los incidentes.
- **Resiliencia** - adoptar medidas de preparación adecuadas para garantizar la continuidad de las funciones críticas.
- Desarrollar asociaciones para el desarrollo y la implementación de políticas.
- Reforzar la cooperación operativa.
- Establecer condiciones de confianza para asociaciones sostenibles.
- Proteger la confidencialidad de los riesgos y la información relacionada con la gestión de riesgos compartida por los operadores con el gobierno para no exponer innecesariamente la reputación y el interés comercial del operador.
- Desarrollar / Fomentar una capacidad de respuesta a incidentes.

³⁵ https://www.oecd-ilibrary.org/science-and-technology/policies-for-the-protection-of-critical-information-infrastructure_ebf55c54-en

³⁶ <https://www.oecd.org/sti/ieconomy/ciip.htm>

³⁷ <https://www.oecd.org/sti/ieconomy/digital-security-of-critical-activities.htm>

- Facilitar la cooperación entre CERTs / CSIRTs³⁸ y operadores.
- Compartir con operadores y otros actores, datos estadísticos agregados de manera apropiada de los informes de incidentes y trabajo a nivel internacional para asegurar la comparabilidad internacional de dichas estadísticas.
- Alentar la adopción de esquemas de divulgación de vulnerabilidad, responsables y coordinados.

³⁸ Equipos de respuesta a emergencias informáticas (CERT por su sigla en inglés), o también llamado equipo de respuesta a incidentes de seguridad informática (CSIRT por su sigla en inglés), se refiere a grupo de expertos que manejan incidentes de seguridad informática.

ANEXO B: MARCO NORMATIVO EXTRANJERO

1. AUSTRALIA, AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY (APRA)

El APRA es una autoridad estatutaria independiente que supervisa las instituciones de banca, seguros y pensiones, promoviendo la estabilidad del sistema financiero en Australia. Opera bajo las leyes determinadas por el Parlamento Australiano, que la faculta con poderes para el establecimiento de Estándares y Guías de Prácticas Prudenciales que tienen como objetivo mantener la seguridad y solidez de las instituciones que regula APRA.

Al respecto, en el Estándar Prudencial **CPS 220**³⁹ sobre Gestión de Riesgo se destaca lo siguiente:

Marco de Gestión de Riesgos

Establece que una compañía debe mantener un Marco de Gestión de Riesgos que le permita el desarrollo e implementación apropiado de estrategias, políticas, procedimientos y controles para administrar diferentes tipos de riesgos materiales, entre los cuales se incluye el Riesgo Operacional, y provee al directorio de una amplia y completa visión de los riesgos materiales de la compañía.

Relativo a los elementos constitutivos del Marco, establece que éste debe incluir aspectos tales como:

- Una declaración de apetito de riesgo apropiada, clara y concisa que incluya todos los riesgos materiales de la compañía. El directorio es responsable de la aprobación y establecimiento del apetito por riesgo de la compañía.
- Una estrategia de gestión de riesgo documentada, aprobada por el directorio, que describa los riesgos materiales declarados por la compañía, la relación entre el directorio y la administración en relación al Marco de Gestión de Riesgo y que busque garantizar que todas las personas dentro de la compañía lo conozcan, así como la relación con su función, inculcando de esa manera una cultura de riesgos adecuada en toda la compañía.
- Un Plan de Negocios de la compañía escrito y aprobado por el directorio que establezca:
 - a. el enfoque de implementación de los objetivos estratégicos.
 - b. una duración de al menos tres años y revisión anual, cuyos resultados deben informarse al directorio.

³⁹ <https://www.legislation.gov.au/Details/F2019L00669>

- c. Identificación y consideración de los riesgos materiales asociados a los objetivos estratégicos y al plan de negocios y gestionarlos a través del Marco de Gestión de Riesgos.
- Políticas y procedimientos que respalden roles, responsabilidades y estructuras de informes formales claramente definidos y documentados para la gestión de riesgos materiales en toda la compañía.
 - Función de Gestión de Riesgos, que como mínimo; sea responsable de apoyar al directorio y sus comités a mantener el Marco de Gestión de Riesgos; apropiado al tamaño y complejidad de la compañía; independiente; que cuente con autoridad y línea directa suficientes para el reporte al directorio, Comités y Administración.
 - Un sistema de gestión de información adecuado bajo situaciones normales o de estrés para la medición, evaluación y reporte de todos los riesgos materiales de la compañía.
 - Un proceso de revisión que garantice la efectividad del Marco de Gestión de Riesgos.
 - Requerimiento de notificación al regulador tan pronto y en no más de 10 días después de tomar conocimiento de:
 - a. Incumplimiento o desviación significativa del marco de gestión de riesgo;
 - b. Que el Marco de Gestión de Riesgo no abordó adecuadamente un riesgo material;
 - c. Cualquier cambio material o posibles cambios materiales en el tamaño, mix de negocios y complejidad de la compañía;
 - d. Que, cuando una compañía regulada, realice negocios en jurisdicciones extranjeras, su derecho de desarrollar negocios ha sido afectado materialmente por las leyes o normas de tales jurisdicciones y/o su derecho ha cesado.

Por su parte, la Guía Práctica Prudencial **CPG 220**⁴⁰ tiene como objetivo ayudar a las instituciones reguladas por el APRA a cumplir con la Norma Prudencial de Gestión de Riesgos CPS 220 y, de manera más general, esbozar prácticas prudentes en relación con la gestión de riesgos.

⁴⁰ <https://www.apra.gov.au/sites/default/files/CPG%20220%20April%202018.pdf>

Establece que la Gobernanza de Riesgo de una compañía es una parte integral de su Marco de Gestión de Riesgo, cuya estructura dependerá del tamaño, mix de negocios y complejidad de la compañía.

Al respecto, el objetivo de esta Guía Práctica es fomentar un modelo efectivo de gobernanza de riesgos que contenga controles y equilibrios para respaldar la inclusión adecuada de la gestión de riesgos en todas las compañías reguladas por el APRA. Uno de los modelos ampliamente utilizado y que proporciona un marco eficaz para la gobernanza del riesgo es el modelo de las tres líneas de defensa. Este modelo proporciona responsabilidades definidas de propiedad del riesgo con supervisión y aseguramiento funcionalmente independientes

Primera Línea de Defensa

La primera línea de defensa comprende la línea de negocios que tiene la propiedad de los riesgos. Es responsable de la toma de decisiones de gestión de riesgos cotidiana, que comprende la identificación, evaluación, mitigación, monitoreo y gestión de riesgos. El APRA espera que los roles y responsabilidades de los propietarios de los riesgos se definan claramente y, cuando corresponda, se incorporen a las revisiones de desempeño.

La primera línea de defensa es responsable de:

- La implementación efectiva del Marco de Gestión de Riesgo, incluido la presentación de informes y el escalamiento de información relevante a la alta gerencia, la segunda línea de defensa y a los comités o directorio, según sea necesario;
- Gestionar el Riesgo de forma coherente con el Marco de Gestión de Riesgo.

La administración garantizaría que la propiedad del riesgo esté claramente definida y que el marco de gestión de riesgo se implemente de manera efectiva y apoye la toma de decisiones. Esto normalmente incluiría procedimientos de notificación, escalada y monitoreo que sean apropiados para la gestión de diferentes categorías de riesgo.

Segunda Línea de Defensa

La segunda línea de defensa comprende las funciones especializadas de gestión de riesgos que son funcionalmente independientes de la primera línea de defensa. La segunda línea de defensa apoya al directorio y sus comités a través de:

- Desarrollar políticas, sistemas y procesos de gestión de riesgos para facilitar un enfoque coherente para la identificación, evaluación y gestión de riesgos;

- Proporcionar asesoramiento especializado y capacitación a la Junta, los comités de la junta y la primera línea de defensa en asuntos relacionados con el riesgo;
- Revisión objetiva y desafíos:
 - i. La implementación consistente y efectiva del Marco de Gestión de Riesgos en toda la compañía regulada por APRA;
 - ii. Los datos y la información obtenidos como parte del Marco de Gestión de Riesgos que se utilizan en los procesos de toma de decisiones dentro del negocio, en particular la integridad y adecuación de la identificación y análisis de riesgos, la efectividad continua de los controles de riesgos y la priorización y gestión de planes de acción; y
 - iii. Supervisión del nivel de riesgo en la compañía y su relación con el apetito por el riesgo, y cualquier informe necesario y escalamiento al directorio o sus comités.

Para lograr eficacia, las funciones de gestión de riesgos deben:

- Contar con personal experimentado con conocimiento técnico relevante que facilite el desarrollo, la revisión continua y la validación del Marco de Gestión de Riesgos; y
- Adecuada antigüedad y autoridad, con acceso a los comités de directorio.

Las compañías más pequeñas y menos complejas reguladas por el APRA generalmente combinan las funciones de gestión de riesgos con otras funciones. Al respecto, el APRA espera que se tomen las precauciones adecuadas para garantizar que se mantenga la objetividad de la función de gestión de riesgos y que se identifiquen y gestionen adecuadamente los conflictos de intereses.

Tercera Línea de Defensa

La tercera línea de defensa comprende funciones que proporcionan al directorio y su Comités de:

- Al menos anualmente, aseguramiento independiente del cumplimiento del Marco de Gestión de Riesgos y de su funcionamiento efectivo, y
- Al menos cada tres años, una revisión exhaustiva de la idoneidad, efectividad y adecuación del Marco de Gestión de Riesgos.

La aplicación de la tercera línea de defensa variará según el tamaño, mix de negocios y complejidad de la compañía. La función de aseguramiento independiente podría, por

ejemplo, incluir auditoría interna/externa o una combinación de ambas. Una consideración clave es la independencia apropiada, experiencia y conocimiento técnico.

Por su parte, el **Prudential Standard CPS 234 Information Security**⁴¹ tiene como objetivo garantizar que una entidad regulada por APRA, entre ellas las compañías de seguros Generales, Vida y Salud ⁴², tome medidas para ser resiliente frente los incidentes de seguridad de la información (incluidos los ataques cibernéticos), manteniendo una capacidad de seguridad de la información acorde con las vulnerabilidades y amenazas de la seguridad de la información. Esto con el objetivo de *“minimizar la probabilidad y el impacto de los incidentes de seguridad de la información en la confidencialidad, integridad o disponibilidad de los activos de información, incluidos los activos de información administrados por partes relacionadas o terceros”*. La Junta de directorio de una entidad regulada bajo el APRA es el responsable último de garantizar la seguridad de la información.

En cuanto a los requerimientos clave que determina el estándar prudencial, aplicable a las entidades bajo su supervisión, son los siguientes:

- Definir claramente las funciones/roles y responsabilidades relacionadas con la seguridad de la información de la Junta de Directorio, la alta gerencia, los cuerpos directivos (comités) y responsabilidades individuales;
- Mantener una capacidad de seguridad de la información acorde con el tamaño y el alcance de las amenazas a sus activos de información, y que permita el funcionamiento continuo y sano/sólido de la entidad;
- Implementar controles para proteger sus activos de información acordes con la criticidad y la sensibilidad de esos activos, y llevar a cabo pruebas y garantías sistemáticas con respecto a la efectividad de esos controles; y
- Notificar a APRA de los incidentes de seguridad de información de **carácter material**.

La norma instruye respecto a los siguientes puntos respecto los deberes de las entidades reguladas por APRA:

a) Roles y Responsabilidades

- a. Definición de funciones y responsabilidades
- b. La Junta de Directorio es el último responsable de la seguridad de la información de la entidad.

b) Capacidad de la Seguridad de la Información:

- a. Los sistemas de seguridad deben ser acordes al tamaño y amenazas respecto a sus activos de información.
- b. Cuando los activos son administrados por un tercero la entidad debe evaluar la capacidad de seguridad de la información de esa parte, de acuerdo con las

⁴¹ https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf

⁴² Facultada para aplicar a todas las Compañías de seguros Generales por la Subsección 32(1) de la *Insurance Act 1973*, Compañías de seguros de Vida por la Subsección 230A(1) de la *Life Insurance Act 1995* y Seguros de Salud Privados por la Subsección 92(1) de la *Private Health Insurance 2015*.

posibles consecuencias de un incidente de seguridad de la información que afecte a esos activos.

