Dicha estrategia, atendida la importancia relativa y el volumen de operaciones de la entidad, debe contemplar una definición clara de lo que considerará como riesgo operacional y establecer los principios para su identificación, evaluación, control y mitigación. En este sentido, si la exposición al riesgo es significativa, cobra relevancia la existencia de definiciones precisas de lo que se entenderá por pérdidas operacionales, ya sean esperadas o inesperadas, por cuanto los tratamientos de mitigación son diferentes en uno y otro caso.

Asimismo, es esencial que las instituciones cuenten con una clara definición, caracterización e identificación de los principales activos de información y de la infraestructura física que soporta y resguarda la seguridad de los mismos. En este ámbito, las entidades también deben gestionar la seguridad de sus activos de información expuestos a riesgos en el ciberespacio, entendido este como el entorno que permite la interacción lógica, es decir, no física, mediante la conexión de redes tecnológicas.

En la evaluación que hará este Organismo, interesa observar la compatibilidad entre las políticas y procedimientos aprobados por el Directorio, con respecto al volumen, sofisticación y naturaleza de sus actividades. Asimismo, se examinará la manera en que se han establecido las políticas y la forma en que el Directorio de la empresa participa en su aprobación y supervisa su cumplimiento.

Será también materia de examen comprobar si la posición independiente de la función de auditoría interna permite una adecuada cobertura y profundidad de las revisiones y la adopción oportuna de medidas correctivas por parte de las áreas auditadas.

En ese sentido, revelan una buena gestión, por ejemplo, situaciones o hechos tales como:

- El Directorio procura el establecimiento de una definición de riesgo operacional y lo reconoce como un riesgo gestionable. Especial importancia tendrá la existencia de una función encargada de la administración de este tipo de riesgo.

- La entidad mantiene políticas para la administración de los riesgos operacionales aprobadas por el Directorio, que atienden la importancia relativa de los riesgos operacionales considerando el volumen y complejidad de las operaciones.

- La estrategia de administración del riesgo operacional definida por el banco, es consistente con el volumen y complejidad de sus actividades y considera el nivel de tolerancia al riesgo del banco, incluyendo líneas específicas de responsabilidad. Esta estrategia ha sido implementada a través de toda la organización bancaria, y todos los niveles del personal asumen y comprenden sus responsabilidades respecto a la administración de este riesgo.

- La entidad administra los riesgos operacionales considerando los impactos que pudieran provocar en el banco (severidad de la pérdida) y la probabilidad de ocurrencia de los eventos.

- La entidad realiza evaluaciones del riesgo operacional inherente a todos los tipos de productos, actividades, procesos y sistemas. Asimismo, se asegura que antes de introducir nuevos productos, emprender nuevas actividades, o establecer nuevos procesos y sistemas, el riesgo operacional inherente a los mismos esté sujeto a procedimientos de evaluación.

- El banco ha integrado a sus actividades normales el monitoreo del riesgo operacional y ha identificado indicadores apropiados que entreguen alertas de un aumento del riesgo y de futuras pérdidas.

- El banco es capaz de cuantificar los impactos de las pérdidas asociadas al riesgo operacional y constituir prudencialmente los resguardos necesarios.

- Los sistemas de información permiten hacer un monitoreo continuo de la exposición a los riesgos operacionales. Poseen la cobertura y profundidad necesarias para servir en forma eficiente al proceso de toma de decisiones, de acuerdo a las necesidades propias de las distintas instancias organizacionales.

- El banco cuenta con políticas para administrar los riesgos asociados a las actividades entregadas a terceras partes y lleva a cabo verificaciones y monitoreos a las actividades de dichas partes.

- El banco realiza inversiones en tecnología de procesamiento y seguridad de la información, que permiten mitigar los riesgos operacionales y que son concordantes con el volumen y complejidad de las actividades y operaciones que realiza.

- El banco cuenta con una adecuada planificación a largo plazo para la infraestructura tecnológica y dispone de los recursos necesarios para el desarrollo normal de sus actividades y para que los nuevos proyectos previstos se concreten oportunamente.

