REF: **IMPARTE INSTRUCCIONES SOBRE GESTIÓN DE RIESGO OPERACIONAL. DEROGA CIRCULARES N° 1.939 y 2.020, Y LA NORMA DE CARÁCTER GENERAL N° 256. MODIFICA LA NORMA DE CARÁCTER GENERAL N° 480.**

NORMA DE CARÁCTER GENERAL N°510

8 de mayo de 2024

Esta Comisión en uso de las atribuciones conferidas en el Decreto Ley N°3.538, la Ley N°18.045, la Ley N°18.876, la Ley N°19.220, la Ley N°20.345, la Ley N°20.712 y Ley N°21.521; y teniendo en consideración que su mandato legal es velar por el correcto funcionamiento, desarrollo y estabilidad del mercado financiero, ha estimado pertinente impartir las siguientes instrucciones respecto de la gestión de riesgo operacional para Administradoras Generales de Fondos, Bolsas de Valores, Bolsas de Productos, Sociedades Administradoras de Sistemas de Compensación y Liquidación de Instrumentos Financieros y Entidades de Depósito y Custodia de Valores.

I. GESTIÓN DE RIESGO OPERACIONAL

El riesgo operacional corresponde al riesgo que las deficiencias que puedan producirse en los sistemas de información, los procesos internos o el personal, o las perturbaciones ocasionadas por acontecimientos externos provoquen la reducción, el deterioro o la interrupción de los servicios que presta la entidad y, eventualmente, le originen pérdidas financieras. Incluye el riesgo de pérdidas ante cambios regulatorios que afecten las operaciones de la entidad, como también pérdidas derivadas de incumplimiento o falta de apego a la regulación vigente.

La entidad deberá tener la capacidad de seguir entregando sus servicios en caso de que se presente un evento disruptivo, para lo cual deberá gestionar el riesgo operacional mediante una adecuada combinación de políticas, procedimientos, controles, estructura organizacional y sistemas de información, conforme a la naturaleza, volumen y complejidad de sus operaciones.

Con el objeto de que la entidad desarrolle una adecuada gestión de riesgo operacional, se deberá dar cumplimiento a los principios y elementos que se señalan a continuación:

1. Las políticas y procedimientos de gestión de riesgo operacional deberán estar formalmente establecidas y documentadas, debiendo formar parte de las políticas y procedimientos de gestión de riesgos de la entidad, de acuerdo con la normativa de gobierno corporativo y gestión de riesgos emitida a tal efecto por esta Comisión.

2. Los planes de trabajo y la emisión de informes de gestión de riesgo operacional al

directorio, u órgano equivalente, deberán formar parte de la gestión de riesgo integral, de acuerdo con la normativa de gobierno corporativo y gestión de riesgos de la entidad.

3. Las políticas y procedimientos de gestión de riesgo operacional deberán incluir, al menos, los siguientes ámbitos relacionados, descritos en las próximas secciones: A) seguridad de la información y ciberseguridad, B) continuidad de negocio; y C) externalización de servicios. Los ámbitos mencionados deberán ser considerados por la entidad en los informes que realicen las instancias encargadas de la gestión de riesgos y la auditoría interna, según corresponda.

4. Las políticas de gestión de riesgo operacional deben estar diseñadas para brindar una seguridad razonable que la entidad pueda desarrollar las operaciones del negocio en forma continua y eficiente, incluso ante la presencia de eventos disruptivos, salvaguardando sus servicios, procesos y activos de información. Estas políticas deben ser aprobadas por el directorio, u órgano equivalente, y ser difundidas a todo el personal dentro de la organización. Además, dichas políticas deben establecer los niveles de apetito por riesgo definidos por el directorio u órgano equivalente, que determinará la necesidad de implementar un plan de tratamiento, de forma de evitar, reducir, transferir o aceptar los riesgos, y acorde con ello, diseñar controles mitigantes.

5. El directorio, u órgano equivalente, debe velar porque las políticas, procesos y sistemas dentro de la organización sean consistentes con el apetito por riesgo definido y contengan líneas claras de responsabilidad sobre la gestión de riesgo operacional. Asimismo, deberá dotar a las instancias pertinentes de la entidad con los recursos y personal necesario para la gestión de riesgo operacional, en función del volumen y complejidad de las operaciones de la entidad.

6. Contar con indicadores claves de medición del riesgo operacional consistentes con la metodología de evaluación y monitoreo de riesgos integrales de la entidad, permitiendo al mismo tiempo establecer niveles de alerta y evaluar la eficacia de los controles adoptados. El detalle de cálculo de estos indicadores deberá ser incluido expresamente en las políticas y procedimientos de gestión de riesgo operacional de la entidad.

A. SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

A.1. Disposiciones generales

En el ámbito de seguridad de la información y ciberseguridad, la gestión de riesgo operacional deberá incluir los siguientes elementos, tomando en consideración el volumen y complejidad de las operaciones de la entidad:

1. Contar con una política de seguridad de la información y ciberseguridad que considere al menos lo siguiente:

1.1. Procedimientos para la implementación y mantención de un sistema de gestión de seguridad de la información y ciberseguridad, de forma resguardar la disponibilidad, confidencialidad e integridad de los activos de información.

1.2. Niveles de apetito por riesgo en materia de seguridad de la información y ciberseguridad.

1.3. Principales funciones y responsabilidades sobre la materia.

1.4. Procedimientos para la evaluación de los riesgos de seguridad de la información y

ciberseguridad que se podrían estar asumiendo al introducir nuevos productos, sistemas, emprender nuevas actividades o definir nuevos procesos.

1.5. Una actualización al menos anual o cuando ocurran cambios significativos, debiendo ser aprobada dicha actualización por el directorio, u órgano equivalente.

2. Contar con una política de tecnologías de información y comunicación (TIC), que considere al menos lo siguiente:

2.1. Definición de las líneas de responsabilidad en cuanto a la gestión de los activos de información en la entidad.

2.2. Definición de los procesos TIC que aseguren un adecuado diseño, transición, operación de servicio y gestión a través de sus activos de información.

2.3. Definición de los procedimientos que se deberán seguir para la adecuada gestión de los procesos TIC.

3. Definir el perfil y número necesario de personas con conocimientos comprobables en estándares de seguridad de la información y ciberseguridad.

4. Establecer los procedimientos para que el personal de la entidad, incluyendo el directorio u órgano equivalente, contribuya a una adecuada gestión de los riesgos de seguridad de la información y ciberseguridad, de conformidad con sus roles y responsabilidades, mediante la implementación de:

4.1. Procedimientos de difusión, capacitación y concientización que traten sobre los riesgos, vulnerabilidades y amenazas a la seguridad de la información, la gestión de los mismos, y las lecciones aprendidas respecto de los incidentes en esta materia para garantizar que el personal de la entidad esté debidamente preparado para enfrentar los escenarios de contingencia definidos y que comprendan sus responsabilidades en la gestión de dichos riesgos.

4.2. Acuerdos contractuales con los empleados que establezcan sus responsabilidades y las de la entidad en materia de seguridad de la información y ciberseguridad, incluyendo sanciones. Asimismo, dichos acuerdos deberán incluir la revocación de derechos de acceso a información y devolución de activos de información ante un proceso de cambio de posición o desvinculación de un empleado.

5. Auditar los procesos de gestión de la seguridad de la información y ciberseguridad, con la profundidad y alcance necesario, que considere aspectos tales como el cumplimiento de las políticas y la eficacia de los procedimientos y controles definidos en estas materias.

6. Establecer procedimientos que le permitan al directorio u órgano equivalente mantenerse informado en forma oportuna y periódica sobre el sistema de gestión de la seguridad de la información y ciberseguridad. Deberá dejarse constancia del reporte de la información de estas materias en las respectivas actas del directorio u órgano equivalente y los comités que se conformen para revisar estas materias.

7. En el caso de las Bolsas de Valores, Bolsas de Productos, Entidades de Depósito y Custodia y Sociedades Administradoras de Sistemas de Compensación y Liquidación, se deberá dar cumplimiento a las siguientes disposiciones adicionales:

7.1. Efectuar la gestión de los riesgos de seguridad de la información y ciberseguridad a nivel de activos.

7.2. Realizar una evaluación del estado actual de la seguridad de la información y ciberseguridad de la entidad a partir de un estándar o práctica internacional de común aceptación, y definir el estado deseado.

7.3. Establecer los planes que se deberán implementar para llegar al estado deseado.

7.4. Disponer de una estructura de alto nivel para la administración de crisis, con las atribuciones necesarias para gestionar los eventos disruptivos relacionados con la seguridad de la información y ciberseguridad que se puedan presentar.

7.5. Cuantificar el riesgo, ya sea a través de un modelo cuantitativo o cualitativo, teniendo en consideración, a lo menos, la criticidad del activo y el efecto en las dimensiones de disponibilidad, confidencialidad e integridad. Asimismo, en la definición de la probabilidad del riesgo se deberá tener en consideración, entre otros, la base de incidentes operacionales.

7.6. Identificar las amenazas y vulnerabilidades que puedan afectar a los activos de información, para lo cual se deberá tener en consideración toda la información disponible, interna y especialmente externa, tales como las bases de conocimiento disponibles o marcos de trabajo, públicas y no públicas, que detallen tácticas y técnicas de ataque y vulnerabilidades de activos.

7.7. Contar con una persona encargada de la seguridad de la información, independiente de las áreas operativas y de auditoría interna, que evalúe y provea información relevante al directorio, gerente general y otras áreas sobre el nivel de exposición a los riesgos de seguridad de la información y ciberseguridad. Sus funciones podrán ser desempeñadas por una persona del grupo empresarial al que pertenezca la entidad, siempre que mantenga su independencia de las áreas operativas y de auditoría interna del grupo.

A.2. Procedimientos para la gestión de seguridad de la información y ciberseguridad

Sin perjuicio de lo establecido en el literal A.1 de esta sección, las entidades mencionadas a continuación deberán considerar los siguientes procedimientos:

A.2.1. Administradoras Generales de Fondos

a. Identificación

1. Contar con una definición clara de activos de información que sea suficiente para la adecuada gestión de los riesgos asociados.

2. Clasificar la información, teniendo en consideración las dimensiones de disponibilidad, confidencialidad e integridad.

3. Definir los activos de información críticos, que son los activos considerados como indispensables para el funcionamiento del negocio, con un nivel suficiente de detalle que permita su gestión, clasificados desde una perspectiva de disponibilidad, confidencialidad e integridad.