- c. Mantener activamente su capacidad de seguridad de la información con respecto a los cambios en las vulnerabilidades y amenazas, incluidas aquellas resultantes de los cambios en los activos de información o su entorno empresarial.

c) Marco de Políticas

- a. Mantener un marco de políticas de seguridad de la información acorde con su exposición a vulnerabilidades y amenazas.
- b. El marco de la política de seguridad de la información debe proporcionar orientación/direccionamientos/directrices sobre las responsabilidades de todas las partes que tienen la obligación de mantener la seguridad de la información.

d) Identificación y clasificación de activos de información

- a. Deberá clasificar sus activos de información, incluidos aquellos gestionados por partes relacionadas y terceros, por criticidad y sensibilidad. Esta clasificación debe reflejar el grado en que un incidente de seguridad de la información que afecte a un activo de información tiene el potencial de afectar, financiera o no, a la entidad o los intereses de los depositantes, asegurados, beneficiarios u otros clientes.

e) Implementación de Controles

- a. Deberá tener controles de seguridad de la información para proteger sus activos de información, incluidos aquellos administrados por partes relacionadas y terceros, que se implementan de manera oportuna y que son proporcionales a:
 - i. vulnerabilidades y amenazas a los activos de información;
 - ii. la criticidad y sensibilidad de los activos de información;
 - iii. la etapa en que los activos de información se encuentran dentro de su ciclo de vida;
 - iv. las posibles consecuencias de un incidente de seguridad de la información.
- b. Cuando los activos de información de una entidad regulada por APRA son administrados por una parte relacionada o un tercero, la entidad regulada por APRA debe evaluar el diseño de los controles de seguridad de la información de esa parte que protegen los activos de información de la entidad regulada por APRA.

f) Manejo/Administración de incidentes

- a. Deberá contar con mecanismos sólidos para detectar y responder a los incidentes de seguridad de la información de manera oportuna.
- b. Mantener planes para responder a los incidentes de seguridad de la información que la entidad considera plausiblemente ocurrir (planes de respuesta de

seguridad de la información). Los planes de respuesta de seguridad de la información deben incluir los mecanismos establecidos para:

- i. gestionar todas las etapas relevantes de un incidente, desde la detección hasta la revisión posterior al incidente; y
 - ii. la escalada⁴³ y la notificación de incidentes de seguridad de la información a la Junta de Directores, a otros cuerpos directivos/comités e individuos responsables de la gestión y supervisión de incidentes de seguridad de la información, según corresponda.
- c. Revisar y Probar anualmente sus planes de respuesta de seguridad de la información para garantizar que sigan siendo efectivos y adecuados para su propósito.

g) Pruebas y control de Efectividad

- a. Deberá probar la efectividad de sus controles de seguridad de la información a través de un programa de prueba sistemático. La naturaleza y la frecuencia de las pruebas sistemáticas deben ser acordes con:
 - i. la velocidad a la que cambian las vulnerabilidades y amenazas;
 - ii. la criticidad y sensibilidad del activo de información;
 - iii. las consecuencias de un incidente de seguridad de la información;
 - iv. los riesgos asociados con la exposición a entornos en los que la entidad regulada por APRA no puede hacer cumplir sus políticas de seguridad de la información;
 - v. La materialidad y frecuencia del cambio a los activos de información.
- b. Cuando los activos de información son administrados por una parte relacionada o un tercero, y la entidad depende de las pruebas de control de seguridad de la información de esa parte, la entidad debe evaluar si la naturaleza y frecuencia de la prueba de los controles con respecto a esos activos de información es proporcional a los párrafos (a) y (e).
- c. Deberá escalar e informar a la Junta de Directorio o a la alta gerencia cualquier resultado de prueba que identifique deficiencias en el control de seguridad de la información que no puedan remediarse de manera oportuna.
- d. Deberá garantizar que las pruebas sean realizadas por especialistas debidamente capacitados y funcionalmente independientes.
- e. Deberá revisar la suficiencia del programa de pruebas al menos una vez al año o cuando haya un cambio sustancial en los activos de información o el entorno empresarial.

h) Auditoría Interna

- a. Las actividades de auditoría interna deberán incluir una revisión del diseño y la efectividad operativa de los controles de seguridad de la información, incluidos

⁴³ Transferencia del incidente hacia un nivel superior dependiendo de la complejidad del incidente, ejemplo de un usuario puede resolver problemas comunes, pero si el incidente es más complejo deberá pasar a un nivel superior.

los mantenidos por partes relacionadas y terceros (aseguramiento de/garantizar control de seguridad de la información).

- b. Deberá garantizar que la garantía de control de seguridad de la información sea proporcionada por personal debidamente capacitado para proporcionar dicha garantía.
- c. La función de auditoría interna deberá evaluar el aseguramiento del control de seguridad de la información proporcionada por una parte relacionada o un tercero cuando:
 - i. un incidente de seguridad de la información que afecte a los activos de información tenga el potencial de afectar materialmente, financieramente o no, a la entidad o los intereses de los depositantes, asegurados, beneficiarios u otros clientes; y
 - ii. la auditoría interna pretenda basarse en el aseguramiento del control de seguridad de la información proporcionada por la parte relacionada o un tercero.

i) Notificación a APRA

- a. Deberá notificar a APRA tan pronto como sea posible y, en cualquier caso, no más tarde de 72 horas, después de tener conocimiento de un incidente de seguridad de la información que:
 - i. afectado materialmente, o tenía el potencial de afectar materialmente, financieramente o no, a la entidad o los intereses de los depositantes, asegurados, beneficiarios u otros clientes; o
 - ii. ha sido notificado a otros reguladores, ya sea en Australia u otras jurisdicciones.
- b. Deberá notificar a APRA tan pronto como sea posible y, en cualquier caso, no más tarde de 10 días hábiles, después de que tenga conocimiento de una debilidad de control de seguridad de la información material que la entidad espere que no podrá remediar de manera oportuna.

Este estándar prudencial entró en vigencia en julio de 2019 y se aplica a todas las entidades reguladas por APRA. No obstante, lo anterior, APRA puede ajustar o excluir un requisito prudencial específico en esta norma en relación con una entidad regulada por ella.

2. REINO UNIDO, FINANCIAL CONDUCT AUTHORITY (FCA)

La **Financial Conduct Authority (FCA)** es la entidad que regula la conducta de 58.000 empresas de servicios financieros y de los mercados financieros en el Reino Unido y el regulador prudencial de más de 18 000 de esas empresas. Entre las entidades reguladas se encuentran aseguradoras generales, aseguradoras de vida, proveedores de pensiones e intermediarios de seguros. A su vez la **Prudential Regulation Authority (PRA)** es el regulador prudencial de los bancos, entidades y cajas de ahorros, cooperativas de crédito, compañías de seguros y determinadas empresas de inversión. Ambos reguladores están bajo el alero del Bank of England (**BOE**) quien es el regulador máximo del mercado financiero.

Mientras el **FCA** es la responsable de proteger a los consumidores, mediante la promoción de una competencia efectiva y la regulación de todas las empresas de servicios financieros, el **PRA** es responsable de que los bancos y las aseguradoras cuenten con el suficiente capital y liquidez, siendo este último, para el caso del mercado asegurador, el responsable del cumplimiento y supervisión de la solvencia y requerimiento de capital del mercado (**Solvencia II**). Dada las distintas responsabilidades de cada regulador, los riesgos cibernéticos son abordados con distintos enfoques por parte cada uno de ellos.

FCA SYSC 13: Operational Risk - Systems and Controls for Insurers⁴⁴

Esta guía establece que las compañías deberían tomar las acciones necesarias en el entendimiento de los tipos de riesgo operacional relevantes y sobre las pérdidas operacionales derivadas de estos riesgos. Lo anterior, debería incluir las fuentes de riesgos operacionales, tales como personas, procesos y sistemas y eventos externos.

Requerimientos de Notificación

Según lo establecido en el principio N°11, las compañías deben notificar inmediatamente cualquier evento de riesgo operacional.

Respecto los eventos de riesgo operacional que se espera se notifiquen⁴⁵, se encuentran los siguientes:

- Cualquier evento de riesgo operacional significativo identificado por la compañía.
- La puesta en marcha de un plan de continuidad de negocios.
- Cambios en la organización de la compañía, infraestructura o entorno operativo

⁴⁴ <https://www.handbook.fca.org.uk/handbook/SYSC/13.pdf>

⁴⁵ El SUP 15.3.9 establece que el periodo de notificación al regulador dependerá del evento, aunque el regulador espera que las compañías notifiquen eventos relevantes en una etapa temprana, antes de realizar cualquier compromiso interno o externo.

Términos en la gestión de riesgo

La cultura de riesgo de la compañía debe abarcar conciencia general y comportamiento de sus empleados al riesgo y a la gestión del riesgo dentro de la compañía.

La exposición operacional se refiere al grado de riesgo operacional que enfrenta una compañía y se expresa generalmente en la probabilidad e impacto de un evento particular de pérdida operativa asociado a fraudes, daño de activos físicos, etc.

El perfil de riesgo de una compañía describe la tipología de riesgos operacionales que ésta enfrenta. Incluidos aquellos riesgos operacionales que pueden tener un efecto adverso en la calidad de servicio a clientes y su exposición a estos riesgos.

Recursos Humanos

Una compañía debe mantener apropiados sistemas y controles en la gestión del riesgo operacional, el que puede ser originado por los empleados. Considerando al menos:

- Cultura de riesgo operacional y cualquier cambio en las prácticas de administración de recursos humanos.
- Política de remuneraciones expone a la compañía a incumplimientos regulatorios.
- Capacitaciones inadecuadas en atención de clientes.
- Cumplimiento regulatorio relacionados al bienestar y seguridad de los empleados.
- Continuidad operacional en periodos de baja disponibilidad de recursos humanos.

Responsabilidades de los empleados

Las compañías se deben asegurar que sus funcionarios son capaces de desempeñar y estar conscientes de sus responsabilidades en la administración del riesgo operacional, lo que incluye establecer y mantener:

- Apropiada segregación de funciones, supervisión del desempeño de sus responsabilidades.
- Apropiada segregación y supervisión de funciones.
- Adecuados procesos de selección y seguimiento.
- Políticas, procedimientos y manuales de sistemas claros y efectivamente comunicados y disponibles para los empleados.
- Procesos de capacitación adecuados.
- Medidas disciplinarias, procesos de desvinculación y políticas apropiadas.

Procesos y sistemas

Las compañías deben establecer y mantener apropiados sistemas de controles en la gestión de riesgo operacional, considerando lo siguiente:

- Importancia y complejidad de los procesos y sistemas utilizados en las operaciones.
- Controles preventivos y de identificación de fallas.
- Procesos y sistemas permiten a la compañía el cumplimiento regulatorio.
- Planes de continuidad operacional.
- Indicadores de monitorio de riesgos de procesos y sistemas.

Sistemas de Tecnología de Información

Los Sistemas de Tecnologías de Información, IT, incluyen los sistemas computacionales e infraestructura requerida para los procesos de automatización. Procesos que pueden reducir la exposición de las compañías a los riesgos operacionales ocasionados por las personas, pero incrementan los riesgos de dependencia en los sistemas.

En la implementación y mantenimiento de un apropiado sistema de control en la gestión del riesgo operacional IT, las compañías deben considerar:

- La organización y estructura de informes de operaciones tecnológicas, incluida la supervisión de la alta dirección.
- Alineamiento de los requerimientos tecnológicos con la estrategia de negocios.
- Apropiados sistemas de compras, desarrollo y mantenimiento de actividades.
- Apropiadas actividades de soporte operacional de los sistemas IT.