- El banco cuenta con una estructura dedicada que permite administrar la seguridad de la información en general y de *Ciberseguridad* en particular, en términos de resguardar su confidencialidad, integridad y disponibilidad. Respecto a la gestión de la *Ciberseguridad*, la entidad al menos contempla los aspectos descritos en el Anexo N° 3 de este Capítulo y en el numeral 2 del Capítulo 20-8 de esta Recopilación.

- El banco considera en sus planes de continuidad del negocio y contingencia, diversos escenarios y supuestos que pudieran impedir que cumpla toda o parte de sus obligaciones y en ese sentido ha desarrollado una metodología formal que considera en sus etapas, la evaluación de impacto y criticidad de sus servicios y productos, la definición de estrategias de prevención, contención y recuperación, así como pruebas periódicas de tales estrategias.

- El banco ha implementado un proceso para controlar permanentemente la incorporación de nuevas políticas, procesos y procedimientos, que permiten detectar y corregir sus eventuales deficiencias de manera de reducir la frecuencia y severidad de los eventos de pérdida. Asimismo, el Directorio y la alta administración reciben reportes periódicos, con la información pertinente al rol que desempeñan.

- La entidad bancaria ha adoptado una estrategia y sistema de gestión de calidad respecto de sus productos, servicios, e información que suministra a sus clientes, reguladores y a otros entes.

- La extensión y profundidad de las auditorías es proporcional al nivel de riesgo y al volumen de actividad. La función de auditoría está en posición de evaluar en forma independiente el cumplimiento de las políticas, la eficacia de los procedimientos y los sistemas de información.

Sin perjuicio de lo anterior, en lo que se refiere específicamente a la gestión de la continuidad del negocio, la evaluación de esta Superintendencia cubrirá los aspectos que se detallan en el Capítulo 20-9 de esta Recopilación.

D) Administración de los riesgos de exposiciones en el exterior y control sobre las inversiones en sociedades.

La evaluación abarcará el control sobre las sucursales en el exterior, filiales y sociedades de apoyo al giro, ubicadas en el país o en el extranjero. Por otra parte, también incluye la gestión global de las operaciones de crédito hacia el exterior, las inversiones minoritarias en sociedades y las transacciones efectuadas en el extranjero, en general.

En lo que se refiere a la presencia de sucursales en el exterior, filiales y sociedades de apoyo al giro, interesa la suficiencia y efectividad del control ejercido por la matriz. Al respecto se espera un control permanente de las entidades, acorde con las peculiaridades del entorno en que ellas se desenvuelven y su grado de autonomía, que permita el seguimiento de su marcha y una reacción oportuna frente a factores perturbadores.

En la evaluación de la gestión global de los préstamos y operaciones en el exterior, incluidas aquellas efectuadas desde el exterior con terceros países, constituye un elemento clave el dominio que tiene el banco sobre el riesgo-país (riesgo soberano y de transferencia), y que pasa por un análisis permanente de la situación de los países en que compromete sus recursos y la fijación de límites en relación con la concentración de cartera en cada país.

Con respecto al riesgo de crédito, el enfoque de la evaluación no difiere del mencionado en la letra A) de este numeral 3.2. Por lo mismo, interesa particularmente la suficiencia de la información relativa a los deudores y al comportamiento de su entorno, y los criterios para la fijación de límites de crédito que atiendan a las características de los deudores y tipo de financiamiento.

Por otra parte, dado que en las operaciones con el exterior adquiere una relevancia especial el manejo del riesgo legal, merece destacarse también el examen de los procedimientos que permiten operar con un conocimiento fundado y oportuno de los efectos contractuales.

Al igual que en las otras materias antes descritas, la evaluación apunta asimismo a asegurarse de la eficacia de las auditorías internas. En el caso de las sucursales en el exterior, filiales y sociedades de apoyo al giro, tanto nacionales como en el exterior, es importante también, en este aspecto, la forma en que se cubre la función de auditoría.

Una gestión óptima en relación con lo señalado en este numeral, la mostrarían, por ejemplo, situaciones globales como las siguientes:

- El Directorio ejerce una supervisión efectiva sobre la alta administración, para asegurar que el banco maneja los riesgos de sus inversiones y operaciones internacionales en forma sana y segura.

