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 Nº 454

A todas las entidades aseguradoras y reaseguradoras

18 de mayo de 2021

Esta Comisión, 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° 235 del 13 de mayo de 2021, 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 pérdidas financieras que resulta de fallos en los procesos, personas o sistemas, ya sea ante eventos internos o externos. 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 GESTION 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 su apropiada identificación y gestión.

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).

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 asegurador[1], 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

[1] https://www.iaisweb.org/file/61857/issues-paper-on-cyber-risk-to-the-insurance-sector

referencia de diversas fuentes tales como: el *NIST Cybersecurity Framework*[2], publicado por el Instituto Nacional de Estándares y Tecnología (NIST); el *G7 Fundamental Elements of Cyber Security for the Financial Sector (G7FE)*[3]; el *G7 Fundamental Elements for Effective Assessment of Cybersecurity for the Financial Sector (G7FEA)*[4] y en la *Guidance on Cyber Resilience for Financial Market Infrastructures (CPMI-IOSCO Guidance)*[5]. 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

[2] https://www.nist.gov/cyberframework
[3] https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf
[4] http://www.mef.gov.it/inevidenza/documenti/PRA_BCV_4728453_v_1_G7_Fundamental.pdf
[5] https://www.bis.org/cpmi/publ/d146.pdf

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)".

   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 al directorio. 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:

<u>Identificación y clasificación de funciones.</u>

- 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 Ingles) 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 almacenamiento[6] 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.

[6] 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.

- 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. 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), *"E*stablecer 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 de ser 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), *"R*eanudar 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 ingles), 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 que la compañía tome conocimiento de dicho (s) incidente (s).

Para estos efectos, la entidad deberá definir un funcionario titular y su reemplazo, quien realizará los reportes y enviará la información según lo indicado en este numeral. El funcionario titular y quien lo 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. Su designación y/o reemplazo deberá ser comunicado mediante carta a la CMF dentro del plazo comprendido entre la entrada en vigencia de la presente normativa y en forma previa a la entrada en vigencia de la plataforma dispuesta especialmente para la comunicación de

incidentes. Asimismo, cambios en la designación del funcionario titular y/o reemplazo deberá ser comunicado a la CMF a través del mismo mecanismo en forma inmediata a su designación.

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 que afecte a la compañía, ésta 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.

Finalmente, este sistema deberá estar en funcionamiento a contar del 30 de septiembre de 2021.

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.

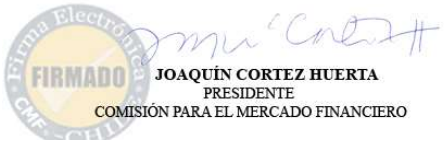
VII. VIGENCIA Y APLICACIÓN

La presente norma entra en vigencia a contar del 30 de septiembre de 2021.

La autoevaluación relativa a riesgo operacional se deberá realizar en régimen con una periodicidad cada dos años, debiendo ser informada el 30 de septiembre de cada año que se realice dicha autoevaluación. En lo relativo a la autoevaluación de ciberseguridad, ésta se deberá realizar en forma anual y quedar disponible el 30 de septiembre de cada año. En ambos casos, la autoevaluación respectiva, deberá estar referida a la situación de la compañía al 30 de junio de cada año.

Disposición Transitoria

La autoevaluación del cumplimiento de los principios de riesgo operacional establecidos en esta norma, deberá efectuarse e informarse por primera vez a más tardar el 31 de diciembre de 2021, referida a la situación de la compañía al 30 de septiembre de 2021. Para el caso de la autoevaluación de los principios de ciberseguridad establecidos en esta norma, deberá efectuarse y quedar disponible el 31 de diciembre de 2021, referida a la situación de la compañía al 30 de septiembre de 2021.



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. **Observado:** 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. **Ampliamente observado:** 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 observado:** 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 observado:** La compañía aún no ha implementado esta práctica.

5. **N/A:** La compañía determina que la calificación de 1 a 4 no es aplicable. En dicho caso, se solicita que la compañía 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:				
<u>Taxonomía de Riesgo Operacional</u>				
4-2.01	Taxonomía de riesgo operacional que articule la naturaleza y el tipo de riesgo operacional al que la compañía está potencialmente expuesta.			
<u>Evaluación y Control</u>				
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 internos importantes.			
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. **Observado:** 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. **Ampliamente observado:** 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 observado:** La compañía ha implementado parcialmente el principio, los aspectos principales de la implementación permanecen, y puede haber algunos temas significativos pendientes.

4. **No observado: La compañía aún no ha implementado esta práctica.**

5. **N/A:** La compañía determina que la calificación de 1 a 4 no es aplicable. En dicho caso, se solicita que la compañía 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[7].			
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			

[7] 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.

	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 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 periódicas 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: · 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 de seguros participa en los grupos de trabajo, sobre ciberseguridad, que ha establecido la industria aseguradora, en caso de existir dichas instancias.			

4. Gestión de Riesgos de Amenazas y Vulnerabilidades

Item	Criterio	Evaluación de Cumplimiento	Fundamento de la Evaluación (Diseño de Control y Eficacia)	Plan de acción y plazo(s) para su plena implementación
Detección de Pérdida de Datos / Prevención				
4.01	La compañía ha implementado herramientas para: · 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 almacenamiento online y offline (p. ej., computadores de escritorio, computadores 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.			
Detección y mitigación de incidentes de ciberseguridad				
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).			
Seguridad del Software				

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.			
Infraestructura de Red				
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: · 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: · 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 empresa8, 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.			

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

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.			
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 ingles), análisis de escenarios, procesos de gestión de cambios, indicadores claves de riesgo (KRIs por sus siglas en ingles), 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.			