Seguridad de la Información

La seguridad de la información se refiere a fallas en los procesos de información o en la seguridad de los sistemas, las que puedan resultar en pérdidas operacionales significativas.

En la gestión de este tipo de riesgo, las compañías deben establecer y mantener sistemas y controles apropiados, asegurando:

- **Confidencialidad:** Acceso a la información sólo por personal o sistemas autorizados.
- **Integridad:** Asegurando la exactitud y completitud de la información y su procesamiento.
- **Disponibilidad y autenticación:** Resguardando el acceso, autorizado, a la información cuando esta sea requerida.

- **Responsabilidad:** Asegurar que las personas o sistemas que procesan la información no nieguen sus acciones.

El establecimiento de estándares tales como la ISO⁴⁶ 27002, contribuyen en el cumplimiento de lo anteriormente expuesto. Las compañías deben asegurar la adecuación de los sistemas y controles en la protección del procesamiento y seguridad de la información.

Localización Geográfica

El mantenimiento de sistemas y procesos operativos en ubicaciones geográficas separadas, puede alterar el perfil de riesgo operacional de las compañías. Por lo anterior, las compañías deben entender los efectos de las diferencias en los procesos y sistemas en cada ubicación, en particular en diferentes países, con especial énfasis en:

- Ambiente operativo de negocios de cada país.
- Regulación local y requerimientos de protección de datos y transferencia,
- En qué medida la regulación extranjera puede restringir el cumplimiento regulatorio, acceso a información del regulador local y auditorías.
- Oportunidad del flujo de información y compatibilidad de las estructuras de gestión de riesgos.

Eventos externos y otros cambios

La exposición a riesgo operacional se incrementa en periodos de cambios organizacionales significativos. Antes, durante y después de estos cambios la compañía debe monitorear sus efectos, considerando:

- Funcionarios sin capacitación, desmotivados o una pérdida significativa de ellos durante el periodo de cambio.
- Recursos humanos inadecuados o funcionarios inexpertos que realizan actividades comerciales de rutina debido a la priorización de recursos para el programa o proyecto.
- Inestabilidad de procesos y sistemas debido a integraciones fallidas.
- Procesos inadecuados luego de un proceso de reingeniería de negocios.

La implementación de sistemas y controles adecuados en la gestión de este tipo de riesgos que involucran cambios esperados, asegurando:

- Adecuada organización y estructura de informes de gestión de cambios, incluido la adecuada supervisión de la alta dirección.
- Adecuada estrategia de comunicación de cambios de los sistemas y controles a los empleados.

⁴⁶ International Organization for Standardization

- Adecuados procesos y sistemas de gestión del cambio.

La compañía debe considerar la probabilidad e impacto de una interrupción de la continuidad de sus operaciones producto de eventos inesperados, incluyendo lo siguiente:

- Pérdida o falla de recursos internos o externos (empleados, sistemas y otros activos).
- Pérdida o corrupción de información
- Eventos externos (vandalismo, guerra, etc.)

La compañía debe documentar su estrategia de mantenimiento de continuidad operativa y sus planes de comunicación y testeos regulares de la efectividad de la estrategia definida, estableciendo:

- Plan de continuidad de negocios
- Procedimiento de implementación de los planes de continuidad de negocios
- Procesos de validación de la integridad de la información afectada por la interrupción.
- Procesos de revisión y actualización de planes producto de cambios en el perfil de riesgo operacional producidos por la interrupción y los identificados por testeos internos.

Por su parte, el **FCA** aborda el riesgo cibernético desde el punto de vista conductual poniendo el foco en la Ciber Resiliencia. Según la guía **Buena Ciberseguridad - los cimientos**⁴⁷, de junio de 2017, son ocho las prácticas efectivas en manejo de Ciberseguridad, las cuales son; Manejo del Riesgo, Encriptación de datos sensibles, Recuperación de Desastres, Red y seguridad informática, Credenciales de usuario y dispositivo, Conciencia y educación respecto a riesgos cibernéticos, Acreditación, e Intercambio de información. Posteriormente, en junio de 2018, se emite la infografía llamada **Seguridad de la red - lo básico**⁴⁸, la cual tiene las preguntas que debiese hacerse una institución respecto a puntos tales como; Control de acceso, Acceso inalámbrico seguro, prevención de contenido malicioso, monitoreo de las redes propias, Ejecutar análisis regulares para comprobar las vulnerabilidades, segregación de redes propias y el uso de Firewalls.

En línea con las recomendaciones en manejo de Ciberseguridad, en julio de 2018, la **FCA** emite la **FG 16/5 Guía para empresas que subcontratan a la "nube" y otros servicios de TI de terceros**⁴⁹ cuyo propósito es aclarar los requisitos de las empresas fiscalizadas, con excepción de los bancos, que tienen su propia guía, cuando subcontratan la "nube" y otros servicios de TI de terceros.

⁴⁷ <https://www.fca.org.uk/publication/documents/cyber-security-infographic.pdf>

⁴⁸ <https://www.fca.org.uk/publication/systems-information/network-security-basics.pdf>

⁴⁹ <https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf>

En noviembre de 2018, la FCA publicó el resultado y análisis de la encuesta **Cyber and Technology Resilience**⁵⁰ realizada, entre los años 2017 y 2018, a empresas de la industria financiera. Esta encuesta estaba entendimiento de la capacidad de Resiliencia de la industria y analizó áreas clave como la gobernanza, la gestión de cambios, la gestión de riesgos de terceros y las defensas cibernéticas efectivas. Algunos de los Output de esta encuesta fueron los siguientes:

- Se estimó en un 18% la proporción de los ciberataques del total de incidentes operacionales, con una tendencia al alza en la cantidad de estos. Otro punto fue que la irrupción de las tecnologías en el sector financiero se ha vuelto cada vez más frecuente y que el número de incidentes asociados a estas tecnologías se incrementó en un 187% entre el 2017 y 2018.
- En cuanto a la gobernanza, un 90%, tanto para tecnología como para Ciber, de los encuestados se consideraron que tienen fuertes controles de gobernabilidad, no obstante, algunas empresas identificaron carencias en cuanto al conocimiento de tecnologías y Ciber por parte del directorio.
- La mayoría de las empresas califican la resistencia cibernética como su principal preocupación. Las respuestas de las empresas resaltan las debilidades cibernéticas en 3 áreas: personas, administración de terceros y protección de sus activos clave.
- En cuanto al intercambio de información se percibe que hay margen de mejora. No obstante, existen brechas dependiendo del tamaño de las empresas en cuanto a la importancia que le dan a este intercambio y el rol que juegan en las plataformas de intercambio de información, siendo las empresas grandes quienes juegan un papel activo y dejando a las pequeñas con un menor rol.
- Las empresas también describen los desafíos en la gestión de sus terceros. Los problemas de terceros, como una falla de TI en un proveedor importante, representaron el 15% de los incidentes operacionales informados a la FCA (la segunda causa de incidentes).
- En cuanto a la madurez de las capacidades, en cuanto a Ciber resiliencia, la encuesta arrojó resultados dispares, siendo los bancos retail y las entidades de pago quienes presentan el mayor grado de madurez.

Como complemento y con el fin de ampliar la visión respecto a Ciber seguridad, en marzo de 2019, se publicó el documento **Cyber security - industry insights**⁵¹ en la cual se entregan recomendaciones de prácticas en cuanto a Ciberseguridad, estas son:

⁵⁰ <https://www.fca.org.uk/publications/research/cyber-technology-resilience-themes-cross-sector-survey-2017-18>

⁵¹ <https://www.fca.org.uk/publications/research/cyber-security-industry-insights>

- a. **Poner una buena Gobernanza en su lugar;** Una buena Gobernanza permite a una organización controlar, dirigir y comunicar sus actividades de gestión de riesgos de Ciberseguridad.
- b. **Identifica lo que necesitas proteger;** La complejidad de las organizaciones y el ritmo del cambio hacen que sea difícil realizar un seguimiento de su información y sistemas, y de cómo estos se vinculan y administran. El dominio de identificación resalta la importancia de comprender qué es lo que está tratando de proteger y cómo se vinculan las entidades. Sin esto, no es posible adoptar un enfoque basado en el riesgo dentro de todos los otros dominios.
- c. **Protege tus activos adecuadamente;** Hacer frente a las amenazas externas requiere políticas, normas, procedimientos y controles de Ciberseguridad eficaces. Estos protegerán la confidencialidad, integridad y disponibilidad de sus servicios comerciales, al tiempo que limitan y contienen el impacto de un posible incidente cibernético.
- d. **Utilizar buenos sistemas de detección;** Las empresas deben ser capaces de detectar ataques reales o intentados en sistemas y servicios empresariales. El monitoreo exhaustivo y efectivo del sistema es esencial para la detección, y ayuda a garantizar que los sistemas se utilicen de acuerdo con las políticas de la organización.
- e. **Esté atento a las amenazas y problemas emergentes;** Se debe estar alerta a las amenazas y problemas emergentes para tomar decisiones informadas sobre la resiliencia cibernética. Esta inteligencia puede provenir de una variedad de fuentes internas y externas, lo que resalta la importancia de compartir inteligencia cuando sea posible.
- f. **Esté preparado para responder y recuperarse;** Se producirán incidentes. La capacidad de responder y recuperarse de ellos debe ser una parte clave de la administración de riesgos de la empresa y la planificación de la resiliencia operativa. Reanudar los servicios empresariales críticos rápidamente y con datos precisos requiere una planificación y pruebas continuas de escenarios de ciberataque plausibles. El ejercicio de las personas, los procesos y la tecnología es un aspecto clave en la preparación de la planificación de la respuesta y la recuperación.
- g. **Prueba y refina tus defensas;** Probar las defensas cibernéticas de toda su organización le asegura que comprende la efectividad de los controles a través de las personas, los procesos y la tecnología. Un fuerte régimen de pruebas ayuda a desarrollar una cultura para la mejora continua a medida que se descubren y resuelven los problemas.

En cuanto a el reporte de Ciber incidentes, bajo el Principio 11 del Manual FCA se debe reportar incidentes cibernéticos importantes. Un incidente puede ser material si:

- Produce una pérdida significativa de datos, o la disponibilidad o el control de sus sistemas de TI.
- Afecta a un gran número de clientes.
- Resulta en acceso no autorizado o software malicioso presente en sus sistemas de información y comunicación.

Respecto a cómo se debe reportar los Ciber incidentes materiales estas se deben reportar de la siguiente manera:

- Las empresas fijas⁵² deben ponerse en contacto con sus supervisores de FCA nombrados mientras que las empresas flexibles comunican según los canales oficiales (Número de teléfono y/o Correo Electrónico).

El **PRA** aborda el riesgo cibernético desde el punto de vista del riesgo suscrito por parte de las aseguradoras, y las necesidades de capital y riesgos de dicha suscripción, en línea con lo indicado en Solvencia II. A su vez en cuanto a sistema de gobernanza y valuación de provisiones técnicas está en línea con las instrucciones emanadas de la European Insurance and Occupational Pensions Authority (EIOPA).

Respecto al papel del **PRA en la supervisión de riesgo cibernéticos en el mercado de seguros se encuentran:**

- Apetito de riesgo y estrategia de riesgo respecto a coberturas de riesgos cibernéticos.
- Supervisión de la experticia de las aseguradoras en cuanto a riesgos cibernéticos.
- Supervisión a las entidades aseguradoras respecto a identificar, cuantificar y gestionar los riesgos provenientes de la suscripción Cibernética. Los riesgos cibernéticos se pueden separar en dos tipos; *Riesgos Cibernéticos afirmativos*, que corresponde a los riesgos explícitamente incluidos en la suscripción y los *Riesgos Cibernéticos No-afirmativos*, que corresponden a los riesgos que no están explícitamente incluidos en la suscripción (silenciosos).