- Las sucursales en el exterior, las filiales y sociedades de apoyo al giro en el país y en el extranjero, están sujetas a un control permanente y con medios que permiten tomar las medidas correctivas oportunas en caso de ser necesario, tanto en lo que se refiere a la marcha de los negocios, riesgos (patrimoniales y de reputación), rentabilidad y compromisos de capital, como en lo que se refiere a la verificación del cumplimiento de directrices o políticas de la matriz y, particularmente, para el caso de sucursales en el exterior del cumplimiento de las regulaciones de los países anfitriones.

- Las políticas para administrar el riesgo-país exigen una evaluación permanente de los países en los cuales se mantienen exposiciones y contemplan límites de exposición acordes con la situación financiera general del banco, debidamente aprobados y sujetos a seguimiento. Los procedimientos de evaluación del riesgo país contemplan el análisis por parte de profesionales independientes e idóneos, tanto de los factores económicos como de los políticos y sociales que en alguna medida podrían repercutir en el normal retorno de los flujos de las inversiones.

- Las estrategias comerciales en relación con las operaciones en el exterior, son compatibles con la capacidad del banco para efectuarlas bajo control de los riesgos. Las decisiones sobre nuevos negocios u operaciones con contrapartes radicadas en el exterior, son tomadas sobre la base de un análisis previo de todos los riesgos inherentes, cubriéndose en consecuencia, sistemáticamente, el riesgo país, el riesgo de crédito, el riesgo financiero, el riesgo legal y el riesgo operativo que derive de las peculiaridades de las operaciones.

- En el caso de las filiales, el banco ha establecido mecanismos que le permiten asegurarse de que las políticas relativas a riesgos, son consistentes con sus propias políticas. Asimismo, puede obtener mediciones consolidadas de los riesgos más relevantes, utilizando metodologías adecuadas a la escala y complejidad de los negocios llevados a cabo.

E) Prevención del lavado de activos y del financiamiento del terrorismo.

La evaluación comprende un análisis del rol que desempeña el Directorio sobre las actividades de prevención de lavado de activos y del financiamiento del terrorismo, así como también la existencia de un marco de políticas y procedimientos, los que deben ser acordes al tamaño y complejidad de las operaciones del banco y sus filiales.

Son también materia de revisión, los procedimientos eficaces sobre "conozca a su cliente", la presencia de un oficial de cumplimiento, la existencia de políticas relacionadas con selección de personal, la existencia de un código de conducta interno y de una función de auditoría independiente, responsable de evaluar periódicamente el cumplimiento de las políticas y procedimientos.

En este sentido, revelan una buena gestión, por ejemplo, situaciones o hechos como los siguientes:

- La entidad cuenta con políticas y procedimientos formalmente establecidos sobre "conozca a su cliente" ya sea para clientes permanentes u ocasionales, acordes al tamaño y complejidad de sus operaciones. Estas políticas al menos, contienen criterios de aceptación y de seguimiento proactivo de cuentas que permiten tener un adecuado conocimiento de los clientes y de las actividades que desarrollan.

- Las políticas y procedimientos fueron aprobados por el Directorio, el que a su vez, mantiene una vigilancia permanente sobre su cumplimiento y recibe información periódica sobre las revisiones que se efectúen para verificar su adherencia. A su vez, dicho marco de alineamiento se hace extensivo a las sociedades filiales y de apoyo al giro que corresponda.

- La entidad cuenta con procedimientos establecidos para conducir las relaciones con la banca corresponsal.

- La entidad cuenta con un manual de procedimientos formalizado para reconocer transacciones potencialmente sospechosas, el que es accesible a todo el personal involucrado y es permanentemente actualizado.

- La entidad cuenta con un oficial de cumplimiento con la jerarquía e independencia necesarias para desarrollar su función y con los recursos humanos y tecnológicos adecuados.

- Dependiendo del tamaño de la organización, se ha instaurado un comité de alto nivel encargado de revisar políticas y procedimientos, evaluar su cumplimiento y decidir sobre casos que requieren atención especial.