4. Implementar un inventario de activos de información que permita conocer las principales características del activo, considerando al menos: hardware, software, aplicaciones, dispositivos, sistemas, datos, personal, sistemas de información externos, procesos, instalaciones, estaciones de trabajo, servidores, medios de almacenamiento y documentación física.

5. Actualizar el inventario de activos de información en forma continua, para lo cual los distintos procesos de gestión de riesgo operacional deberán reportar la información que pueda tener efecto en dicho inventario.

b. Protección y Detección

1. Establecer controles de acceso a las instalaciones e infraestructuras de negocios,

operativas y dependencias técnicas, dentro de las que se encuentran los centros de datos, fuentes de energía alternativa y respaldos de datos y aplicativos.

2. Establecer controles de acceso a los sistemas, de manera de mitigar los riesgos de suplantación o uso indebido por parte de terceros. En el caso de instalaciones, infraestructuras y sistemas críticos, se deberá privilegiar el uso de mecanismos de autenticación multifactor.

3. Implementar herramientas de registro, control y monitoreo de las actividades realizadas por los usuarios y administradores de sistemas y activos de información, incluyendo usuarios de alto privilegio.

4. Establecer procedimientos para otorgar, revocar o modificar los privilegios otorgados a los usuarios de los sistemas, servicios de red, sistemas operativos, bases de datos y aplicaciones de negocios en función de los roles y responsabilidades del personal y sólo lo estrictamente necesario para que éste cumpla sus funciones actuales.

5. Establecer controles que permitan mitigar los riesgos derivados del uso de dispositivos móviles y del acceso remoto realizado por personal interno o externo, así como también los dispositivos Internet de las Cosas ("IoT").

6. Establecer mecanismos de control y monitoreo de las condiciones ambientales para la localización segura para los equipos y herramientas, teniendo en consideración las condiciones de humedad, temperatura y la posibilidad de desastres y otras contingencias.

7. Establecer procedimientos de seguridad de las operaciones y comunicaciones de la entidad, mediante la implementación de:

7.1. Herramientas y controles para la detección y protección proactiva de ataques cibernéticos y otras actividades anómalas, diseñadas en función del volumen y complejidad de las operaciones de la entidad. Por ejemplo, el uso de firewalls de aplicaciones web, sistemas de prevención de intrusos, sistemas de prevención de pérdida de datos, sistemas anti-denegación de servicios, filtrado de correo electrónico, antivirus, anti-spyware y anti-malware, entre otros.

7.2. Procesos de gestión de la configuración de los sistemas y activos de información.

7.3. Herramientas y procedimientos para el respaldo, transferencia, restauración y eliminación segura de la información, al interior de la organización y con terceros, incluyendo medios físicos y electrónicos. Para ello se deberá considerar:

a. Disposiciones relativas al respaldo, transferencia, restauración y eliminación de información en las normas que resguardan la protección de datos y los derechos del inversionista, incluyendo acuerdos de no divulgación.

b. Técnicas de encriptación y segmentación de redes para información en tránsito y en reposo.

c. Procesos de administración de respaldos que aseguren la disponibilidad confidencialidad e integridad de la información ante la ocurrencia de un incidente, el que debe ser concordante con el análisis de los riesgos para la gestión de la continuidad del negocio de acuerdo con lo dispuesto en la sección I.B de la presente norma. Los respaldos de la información se deben mantener en ambientes libres de códigos maliciosos y en instalaciones distintas a los sitios de producción. Además, se deben realizar pruebas de restauración de respaldos periódicas, al menos anuales, con el fin de verificar que la información crítica puede ser recuperada en los tiempos predefinidos en caso de que los datos originales se pierdan o se dañen.

d. Herramientas y procedimientos de identificación, autenticación y control de acceso para los canales digitales a través de los cuales la entidad interactúa con sus clientes.

e. Herramientas y procedimientos para que la información que la entidad decidiere almacenar o procesar mediante servicios en la nube conserve sus características de disponibilidad, confidencialidad e integridad.

c. Respuesta y Recuperación

1. La entidad deberá contar con procedimientos para la gestión de incidentes de seguridad de la información y ciberseguridad, considerando:

1.1. Una instancia de alto nivel definida por el directorio u órgano equivalente encargada de la gestión de incidentes de seguridad de la información y ciberseguridad.

1.2. Procedimientos de respuesta y recuperación ante incidentes, aprobados por el directorio u órgano equivalente, que consideren la recuperación oportuna de las funciones críticas, los procesos de respaldo y soporte, los activos de información críticos y las interdependencias con terceros en caso de incidentes. Dichos procedimientos deberán considerar las disposiciones relativas al registro, reporte y comunicación de incidentes de la sección I.D de esta norma. Asimismo, dependiendo de la severidad del incidente, corresponderá escalar la situación al directorio u órgano equivalente para la toma de decisiones. Los procedimientos de respuesta y recuperación ante incidentes deberán actualizarse al menos anualmente y cada vez que se registren cambios en los activos de información o se produzcan incidentes que amenacen la seguridad de éstos.

1.3. Procedimientos de comunicaciones para mantener informado en forma oportuna al directorio u órgano equivalente, a otras partes interesadas (tanto internas como externas), a las autoridades pertinentes en materia de seguridad de la información y ciberseguridad y a esta Comisión de la ocurrencia de un incidente y las medidas adoptadas para resolverlo. Estos procedimientos deberán considerar las disposiciones relativas al registro, reporte y comunicación de incidentes de la sección I.D de esta norma. Asimismo, tratándose de incidentes que afecten la calidad o continuidad de los servicios a los clientes o de un hecho de público conocimiento, la institución será responsable de informar oportunamente a los usuarios sobre la ocurrencia de dicho evento, debiendo actualizar la información disponible hasta que se conozcan las conclusiones sobre las causas del incidente y las medidas adoptadas para resolverlo, incluyendo el cumplimiento de las normas que resguardan la protección de datos personales y los derechos de los inversionistas.

1.4. Sin perjuicio de la información que debe ser reportada a esta Comisión, las entidades deberán evaluar la posibilidad de participar activamente en grupos o 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.

2. Procedimientos para el desarrollo, adquisición y actualización de la infraestructura tecnológica de la entidad, que consideren los siguientes elementos:

2.1. Evaluación de las necesidades de infraestructura tecnológica de la entidad.

2.2. Implementación de un proceso de gestión de cambio, de forma de asegurar que las modificaciones realizadas a los activos de información producto de la introducción de nuevos productos, sistemas y actividades sean efectuadas y monitoreadas de manera segura y controlada.

2.3. Realización de pruebas de carácter funcional, integral, de seguridad, de ciberseguridad, de continuidad y normativas, previo al paso de producción de un servicio o activo de información, con el propósito de asegurar que no se produzca un impacto adverso en la seguridad de la información y en las operaciones del negocio.

2.4. Implementación de un proceso de gestión de obsolescencia tecnológica, que permita mantener el software y hardware con soporte, salvo las excepciones debidamente fundamentadas que no generen efectos adversos para la operación de los servicios de la entidad. Se deberá prevenir el uso de software no autorizado o sin licenciamiento comercial.

2.5. Implementación de un proceso de gestión de actualizaciones de seguridad de software (parches).

3. La entidad deberá contar con un procedimiento para el mejoramiento continuo de las herramientas, procedimientos y controles de seguridad de la información y ciberseguridad que considere:

3.1. La recolección y análisis de información sobre el funcionamiento de activos de información.

3.2. El análisis de los incidentes de seguridad de la información y ciberseguridad y la efectividad de las medidas adoptadas para resolverlo.

3.3. La ejecución de pruebas con periodicidad al menos anual para identificar amenazas y vulnerabilidades en la seguridad de la información, con las siguientes características:

a. Las pruebas deberán ser diseñadas en función del volumen y complejidad de las operaciones de la entidad y supervisadas por la instancia responsable de la gestión de riesgos de la entidad.

Las pruebas deberán estar basadas en escenarios de riesgo planificados diseñados para demostrar que los mecanismos y herramientas implementados para preservar la seguridad de la información cumplen adecuadamente con su objetivo, incluyendo ataques cibernéticos.

b. Los resultados de las pruebas realizadas deberán ser reportados al directorio u órgano equivalente, incluyendo recomendaciones de mejora en las herramientas, procedimientos y controles.

A.2.2. Bolsas de Valores, Bolsas de Productos, Entidades de Depósito y Custodia y Sociedades Administradoras de Sistemas de Compensación y Liquidación

a. Identificación

1. Contar con una definición clara de activos de información que sea suficiente para la adecuada gestión de los riesgos asociados.

2. Clasificar la información, teniendo en consideración las dimensiones de disponibilidad, confidencialidad e integridad. Esta clasificación deberá ser utilizada para la clasificación de los activos de información.

3. Definir los activos de información críticos, que son los activos considerados como indispensables para el funcionamiento del negocio, con un nivel suficiente de detalle que permita su gestión.

4. Implementar un inventario de activos de información, el que deberá estar permanentemente actualizado. Este inventario de activos deberá ser consistente con los procesos de la entidad, además deberá contener la información que permita conocer las principales características del activo. El inventario deberá considerar a lo menos hardware, software, aplicaciones, dispositivos, sistemas, datos, personal, sistemas de información externos, procesos, instalaciones, medios de almacenamiento y documentación física.

5. Implementar un inventario de servicios. Este inventario de servicios deberá ser relacionado con los activos de información, los niveles de servicios acordados y los niveles operacionales acordados.

6. Contar con un registro de todas las redes y subredes implementadas y los activos de información que conforman dichas redes. Además, se deberán identificar las conexiones entre estas redes, con las redes externas y con otras infraestructuras de mercado, nacionales y extranjeras.

7. Actualizar de manera continua los inventarios y registros, para lo cual los encargados de los procesos, tales como gestión de personas, gestión de cambio, gestión de implementación y gestión de configuración, deberán reportar la información que pueda tener efecto en estos inventarios y registros.

b. Protección y Detección

1. Resguardar los activos de información de manera adecuada en términos de seguridad física y ambiental, teniendo en consideración las condiciones de humedad, temperatura y la posibilidad de desastres y otras contingencias como, por ejemplo: la protección de las áreas sensibles de negocios, operativas y dependencias técnicas, dentro de las que se encuentran los centros de datos, fuentes de energía alternativa y respaldos de datos y aplicativos.