En cuanto las expectativas del **PRA** para las aseguradoras sobre la gestión prudente del riesgo de suscripción cibernética se espera contemple tres grandes áreas:

- Manejo activo de Riesgos Cibernéticos no afirmativos.
- Establecer estrategias cibernéticas claramente definidas y apetitos de riesgo acordados por el directorio.
- Construir y desarrollar continuamente la experiencia cibernética de las aseguradoras.

⁵² Pequeño grupo de empresas, reguladas por la FCA, que, en función de factores como el tamaño, la presencia en el mercado y la presencia del cliente, requieren el mayor nivel de atención de supervisión. La mayoría de las empresas están clasificadas como cartera flexible. Fuente: FCA

3. EIOPA: EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY

EIOPA es un órgano consultivo independiente de la Comisión Europea, del Parlamento Europeo y del Consejo de la Unión Europea (UE). Es una de las agencias de la UE que llevan a cabo tareas jurídicas, técnicas o científicas específicas y proporcionan asesoramiento basado en pruebas para ayudar a formular políticas y leyes informadas tanto a nivel de la UE y como a nivel nacional.

Los principales objetivos de EIOPA son:

- Mejorar la protección de los consumidores, reconstruyendo la confianza en el sistema financiero.
- Asegurar un nivel elevado, eficaz y coherente de regulación y supervisión teniendo en cuenta los diversos intereses de todos los Estados miembros y la naturaleza diferente de las instituciones financieras.
- Lograr una mayor armonización y aplicación coherente de las normas aplicables a las instituciones y mercados financieros de la Unión Europea.
- Fortalecimiento de la supervisión de los grupos transfronterizos.
- Promover una respuesta coordinada de la Unión Europea en materia de supervisión.

Las principales responsabilidades de EIOPA consisten en apoyar la estabilidad del sistema financiero, la transparencia de los mercados y los productos financieros, así como la protección de los asegurados y los beneficiarios de los planes de pensiones. La EIOPA está encargada de supervisar e identificar las tendencias, los riesgos potenciales y las vulnerabilidades derivadas del nivel micro-prudencial, a través de las fronteras y entre sectores.

Para tener en cuenta las condiciones específicas en los mercados nacionales y la naturaleza de las instituciones financieras, el Sistema Europeo de Supervisión Financiera es una red integrada de autoridades nacionales y europeas de supervisión que proporciona los vínculos necesarios entre los niveles macro y micro prudencial, dejando la supervisión del día a día a nivel nacional. EIOPA se rige por su Junta de Supervisores, que integran las autoridades nacionales competentes en el ámbito de los seguros y las pensiones de cada Estado miembro. Las autoridades nacionales de supervisión de la Unión Europea son una fuente de conocimientos e información sobre temas de seguros y pensiones.

En septiembre de 2013, EIOPA emitió un documento con “Directrices para el Sistema de Gobernanza”⁵³, el que aborda los siguientes temas:

⁵³ <https://eiopa.europa.eu/publications/eiopa-guidelines>

1. Requisitos generales de gobernanza

1.1 Gestión de riesgos

Directriz 19 - Política de gestión del riesgo operacional.

El artículo 44 de la Directriz de Solvencia II, establece que las autoridades nacionales competentes deben garantizar que:

- En la política de gestión de riesgos, el compromiso cubra, al menos, lo siguiente con respecto al riesgo operacional:
 1. Identificación de los riesgos operacionales a los que está o podría estar expuesto y la evaluación respecto a la forma de mitigarlos;
 2. Actividades y procesos internos para gestionar los riesgos operativos, incluido el sistema de TI que los respalda; y
 3. Límites de tolerancia al riesgo con respecto a las principales áreas de riesgo operacional de la empresa.

- La empresa cuenta con procesos para identificar, analizar e informar sobre los eventos de riesgo operacional. Para este propósito, debe establecer un proceso para recopilar y monitorear eventos de riesgo operacional.

- A efectos de la gestión del riesgo operacional, la empresa desarrolle y analice un conjunto adecuado de escenarios de riesgo operacional basados en al menos los siguientes enfoques:
 1. La falla de un proceso clave, personal o de sistema; y
 2. La ocurrencia de eventos externos.

Este documento incorpora una serie de notas explicativas que abordan los siguientes aspectos:

- Como el riesgo operacional suele ser más difícil de identificar y evaluar que otros tipos de riesgos, es aún más importante para la empresa tener un enfoque consciente de estos en su gestión general de riesgos. Dado que algunos de los riesgos provienen de la propia empresa (por ejemplo, procesos internos, personales o de sistema fallidos o inadecuados), la empresa desempeña un papel en la aparición y el despliegue de los riesgos operativos. Esto también es, en parte, cierto para los riesgos operacionales que tienen como causa un evento externo.

- Es importante tener en cuenta que, dado que los riesgos operacionales tienden a interactuar con los otros tipos de riesgo, no se evaluarán de forma aislada, sino que se considerarán junto con la evaluación de los otros tipos de riesgo.

- El riesgo operacional puede materializarse a través de errores de ejecución del personal, fraudes y fallas en el procesamiento, así como también a través de las consecuencias directas e indirectas de desastres naturales o eventos provocados por el hombre, tales como ataques terroristas, incendios, inundaciones, terremotos y pandemias. Estos desastres naturales o eventos provocados por el hombre son tipos de riesgo operativos de alto impacto y baja frecuencia que deben considerarse al analizar dicho escenario. Como su impacto puede ser potencialmente catastrófico, la empresa les presta especial atención y desarrolla sistemas de alerta temprana que permiten una intervención efectiva y oportuna.
- Para el desarrollo de escenarios, la empresa tiene en cuenta que los diferentes tipos de riesgo operacional que se definen en el artículo 13 de Solvencia II no están estrictamente separados y que utilizan dos puntos de partida (a partir de una falla del proceso interno, de sistema o del personal, o por causas externas) para desarrollar el conjunto de escenarios que brindarán mejores oportunidades de tener una lista más completa de escenarios relevantes. También deben considerarse escenarios muy severos e improbables, pero que no son imposibles.
- Para realizar este análisis, la empresa puede utilizar categorías predefinidas de riesgos operativos y listas de sus procesos clave. Sin embargo, cada empresa es libre de definir una categorización que se adapte mejor a sus especificidades.
- El análisis de las pruebas de estrés y los escenarios para el marco de riesgo operacional puede diferir de otros tipos de análisis de estrés o escenarios (por ejemplo, financiero), ya que la definición de las diferentes etapas del escenario (causa, falla del proceso, impactos) será un elemento clave del análisis y seguimiento de los riesgos. La razón principal de esto es que los controles y las medidas correctivas que implementará la empresa tendrán un efecto en el escenario en sí.
- En el caso del riesgo operacional, la prevención y las acciones correctivas tienen prioridad por sobre la medida exacta. La identificación de los riesgos operacionales está muy relacionada con la prevención, la mitigación y las medidas correctivas.
- El monitoreo y control continuo de los riesgos operativos implica que todo el personal es consciente de la importancia de este tipo de riesgo.
- Los controles y las acciones de mitigación deben revisarse periódicamente, teniendo en cuenta la evolución del riesgo operacional y el conocimiento de la evolución del riesgo operacional.
- Ejemplos de acciones de mitigación son:
 - a. Seguros (seguro de responsabilidad civil, seguro de persona clave, seguro contra incendios, etc.);
 - b. Automatización de procesos; y
 - c. Copia de seguridad de datos.

- También se espera que la empresa establezca indicadores clave de riesgo.
- A efectos del análisis de eventos de riesgo operacional, una empresa también puede considerar cómo los datos externos podrían complementar su recopilación de datos sobre eventos internos de riesgo operacional, para producir estimaciones más confiables de los eventos de riesgo operacional.
- En cada evento en cuestión, se necesita al menos la siguiente información:
 - a. La causa del evento;
 - b. Las consecuencias del evento; y
 - c. Las acciones realizadas y no realizadas en relación al evento.
- Al definir el perímetro (por ejemplo, el umbral de materialidad) de los eventos que serán recogidos, la empresa debería tener en cuenta que:
 - a. El riesgo operacional puede estar relacionado con eventos de alta frecuencia / baja gravedad o con eventos de baja frecuencia / alto impacto; y
 - b. Algunos eventos que no han tenido ningún impacto negativo (por ejemplo, cuasi accidentes) pueden ser muy útiles de analizar para controlar los riesgos operacionales más materiales.

4. USA: NAIC (NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS)

La Asociación Nacional de Comisionados de Seguros (NAIC, por sus siglas en inglés) es la organización de apoyo normativo y regulatorio de los EEUU. Creada y gobernada por los principales reguladores de seguros de los 50 estados, el Distrito de Columbia y cinco territorios de los EEUU. A través de la NAIC, los reguladores estatales de seguros establecen estándares y mejores prácticas, llevan a cabo una revisión por pares y coordinan su supervisión reguladora. El personal de NAIC apoya estos esfuerzos y representa las opiniones colectivas de los reguladores estatales a nivel nacional e internacional. Los miembros de NAIC, junto con los recursos centrales de NAIC, forman el sistema nacional de regulación de seguros estatal en los EEUU.

En relación al riesgo operacional, la NAIC⁵⁴ señala que ha desempeñado un papel en muchos de los escándalos de la industria bancaria que tuvieron lugar en las últimas dos décadas. A medida que el sistema financiero se ha vuelto más interconectado y complejo que nunca, el desafío de comprender y mitigar los riesgos operativos ha aumentado. Las mejoras en la gestión del riesgo operacional (ORM, por sus siglas en inglés) han adquirido un mayor enfoque y visibilidad dentro de la industria de servicios financieros y en muchas otras industrias. En los últimos años, la NAIC, a través de su Iniciativa de Modernización de Solvencia (SMI, por sus siglas en inglés), ha estado explorando formas de aumentar el enfoque regulatorio en el riesgo operativo. Además, como resultado de las regulaciones de Solvencia II, muchas grandes compañías de seguros europeas han comenzado a establecer programas formales de gestión del riesgo operacional.

El riesgo operacional se reconoció como una clase de riesgo importante a mediados de la década de 1990, luego de una serie de insolvencias a gran escala en la industria bancaria causadas o exacerbadas por eventos fuera del mercado y el riesgo crediticio (el Condado de Orange, 1994; Barings Bank, 1995; y Daiwa Bank, 1995, entre otros) y socavaron la confianza en el sistema bancario. En estos casos, se incurrieron en pérdidas significativas debido a fallas de riesgo operacional. En respuesta, el Comité de Supervisión Bancaria de Basilea (BCBS, por sus siglas en inglés) publicó una propuesta en junio de 1999 para reemplazar el Acuerdo de Capital de Basilea de 1988 (Basilea I), que se aplicaba a todos los bancos en los Estados Unidos, con un nuevo marco sensible al riesgo. La propuesta consultiva inicial introdujo una categoría de riesgo operacional y los requisitos de capital correspondientes. Actualmente, el BCBS está implementando un enfoque estandarizado de Basilea III que se espera que esté completamente implementado para 2022 para todos los bancos activos internacionalmente.

A medida que el riesgo operacional se ha reconocido como una categoría de riesgo distinta, el valor de administrar eficazmente el riesgo operacional ha aumentado considerablemente en los últimos tiempos. En los últimos años, el riesgo cibernético se ha enfocado como un riesgo operacional para que los reguladores de seguros lo aborden dado el aumento en los casos de incidentes cibernéticos, incluidas las violaciones de datos; el robo de identidad; ataques de ransomware; y eventos de denegación de servicio. Dichos incidentes pueden tener un impacto material en el capital a través de los costos de restauración y remediación, pérdida de ingresos

⁵⁴ https://content.naic.org/cipr_topics/topic_operational_risk.htm

y sanciones regulatorias. El seguro de riesgo cibernético se está convirtiendo en un producto más popular que se utiliza para mitigar este riesgo operacional.