- Existe un proceso de capacitación formal y periódico con el objeto de difundir las políticas y procedimientos a todo el personal de la entidad. El proceso de capacitación es diferenciado de acuerdo a la función que desempeña cada cual.

- Se cuenta con normas de selección de personal y de conducta con clientes, con el objeto de prevenir la ocurrencia de operaciones de lavado de activos y financiamiento del terrorismo. Además se ha desarrollado un código de conducta del personal que contempla principios respecto de las relaciones que se deben mantener con los clientes del banco.

- La entidad ha desarrollado sistemas de detección de operaciones inusuales, los que son acordes al tamaño y complejidad de sus actividades. Además existen canales formales de información a instancias superiores, los que permiten que estas operaciones sean conocidas a tiempo por la instancia pertinente y puedan ser reportadas a la autoridad competente.

- La función de auditoría realiza actividades periódicas e independientes de aquellas desarrolladas por el oficial de cumplimiento, con el objeto de verificar la adherencia a las políticas y procedimientos del banco para la detección y seguimiento de esas operaciones ilícitas. Su rol también comprende el análisis de las políticas y procedimientos, los sistemas de control, los planes de capacitación del personal, entre otros.

ANEXO Nº 3

GESTIÓN DE LA *CIBERSEGURIDAD*

Para efectos de lo dispuesto a continuación, se entiende que la *Ciberseguridad* es un concepto que comprende al conjunto de acciones para la protección de la información presente en el ciberespacio, así como de la infraestructura que la soporta, que tiene por objeto evitar o mitigar los efectos adversos de sus riesgos y amenazas inherentes, sobre la seguridad de la información y la continuidad del negocio de la institución.

I. GESTIÓN DE LA INFRAESTRUCTURA CRÍTICA DE *CIBERSEGURIDAD*

Una adecuada gestión de la infraestructura crítica en materias de *Ciberseguridad* requiere de un marco de gestión establecido por el Directorio, que contemple la estrategia de administración específica de este riesgo, el nivel de tolerancia admitido, roles y responsabilidades de los participantes, los procesos y las metodologías a utilizar para su gestión en consideración a las mejores prácticas, al volumen y complejidad de sus actividad de negocio y a los estándares internacionales existentes para este efecto.

La gestión de la infraestructura crítica de *Ciberseguridad* es fundamental para el adecuado funcionamiento del sistema financiero, en el caso de eventuales ataques. Con este fin, se evaluará que las instituciones gestionen esta infraestructura considerando al menos los siguientes elementos:

a) La institución ha identificado la infraestructura crítica en términos de *Ciberseguridad*, esto es, aquellos activos de información lógicos que son considerados críticos para el funcionamiento del negocio y del sistema financiero en su conjunto. Asimismo, son parte de esta infraestructura los componentes físicos tales como, *hardware* y sistemas tecnológicos que almacenan, administran y soportan estos activos y que de no operar adecuadamente, exponen a la entidad a riesgos de integridad, disponibilidad y confidencialidad de la información.

b) La institución cuenta con un inventario de activos de la información críticos clasificado de acuerdo a las condiciones de seguridad (confidencialidad, integridad y disponibilidad).

c) La institución ha desarrollado e implementado los resguardos necesarios para proteger la infraestructura definida como crítica. La institución ha establecido las medidas de seguridad adecuadas para prever, detectar y gestionar oportunamente los eventos e incidencias que puedan afectar la *Ciberseguridad* de la infraestructura crítica.

d) La institución revisa regularmente sus políticas y procedimientos para prever la adopción oportuna de medidas ante escenarios de amenazas de *Ciberseguridad*.

e) La institución dispone de planes de recuperación de operaciones o procesos críticos en forma oportuna y eficaz.

f) La institución promueve una cultura de riesgos en materia de *Ciberseguridad*, a través de procesos formales de difusión, capacitación y concientización de todos los empleados, de acuerdo a sus funciones y tiempo de permanencia en la institución; con una periodicidad establecida y oportuna.

g) La institución realiza regularmente pruebas para detectar las amenazas y vulnerabilidades que pudieran existir sobre su sistema de gestión de seguridad de la información en el ciberespacio, tales como *pentesting* y/o *ethical hacking*. Estos análisis deberán ser periódicos y su resultado gestionado por las áreas de seguridad de la información y comunicado al Directorio, al menos semestralmente, quedando evidencia en las actas de los análisis y acuerdos adoptados.