2. Realizar pruebas de carácter funcional, integral, de seguridad, de ciberseguridad, de continuidad y normativas previo al paso de producción de un servicio, proceso o activo de información, o modificaciones de ellos, con el propósito de evitar que se afecte la disponibilidad, confidencialidad e integridad de los servicios vigentes. Se deberán establecer umbrales de aceptación.

3. Implementar un proceso de gestión de cambio, de forma de asegurar que las modificaciones realizadas a los activos de información sean efectuadas de manera segura y controlada, que los cambios realizados son controlados y monitoreados y que las pruebas previas al paso producción hayan cumplido los umbrales definidos.

4. Implementar un proceso de gestión de implementación y despliegue, de forma de asegurar el paso de producción de nuevos componentes, servicios, infraestructura u otros componentes, o la modificación de éstos.

5. Implementar un proceso de gestión de capacidad, que permita asegurar que la infraestructura TIC cubre las necesidades presentes y futuras. El proceso de gestión de capacidad deberá ser a nivel de servicio, sistemas y componentes. Además, se deberá implementar un modelo que relacione las operaciones con el uso de sistemas y componentes.

6. Implementar un proceso de gestión de disponibilidad, de forma de asegurar que se cumplan con los niveles de servicio de disponibilidad acordados.

7. Implementar un proceso de gestión de obsolescencia tecnológica, que permita mantener el software y hardware con soporte, salvo las excepciones debidamente fundamentadas mediante una evaluación de riesgos, y que no generen efectos adversos no previstos para la operación de los servicios de la entidad. Se deberá prevenir el uso de software no autorizado o sin licenciamiento comercial.

8. Implementar un proceso de gestión de configuraciones que permite asegurar adecuados controles a los elementos configurables de los activos de información; y que su acceso sea controlado y monitoreado.

9. Implementar un proceso de gestión de cumplimiento de los niveles de servicios acordados (SLA) y los niveles operacionales acordados (OLA).

10. Implementar un proceso de parches sobre la infraestructura TIC, con apoyo de una herramienta automatizada.

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

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

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

13. Establecer controles que permitan mitigar los riesgos derivados del uso de dispositivos móviles y del trabajo a distancia realizado por personal interno o externo; así como también los dispositivos Internet de las Cosas ("IoT").

14. Implementar herramientas, procedimientos, controles y pruebas que permitan proteger, detectar y contener ataques a los activos de información realizados a través del uso de códigos maliciosos.

15. Implementar una gestión de identidades y de acceso físico y lógico, que contemple adecuados controles para resguardar las áreas de acceso restringido. Se deben establecer procedimientos para otorgar, revocar o modificar los privilegios otorgados a los usuarios de los sistemas, los derechos de accesos a los servicios de red, a los sistemas operativos, a las bases de datos y a las aplicaciones de negocios, entre otros.

16. Contar con apropiados mecanismos de control de acceso a los sistemas, de manera de mitigar, entre otros, los riesgos de suplantación o uso indebido por parte de terceros. En la medida de ser necesario, se deberá implementar un segundo factor de autenticación.

17. Limitar los accesos a lo estrictamente necesario para que el personal cumpla sus funciones.

18. Mantener un registro actualizado de los derechos de acceso individuales y del sistema, de forma de tener conocimiento de los permisos de acceso a los activos de información y sus sistemas de respaldo.

19. Implementar herramientas para controlar, registrar y monitorear las actividades realizadas por los usuarios sobre los activos de información, así como de aquellos con privilegios especiales.

20. Definir procedimientos que determinen la información que requiere ser protegida a través de técnicas de cifrado, así como los algoritmos criptográficos permitidos o autorizados, tanto para la información en tránsito y en reposo.

21. Implementar adecuados resguardos para la conservación, transferencia y eliminación de la información, en conformidad con lo establecido en las políticas internas y la regulación vigente.

22. Implementar procedimientos y herramientas que permitan en forma proactiva identificar, recolectar y analizar información interna y externa respecto de nuevas amenazas y vulnerabilidades que puedan afectar sus activos de información.

23. Implementar procesos de administración de respaldos que le permita asegurar la

disponibilidad, confidencialidad e integridad de su información y de sus medios de procesamiento, ante la ocurrencia de un incidente, desastre u otra contingencia, el que debe ser concordante con el análisis de los riesgos para la gestión de la continuidad del negocio. Los respaldos de la información se debiesen mantener en ambientes libres de códigos maliciosos, adecuadamente controlados, y en instalaciones distintas a los sitios de producción. Además, se deben realizar al menos anualmente pruebas de restauración de sus respaldos, con el fin de verificar que la información crítica puede ser recuperada en caso de que los datos originales se pierdan o se dañen.

24. Implementar un Security Operation Center (SOC), propio o a través de un servicio externo, con instalaciones, herramientas tecnológicas, procesos y personal dedicado y entrenado, a fin de prevenir, detectar, evaluar y responder a amenazas e incidentes de ciberseguridad.

25. Identificar y evaluar en forma continua los vectores de ataque a los cuales pudieran estar expuestos los activos de información, como por ejemplo la manipulación o interceptación de las comunicaciones, phishing, malware, elevación de privilegios, inyección de código, denegación de servicios, ingeniería social, etc.; distinguiendo claramente entre aquellos que pueden afectar la infraestructura física, la infraestructura lógica o el equipamiento de usuarios finales (endpoint).

26. Realizar en forma continua, con el suficiente alcance y profundidad, pruebas de seguridad de infraestructura tecnológica para detectar las amenazas y vulnerabilidades que pudieran existir, tales como pentesting, red team o ethical hacking.

27. Implementar herramientas, procedimientos y controles que permita identificar vulnerabilidades de día cero.

28. Implementar una gestión de vulnerabilidades, para asegurar que las vulnerabilidades identificadas en los activos de información, a través de las diferentes herramientas, procedimientos y controles sean oportunamente solucionadas.

29. Implementar procedimientos para verificar que las principales vulnerabilidades identificadas no han sido explotadas.

30. Implementar procedimientos para la gestión de las alertas o amenazas de seguridad de la información y ciberseguridad, con el fin de detectar, investigar y generar acciones de mitigación de impacto de estos eventos, y resguardar la disponibilidad, confidencialidad e integridad de sus activos de información.

c. Respuesta y Recuperación

1. Implementar procedimientos de respuesta y recuperación ante incidentes de seguridad de la información y ciberseguridad, aprobados por el directorio. Estos procedimientos deberán considerar las disposiciones relativas al registro, reporte y comunicación de incidentes de la sección I.D de esta norma. Asimismo, dependiendo de la severidad del incidente, corresponderá escalar la situación al directorio u órgano equivalente para la toma de decisiones.

Estos planes deben ser probados al menos anualmente, y actualizados cada vez que se registran cambios en los activos de información o se materialicen eventos que amenacen la seguridad de la información y ciberseguridad.

2. Establecer procedimientos de comunicaciones, considerando todas las partes interesadas, ya sea internas o externas, a fin de mantenerlas adecuadamente informadas. Asimismo, tratándose de incidentes que afecten la calidad o continuidad de los servicios a los clientes o de un hecho de público conocimiento, la entidad será responsable de informar oportunamente

a los usuarios sobre la ocurrencia de dicho evento, debiendo actualizar la información disponible hasta que se conozcan las conclusiones sobre las causas del incidente y las medidas adoptadas para resolverlo, incluyendo el cumplimiento de las normas que resguardan la protección de datos personales y los derechos del inversionista.

3. Implementar un proceso de análisis forense para los incidentes relevantes, que incluya al menos las etapas de identificación, recopilación, adquisición, examen y análisis de evidencias digitales, junto con la generación de documentación e informes de la investigación forense, interpretación de evidencia digital y las conclusiones del trabajo realizado; además de los requerimientos necesarios para custodiar adecuadamente las evidencias generadas.

4. Mantener con una base de incidentes de los activos de información suficientemente detallada que le permita perfeccionar la capacidad de respuesta de éstos.

5. Realizar autoevaluaciones al menos anuales para determinar el grado de cumplimiento con las políticas internas, la regulación vigente y la adherencia a las mejores prácticas, de manera de determinar las vulnerabilidades de su infraestructura y tomar las acciones para su mitigación, así como para prever la adopción oportuna de medidas ante escenarios de amenazas de ciberseguridad. Además, se deberá evaluar la certificación a estándares disponibles.

6. En el caso de las Bolsas de Valores y las Bolsas de Productos, éstas deberán evaluar la posibilidad de participar activamente en grupos o 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. Además, también deberán compartir la información de estos incidentes entre sus corredores, disponiendo de sistemas especializados y seguros para este fin.

B. CONTINUIDAD DEL NEGOCIO

B.1. Disposiciones generales

En el ámbito de continuidad de negocio, la gestión de riesgo operacional deberá incluir los siguientes elementos:

1. Contar con una política de continuidad de negocio que contenga al menos lo siguiente:

1.1. Procedimientos de respuesta ante la ocurrencia de eventos internos o externos que pudieran crear una interrupción en la continuidad de las operaciones del negocio. Estos procedimientos se deberán referir al menos a la ejecución de un análisis de impacto de negocio (BIA, por su sigla en inglés) y un Análisis de Impacto de Riesgo (RIA, por su sigla en inglés).

1.2. Principales funciones y responsabilidades sobre la materia, en especial, cuáles serán las instancias encargadas de definir, diseñar, ejecutar y mejorar los procedimientos y metodologías para la gestión de continuidad de negocio. La política de continuidad del negocio formará parte de las políticas de gestión de riesgos de la entidad, debiendo ser actualizada y aprobada al menos anualmente por el directorio u órgano equivalente o ante cambios significativos.

2. Contar con personas con conocimientos comprobables en estándares de continuidad de negocio y experiencia en la gestión de los riesgos asociados, cuyas actividades principales serán el desarrollo y mejora de las políticas, procedimientos y controles para la gestión de continuidad de negocio.

3. Establecer políticas de capacitación y concientización para garantizar que el personal de la entidad esté debidamente preparado para enfrentar los escenarios de contingencia definidos y que comprendan sus responsabilidades en la gestión de los riesgos del sistema de

continuidad de negocio.

4. Disponer de procedimientos que permitan al directorio u órgano equivalente estar informado de manera oportuna y periódica sobre la gestión de continuidad de negocio. Deberá dejarse constancia del reporte de la información en estas materias en las respectivas actas del directorio u órgano equivalente y en los comités que se conformen para revisarlas.