El riesgo operacional sigue siendo difícil de identificar y evaluar, ya que las causas son extremadamente heterogéneas, lo que dificulta el desarrollo de modelos estadísticos para este riesgo. Un modelo de riesgo operacional sólido se extiende mucho más allá de los límites de una cuantificación basada en fórmulas. Abarca las actividades comerciales de una empresa y es una parte integral de un marco eficiente de gestión de riesgos empresariales. El perfil de riesgo operacional subyacente de una aseguradora debe revisarse exhaustivamente en toda su gama de actividades comerciales para identificar y estimar los requisitos de entrada del modelo. El principal desafío es combinar dos fuentes esenciales de información: datos empíricos sobre pérdidas y juicio experto.

Muchas empresas han estado aprovechando la experiencia de la industria bancaria, que se ha centrado en el riesgo operacional durante más de una década. Sin embargo, los datos históricos sobre la frecuencia y la gravedad de las pérdidas a menudo no están disponibles. Por lo tanto, faltan datos históricos uniformes sobre los cuales se puedan construir los cargos de capital por riesgo operacional. Organizaciones, como el Consorcio de Riesgo Operacional (ORIC, por sus siglas en inglés), han comenzado a recopilar datos de las instituciones financieras participantes para desarrollar consorcios de datos de pérdida de riesgo operacional. ORIC fue fundada en 2005 para avanzar en la gestión y medición del riesgo operacional. Facilita el intercambio anónimo y confidencial de datos de riesgo operacional entre las firmas miembro, proporcionando un conjunto diverso y de alta calidad de información cuantitativa y cualitativa sobre exposiciones relevantes al riesgo operacional.

La NAIC, como Regulador estatal de seguros, participa en el Comité de Banca Financiera e Infraestructura de Información del Departamento del Tesoro de los Estados Unidos (FBIC) y en el Foro de Ciberseguridad del Poder Ejecutivo y la Agencias reguladoras Independientes, donde trabajan con los reguladores federales para abordar las amenazas cibernéticas en los EEUU. Los reguladores de seguros también se encuentran en la posición única de regular y monitorear la solvencia de las compañías de seguros que suscriben las políticas de ciberseguridad.

Si bien el Grupo de Trabajo sobre Ciberseguridad fue disuelto a fines del año 2017, sus responsabilidades y funciones fueron integradas al Grupo de Trabajo de Innovación y Tecnología y los miembros de la NAIC adoptaron varias de las recomendaciones de este grupo entre las que se cuentan:

1. Adoptar los **Principios para la Ciberseguridad Efectiva: Guía Reguladora de Seguros**. Los 12 principios se dirigen a los aseguradores, productores y otras entidades reguladas para identificar mejor los riesgos y desarrollar soluciones prácticas para proteger la información del consumidor.
2. Adoptar la Hoja de ruta de la NAIC para la protección del consumidor en materia de ciberseguridad, un proyecto destinado a reforzar la protección del consumidor.
3. Se actualizó el Manual de Examinadores de Condiciones Financieras para los protocolos revisados de ciberseguridad.

4. Se recomendó que el Manual de Regulación del Mercado sea actualizado de manera similar.
5. Adoptar la nueva **Ley Modelo de Seguridad de Datos de Seguros (ML - 668)**: El modelo N°668 requiere que los aseguradores y otras entidades con licencia de los departamentos de seguros estatales desarrollen, implementen y mantengan un programa de seguridad de la información; investigar cualquier evento de ciberseguridad; y notificar al comisionado estatal de seguros de tales hechos. A partir del 24 de octubre de 2017, fecha de adopción de la Ley Modelo, los estados están trabajando para introducir el modelo en sus legislaturas.

Adicionalmente los miembros de la NAIC han incluido un requerimiento de información suplementaria respecto a las coberturas de seguro de ciberseguridad y robo de identidad para los estados financieros de aseguradoras de no vida con el fin de recopilar información sobre los mercados de seguros de ciberseguridad. Esta data se ha recolectado desde el año 2015.

Principios para la Ciberseguridad Efectiva: Guía Reguladora de Seguros

Como respuesta a la creciente preocupación de en materia de seguridad y a la importancia que esta tiene para los reguladores estatales de seguros, el año 2015 la NAIC ve la necesidad de proporcionar una guía eficaz de Ciberseguridad con respecto a la protección de la infraestructura y la seguridad de los datos del sector de seguros. En esta se establecen 12 principios, los cuales tienen como finalidad servir como estándar para identificar riesgos y ofrecer soluciones prácticas en el marco de la relación entre los reguladores estatales y la industria aseguradora, a la vez que se protege a los consumidores. Los principios son los siguientes:

1. Principio 1: La responsabilidad de los reguladores estatales para con la información personal de los asegurados, y la exigencia y requerimientos que deben cumplir las entidades reguladas para con la protección contra riesgos de Ciberseguridad, así como alertar a los consumidores de manera oportuna en caso de una violación de la ciberseguridad.
2. Principio 2: La salvaguarda de los datos de los consumidores por entidades reguladas.
3. Principio 3: La responsabilidad de los reguladores para con la información recopilada y almacenada y/o transferida dentro o fuera de un departamento estatal seguros o la NAIC.
4. Principio 4: La guía reguladora de ciberseguridad para aseguradores y productores de seguros debe ser flexible, escalable, práctica y coherente con los esfuerzos reconocidos a nivel nacional.
5. Principio 5: Coherencia entre los riesgos de ciberseguridad y los estándares mínimos exigidos para quienes operen a través de internet.
6. Principio 6: Proporcionar una supervisión reguladora adecuada, que incluye, entre otros, la realización de exámenes financieros basados en el riesgo y / o exámenes de conducta de mercado relacionados con la ciberseguridad.
7. Principio 7: La planificación de la respuesta a incidentes por parte de entidades reguladas y reguladores estatales es un componente esencial para un programa de ciberseguridad eficaz.

8. Principio 8: Entidades reguladas y reguladores estatales deben tomar las medidas adecuadas para garantizar que los terceros y los proveedores de servicios tengan controles para proteger la información de identificación personal.
9. Principio 9: Los riesgos de ciberseguridad deben incorporarse y abordarse como parte del proceso de gestión de riesgos de la empresa (**ERM**) de una entidad regulada y esta se debe incluir todas las facetas de una organización.
10. Principio 10: Los riesgos de Ciberseguridad detectados por auditoría interna y que representen un riesgo material para los asegurados deben ser revisado por la Junta de Directores o Comités Apropriados.
11. Principio 11: Es esencial que las aseguradoras y los productores de seguros utilicen una organización de análisis e intercambio de información (**ISAO**) para compartir información y mantenerse informados sobre las amenazas o vulnerabilidades emergentes, así como el análisis y el intercambio de inteligencia de amenazas físicas.
12. Principio 12: Capacitación periódica y oportuna, combinada con una evaluación, para los empleados para entidades reguladas y otros terceros, con respecto a los problemas de ciberseguridad.

Ley Modelo de Seguridad de Datos de Seguros

En octubre de 2017 la NAIC adoptó la **Ley Modelo de Seguridad de Datos de Seguros (ML #668)** con el fin de actualizar los requisitos regulatorios de seguros de cada estado, llamados seguros estatales de ahora en adelante, relacionados con la seguridad de los datos, la investigación de un evento de ciberseguridad y la notificación a los comisionados de seguros estatales de eventos de ciberseguridad en entidades reguladas.

La ley está dividida en 13 secciones, de las cuales se destacan los siguientes aspectos:

I. Sección 2 Propósito e intención

“El propósito y la intención de esta Ley es establecer estándares de seguridad de datos y estándares para la investigación y notificación al Comisionado de un Evento de Ciberseguridad aplicable a los Licenciarios, según lo definido en la sección 3.”

II. Sección 3 Definiciones

En esta sección se define los términos importantes que se refieren el resto de las secciones. En esta están definidos términos como *“evento de ciberseguridad”, “Licenciario”, “Sistema de Información”, “Información no pública”,* entre otros.

III. Sección 4 Programa de Seguridad de la Información

Esta sección a su vez esta subdividida en nueve puntos importantes:

- a. **Implementación de un Programa de Seguridad de la Información;** Esta debe ser proporcional al tamaño y complejidad de las actividades del Licenciario, incluidas aquellas que usen servicios proporcionados por terceros. Deberá desarrollar, implementar y mantener un programa completo de seguridad de la información por escrito basado en el Evaluación de riesgos del licenciario y

que contiene medidas de seguridad administrativas, técnicas y físicas para el Protección de la información no pública y del sistema de información del licenciatario

- b. Objetivos del Programa de Seguridad de la Información;** Define los Objetivos que deberá tener en cuenta el Licenciatario respecto diseño del Programa de Seguridad de la Información.
- c. Evaluación de riesgos;** Define los deberes del Licenciatario respecto a la evaluación de riesgos.
- d. Gestión de Riesgos;** Define los deberes del Licenciatario sobre la base de su Evaluación de Riesgos.
- e. Supervisión Junta directiva;** En el caso de disponer una junta directiva o comité apropiado, se establece un mínimo de requerimientos que deberá cumplir.
- f. Supervisión de los acuerdos de proveedores de servicios de terceros;** El Licenciatario deberá ejercer la diligencia debida al seleccionar a su Proveedor de servicios externo y requerir que este implemente una administración apropiada, Medidas técnicas y físicas para proteger y asegurar los Sistemas de Información y la Información No Pública a la que tenga acceso o esté en su poder.
- g. Ajustes al programa;** El licenciatario deberá supervisar, evaluar y ajustar, según corresponda, el Programa de Seguridad de la Información según los criterios contenidos en este punto.
- h. Plan de respuesta a incidentes:** Como parte de su Programa de Seguridad de la Información, cada Licenciatario establecerá un plan de respuesta a incidentes por escrito diseñado para responder rápidamente a, y recuperarse de, cualquier Evento de Ciberseguridad que se comprometa con la confidencialidad, integridad o disponibilidad de la Información no pública en su poder, los Sistemas de Información del Licenciatario, o la continuidad del funcionamiento de cualquier aspecto del negocio u operaciones del Licenciatario. Dicho plan de respuesta a incidentes deberá abordar las siguientes áreas:
 - (a) El proceso interno para responder a un Evento de Ciberseguridad;
 - (b) Los objetivos del plan de respuesta a incidentes;
 - (c) La definición de roles claros, responsabilidades y niveles de autoridad para tomar decisiones;
 - (d) Comunicaciones externas e internas e intercambio de información;
 - (e) Identificación de los requisitos para remediar cualquier debilidad identificada en Sistemas de información y controles asociados;
 - (f) Documentación y presentación de informes sobre eventos de ciberseguridad y actividades relacionadas con la respuesta a incidentes;
 - y
 - (g) La evaluación y revisión, según sea necesario, del plan de respuesta a incidentes después de un evento de ciberseguridad
- i. Certificación Anual al Comisionado de Estado Domiciliario;** Anualmente cada asegurador domiciliado en su respectivo estado deberá presentar al Comisionado una declaración escrita con fecha 15 de febrero certificando que

la aseguradora cumple con los requisitos establecidos en la Sección 4 de este Acto/Ley.

IV. *Sección 5 Investigación de un evento de ciberseguridad*

Si el Licenciatario se entera de que un Evento de Ciberseguridad ocurrió, o pudo haber ocurrido, el Licenciatario o proveedor externo y / o proveedor de servicios designado para actuar en nombre del Licenciatario, deberá realizar una investigación inmediata. Durante Esta investigación el Licenciatario, o su representante, deberá, como mínimo, determinar la mayor cantidad de la siguiente información como sea posible:

- (a) Determine si ha ocurrido un Evento de Ciberseguridad;
- (b) Evaluar la naturaleza y el alcance del Evento de Ciberseguridad;
- (c) Identifique cualquier información no pública que pueda haber estado involucrada en el evento de ciberseguridad; y
- (d) Llevar a cabo o supervisar medidas razonables para restablecer la seguridad de los sistemas de información comprometidos en el evento de ciberseguridad, con el fin de evitar la adquisición, divulgación o uso no autorizados de información no pública en posesión, custodia o control del Licenciatario.