CAPÍTULO 20-8

INFORMACIÓN DE INCIDENTES OPERACIONALES RELEVANTES Y BASE DE DATOS DE INCIDENTES DE *CIBERSEGURIDAD*.

La evolución de la industria financiera, particularmente la incorporación de la tecnología en la forma de generar, procesar y administrar sus activos de información, involucran riesgos operacionales que afectan a los procesos del negocio de la institución.

Al respecto, resulta relevante que las entidades dispongan de sistemas, procedimientos y mecanismos de gestión que permitan identificar, registrar, evaluar, controlar, mitigar, monitorear y reportar incidentes operacionales, y en especial aquellos incidentes relacionados con la *Ciberseguridad*. Estos sistemas deben permitir al banco tener una visión oportuna de los incidentes y, a la vez, asegurar la existencia de herramientas para hacer el seguimiento y correlacionar eventos, a objeto de detectar otros incidentes, identificar vulnerabilidades de la infraestructura física y virtual comprometida, *modus operandi* de los eventuales ataques, entre otros.

En virtud de lo anterior, este Capítulo establece requisitos relativos a la información que se debe enviar a esta Superintendencia cuando ocurran incidentes operacionales relevantes, así como la generación y mantención de una base de incidentes relacionados con la *Ciberseguridad*.

1. COMUNICACIÓN DE INCIDENTES OPERACIONALES RELEVANTES

Los bancos deberán comunicar de inmediato a esta Superintendencia, para el solo efecto de mantenerla informada, los incidentes operacionales relevantes.

Se entiende que son relevantes aquellos eventos que afecten la continuidad del negocio, la seguridad de la información o la imagen de la institución.

La información se enviará tan pronto se identifique el incidente, mediante un correo electrónico dirigido a la casilla habilitada por esta Superintendencia para recibir tales comunicaciones en cualquier horario, tanto de días hábiles como inhábiles. El correo deberá incluir la siguiente información:

- Nombre de la entidad informante.
- Datos de la persona encargada de enviar la información: nombre, cargo, correo electrónico y teléfono celular.
- Fecha y hora de inicio del evento.
- Explicación del incidente: la situación que originó y su causa inmediata.

- Proveedores involucrados, señalando su participación en el proceso afectado por el incidente, cuando sea el caso.

- Estimación de tipo y número de clientes afectados, cuando corresponda.

El encargado de enviar la información, o quien lo reemplace, deberá ser una persona de nivel ejecutivo, designado por la institución tanto para ese efecto como para responder eventuales consultas de esta Superintendencia.

2. BASE DE INCIDENTES DE CIBERSEGURIDAD

2.1 Condiciones mínimas para el desarrollo y mantención de una Base de Incidentes

La Ciberseguridad en las instituciones financieras es esencial para evitar los efectos adversos sobre su continuidad operacional, así como la seguridad de los activos que administran.

Al respecto, resulta relevante que las entidades dispongan de sistemas, procedimientos y mecanismos de gestión que permitan identificar, registrar, evaluar, controlar, mitigar, monitorear y reportar incidentes operacionales relacionados con la *Ciberseguridad*.

A continuación se detallan algunos de los elementos que serán parte de la evaluación de gestión, en los términos del Capítulo 1-13 de la RAN, respecto a la generación de la base de incidentes:

a) El Directorio de la institución toma regularmente conocimiento de estos incidentes y se pronuncia sobre ellos al menos una vez al año, con el fin de mejorar su gestión y prevención.

b) La entidad cuenta con una base de incidentes de Ciberseguridad, donde registra los eventos no planificados por la institución que ponen en riesgo la seguridad de los activos de información presentes en el ciberespacio e identificando de manera individual cada uno de estos incidentes.