B.2. Procedimientos para la Gestión de la Continuidad de Negocios

Sin perjuicio de lo establecido en el literal B.1, se deberán implementar los siguientes elementos mínimos para la gestión de la continuidad de negocios:

1. Contar con un Plan de Continuidad de Negocio y Recuperación de Desastres, aprobado anualmente por el directorio u órgano equivalente, que contenga:

1.1. Los procedimientos para la gestión de eventos de continuidad, con un nivel de detalle que permita a las distintas instancias afectadas determinar las actividades a desarrollar en cada escenario definido.

1.2. Los criterios para la activación del Plan y para la vuelta a la normalidad. Esto incluye evaluar oportunamente los riesgos asociados a la continuidad de negocios que se podrían estar asumiendo al introducir nuevos productos, sistemas, emprender nuevas actividades o definir nuevos procesos.

1.3. Roles y responsabilidades del personal.

La periodicidad de actualización de este Plan podría ser mayor dependiendo de la normativa propia de la entidad, o a requerimiento de esta Comisión.

2. Realizar o actualizar, al menos anualmente o ante eventos que amenacen la continuidad de las operaciones del negocio, un BIA con el objeto de identificar los procesos de mayor relevancia para la continuidad de negocio, el impacto que tendría una interrupción de esos procesos, y los tiempos y recursos necesarios para la continuidad y recuperación de éstos. El BIA deberá realizarse a nivel estratégico, táctico y operativo. De esos procesos, y considerando los niveles de apetito por riesgo definidos, se deberá determinar:

2.1. Los tiempos máximos tolerables de interrupción (MTPD por sus siglas en inglés);

2.2. Los tiempos objetivos de recuperación (RTO por sus siglas en inglés);

2.3. Los puntos objetivos de recuperación (RPO por sus siglas en inglés);

2.4. Los niveles mínimos aceptables de operación (MBCO por sus siglas en inglés); y

2.5. Los recursos humanos, tecnológicos y de infraestructura e información necesarios para su continuidad y recuperación.

Los resultados del BIA deberán ser aprobados por el directorio u órgano equivalente.

3. Disponer de un sitio secundario físico o en la nube que permita a la entidad reanudar la operación en caso de que esta se vea interrumpida en el sitio principal, permitiendo restablecer los procesos de mayor relevancia del negocio, tales como plataformas, infraestructura, sistemas y procesamiento de datos.

4. Realizar o actualizar, al menos anualmente, una evaluación de impacto de riesgos (RIA) que permita identificar y analizar los riesgos de continuidad de negocio que, de materializarse, provocarían una interrupción en los procesos de mayor relevancia de la entidad. Para lo anterior, se deberá considerar escenarios internos y externos, contemplando, entre otros, la falta total y parcial de los sistemas tecnológicos; ataques maliciosos que afecten la ciberseguridad; la ausencia de personal crítico; la imposibilidad de acceder o utilizar las instalaciones físicas y la falta de provisión de los servicios críticos contratados a proveedores.

5. Definir, en base a los resultados del BIA y el RIA, una estrategia de continuidad de negocio que tenga por objetivo mantener la continuidad de los procesos de mayor relevancia, considerando medidas preventivas para reducir la probabilidad de materialización de daños, minimizar el tiempo de recuperación y limitar el impacto en las operaciones del negocio de la entidad.

6. Implementar un Plan de gestión de crisis en el que se determine los procedimientos de escalamiento, comunicaciones, gestión y reporte de eventos de continuidad operacional para mantener informado en forma oportuna al directorio u órgano equivalente, a todas las partes interesadas y a esta Comisión, respecto de información relevante del evento de continuidad, las medidas adoptadas para resolverlo y la coordinación de una respuesta adecuada. La coordinación de una respuesta adecuada deberá considerar los puntos objetivos y tiempos objetivos de recuperación previstos en el BIA.

7. Contar con un procedimiento para el mejoramiento continuo de las políticas, planes y procedimientos de continuidad del negocio con el objeto de disminuir los tiempos de respuesta cuando se repita un incidente igual o similar; identificar posibles mejoras en los procesos; facilitar el intercambio de conocimientos; y disponer de información que permita apoyar la toma de decisiones en caso de materializarse nuevos incidentes.

8. Probar anualmente el Plan de Continuidad de Negocio y Recuperación de Desastres, de forma de asegurar que son adecuados y efectivos. Lo anterior, sin perjuicio de que esta Comisión pueda solicitar una periodicidad diferente en función del volumen y complejidad de las operaciones de la entidad. Estas pruebas deberán considerar al menos lo siguiente:

8.1. Deberán ser diseñadas en función del volumen y complejidad de operaciones de la entidad y ser supervisadas por la instancia responsable de la Gestión de Riesgos de la entidad.

8.2. Deberán estar basadas en escenarios de riesgo que se asimilen a eventos reales, incluyendo escenarios severos pero plausibles. Lo anterior, para demostrar que los procedimientos de continuidad de negocio funcionarán en caso de ser necesarios, incluyendo ataques cibernéticos, desastres y otras contingencias.

Se deberán emitir reportes de los resultados de las pruebas realizadas al directorio u órgano equivalente, que contengan recomendaciones y acciones para implementar mejoras al Plan de Continuidad de Negocio y Recuperación ante Desastres.

B.3. Disposiciones adicionales para Bolsas de Valores, Bolsas de Productos, Entidades de Depósito y Custodia y Sociedades Administradoras de Sistemas de Compensación y Liquidación

1. Contar con una persona encargada de la continuidad del negocio, independiente de las áreas operativas y de auditoría interna, que evalúe y provea información relevante al directorio, gerente general y otras áreas sobre el nivel de exposición a los riesgos de continuidad de negocios. Sus funciones podrán ser desempeñadas por una persona del grupo empresarial al que pertenezca la entidad, siempre que mantenga su independencia de las áreas operativas y de auditoría interna del grupo.

2. Diseñar e implementar el Plan de Continuidad del Negocio y Recuperación ante Desastres para permitir la reposición de los servicios con un tiempo objetivo de recuperación no mayor a 2 horas y un punto objetivo de recuperación cercano a 0.

3. En el caso de las Bolsas de Valores:

3.1. Contar con infraestructura y sistemas que tengan una capacidad instalada que permita procesar el mayor entre: (i) el doble del mayor número de transacciones por segundo registrado en las bolsas del país durante los últimos cinco años o; (ii) mil órdenes

por segundo. Sin perjuicio de lo anterior, las bolsas deberán garantizar que sus sistemas puedan hacer frente a un aumento súbito de transacciones, sin deterioro importante del funcionamiento de los sistemas. Lo anterior debe ser probado anualmente.

A su vez, la bolsa deberá adoptar los resguardos que sean necesarios para garantizar que sus sistemas comunicarán en tiempo real y con la menor latencia posible a los sistemas de las otras bolsas aquellas órdenes compatibles con la mejor oferta vigente en tales sistemas. Además, que esos sistemas comunicarán los calces y anulaciones que en ellos ocurran a la bolsa de la que emanó la orden respectiva.

3.2. Contar con un centro de procesamiento de datos principal y, al menos, uno de respaldo, permanentemente homologados en infraestructura y software, con capacidad, en cuanto a energía, refrigeración y mantenimiento, para alcanzar una disponibilidad de operación de a lo menos 99,98% o downtime de 1,6 horas anuales. El diseño, construcción y operación de esos centros de procesamiento de datos debe ser certificado por una entidad especializada e independiente. Estos sitios deben estar ubicados de forma tal de evitar quedar expuestos a los mismos riesgos.

No obstante, quedarán exceptuadas de cumplir con la certificación de uno de los centros de procesamiento de datos aquellas bolsas de valores que, dentro de los doce meses anteriores al día de cálculo, no hayan alcanzado un volumen igual o superior a las 400 mil operaciones mensuales sobre instrumentos de renta variable en sus sistemas de calce automático. A partir de los 15 meses posteriores de alcanzado ese volumen de operaciones, dicha bolsa deberá tener certificados ambos centros de procesamiento de datos. El centro de procesamiento certificado deberá corresponder al sitio principal, en caso de no poseer la modalidad activo-activo entre ambos centros de procesamiento de datos.

Similar obligación en cuanto a la mantención de centros de procesamiento será aplicable para las Bolsas de Productos, no obstante, la certificación solo será exigible a uno de los sitios, debiendo ser el sitio principal, en caso de no poseer la modalidad activo-activo.

3.3. Establecer niveles mínimos de servicio, tales como disponibilidad y latencia para los servicios brindados, los que deben ser aprobados por el directorio. Estos niveles mínimos de servicio deberán ser definidos considerando las obligaciones establecidas en el marco normativo y las necesidades de mercado. A partir de estos niveles de servicios, se deben definir los niveles operacionales acordados para la infraestructura que soporta los servicios, debiéndose verificar el cumplimiento de estos niveles. Se debe implementar un proceso de gestión de cumplimiento de los niveles de servicios acordados y los niveles operacionales acordados.

3.4. Contar con la infraestructura de telecomunicaciones y equipamiento computacional con la redundancia necesaria de forma de evitar los puntos únicos de falla.

3.5. Remitir información sobre disponibilidad y latencia de sus sistemas, información operacional, Plan de Continuidad Operacional y Recuperación ante Desastres, planificación de ejercicios de continuidad operacional y proyectos de infraestructura tecnológica en los plazos y condiciones establecidos en las normativas de envío de información de Bolsas de Valores de esta Comisión.

C. EXTERNALIZACIÓN DE SERVICIOS

C.1. Riesgos de externalización

1. Los servicios prestados por los proveedores, relacionados con el cumplimiento normativo, la continuidad del negocio, la seguridad de la información y la calidad de los servicios,

productos, información e imagen de la entidad contratante, deberán ser considerados en los procesos de gestión de riesgo de la entidad. En tal sentido, para la evaluación de riesgos de contratación de proveedores, se deberán considerar, entre otros, los siguientes riesgos:

1.1. Riesgo de sustitución: la posibilidad de sustituir o no a un proveedor dentro de un plazo determinado que garantice la continuidad del servicio contratado.

1.2. Riesgo de intervención: la posibilidad que la entidad tenga que hacerse cargo de la función contratada.

1.3. Riesgo de subcontratación: la posibilidad que el proveedor subcontrate a su vez todo o parte del servicio, reduciendo la capacidad de la entidad de supervisar la función subcontratada.

1.4. Riesgo de concentración: la posibilidad que una entidad contrate uno o varios servicios en un mismo proveedor que sea difícil de sustituir, incrementando la posibilidad de fallas o interrupciones prolongadas.