En el caso que el Licenciatario se entera de que un Evento de Ciberseguridad ocurrió, o pudo haber ocurrido, en un sistema mantenido por un Proveedor de Servicios de Terceros, el Licenciatario completará los pasos enumerados en la Sección 5B anterior o confirmará y documentará que el Proveedor de Servicios de Terceros ha completado esos pasos.

El titular de la licencia deberá mantener registros relativos a todos los eventos de ciberseguridad por un período de al menos cinco años a partir de la fecha del evento de ciberseguridad y deberá presentar dichos registros a petición del Comisionado.

V. *Sección 6. Notificación de un evento de ciberseguridad*

Licenciatario deberá notificar al Comisionado tan pronto como sea posible, pero en ningún caso después de 72 horas a partir de una determinación de que se ha producido un Evento de Ciberseguridad, cuando cualquiera de los Criterios contenidos en la Letra A de esta Sección sea acreditado:

- Posee licencia de un determinado estado (domiciliado),
- El licenciatario cree que existe una duda razonable que información no publica afecte a más de 250 consumidores y cumple con cualquiera de los siguientes criterios;
 - El evento de ciberseguridad cumple con los requisitos para que deba ser notificado a cualquier agencia gubernamental u otro organismo supervisor, o
 - Existe una probabilidad razonable de daño a;
 - Cualquier consumidor residente de un determinado estado, o
 - Cualquier parte material de la normal operación de un licenciatario

El licenciatario deberá proporcionar la mayor de la siguiente información que le sea posible y proveer esta información en forma electrónica según lo indique el comisionado. El Licenciatario tendrá la obligación continua de actualizar y complementar las notificaciones iniciales y posteriores al Comisionado en relación con el evento de ciberseguridad. La información a proporcionar es la siguiente:

- (1) Fecha del Evento de Ciberseguridad;
- (2) Descripción de cómo la información fue expuesta, perdida, robada o violada, incluidas las funciones y responsabilidades específicas de los proveedores de servicios de terceros, si los hubiera;
- (3) Cómo se descubrió el Evento de Ciberseguridad;
- (4) Si cualquier información perdida, robada o violada ha sido recuperada y, de ser así, cómo se hizo;
- (5) La identidad de la fuente del Evento de Ciberseguridad;
- (6) Si el licenciatario ha presentado un informe policial o ha notificado a algún organismo regulador, gubernamental o del orden público y, en caso afirmativo, cuándo se proporcionó dicha notificación;
- (7) Descripción de los tipos específicos de información adquirida sin autorización. Tipos específicos de información significan elementos de datos particulares que incluyen, por ejemplo, tipos de información médica, tipos de información financiera o tipos de información que permiten la identificación del Consumidor;
- (8) El período durante el cual el Sistema de información se vio comprometido por el evento de ciberseguridad;
- (9) El número total de consumidores, en un determinado estado, afectados por el evento de ciberseguridad. El Licenciatario deberá proporcionar la mejor estimación en el informe inicial al Comisionado y actualizar esta estimación con cada informe subsiguiente al Comisionado de conformidad con esta sección;
- (10) Los resultados de cualquier revisión interna que identifique un lapso en los controles automatizados o en los procedimientos internos, o que confirme que se siguieron todos los controles automáticos o procedimientos internos;
- (11) Descripción de los esfuerzos que se están realizando para remediar la situación que permitió que ocurriera el Evento de Ciberseguridad;
- (12) Una copia de la política de privacidad del Licenciatario y una declaración que describa los pasos que tomará para investigar y notificar a los Consumidores afectados por el Evento de Ciberseguridad; y
- (13) Nombre de una persona de contacto que está familiarizada con el Evento de Ciberseguridad y autorizada para actuar para el /en representación del Licenciatario.

El licenciatario deberá cumplir con la ley de notificación de violación de datos del respectivo estado, y proporcionar una copia de la notificación enviada a los consumidores en virtud de ese estatuto al Comisionado, Esto en el caso que aplique la notificación de un licenciatario a un comisionado.

A su vez en esta Sección se instruye de como deberá dar aviso sobre eventos de ciberseguridad de proveedores de servicios externos. Este tipo de eventos deberán ser

tratados de igual manera que los catalogados en la letra A de esta sección. Los plazos de notificación del licenciatario empezaran a correr desde el momento que este es notificado por el proveedor de servicios externos o desde que desde que el licenciatario tenga conocimiento del evento de ciberseguridad.

Para finalizar, se entregan los lineamientos en cuanto a aviso sobre eventos de ciberseguridad de un Reasegurador a un Asegurador y aviso sobre eventos de ciberseguridad de un Asegurador a un intermediario (en caso de que el consumidor adquiera el producto o servicio a través de uno).

VI. Sección 7. Poder del comisionado

Esta Sección detalla el poder del comisionado en cuanto a examinar e investigar los asuntos de cualquier Licenciatario para determinar si el Licenciatario ha participado o está involucrado en alguna conducta que infrinja esta Ley.

VII. Sección 8. Confidencialidad

Esta Sección detalla aspectos de confidencialidad de la información recibida y que aplican a los comisionados.

VIII. Sección 9. Excepciones

Esta Sección detalla las excepciones a la aplicación de esta ley.

IX. Sección 10. Penalizaciones

En el caso de una violación de esta Ley, un Licenciatario podrá ser penalizado de acuerdo con la legislación general estatal de penalización correspondiente.

X. Sección 11. Reglas y regulaciones

El comisionado podrá emitir los reglamentos necesarios para llevar a cabo lo dispuesto en esta ley.

XI. Sección 12 Separabilidad

La invalidez o inaplicabilidad de alguna disposición que emane de esta ley a cualquier persona o circunstancia no afectará el resto de las disposiciones contenidas en la ley u/o aplicación de dicha disposición a otras personas o circunstancias.

5. OSFI: OFFICE OF THE SUPERINTENDENT OF FINANCIAL INSTITUTIONS

La Oficina del Superintendente de Instituciones Financieras (OSFI) es una agencia gubernamental federal independiente que regula y supervisa más de 400 instituciones financieras reguladas por el gobierno federal de Canadá y 1.200 planes de pensiones cuyo objetivo es evaluar y determinar su posición financiera y el cumplimiento de los requerimientos regulatorios.

Regula el mercado a través del desarrollo de normativa, interpretando leyes y regulaciones, proporcionando autorizaciones regulatorias para ciertos tipos de transacciones. Asimismo, contribuye en los nuevos estándares en temas contables, de auditoría y actuariales. Lo anterior, debe equilibrar los objetivos de seguridad y solidez con la necesidad de que las instituciones operen en un mercado competitivo.

Supervisa el mercado analizando las tendencias financieras y económicas para identificar problemas emergentes que podrían afectar negativamente a las instituciones. Evalúa la condición financiera de una institución, los riesgos materiales y la calidad de su gobierno, gestión de riesgos y nivel de cumplimiento. Una vez identificadas las debilidades, interviene de manera oportuna, trabajando con el directorio y la plana ejecutiva para corregir los problemas.

En lo relacionado a la administración de riesgo operacional, la OSFI emite en 2016 el documento guía N° E21⁵⁵, estableciendo un esquema de administración de riesgo operacional basado en principios y buenas prácticas, cuyo objetivo es el establecimiento de un marco de administración de riesgo operacional, declaración del apetito por riesgo, tres líneas de defensa y la identificación y evaluación del riesgo operacional, manteniendo coherencia con la guía de Gobierno Corporativo, reflejando los estándares internacionales en la gestión de riesgo operacional.

MARCO DE GESTIÓN DE RIESGO OPERACIONAL

Principio 1: La gestión del riesgo operacional debe integrarse completamente en el sistema de gestión de riesgos de las compañías y documentarse adecuadamente.

DECLARACIÓN DE APETITO DE RIESGO OPERACIONAL

Principio 2: La gestión del riesgo operacional debe servir para respaldar la estructura general de gobierno corporativo de las compañías. Como parte de esto, las compañías deben desarrollar y utilizar una declaración de apetito de riesgo operacional, o en el caso de las compañías pequeñas y menos complejas con perfiles de riesgo operacional más bajos, el uso de los umbrales de informe / escalamiento para eventos de riesgo operacional importantes.

⁵⁵ https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/e21_gias.aspx

TRES LINEAS DE DEFENSA

Principio 3: Las compañías deben garantizar la rendición de cuentas efectiva para la gestión del riesgo operacional. Un enfoque de “tres líneas de defensa”, o una estructura apropiadamente robusta, debe servir para delinear las prácticas clave de la gestión del riesgo operacional y proporcionar una visión objetiva adecuada y un desafío. La forma en que esto se haga operativo en la práctica, en términos de la estructura organizativa de una compañía, dependerá de su modelo de negocio y perfil de riesgo.

IDENTIFICACIÓN Y EVALUACIÓN DEL RIESGO OPERACIONAL

Principio 4: Las compañías deben garantizar una identificación y evaluación exhaustivas del riesgo operacional mediante el uso de herramientas de gestión adecuadas. El mantenimiento de un conjunto de herramientas de gestión de riesgos operacionales proporciona un mecanismo para recopilar y comunicar información relevante sobre riesgos operacionales, tanto dentro de la compañía, como a las autoridades de supervisión relevantes.

OSFI es la encargada de supervisar los incidentes de Ciberseguridad ocurridos en las entidades que están bajo su fiscalización, entre ellas las aseguradoras. Si bien es cierto, actualmente no planea establecer una guía específica para el control y la gestión del riesgo cibernético, es través de su “Guía de Autoevaluación de Ciberseguridad” que recomienda utilicen esta herramienta, o herramientas similares de evaluación, para evaluar su nivel actual de preparación, y para desarrollar y mantener prácticas eficaces de Ciberseguridad.

ANEXO C: MARCO NORMATIVO LOCAL

1. COMISIÓN PARA EL MERCADO FINANCIERO, CMF, ÁREA SEGUROS:

La NCG N° 325, de 2011, imparte instrucciones sobre el sistema de gestión de riesgos de las aseguradoras y la evaluación de solvencia de las compañías por parte de la Comisión, e incluye dentro de la gestión de riesgos de las aseguradoras el tema del riesgo operacional.

Respecto a la gestión del riesgo operacional, la NCG N° 325, establece algunos aspectos que se deberían contemplar en el Sistema de Gestión de Riesgo, respecto de la gestión de riesgo operacional (N°2.5.2 de la norma):

- a) Procedimientos y metodologías explícitas para la gestión del riesgo operacional y tecnológico, incluyendo los riesgos asociados con sus sistemas informáticos, outsourcing, continuidad del negocio, recursos humanos inadecuados, fraude interno y externo, administración de proyectos, y en general los riesgos relacionados con los procesos operacionales de la compañía.
- b) Los procedimientos señalados deberían considerar:
 - i) Identificación y evaluación del riesgo.
 - ii) Controles internos y estrategias de mitigación.
 - iii) Capacitación del personal y difusión de las medidas de control y mitigación de los riesgos.
 - iv) Planes para el desarrollo de proyectos y nuevos productos, con impacto operacional, incluyendo aspectos como sus objetivos, identificación y evaluación de riesgos, análisis costo beneficio, monitoreo de cumplimiento de objetivos y tiempos del proyecto, y revisión post implementación.
 - v) Definición de responsabilidades y segregación clara de funciones.
 - vi) Métodos para monitorear el cumplimiento de los procedimientos, metodologías y estrategias de mitigación establecidas y reportar los incumplimientos detectados.

2. COMISIÓN PARA EL MERCADO FINANCIERO, CMF, ÁREA BANCOS:

- El documento *Modelo Chileno de Supervisión Basada en Riesgos*⁵⁶ indica que un elemento distintivo fundamental en la supervisión bancaria moderna, consiste en la verificación de la idoneidad de la gestión de los riesgos (evaluar la gestión), en las instituciones bancarias, lo que implica complementar la supervisión basada en el cumplimiento de reglas con una supervisión basada en el cumplimiento de principios de gestión de riesgos.