c) La institución gestiona sus incidentes de Ciberseguridad, con el fin de detectar, investigar y generar acciones de mitigación del impacto de estos eventos, resguarda la confidencialidad, disponibilidad e integridad de sus activos de información.

d) La base de incidentes completa deberá mantenerse a disposición de esta Superintendencia para cuando sea requerida. La suficiencia de la base de incidentes es parte de las revisiones de la función de auditoría interna.

e) La institución considera la base de incidentes como un insumo para la realización de pruebas que permiten detectar las amenazas y vulnerabilidades que pudieran existir sobre su sistema de gestión de seguridad de la información en el ciberespacio, las cuales están indicadas en la letra g del Título I del Anexo N° 3 del Capítulo 1-13 de esta Recopilación .

2.2 Variables mínimas a considerar para la elaboración de la base de incidentes de *Ciberseguridad*

a) Identificación única del incidente: Se entenderá como incidente, aquel evento que afecte negativamente a la institución. La base de incidentes debe reportar no solo los eventos materializados, sino también aquellos que la institución logró detectar en una fase temprana y no produjeron daños efectivos.

b) Especificar si se trató de un incidente materializado o no.

c) Fecha del evento: fecha y hora del inicio del incidente.

d) Fecha del reporte: fecha y hora en la que el incidente es detectado.

e) Fecha de la mitigación: fecha y hora en la que el incidente se mitigó, cuando corresponda.

f) Tipo de vulnerabilidad: determinar la causa del incidente, materializado o no, a partir del tipo de vulnerabilidad que pone en riesgo a los activos de información de acuerdo a la clasificación presentada a continuación:

1. Incumplimiento de las políticas establecidas para el control del riesgo de *Ciberseguridad*.
2. Inadecuada definición, instalación o mantención de la estructura física que soporta los activos de información lógicos.
3. Inadecuada definición o control de los accesos físicos.
4. Inadecuada definición o control de los accesos lógicos.
5. Inadecuada definición de los servicios provistos por agentes externos.
6. Inadecuada definición o control de la arquitectura tecnológica.
7. Prácticas inadecuadas de los usuarios internos de la organización.
8. Prácticas inadecuadas de los usuarios externos de la organización.
9. Otro (especificar)

g) Descripción del incidente: breve descripción del incidente que permita entender sus causas externas, especificando el tipo de amenazas, ataques físicos como robo o hurto de dispositivos, vandalismo, acceso físico de personal no autorizado, entre otros; interrupciones producto de huelgas, servicio de red, energía o falta de recursos, etcétera; actividades ilegales como robo de identidad, virus, certificados maliciosos, malware, denegación de servicio, ingeniería social, entre otros; desastres naturales o medioambientales; fallas o mal funcionamiento, accidentes, amenazas legales, secuestros, daños o pérdidas de activos de información tecnológicos, etcétera. Se sugiere utilizar las definiciones asociadas a estándares internacionales sobre la materia.

h) Activos involucrados: especificación de los activos afectados, distinguiendo aquellos efectivamente vulnerados de los potencialmente en riesgo.

i) Tipo de productos o servicios involucrados: detallar, cuando corresponda, aquellos productos o servicios prestados por la institución que fueron afectados por el incidente, ya sea en su disponibilidad o funcionamiento.

j) Número de clientes directamente afectados (cuando corresponda).

k) Identificación de los proveedores (cuando corresponda, esto es, cuando exista un proveedor externo involucrado en la vulnerabilidad detectada).

l) Costos de incidentes: costos asociados al incidente, entendidos como el valor presente de las pérdidas reales, cuando corresponda.

m) Costos de mitigación y reparación: costos de eventuales medidas de mitigación y reparación asociados al incidente, sea que este se haya o no materializado**.**

n) Descripción de las acciones realizadas y áreas responsables de su implementación (cuando corresponda).

o) Estado del incidente: indicar para cada evento si los planes de acción para su corrección definitiva se encuentran implementados.

———

_____

Materia **Capítulo**

CRÉDITOS A PERSONAS RELACIONADAS Y TRABAJADORES

CRÉDITOS AL EXTERIOR

CONTINUIDAD DEL NEGOCIO

CUENTAS CORRIENTES

Materia **Capítulo**