1.5. Riesgo legal: la posibilidad de contingencias legales que pudieran afectar la integridad y exactitud de la información que mantiene la entidad de proveedores para fines de cumplimiento regulatorio.

C.2. Procedimientos para la gestión de servicios externalizados

En el ámbito de externalización de servicios, la gestión de riesgo operacional de los servicios referidos en la sección C.1 deberá considerar los siguientes elementos:

1. Contar con una política para la externalización de servicios que considere a lo menos lo siguiente:

1.1. Definir la estructura de gobierno y de los procedimientos a seguir para autorizar y gestionar la externalización de servicios por terceros, incluyendo las líneas de reporte y de responsabilidad.

1.2. Establecer los objetivos en materia de externalización de servicios.

1.3. Establecer los niveles de apetito a los riesgos definidos en la sección C.1 y las estrategias de mitigación.

1.4. Cumplir con las disposiciones en materia de seguridad de la información, ciberseguridad y continuidad de negocios.

1.5. Establecer los procedimientos para la determinación de los servicios críticos. En tal sentido, para entender como crítico un servicio se deberán tener en cuenta lo siguiente:

a. El efecto que una debilidad o falla en la provisión o ejecución del servicio tenga sobre el cumplimiento normativo, continuidad del negocio, seguridad de la información y la calidad de los servicios, productos, información e imagen de la entidad contratante.

b. La complejidad de las funciones comerciales asociadas.

c. El grado en que el servicio puede transferirse rápidamente a otro proveedor, considerando los costos y el tiempo para hacerlo.

1.6. Definir los servicios que solo pueden ser externalizados con la aprobación previa del directorio u órgano equivalente.

1.7. Definir los elementos mínimos que deberá incorporar el contrato de prestación de servicios.

1.8. Definir los elementos de la gestión de riesgo que no serán aplicados a actividades que

por su naturaleza no tengan impacto relevante en la prestación de los servicios.

1.9. Incluir a la política de externalización de servicios como parte de las políticas de gestión de riesgos de la entidad, debiendo ser aprobada y actualizada al menos anualmente por el directorio u órgano equivalente, o con una frecuencia mayor en caso de cambios internos o externos significativos.

2. Establecer procedimientos para la selección, contratación y monitoreo de proveedores que consideren:

2.1. Una definición de los criterios particulares de contratación, cuando el proveedor se trate de una entidad relacionada. Estos criterios deberán estar destinados a evitar los conflictos de interés que se pueden presentar. En el caso de Administradoras Generales de Fondos, la gestión de servicios externalizados deberá también considerar aquellos servicios que se encuentren externalizados para los fondos fiscalizados administrados por ella.

2.2. La incorporación al análisis de elementos que permitan llevar a cabo un proceso de debida diligencia, de forma de asegurar que los proveedores tengan una adecuada reputación comercial, solvencia financiera, experiencia y recursos suficientes para garantizar la calidad de la provisión del servicio. En el caso de servicios de procesamiento de datos realizados en el extranjero, el directorio u órgano equivalente de la entidad deberá revisar y evaluar antecedentes que respalden la calidad del servicio prestado, la solidez financiera del proveedor y la existencia de una adecuada legislación de protección de datos personales en la jurisdicción aplicable, haciéndose responsable por la disponibilidad, confidencialidad e integridad de la información entregada al proveedor contratado.

3. Contemplar en los contratos con los proveedores de servicios externalizados los siguientes contenidos mínimos:

3.1. Una descripción clara del servicio contratado y el plazo de vigencia.

3.2. Las obligaciones de prestación del servicio por parte del proveedor, definiendo niveles de servicio acordados. La entidad deberá definir las situaciones que se considerarán graves incumplimientos contractuales y causales de término anticipado del contrato.

3.3. La obligación de comunicar cualquier acontecimiento que pueda tener un impacto material en la capacidad para llevar a cabo el servicio externalizado.

3.4. Los requisitos de seguridad de la información, ciberseguridad y continuidad de negocios que deberá cumplir el proveedor, que deben ser concordantes con las disposiciones establecidas en esta materia por la entidad. Los proveedores deberán contar con procedimientos de gestión de incidentes y continuidad de negocios que le permitan seguir brindando los servicios en el evento que se presenten situaciones disruptivas.

3.5. La documentación de los procedimientos operacionales, administrativos y tecnológicos propios del servicio contratado. En el caso de existir subcontratación en cadena, la entidad deberá verificar el cumplimiento de las condiciones pactadas con el proveedor de servicios inicial y las entidades subcontratadas por este último.

3.6. Los procedimientos para la evaluación y monitoreo periódico de la calidad de la provisión del servicio externalizado. La entidad podrá pactar con el proveedor la realización de auditorías por terceros designados o por la propia entidad, quien será responsable en última instancia por garantizar la calidad de la provisión del servicio externalizado.

3.7. Las estrategias para el término de la prestación de servicios externalizados sin perjudicar las operaciones de la entidad, incluyendo el caso en que se produzcan contingencias legales. Estas situaciones deberán ser consideradas en el Plan de Continuidad del Negocio y Recuperación ante Desastres.

4. Contar con un registro de servicios externalizados para gestionar los riesgos de subcontratación. Dicho registro deberá estar disponible para su consulta permanente por esta Comisión y deberá incluir al menos la siguiente información:

4.1. Identificación del servicio externalizado, incluyendo una breve descripción del mismo y de los datos involucrados si corresponde a un servicio crítico, el área usuaria, si existe subcontratación en cadena, y si se lleva a cabo en la nube.

4.2. Identificación del proveedor, incluyendo si corresponde a una entidad relacionada o no.

4.3. Fecha de inicio, renovación y término del servicio.

4.4. En el caso de servicios de procesamiento de datos, una descripción de los datos y tratamientos que se subcontratan, las medidas de seguridad adoptadas, y la ubicación geográfica del proveedor.

4.5. En caso de subcontratación en cadena, se deberá detallar cuáles son las entidades a las que el proveedor subcontrata el servicio, una descripción de los riesgos asociados y si el proveedor realiza un control de la calidad de la provisión del servicio subcontratado en cadena.

5. Monitorear periódicamente que los proveedores cumplen con las condiciones pactadas para garantizar la calidad de la provisión del servicio. La entidad será responsable de la calidad de los servicios externalizados.

6. En el caso que la entidad decida contratar servicios de acceso y tratamiento de información en la nube, o que el proveedor como parte de la subcontratación en cadena considere los servicios en la nube, realizar un análisis reforzado de los riesgos inherentes a esos servicios, analizando en particular cómo podría afectarse la disponibilidad, confidencialidad e integridad de la información, y la continuidad de negocio de la entidad. Ese análisis deberá tener en consideración factores tales como:

6.1. Las certificaciones independientes respecto a la gestión de la seguridad de la información y la calidad de la prestación del servicio del proveedor.

6.2. La celebración del contrato de externalización de servicios directamente entre la entidad y el proveedor, con la finalidad de minimizar los riesgos que podría aportar el intermediario en este tipo de servicios.

6.3. El procesamiento o almacenamiento de información en otras jurisdicciones, y en ese caso la existencia de normas que resguardan la protección de datos personales, la disponibilidad, confidencialidad e integridad de la información y la resolución de contingencias legales.

6.4. La existencia de adecuados mecanismos de seguridad del proveedor, tanto físicos como lógicos, que permitan aislar los componentes de la infraestructura en la nube que la entidad comparte con otros clientes del proveedor, de manera de prevenir fugas de información o eventos que puedan afectar la disponibilidad, confidencialidad e integridad de los datos de la entidad.

6.5. La utilización de técnicas de encriptación para los datos que la entidad establezca, de acuerdo con su naturaleza y sensibilidad.

7. Evaluar que el proveedor de los servicios contratados posea adecuados conocimientos y experiencia.

8. Mantener personal con el debido conocimiento para efectuar el control de la prestación de servicios efectuada por sus proveedores. Asimismo, también deberá vigilar el debido cumplimiento de aquellos aspectos regulatorios y legales que pudiesen afectar la provisión de

los servicios contratados.

El directorio u órgano equivalente deberá mantenerse informado sobre las materias referidas a la externalización de servicios, para lo cual deberá disponer de procedimientos que le permitan informarse de manera oportuna y periódica. Deberá dejarse constancia del reporte de la información en estas materias en las respectivas actas del directorio u órgano equivalente y en los comités que se conformen para revisar estas materias.

D. INFORMACIÓN DE INCIDENTES OPERACIONALES

D.1. Registro y comunicación de incidentes operacionales

1. Las entidades deberán comunicar a esta Comisión los incidentes operacionales que afecten la continuidad del negocio, los recursos e información de la entidad o de sus clientes y la calidad de los servicios. A modo de ejemplo, y sin el objeto de ser exhaustivos ni taxativos, deberán ser reportadas las fallas en servicios y sistemas importantes para las operaciones del negocio; problemas tecnológicos que afecten la seguridad de la información; ataques del ciberespacio; virus o malware detectados en los activos de información críticos; eventos de indisponibilidad o interrupción de algún servicio o producto que afecte a los clientes, en cualquier canal; pérdidas o fugas de información de la entidad o de clientes; los incidentes que afecten el patrimonio de la entidad producto de fraudes internos o externos; problemas que afecten la continuidad de proveedores de servicios críticos; entre otros. Esta información deberá ser mantenida por la entidad en una base de datos de incidentes y otra base de datos de pérdidas operacionales para el mejoramiento continuo del proceso de gestión de riesgo operacional.

En el caso de las Bolsas de Valores y Bolsas de Productos, a modo de ejemplo, también deberá considerarse lo siguiente: eventos de aumento de latencia de los servicios de negociación; eventos de caída de rendimiento sobre el registro y calce de las órdenes en los sistemas de negociación; eventos que afecten el accesos a los sistemas por parte de los corredores o de los clientes de éstas; problemas de comunicación con otras bolsas o entidades relevantes como Sociedades Administradoras de Sistemas de Compensación y Liquidación de instrumentos financieros y Entidades de Depósito y Custodia de valores; los incidentes que afecten la disponibilidad, confidencialidad, integridad y oportunidad de divulgación de información bursátil a través de los distintos canales que posea.

2. En el caso de las Bolsas de Valores, Bolsas de Productos, Sociedades Administradoras de Sistemas de Compensación y Liquidación y Entidades de Depósito y Custodia de Valores, la ocurrencia de un incidente operacional de aquellos mencionados en el numeral anterior deberá ser informada a esta Comisión en un plazo máximo de 15 minutos transcurridos desde que la entidad tomó conocimiento del hecho. En el caso de las Administradoras Generales de Fondos, el plazo máximo será de 2 horas desde que la entidad tomó conocimiento del hecho. Las instrucciones para reportar los incidentes operacionales a esta Comisión se encuentran en los Anexos N° 2 y 4.