Desde el punto de vista del Riesgo Operacional, la evaluación de gestión tiene como propósito emitir una opinión sobre la calidad de la gestión de cada uno de los ámbitos que lo componen, examinando el rol del directorio y la alta administración en la gestión de riesgos. Además, se verifica la existencia, suficiencia y compatibilidad entre las políticas y los procedimientos establecidos por la entidad, como también la forma en que la dirección de la institución participa en su aprobación y supervisa su cumplimiento. Se revisan las metodologías dispuestas para identificar, medir, monitorear y controlar en cada riesgo de la materia. Asimismo, se evalúa la efectividad de las funciones de riesgo y auditoría interna.

La evaluación de la gestión de riesgos considera el grado de adhesión de las entidades a un conjunto de principios, lineamientos generales de buenas prácticas a seguir por las instituciones en la gestión de los distintos riesgos.

Los principios de gestión aplicables al Riesgo Operacional son los siguientes:

- **Principio 17.** El directorio ha dispuesto un adecuado marco de gobierno para la gestión de los riesgos operacionales.
- **Principio 18.** La entidad dispone de una estructura de comités funcional a los principales riesgos operacionales a que está expuesta.
- **Principio 19.** La institución cuenta con una función de riesgos que es una contraparte efectiva de las áreas generadoras de riesgos, encargada del diseño y mantención de un adecuado sistema de identificación, evaluación, seguimiento y control y mitigación de los riesgos operacionales.
- **Principio 20.** La entidad desarrolla sus actividades al amparo de políticas que cubren adecuadamente los riesgos asumidos.
- **Principio 21.** La entidad bancaria desarrolla sus actividades al amparo de procedimientos compatibles con las políticas de riesgo operacional.
- **Principio 22.** La entidad dispone de metodologías para la identificación, evaluación, seguimiento, control y mitigación de los riesgos tanto internos como externos que afecten el Riesgo operacional.

⁵⁶<https://www.sbif.cl/sbifweb/servlet/Publicaciones?indice=15.3&idPublicacion=480&idContenido=12020&idCategoria=2517>

- **Principio 23.** La entidad dispone de una metodología que le permite gestionar adecuadamente la continuidad del negocio.
 - **Principio 24.** La institución realiza una adecuada administración de seguridad de la información en términos de resguardar su confidencialidad, integridad y disponibilidad.
 - **Principio 25.** La institución dispone de una metodología adecuada para gestionar los servicios externalizados.
 - **Principio 26.** La entidad dispone de una infraestructura tecnológica que le permite cubrir las necesidades del negocio actuales y proyectadas, así como adecuados procesos tecnológicos para soportar las actividades del negocio.
 - **Principio 27.** La función de auditoría constituye una instancia de control efectivo respecto de la gestión de riesgo operacional.
- El capítulo **1-13 de la RAN, sobre Clasificación de Gestión y Solvencia**⁵⁷, la letra C) del numeral 3.2 del Título II, relacionado a la evaluación de la gestión de los bancos, indica que resultará de interés, en la evaluación de la gestión de Riesgo Operacional, el rol asumido por el directorio y la aprobación que han dado a la estrategia a utilizar en su administración, la que deberá contemplar una definición clara de lo que considerará como Riesgo Operacional, establecer principios para su identificación, evaluación control y mitigación. Si la exposición al riesgo es significativa, cobra relevancia la existencia de definiciones precisas de lo que se entenderá por pérdidas operacionales ya sean esperadas o inesperadas.

Asimismo, interesará revisar la compatibilidad entre las políticas y procedimientos aprobados por el directorio en volumen, sofisticación y naturaleza de sus actividades. Como así también, examinar la independencia de la función de auditoría interna en la cobertura y profundidad de las revisiones y la adopción oportuna de medidas correctivas.

Con todo, se consideran como ejemplos de buena gestión de riesgo operacional:

- El directorio procura el establecimiento de una definición de riesgo operacional y lo reconoce como un riesgo gestionable.
- La entidad mantiene políticas para la administración de los riesgos operacionales aprobadas por el directorio.
- La estrategia de administración del riesgo operacional definida por el banco, es consistente con el volumen y complejidad de sus actividades y considera el nivel de tolerancia al riesgo del banco, incluyendo líneas específicas de responsabilidad.
- La entidad administra los riesgos operacionales considerando los impactos que pudieran provocar en el banco (severidad de la pérdida) y la probabilidad de ocurrencia de los eventos.
- La entidad realiza evaluaciones del riesgo operacional inherente a todos los tipos de productos, actividades, procesos y sistemas.

⁵⁷ <https://www.sbif.cl/sbifweb/servlet/LeyNorma?indice=C.D.A&idContenido=29>

- El banco ha integrado a sus actividades normales el monitoreo del riesgo operacional y ha identificado indicadores apropiados que entreguen alertas de un aumento del riesgo y de futuras pérdidas.
 - El banco es capaz de cuantificar los impactos de las pérdidas asociadas al riesgo operacional y constituir prudencialmente los resguardos necesarios.
 - Los sistemas de información permiten hacer un monitoreo continuo de la exposición a los riesgos operacionales.
 - El banco cuenta con políticas para administrar los riesgos asociados a las actividades entregadas a terceras partes y lleva a cabo verificaciones y monitoreo a las actividades de dichas partes.
 - El banco realiza inversiones en tecnología de procesamiento y seguridad de la información, que permiten mitigar los riesgos operacionales y que son concordantes con el volumen y complejidad de las actividades y operaciones que realiza.
 - El banco cuenta con una adecuada planificación a largo plazo para la infraestructura tecnológica y dispone de los recursos necesarios para el desarrollo normal de sus actividades.
 - 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.
 - El banco considera en sus planes de continuidad del negocio y contingencia, diversos escenarios y supuestos que pudieran impedir que cumpla toda o parte de sus obligaciones y en ese sentido ha desarrollado una metodología formal que considera en sus etapas, la evaluación de impacto y criticidad de sus servicios y productos, la definición de estrategias de prevención, contención y recuperación, así como pruebas periódicas de tales estrategias.
 - El banco ha implementado un proceso para controlar permanentemente la incorporación de nuevas políticas, procesos y procedimientos, que permiten detectar y corregir sus eventuales deficiencias de manera de reducir la frecuencia y severidad de los eventos de pérdida.
 - La entidad bancaria ha adoptado una estrategia y sistema de gestión de calidad respecto de sus productos, servicios, e información que suministra a sus clientes, reguladores y a otros entes.
 - La extensión y profundidad de las auditorías es proporcional al nivel de riesgo y al volumen de actividad. La función de auditoría está en posición de evaluar en forma independiente el cumplimiento de las políticas, la eficacia de los procedimientos y los sistemas de información.
- El capítulo **20-7 de la RAN, sobre Externalización de Servicios**⁵⁸, el Título II indica que una sólida gestión de riesgos se basa en la existencia de una adecuada estructura de gobierno, un marco con políticas, normas y procedimientos, así como un entorno que permita identificar, evaluar, controlar, mitigar, monitorear y reportar los riesgos más relevantes asociados al outsourcing de actividades, proceso que en el caso del riesgo

⁵⁸ <https://www.sbif.cl/sbifweb/servlet/LeyNorma?indice=C.D.A&idContenido=191>

operacional debe cumplirse en concordancia con lo indicado en la letra C) del numeral 3.2 del Título II del Capítulo 1-13.

Asimismo, el Capítulo III, letra I) expresa que la entidad debe incorporar en sus reportes de riesgo operacional que elabora para el directorio, o para quien haga sus veces, información respecto de la gestión que realiza la institución para administrar los riesgos de outsourcing, incluyendo los cambios en el perfil de riesgos de los proveedores (como por ejemplo, cambios relevantes en sus procesos y áreas geográficas de donde se prestan los servicios) y la exposición a aquellos servicios considerados críticos.

- El capítulo **20-8 de la RAN, sobre Información de Incidentes Operacionales**⁵⁹, establece que la incorporación de tecnología en la forma de generar, procesar y administrar sus activos de información, involucran riesgos operacionales que afectan los procesos del negocio de la institución.

Por lo anterior, es relevante que las entidades dispongan de sistemas, procedimientos y mecanismos de gestión que permitan identificar, registrar, evaluar, controlar, mitigar, monitorear y reportar incidentes operacionales.

Así, las entidades deberán comunicar a la Comisión los incidentes operacionales que afecten o pongan en riesgo la continuidad del negocio, los fondos o recursos de la entidad o de sus clientes, la calidad de los servicios o la imagen de la institución en un plazo máximo de 30 minutos luego de su ocurrencia. El banco, en caso de incidentes, será responsable de mantener informada a la Comisión de la situación en desarrollo y de las medidas o acciones de detección, respuesta y recuperación del incidente.

- Finalmente, el capítulo **20-9 de la RAN, sobre Gestión de Continuidad del Negocio**⁶⁰, establece un conjunto de lineamientos y buenas prácticas que las entidades deben considerar en la gestión de los riesgos de continuidad del negocio en términos de proporcionalidad. Complementando lo que señala la letra c) del numeral 3.2 del Título II del Capítulo 1-13 de esta Recopilación sobre la evaluación del riesgo operacional, como asimismo lo dispuesto en el Capítulo 20-7 en lo que se refiere a los riesgos que se asumen en la externalización de servicios.

Por su parte, dado el contexto del mercado nacional, en cuanto a establecer mejoras en la gestión de la seguridad de los activos de información sujetos a riesgo en el ciberespacio, la Comisión se planteó la necesidad de incorporar aspectos específicos en materia de riesgos, en el caso puntual de **Ciberseguridad**.

En línea con los objetivos alineados con Política Nacional de Ciberseguridad (abril 2017), que otorga un marco específico en materias de seguridad de la información en el ciberespacio, es que se desarrolló una serie de Modificaciones Normativas las cuales apuntan a los siguientes objetivos estratégicos:

⁵⁹ <https://www.sbif.cl/sbifweb/servlet/LeyNorma?indice=C.D.A&idContenido=14321>

⁶⁰ https://www.sbif.cl/sbifweb3/internet/archivos/norma_11364_1.pdf

- Establecer lineamientos mínimos que deben ser considerados por las instituciones a fin de gestionar la seguridad de sus activos de información sujetos a riesgos en el ciberespacio.
- Necesidad de generar una base de incidentes de *Ciberseguridad* bajo un estándar común, que tiene por objeto establecer un lenguaje y nivel de información mínimo y homogéneo en la industria.

A continuación, se detalla la normativa vigente circunscrita al ámbito de **Ciberseguridad**.

Capítulo 1-13 CLASIFICACIÓN DE GESTIÓN Y SOLVENCIA⁶¹

En el Capítulo 1-13 de la Recopilación Actualizada de Normas la letra C) del numeral 3.2 del Título II sobre la Administración del Riesgo Operacional introduce el carácter **esencial** de que las instituciones cuenten con una clara definición, caracterización e identificación de los principales activos de información y de la infraestructura física que soporta y resguarda la seguridad de los mismos. Adicionalmente, la norma hace referencia al Capítulo 20-10 “GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD” para una adecuada gestión de la seguridad de información y ciberseguridad.

El Anexo N°3 de la normativa establece aspectos mínimos a tener en cuenta en la definición y gestión de la infraestructura crítica y la generación y gestión de la base de incidentes de Ciberseguridad. La infraestructura crítica contempla a aquellos activos de información lógicos que son considerados críticos para el funcionamiento del negocio. Asimismo, considera la infraestructura física, hardware y sistemas tecnológicos que almacenan, administran y soportan estos activos y que, de no operar adecuadamente, exponen a la entidad a riesgos de integridad, disponibilidad y confidencialidad de la información.