Los plazos señalados anteriormente son sólo para efectos de notificar a esta Comisión de la ocurrencia del incidente con la información disponible en ese momento y no implica que la entidad deba tener resuelto el problema, haber tomado determinadas acciones o tener aclarada las causas del incidente, lo que podría ser materia de reportes de seguimiento del incidente enviados a esta Comisión posteriormente.

3. Para estos efectos, el directorio u órgano equivalente deberá definir un funcionario encargado y un suplente para la realización de reportes y envío de información según lo indicado en esta sección. Estas personas deberán tener un nivel ejecutivo y ser designados por la entidad, tanto para este efecto como para responder eventuales consultas por parte de

esta Comisión.

4. En los casos en que esta Comisión lo estime necesario, podrá requerir a la entidad la elaboración de un informe interno que contenga al menos: el análisis de las causas del incidente; la generación de documentación e informes de investigación; un análisis del impacto generado en los servicios; el plan de tratamiento para evitar con alto grado de seguridad que se vuelva a presentar; y las materias adicionales que esta Comisión pueda requerir.

5. Sin perjuicio de lo anterior, la entidad deberá mantener informado en forma oportuna al directorio u órgano equivalente de todos los incidentes operacionales relevantes y las medidas adoptadas para resolverlo.

6. En adición a lo expuesto, las Sociedades Administradoras de Sistemas de Compensación y Liquidación de Instrumentos Financieros y las Entidades de Depósito y Custodia con las disposiciones adicionales establecidas en el Anexo N° 4 de esta norma.

D.2. Registro y comunicación de pérdidas operacionales

1. Se entiende por pérdida operacional toda pérdida financiera resultante de la materialización del riesgo operacional de acuerdo con lo definido anteriormente. Esto incluye las pérdidas financieras debido a cambios legales o regulatorios que afecten las operaciones de la entidad, o producto de incumplimientos con la regulación vigente.

2. Las entidades deberán enviar a esta Comisión la información de todos los incidentes que se materialicen individualmente en pérdidas operacionales mayores a 150 Unidades de Fomento, de acuerdo con las instrucciones del Anexo N° 3 de la presente norma, 15 días hábiles después del cierre de junio y diciembre de cada año.

3. Los criterios para la confección del registro de pérdidas operacionales son los siguientes:

3.1. La entidad deberá contar con procesos y procedimientos documentados para la identificación, recopilación, uso y comunicación de los registros de pérdida operacional. Esta Comisión podrá exigir que el cumplimiento de tales requisitos sea validado a través de un pronunciamiento emitido por empresas de auditoría externa, de aquellos inscritos en el Registro de Empresas de Auditoría Externa de esta Comisión, que cuenten con unidades especializadas en la evaluación de procedimientos y mecanismos de gestión de riesgo operacional, con una experiencia no inferior a 5 años en dichas materias.

3.2. Los registros internos sobre pérdidas operacionales de la entidad deberán ser integrales e incluir la totalidad de las actividades y exposiciones relevantes, en todos los sistemas y en todas las ubicaciones geográficas pertinentes.

3.3. La entidad deberá recopilar información sobre los importes brutos de las pérdidas, y sobre las fechas de referencia de los eventos de riesgo operacional. Además, la entidad deberá recoger información sobre recuperaciones de importes brutos de pérdidas, e información descriptiva sobre los factores determinantes o las causas del evento de pérdida. El grado de detalle de la información descriptiva deberá ser proporcional al importe bruto de la pérdida.

3.4. La entidad deberá utilizar la fecha de contabilización del evento para construir el conjunto de registros sobre pérdidas. En el caso de eventos legales, la fecha de contabilización se refiere a cuando se constituye una provisión para esta contingencia legal en el estado de situación financiera, con su reflejo correspondiente en el estado de resultados.

3.5. Las pérdidas causadas por un evento de riesgo operacional común o por varios eventos de riesgo operacional relacionados a lo largo del tiempo, pero contabilizadas en el

transcurso de varios años, deberán asignarse a los años correspondientes en la base de datos de pérdidas, en consonancia con su tratamiento contable.

4. Por pérdida bruta se entiende una pérdida antes de recuperaciones de cualquier tipo.

4.1. Los siguientes ítems deberán ser incluidos en los cálculos de las pérdidas brutas para la base de datos de pérdidas:

a. Cargos directos en las cuentas de estados de resultados de la entidad y amortizaciones debido a eventos de riesgo operacional del período. Por ejemplo, costos incurridos como consecuencia de un evento, incluyendo gastos externos con una relación directa al evento por riesgo operacional (por ejemplo, gastos legales directamente relacionados al evento y comisiones pagadas a los asesores, abogados o proveedores) y costos de reparación o reemplazo incurridos para restaurar la posición que prevalecía antes del evento de riesgo operacional.

b. Cargos directos en las cuentas de estados de resultados de la entidad y amortizaciones debido a eventos por riesgo operacional de ejercicios contables previos que afecten los estados financieros de la entidad en el presente periodo.

4.2. Los siguientes ítems deberán ser excluidos de las pérdidas brutas registradas en la base de datos de pérdidas:

a. Costos por contratos de mantenimientos generales de la propiedad, planta o equipos.

b. Gastos internos o externos con el fin de mejorar el negocio después de las pérdidas por riesgo operacional: actualizaciones, mejoras, iniciativas de gestión del riesgo y mejoras en ellas.

c. Primas de seguro.

5. Por pérdida neta se entiende la pérdida después de tener en consideración los efectos de las recuperaciones. La recuperación es un hecho independiente, relacionado con el evento de pérdida inicial, que no necesariamente se efectúa en el mismo periodo en el que se perciben los fondos respectivos.

La entidad deberá ser capaz de identificar las recuperaciones no procedentes de seguros y las recuperaciones originadas por el pago de indemnizaciones de seguros para todos los eventos de pérdidas operacionales. Asimismo, deberá utilizar las pérdidas netas de recuperaciones (incluidas las procedentes de seguros) en el conjunto de registros sobre pérdidas operacionales, aunque las recuperaciones sólo podrán utilizarse para reducir las pérdidas cuando se haya recibido el pago.

II. DISPOSICIONES ADICIONALES PARA SOCIEDADES ADMINISTRADORAS DE SISTEMAS DE COMPENSACIÓN Y LIQUIDACIÓN Y ENTIDADES DE DEPÓSITO Y CUSTODIA DE VALORES

Las Sociedades Administradoras de Sistemas de Compensación y Liquidación de Instrumentos Financieros y las Entidades de Depósito y Custodia de Valores, deberán adoptar las siguientes disposiciones adicionales en materia de gestión de riesgo operacional:

1. Establecer sus políticas de gestión de riesgo operacional en línea con los Principios para las Infraestructuras del Mercado Financiero del Comité de Sistemas de Pago y Liquidación y el Comité Técnico de la Organización Internacional de Comisiones de Valores.

2. Gestionar los riesgos derivados de su interdependencia con proveedores externos de servicios, participantes de sistemas de compensación y liquidación de instrumentos

financieros, sociedades administradoras de dichos sistemas, entidades de depósito y custodia de valores y otras entidades del mercado financiero. Para ello deberán:

2.1. Implementar procedimientos para recopilar y analizar información de sus operaciones en forma continua, con el fin de asegurar la provisión de servicios de infraestructura en distintos escenarios (por ejemplo, cambios en la demanda por sus servicios) acorde con los niveles de apetito por riesgo definidos.

2.2. Disponer de acuerdos preestablecidos de intercambio de información con proveedores, clientes y otras entidades relacionadas que faciliten la prevención y gestión de incidentes (por ejemplo, comunicar la firma de acuerdos de interconexión y subcontratación de servicios críticos).

3. Disponer de un sitio secundario físico o en la nube que deberá contar con recursos, capacidades y funcionalidades adecuadas, idealmente ubicado a una distancia geográfica del sitio principal que sea suficiente para tener un perfil de riesgo distinto. Lo anterior debería incluir la realización de pruebas, como mínimo anualmente, conjuntas con proveedores externos, participantes y entidades relacionadas.

4. Incluir en el Plan de Continuidad y Recuperación ante Desastres escenarios donde la entidad deba adaptar su infraestructura tecnológica ante cambios en la demanda por sus servicios, tanto en condiciones normales como de estrés, resguardando restablecer sus operaciones de manera oportuna.

5. En el caso de las sociedades administradoras de sistemas de compensación y liquidación, los participantes de tales sistemas deberán acreditar ante ella el cumplimiento de los requisitos que se establecen a continuación, tanto en forma previa a la aceptación de la entidad que hubiere solicitado adquirir el carácter de participante, como permanentemente una vez adquirida esa condición:

5.1. Capacidades operativas de los participantes: Los participantes deberán asegurar una adecuada disponibilidad, conectividad y capacidad de sus sistemas informáticos y de comunicación, así como de sus fuentes de datos, para soportar el procesamiento de sus transacciones. Adicionalmente, deberán contar con un Plan de Continuidad de Negocio y Recuperación ante Desastres aprobado anualmente por el directorio. Con este fin, las sociedades administradoras deberán establecer en el contrato de adhesión al sistema y en las normas de funcionamiento del mismo, la facultad para que ella pueda evaluar lo indicado en este numeral. Al respecto, la sociedad administradora deberá establecer procedimientos para salvaguardar la disponibilidad, confidencialidad e integridad de la información a la que tenga acceso a causa de dicha facultad.

5.2. Idoneidad del personal que administra los sistemas del participante: El personal del participante, encargado de operar las aplicaciones provistas por la sociedad administradora, deberá contar con la experiencia y formación profesional acorde a las responsabilidades de su cargo y cumplir al menos con haber recibido y aprobado un programa de capacitación que defina la sociedad administradora.

5.3. Gestión de riesgo operacional de los participantes: Los participantes de un sistema de compensación y liquidación deberán contar con procedimientos para la gestión de riesgo operacional en los ámbitos de seguridad de la información y ciberseguridad, continuidad del negocio y externalización de servicios, sobre los procesos relativos a la compensación y liquidación de instrumentos financieros, incluidos aquellos que se generen por el ingreso directo de órdenes de compensación por parte de los clientes de un participante. Tales procedimientos tendrán como objetivo evaluar, controlar y monitorear los riesgos que sean inherentes a dichos procesos.

Los procedimientos mencionados dependerán del tamaño del participante, el volumen de órdenes de compensación que ingrese al sistema y del tipo de instrumentos financieros sobre los cuales opere. No obstante lo anterior, deberán incluir al menos los siguientes elementos:

a. Una política de gestión de riesgo operacional aprobada anualmente por el directorio, incluyendo niveles de apetito al riesgo definidos.

b. Un manual de procedimientos, formal y actualizado, que al menos describa los procesos que interactúan con los sistemas de compensación y liquidación de instrumentos financieros, así como una descripción de los riesgos identificados y sus controles, junto a los mecanismos de monitoreo y mitigación que sean pertinentes.

c. Una persona o unidad responsable de desarrollar, implementar e impulsar la gestión de riesgo operacional sobre las materias indicadas en el primer párrafo de este literal.

d. Una persona o unidad responsable de evaluar, de forma permanente e independiente de aquella indicada en la letra c anterior, la efectividad de las políticas y procedimientos de la gestión de riesgo operacional, la cual debe informar de su labor directamente al directorio del participante, pudiendo recaer esta función en la unidad o persona que cumple las funciones de auditoría interna.

5.4. La sociedad administradora podrá exigir que el cumplimiento de tales requisitos sea validado a través de un pronunciamiento emitido por Empresas de Auditoría Externa, de aquellas inscritas en el Registro de Empresas e Auditoría Externa de esta Comisión, que cuenten con unidades especializadas en la evaluación de procedimientos y mecanismos de gestión de riesgo operacional, con una experiencia no inferior a 5 años en dichas materias.

5.5. Asimismo, la sociedad administradora podrá establecer requisitos tecnológicos diferenciados a los participantes, en la medida que ello obedezca a una segmentación basada en criterios objetivos, los cuales deberán contemplarse en las normas de funcionamiento de los respectivos sistemas.

5.6. Por último, en caso de que la entidad que hubiere solicitado adquirir el carácter de participante no cumpla con los requerimientos mínimos exigibles, la sociedad administradora deberá emitir un informe en el cual se fundamenten los elementos que deberán ser considerados para satisfacer dichos requerimientos.

III. MODIFICACIONES

1. Elimínese los numerales 1, 2 y 3 de la letra b) de la sección III de la Norma de Carácter General N°480.

2. Reemplácese el primer párrafo de la letra b) de la sección III de la Norma de Carácter General N° 480 por el siguiente:

"Para efectos de poder acceder al mecanismo de interconexión en tiempo real de sistemas de calce automático establecido por el artículo 44 bis de la Ley N°18.045, la bolsa de valores respectiva deberá contar con los requisitos establecidos en la normativa de gobierno corporativo y gestión de riesgos y en la normativa de gestión de riesgo operacional de dicha entidad."

3. Reemplácese el primer párrafo de la sección "Vigencia" de la Norma de Carácter General N° 480 por el siguiente:

"Las instrucciones establecidas en la presente Norma de Carácter General rigen a contar de esta fecha".

IV. DEROGACIÓN

Deróguese las Circulares N° 1.939 y 2.020, y la Norma de Carácter General N°256.

V. VIGENCIA

Las instrucciones establecidas en la presente Norma de Carácter General rigen a contar del 1 de febrero de 2025.

Bernardita Piedrabuena Keymer

Firmado digitalmente por Bernardita Piedrabuena Keymer
Fecha: 2024.05.08 14:06:39 -04'00'

BERNARDITA PIEDRABUENA KEYMER
PRESIDENTA (S)
COMISIÓN PARA EL MERCADO FINANCIERO

ANEXO N° 1: DEFINICIONES

Activos de información: corresponde a los recursos de información o elementos relacionados con el tratamiento de la información, los cuales pueden ser primarios como la información (física y lógica) y los procesos y actividades de negocio, o de soporte como hardware; software; redes de comunicación; personal; entre otros.

Amenaza: se refiere a cualquiera circunstancia o evento que pudiera explotar una vulnerabilidad.

Análisis de impacto del negocio o BIA: es el procedimiento de análisis de los efectos que puede tener en los procesos de la entidad una interrupción del negocio.

Apetito por riesgo: nivel agregado y tipos de riesgo que una entidad está dispuesta a asumir, previamente decidido y dentro de su capacidad de riesgo, a fin de lograr sus objetivos estratégicos y plan de negocio.

Ataque: en el contexto de ciberseguridad, se refiere a un evento que tuviera como intención destruir, exponer, alterar, deshabilitar, robar, u obtener acceso o hacer un uso no autorizado de un activo de información.

Ciberseguridad: corresponde al conjunto de acciones que realiza la entidad para mitigar los riesgos y proteger la información e infraestructura que la soporta, de eventos del ciberespacio, siendo este último el entorno resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red.

Confidencialidad de la información: protección de los datos contra el acceso y la divulgación no autorizados, definido por el directorio u órgano equivalente. Incluye los medios para proteger la privacidad personal y la información reservada, en especial de los clientes de la entidad.

Downtime: la cantidad de tiempo que el proceso o negocio es interrumpido.

Ethical hacking: los hackers éticos realizan evaluaciones de vulnerabilidad de seguridad y pruebas de penetración de acuerdo con métodos y protocolos aceptados por la industria. Analizan los sistemas en busca de posibles vulnerabilidades que pueden resultar de una configuración incorrecta del sistema, fallas de hardware o software o debilidades operativas.

Externalización de servicios: es la ejecución por un proveedor externo de servicios o actividades en forma continua u ocasional, las que normalmente podrían ser realizadas por la entidad contratante

Incidente: evento único o serie de eventos de seguridad de la información inesperados o no deseados, que resultaren en un intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la política de seguridad de la información de la entidad.

Instancia: se refiere a un nivel o grado de la estructura organizacional de la entidad, esto incluye, comité, unidad, división, departamento u otro equivalente.

Malware: software destinado a realizar un proceso no autorizado que tendrá un impacto adverso en la disponibilidad, confidencialidad e integridad de un sistema de información. Un virus, "worm", troyano u otra entidad basada en código que infecta un host. El "spyware" y algunas formas de adware también son ejemplos de código malicioso.

Mecanismos de autenticación: mecanismos utilizados para confirmar la identidad de un usuario. Estos mecanismos pueden utilizar uno o más factores de autenticación, por ejemplo, credenciales, contraseñas, certificados digitales, o características biométricas o biológicas. El mecanismo de autenticación es multifactor cuando utiliza una combinación de factores de autenticación para confirmar la identidad.

Niveles mínimos aceptables de operación: corresponde al mínimo nivel de servicios o productos que se consideran aceptables para que la entidad cumpla con sus objetivos durante una interrupción.

Partes interesadas: se refiere a las personas u organizaciones que se relacionan con las actividades y decisiones de una empresa, tales como empleados, proveedores, clientes, reguladores, entre otros.

Phishing: técnica para intentar adquirir datos confidenciales, como números de cuentas bancarias, a través de una solicitud fraudulenta por correo electrónico o en un sitio web, en la que el perpetrador se hace pasar por una empresa legítima o una persona de confianza.

Procesamiento de datos: tratamiento electrónico de datos o de los elementos básicos de información, sometidos a operaciones programadas.

Proveedor de servicios: entidad relacionada o no a la institución contratante, que preste servicios o provea bienes e instalaciones a éste.

Prueba de penetración: metodología de prueba en la que los evaluadores, que normalmente trabajan bajo restricciones específicas, intentan eludir o derrotar las características de seguridad de un sistema.

Punto objetivo de recuperación (RPO): período de tiempo máximo antes que la pérdida de datos que sigue a un incidente se vuelva inaceptable de acuerdo a los estándares de calidad de la propia entidad.

Red Team (Equipo Rojo): grupo de personas autorizadas y organizadas para emular las capacidades de ataque o explotación de un adversario potencial contra la postura de seguridad de una empresa. El objetivo del Equipo Rojo es mejorar la ciberseguridad empresarial demostrando los impactos de los ataques exitosos y demostrando lo que funciona para los defensores (es decir, el Equipo Azul) en un entorno operativo.

Security Operations Center (SOC): el Centro de Operaciones de Seguridad, SOC (por sus siglas en inglés), se refiere al equipo encargado de garantizar la seguridad de la información. El objetivo del SOC es analizar, identificar y corregir incidentes de seguridad de la información utilizando soluciones tecnológicas y enfoques diferentes.

Servicios en la nube: servicios que proveen infraestructura, plataformas o software a lo que el cliente accede a través de la red, sin la necesidad de instalarlos en su propia infraestructura, sino que están ubicados en un servidor remoto del proveedor del servicio.

Riesgo residual: aquel riesgo que persiste luego de adoptar las medidas de control y mitigación por parte de la entidad.

Subcontratación en cadena de servicios externalizados: las formadas por terceros subcontratados por el proveedor inicial de servicios para realizar parte importante de las actividades contratadas con éste (subcontrato de otros proveedores).

Tiempos máximos tolerables de interrupción: tiempo máximo tolerable en que un proceso pudiera estar interrumpido sin provocar efectos relevantes en la continuidad operacional.

Tiempo objetivo de recuperación: periodo de tiempo que sigue a un incidente dentro del cual: a) debe reanudarse un producto, servicio o actividad; o b) los recursos deben ser recuperados (entendiendo por recursos los activos, personas, habilidades, información, tecnología, instalaciones, suministros e información necesarios para las operaciones del negocio).

Vulnerabilidad: en el contexto de ciberseguridad, se refiere a cualquier debilidad de un activo de información o de un mecanismo de control que pudiera ser explotada por un ataque, es decir, puede ser un fallo en un sistema que lo torna accesible a los atacantes o cualquier tipo de debilidad en el propio activo en los procedimientos que deje la seguridad de la información de la entidad expuesta a una amenaza.