Adicionalmente el capítulo contiene tres ejemplos de buena gestión las situaciones /ejemplos relativos a; gestión de incidentes de ciberseguridad, base de datos de incidentes de ciberseguridad y uso de esta base de datos de incidentes como input para detectar amenazas y vulnerabilidades que pudiesen existir en el sistema de seguridad e la información.

⁶¹ <https://www.sbif.cl/sbifweb/servlet/LeyNorma?indice=C.D.A&idContenido=29>

Capítulo 20-8 INFORMACIÓN DE INCIDENTES OPERACIONALES⁶².

El Capítulo 20-8 “Información de Incidentes Operacionales Relevantes y Base de Datos de Incidentes de Ciberseguridad”, establece la obligación de informar a la Superintendencia los incidentes operacionales relevantes, **en especial aquellos relacionados con la Ciberseguridad**, y además establece las condiciones que se deben observar para generar y mantener una base de incidentes en el ámbito de la Ciberseguridad. Adicionalmente;

- Precisa conceptualmente el tipo de incidentes operacionales que deben ser comunicados a la Superintendencia; incidentes operacionales que afecten o pongan en riesgo la continuidad del negocio, los fondos o recursos de la entidad o de sus clientes, la calidad de los servicios o la imagen de la institución.
- Establece la oportunidad, contenido mínimo y mecanismo de comunicación de los incidentes operacionales.
- Define el tipo de información que debe ser proporcionada a los clientes y a la industria, respectivamente.

Capítulo 20-9 GESTION DE LA CONTINUIDAD DEL NEGOCIO⁶³.

- Establece a los “ataques maliciosos que afecten la Ciberseguridad” como mínimo escenario de contingencia a considerar. (contenido en el numeral I. *ELEMENTOS GENERALES DE GESTIÓN.*)
- Considera la “Operación de los sitios de procesamiento de datos se encuentran certificados por una entidad especializada e independiente” como ejemplo de hecho que manifiesta una adecuada gestión y que contribuye a fortalecer la resiliencia operacional de las entidades. (contenido en el numeral II. *SITIOS DE PROCESAMIENTO DATOS E INFRAESTRUCTURA TECNOLÓGICA.*)

Carta Circular N° 06-2018 Manual Sistema de Información incidentes Ciberseguridad, Archivo I12⁶⁴, del 18 de diciembre de 2018

Con el Objetivo contar con una base consolidada de los eventos en materia de Ciberseguridad, y dar seguimiento a los mismos, se introduce el archivo I12 mediante el cual los bancos informarán todos los incidentes en materia de Ciberseguridad ocurridos en el mes en curso, incluida la información actualizada o complementaria de incidentes reportados en periodos anteriores.

⁶² <https://www.sbif.cl/sbifweb/servlet/LeyNorma?indice=C.D.A&idContenido=14321>

⁶³ <https://www.sbif.cl/sbifweb/servlet/LeyNorma?indice=C.D.A&idContenido=15751>

⁶⁴ https://www.sbif.cl/sbifweb3/internet/archivos/norma_12358_3.pdf

Para finalizar en el mes de agosto de 2019 y mediante carta enviada a los Gerentes Generales de cada Banco se solicitó completar la encuesta “Estado de la ciberseguridad en las Instituciones Financieras 2019” la cual tiene como objetivo conocer a nivel general el estado de desarrollo de las prácticas de ciberseguridad en las entidades supervisadas por la Comisión para el Mercado Financiero.

Capítulo 20-10 GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD⁶⁵.

Norma establece nuevos lineamientos de sanas prácticas para una adecuada gestión de la seguridad de información y ciberseguridad. Este nuevo Capítulo refunde además las disposiciones actualmente vigentes en ciberseguridad del Capítulo 1-13 de la Recopilación Actualizada de Normas.

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 señala 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 define una especial diligencia para gestionarlos. La última sección, indica consideraciones que deben tener las instituciones al formar parte relevante de la infraestructura crítica del país. Los lineamientos que contiene la norma se resumen en los siguientes puntos:

- 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 establece 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 crítica 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.

⁶⁵ http://www.cmfchile.cl/portal/principal/605/articles-29310_doc_pdf.pdf

3. POLÍTICA NACIONAL DE CIBERSEGURIDAD (PNCS)

Los hechos recientes de seguridad informática crearon un ambiente donde Chile es percibido como un país altamente vulnerable a delitos informáticos o hackeos masivos. El desarrollo tecnológico y la digitalización de los procesos ha superado la velocidad de actualización de las normativas o leyes, por lo que se está trabajando en iniciativas para subir estándares y establecer normas de ciberseguridad.

En abril de 2017 el gobierno de la ex presidenta Michelle Bachelet dio a conocer la Política Nacional de Ciberseguridad⁶⁶ 2017-2022, (en adelante, PNCS), constituyéndose en el primer instrumento de política pública del Estado de Chile tendiente a desarrollar una estrategia nacional en esta materia, con el propósito de contar con un ciberespacio libre, abierto, seguro y resiliente.

La PNCS se articula en dos secciones centrales, la primera de ella establece una agenda con disposiciones específicas para ser implementadas entre los años 2017-2018, y la segunda una política de Estado diseñada con objetivos a largo plazo orientados al año 2022.

Dentro de los motivos que hicieron necesaria la emisión de la Política Nacional de Ciberseguridad se encuentran:

- Respuesta a la masificación en el uso de tecnologías de información y comunicaciones (TIC) y a los riesgos que esta realidad conlleva.
- Compromiso presidencial de **“desarrollar una estrategia de seguridad digital que proteja a los usuarios privados y públicos”**.
- Documento en si contiene una mirada que apunta al año 2022, para alcanzar el objetivo de contar con un **ciberespacio libre, abierto, seguro y resiliente**.

Fundamentos que hacen necesaria una Política Nacional de Ciberseguridad:

- a) Resguardar la seguridad de las personas en el ciberespacio
- b) Proteger la seguridad del país.
- c) Promover la colaboración y coordinación entre instituciones
- d) Gestionar los riesgos del ciberespacio

Estado actual de la ciberseguridad: normas, instituciones, panorama de riesgos

- a) **Normas e instituciones:** la institucionalidad vigente en materia de ciberseguridad se encuentra distribuida en diversos organismos y entidades⁶⁷. Esto hace necesario la coordinación estratégica de los distintos esfuerzos, de sus roles y funciones, y el establecimiento de prácticas y criterios técnicos comunes, con el objetivo de mejorar la eficiencia y eficacia en el ámbito de la ciberseguridad. Adicionalmente, se hace necesaria la revisión de las normas y reglamentos que se hacen cargo, directa e indirectamente, del tema

⁶⁶ <https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf>

⁶⁷ Anexo N°1 de la PNCS incluye detalle de normas relevantes a nivel nacional (Constitución Política de la República, Leyes y Decretos), así como instituciones intervinientes en materia de Ciberseguridad (Ministerios, Universidades, Instituto Nacional de Normalización, Ministerio Público y Poder Judicial).

ciberseguridad, acogiendo las directrices de esta política y los compromisos internacionales, por ejemplo, la ley N° 19.223 sobre delitos informáticos o la ley N° 19.628 sobre protección de la vida privada, entre otras.

b) Panorama de riesgos: naturaleza global de los riesgos (amenazas provienen de Chile y del exterior). La política considera las diversas clases de amenazas que afecten las infraestructuras críticas del país.

- **Agenda Digital 2020⁶⁸:** La Agenda Digital 2020 es una hoja de ruta para avanzar hacia el desarrollo digital del país, mediante la definición de objetivos de mediano plazo, líneas de acción y medidas concretas. Fue lanzada el segundo semestre de 2015. En la agenda existe una medida específica (N°25) que apunta a la elaboración de una estrategia de ciberseguridad.
- **Política nacional de ciberdefensa:** Relación a la defensa nacional a cargo del Ministerio de Defensa.
- **Política internacional para el ciberespacio:** cooperación y relaciones internacionales en torno a la ciberseguridad en el contexto global a cargo del Ministerio de Relaciones Exteriores.

Objetivos de política para el año 2022

En este eje articulador, se establecen los lineamientos generales que la Política Nacional de Ciberseguridad pretende alcanzar al año 2022, así como también los sub objetivos necesarios para poder concretarlos.

A continuación, se describen estos pilares y sus respectivos cursos de acción:

1. El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos.

Este primer pilar busca llegar a contar con una infraestructura de la información robusta y resiliente⁶⁹, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos.

Para el logro de lo planteado se hace necesario cumplir con:

- estipular medidas técnicas tendientes a prevenir, gestionar y superar los riesgos cuando estos se verifican a fin de proteger la infraestructura de la información;
- identificar y jerarquizar las infraestructuras críticas de la información;
- contar con equipos de respuesta a incidentes de ciberseguridad;

⁶⁸ <http://www.agendadigital.gob.cl>

⁶⁹ La Resiliencia en el ámbito de la Tecnología de la Información (TI) se entiende como la capacidad de la infraestructura, ya sea de servidores, comunicaciones o de seguridad, de proveer y mantener una continuidad operacional, a pesar de las fallas, tales como: problemas por sobrecarga, fallas en el datacenter, ancho de banda saturada, tráfico malicioso en la organización, amenazas avanzadas al descubierto, filtración de información confidencial y de ataques de secuestro digital de información (ransomware), etc.. Esta capacidad adquiere especial importancia en la Administración Pública y los Sistemas de Información y Telecomunicaciones.

- implementar mecanismos estandarizados de reporte, gestión y recuperación de incidentes;
- fijar estándares diferenciados en materia de ciberseguridad.
-

2. El Estado velará por los derechos de las personas en el Ciberespacio

Este objetivo se centra en proteger los derechos de los ciudadanos en el ciberespacio, responsabilidad que recae en el Estado. Para su cumplimiento será necesario:

- la prevención de ilícitos y generación de confianza en el ciberespacio;
- el establecimiento de prioridades en la implementación de medidas sancionatorias;
- la existencia de prevención multisectorial;
- el respeto y la promoción de derechos fundamentales.

3. Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales.

La necesidad de educar a los ciudadanos en una cultura ciber lleva al desarrollo de este tercer pilar estratégico:

- Una cultura de la ciberseguridad;
- Sensibilización e información a la comunidad;
- Formación para la ciberseguridad.

4. El país establecerá relaciones de cooperación en ciberseguridad con otros actores y participará activamente en foros y discusiones internacionales.

El ciberespacio constituye un ámbito mundial por lo que se hace necesario desplegar estrategias globales para su pleno y positivo desarrollo. La cooperación internacional resulta imprescindible para enfrentar el desafío de esta Revolución Científica y Tecnológica.

Para ello la PNCS propone las siguientes acciones:

- Principios de política exterior chilena;
- Cooperación y asistencia;
- Reforzar la participación en instancias multilaterales y en instancias de múltiples partes interesadas (multistakeholder);
- Fomentar normas internacionales que promuevan la confianza y seguridad en el ciberespacio.

5. El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos.

El avance en el desarrollo de los países hoy está íntimamente ligado a la creación y manejo de nuevas tecnologías. Este objetivo busca impulsar el estudio y comprensión del ciberespacio para colocar al país en la vanguardia del conocimiento.

- Importancia de la innovación y desarrollo en materia de ciberseguridad;
- Ciberseguridad como medio para contribuir al desarrollo digital de Chile;
- Desarrollo de la industria de ciberseguridad en Chile;

- Contribuir a la generación de oferta por parte de la industria local;
- Generación de demanda de parte del sector público basado en los intereses estratégicos del Estado.

Durante el gobierno del Presidente Sebastián Piñera se ha decidido no solo dar continuidad a la PNCS sino profundizar en ella. Una de las medidas tomadas por parte del Ejecutivo fue separar las competencias propias de la Ciberdefensa, dejándolas en manos de la cartera del ramo; **Ciberseguridad**, que pasan a ser asumidas por el Ministerio del Interior; y **Ciberinteligencia**, definidas desde la óptica de la Agencia Nacional de Inteligencia (ANI), si bien todas ellas coordinadas a través del Comité Interministerial de Ciberseguridad.