ANEXO N° 2: REPORTE DE INCIDENTES OPERACIONALES

A través del menú "INCIDENTES Y PÉRDIDAS OPERACIONALES" del canal oficial de comunicación y envío de información entre la Comisión y sus fiscalizados, la entidad deberá reportar el detalle de cada incidente descrito en la sección I.D.1 de acuerdo con el siguiente esquema:

INFORMACION	DETALLE
Fecha y hora de inicio del incidente	
Tipo de incidente	
Descripción detallada del incidente	
Causas posibles o identificadas	
Dependencias o activos afectados	
Dirección dependencias afectadas	
Canales afectados	
Nombre de proveedores involucrados	
Tipo de proveedores involucrado	
Número de clientes afectados	
Tipo de clientes afectados	
Productos o servicios afectados	
Número de transacciones afectadas	
Medidas adoptadas y en curso	
Otros antecedentes	
Nombres y cargos de las personas de contacto	
Teléfono de contacto	
Fecha y hora de cierre del incidente	

Para aquellos campos en los que al momento del reporte no se cuente con la información, se debe indicar con texto "En evaluación", y para el caso de los campos numéricos, de no contarse con el dato, éstos deben completarse con un cero.

Será responsabilidad de la entidad la actualización de los antecedentes mencionados cuando se disponga de nueva información y hasta el cierre del incidente (fecha de cierre del incidente).

FECHA Y HORA DEL INICIO DEL INCIDENTE
Se debe señalar la fecha (DD/MM/AAAA) y la hora (HH:MM:SS) en que comenzó el incidente.

TIPO DE INCIDENTE
En este campo se debe señalar el tipo de incidente, eligiendo entre las siguientes opciones:

- Afectación de instalaciones
- Ausencia de Colaboradores
- Sin acceso dependencias y otras áreas específicas
- Falla Sistemas Base (SO, BD)
- Falla aplicativos (negocio, web, batch)

- Falla de comunicaciones
- Falla Hardware
- Falla en servicios básicos (electricidad/agua)
- Pérdida de Recursos Monetarios de la entidad, sus clientes y otras partes interesadas
- Pérdida de Información de la entidad, sus clientes y otras partes interesadas
- Interrupción/ latencia en servicios
- Error de envío de información
- Otros: especificar

DESCRIPCIÓN DETALLADA DEL INCIDENTE
En este campo se debe detallar en qué consiste el incidente reportado.

CAUSAS POSIBLES O IDENTIFICADAS
En este campo se debe realizar un análisis sobre las causas del incidente y sobre la efectividad de las medidas adoptadas para resolverlo.

DEPENDENCIAS AFECTADAS
En este campo se deben señalar las dependencias afectadas, eligiendo entre las siguientes opciones:

- Oficinas
- Sitio Producción
- Sitio Contingencia
- Dependencias proveedor
- Otros: especificar

DIRECCIÓN DEPENDENCIAS AFECTADAS (CALLE, COMUNA, REGIÓN)
En este campo se debe informar la dirección completa de la dependencia afectada. Si existe más de una dependencia afectada, se debe indicar la dirección de cada una de ellas, separándolas con un punto y coma (;).

CANALES AFECTADOS
En este campo se deben seleccionar los canales afectados por el incidente (lo que sea aplicable):

- Terminales
- Mensajería
- Servicios de custodia
- Sucursales
- Otros: especificar

NOMBRE DE PROVEEDORES INVOLUCRADOS
Corresponde al nombre o razón social del proveedor.

TIPO DE PROVEEDOR INVOLUCRADO

- Servicios básicos
- Telecomunicaciones
- Infraestructura tecnológica
- Procesamiento
- Atención telefónica
- Otros: especificar

NÚMERO DE CLIENTES AFECTADOS:

En este campo se debe completar el número de clientes que fueron afectados por el incidente que se reporta.

TIPO DE CLIENTES AFECTADOS:
En este campo se debe seleccionar el tipo de cliente afectado, entre las siguientes opciones:

- Personas
- Empresas no financieras
- Empresas financieras (Especificar)
-
- Otros: Especificar

NÚMERO DE EMPLEADOS AFECTADOS
En este campo se debe completar con el número de empleados que fueron afectados por el incidente que se reporta.

PRODUCTOS O SERVICIOS AFECTADOS
En este campo se deben informar en detalle los productos o servicios afectados por el incidente.

NÚMERO DE TRANSACCIONES AFECTADAS
En este campo se debe completar el número de transacciones que fueron afectadas por el incidente que se reporta (en caso de no conocer el número exacto de transacciones afectadas, se debe completar con 0; luego, en la medida que se tenga más información, se debe actualizar la cifra).

MEDIDAS ADOPTADAS
En este campo se deben informar en detalle las acciones realizadas por la entidad para superar el incidente.

NOMBRE Y CARGO DE PERSONAS DE CONTACTO
Corresponden a las personas que informan el incidente y sus cargos.

TELÉFONO DE CONTACTO
Se debe señalar en este campo el teléfono celular de las personas de contacto.

FECHA Y HORA DE TÉRMINO DEL INCIDENTE
Este campo se incluirá cuando se cierra el incidente. Se debe completar la fecha (DD/MM/AAAA) y la hora (HH:MM:SS) en que éste finalizó.

ANEXO N° 3: REPORTE DE PÉRDIDAS OPERACIONALES

A través del menú "INCIDENTES Y PERDIDAS OPERACIONALES" del canal oficial de comunicación y envío de información entre la Comisión y sus fiscalizados, la entidad deberá reportar al último día hábil de junio y diciembre de cada año el detalle de todos los eventos que materialicen individualmente en pérdidas operacionales mayores a 150 Unidades de Fomento. Además, se deberán reportar los montos de gastos y recuperaciones asociados a pérdidas operacionales asociados a un mismo evento.

INFORMACION	DETALLE
Número de identificación del incidente asignado por la CMF	
Fecha de descubrimiento	
Fecha de contabilización	
Tipo de monto	
Tipo de gasto	
Tipo de recuperación	
Monto	
Nombre y cargo del informante	

NUMERO DE IDENTIFICACIÓN DEL INCIDENTE ASIGNADO POR LA CMF
Corresponde al código que identifica en forma unívoca el incidente reportado, asignado por la CMF cuando se reportó el inicio del incidente a través del menú "INCIDENTES Y PÉRDIDAS OPERACIONALES" del canal oficial de comunicación y envío de información entre la Comisión y sus fiscalizados.

FECHA DE DESCUBRIMIENTO
Seleccionar el día y hora que se desplegará en este campo correspondiente a la fecha en la que se identificó el evento de pérdida.

FECHA DE CONTABILIZACIÓN
Seleccionar el día y hora que se desplegará en este campo correspondiente a la fecha en la que se imputa contablemente la pérdida o recupero en los estados financieros.

TIPO DE MONTO
Seleccionar el código que identifica el tipo de monto a reportar, de acuerdo a la siguiente codificación que se desplegará en este campo:

CODIGO	TIPO DE MONTO
1	Pérdida (cargos directos en los estados de resultados)
2	Gastos (costos incurridos internos o externos con relación directa al evento operacional)
3	Recuperación

TIPO DE GASTO

Seleccionar el código que identifica el principal tipo de gasto asociado al evento de pérdida, ya sea interno o externo directamente atribuible al evento operacional, de acuerdo a la siguiente codificación que se desplegará en este campo:

CODIGO	TIPO DE GASTO
1	Legales
2	Proveedores
3	Asesorías
4	Internos
5	Otros
9	No aplica (debe reportarse cuando el campo "TIPO DE MONTO" toma valores 1 o 3)

TIPO DE RECUPERACIÓN

Seleccione el código asociado a las causas de la recuperación operacional, de acuerdo a la siguiente codificación que se desplegará en este campo:

CODIGO	TIPO DE RECUPERACIÓN
1	Compañías de seguros
2	Acciones judiciales
3	Otros (liberación de provisión)
4	No aplica

MONTO

Corresponde al monto de las pérdidas, gastos o recuperaciones que deben reportarse en la fecha en la que se contabilicen.

NOMBRE Y CARGO DEL INFORMANTE

Corresponde a la persona que informa el incidente y su cargo.

ANEXO N° 4: DISPOSICIONES ADICIONALES RELATIVAS AL REPORTE DE INCIDENTES PARA SOCIEDADES ADMINISTRADORAS DE SISTEMAS DE COMPENSACIÓN Y LIQUIDACIÓN Y ENTIDADES DE DEPÓSITO Y CUSTODIA DE VALORES

Las Sociedades Administradoras de Sistemas de Compensación y Liquidación de Instrumentos Financieros y las Entidades de Depósito y Custodia a los que se refiere la ley N° 18.876 deberán considerar como parte de los incidentes a reportar definidos en la sección I.D.1:

- Eventos que provoquen la falta de disponibilidad de uno o más servicios por, al menos, 15 minutos.
- Eventos que impliquen la solicitud de una extensión horaria, se haga o no ésta efectiva, al Banco Central de Chile en su calidad de administrador del Sistema de Liquidación Bruta en Tiempo Real.

Esta Comisión deberá ser informada de toda solicitud de extensión horaria al Banco Central de Chile tan pronto ésta ocurra, y ser incluida como destinatario en el caso de boletines electrónicos u otras comunicaciones a sus depositantes u otras entidades que tengan por objetivo informar acerca de esta materia.

En caso de incidentes que no hayan sido resueltos luego de transcurridos 30 minutos desde su ocurrencia, la entidad afectada deberá comunicar al menos a sus usuarios, a las entidades no afectadas y al Banco Central de Chile esta situación, indicando la siguiente información:

- Ocurrencia de un incidente.
- Tiempo previsto para resolver incidente.
- Tiempo de extensión horaria otorgado por el Banco Central de Chile, en caso de haber sido solicitado.
- Recomendaciones para los usuarios.

En el mismo momento, la referida comunicación deberá ser enviada a esta Comisión a través del menú "INCIDENTES Y PERDIDAS OPERACIONALES" del canal oficial de comunicación y envío de información entre la Comisión y sus fiscalizados.

Si el incidente se prolongara por sobre el tiempo previsto para resolverlo, se deberá remitir una nueva comunicación en los mismos términos descritos anteriormente, con la información requerida actualizada y enviar copia de esta comunicación a esta Comisión a través del menú "INCIDENTES Y PERDIDAS OPERACIONALES".

La entidad deberá implementar y ejecutar procedimientos para identificar el problema que originó el incidente y prevenir su ocurrencia futura. Para la fase de identificación del problema deberá documentarse con precisión la metodología a emplear, la cual deberá ser una de amplia utilización en el ámbito de tecnologías de información y comunicación, validada por estándares internacionales en la materia. La información de incidentes y pérdidas operacionales a la que se refiere la sección I.D deberá remitirse al Comité de Riesgos (y al Comité de Vigilancia, cuando corresponda) de las Sociedades Administradoras de Sistemas de Compensación y Liquidación de Instrumentos Financieros y las Entidades de Depósito y Custodia, dentro de los plazos previstos en dicha sección.