CAPÍTULO 20-8

INFORMACIÓN DE INCIDENTES OPERACIONALES.

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, en especial aquellos 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, la obligación de mantener adecuadamente informados a los clientes en determinados eventos y el deber de los bancos de compartir información de ataques relacionados a Ciberseguridad.

1. COMUNICACIÓN DE INCIDENTES OPERACIONALES

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

Asimismo, deben ser informados los incidentes que afecten a un grupo de clientes que puedan impactar la imagen y reputación de la entidad en forma inmediata, o con posterioridad a ocurrido un determinado evento.

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

1.1 Envío de la información a la Superintendencia

La información deberá ser enviada mediante la casilla habilitada por esta Superintendencia a través de su Extranet, en cualquier horario, tanto en días hábiles como inhábiles, en el plazo máximo de 30 minutos luego de su ocurrencia.

Para estos efectos, la entidad deberá definir un funcionario encargado, quien realizará los reportes y enviará la información según lo indicado en este numeral. Esta persona o quien la reemplace deberán tener un nivel ejecutivo y ser designados por la institución tanto para este efecto, como para responder eventuales consultas por parte de este Organismo.

La información deberá ser reportada de acuerdo al siguiente esquema:

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

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

El no contar con toda la información de los campos mencionados previamente no debe ser impedimento para el envío de la comunicación dentro del plazo definido en este numeral.

En los casos que este Organismo lo estime necesario, se podrá requerir a las instituciones un plan de recuperación.

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

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

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

Adicionalmente, en los casos que este Organismo lo estime necesario, podrá requerir informes complementarios a la entidad (por ejemplo, informes forenses).

1.2 Información a clientes o usuarios

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

1.3 Información a la industria

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

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

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

- 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, entre estas las políticas de actualización y parche de software, y para que los nuevos proyectos previstos se concreten oportunamente.

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

- La entidad cuenta con una base comprensiva de incidentes de Ciberseguridad, que registra los eventos que ponen en riesgo la seguridad de los activos de información presentes en el ciberespacio, identificados de manera individual. Esta base contempla, como mínimo, los campos solicitados mensualmente en el archivo que para este fin existe en el Manual de Sistema de Información de esta Superintendencia. La suficiencia de la base de incidentes debe ser parte de las revisiones de la función de auditoría interna.

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

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

- 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.

F) Administración de la estrategia de negocios y gestión del capital.

La evaluación comprende el proceso global de diseño, formulación y seguimiento de la estrategia de negocios como también la elaboración y control de los planes desarrollados por el banco.

Será objeto de calificación la forma en que el banco administra el proceso de formulación de su estrategia de negocios, en lo que se refiere al manejo de los fundamentos e información que le otorgan un grado razonable de viabilidad como, asimismo, la manera en que las condiciones generales del entorno y de la entidad, particularmente en lo relativo a necesidades de capital, han sido incorporadas en su definición.

Debe tenerse presente, tal como se señaló en el numeral 4.1 del título I, que existe una estrecha relación entre los niveles de capital mantenidos por el banco y la estrategia de negocios. En rigor, el mero cumplimiento de los requisitos mínimos de capital establecidos en la ley constituye un acatamiento a las disposiciones normativas, pero no refleja necesariamente una gestión razonada de los requerimientos de capital idóneos a la estrategia de negocios de la entidad.

En este sentido, se examinará si el proceso de planificación tiene en cuenta el análisis de los requerimientos de capital actuales y futuros del banco con relación a sus objetivos estratégicos, así como respecto de la implementación de los procesos de gestión de riesgo y de sus controles internos, como base de una evaluación eficaz de la suficiencia de capital mantenido por la entidad.

Una buena gestión en relación con lo descrito puede manifestarse en lo siguiente:

- El Directorio comprende la naturaleza y el nivel del riesgo asumido por el banco y la forma en que este riesgo se corresponde con niveles de capital suficientes y con sus planes de negocios. En este sentido, el Directorio contempla la planificación del capital como un elemento fundamental para la definición, implementación y logro de los objetivos estratégicos.

- El análisis de los requerimientos de capital y los riesgos, son parte integral del proceso de formulación de la estrategia de negocios. En efecto, dicha estrategia recoge con claridad las necesidades de capital del banco y sus fundamentos, los aportes de capital previstos, el nivel y composición de capital deseable y las fuentes externas de capital, como también el nivel y perfil de riesgo proyectado para las distintas líneas de negocios.

- El banco realiza análisis permanentes del entorno económico y de sus condiciones internas, así como de su posición comparativa en el mercado, que le permiten mantener una estrategia bien fundada y sostenible.

- La estrategia de negocios ha sido integralmente plasmada en los planes y presupuestos operacionales, y adecuadamente transmitida a los niveles pertinentes. El Directorio manifiesta su plena concordancia respecto a la orientación, ejecución y a su concreción.

- La entidad cuenta con sistemas de información que permiten una supervisión efectiva sobre el cumplimiento de los planes de negocios, la naturaleza y cuantía de los riesgos, como también respecto de la adecuación de capital económico y regulatorio.

- La estrategia de negocios está sujeta a revisiones periódicas, bajo procedimientos que permiten acciones correctivas oportunas o redefiniciones de los objetivos o planes de acción. Esto contempla una evaluación rigurosa de los requerimientos de capital y la realización de pruebas de tensión que incorporan posibles acontecimientos o cambios en las condiciones de mercado que pudieran afectar negativamente al banco.

- El banco ha establecido metas, plazos y responsables del cumplimiento de los planes de negocios y se han asignado los recursos necesarios para ello.

G) Gestión de la calidad de atención a los usuarios y transparencia de información.

La buena calidad en la atención de los clientes así como la calidad de la información que les es divulgada, constituyen aspectos importantes de la imagen que los bancos proyectan y, por cierto, son concordantes con una adecuada gestión de la entidad.

La evaluación de esta materia contempla la existencia de políticas y procedimientos que consideren la adecuada atención de sus clientes, la administración de controversias y la entrega de información al público con los cobros que afectan a los productos y servicios ofrecidos por el banco.

Es también parte de este examen, comprobar si la función de auditoría es suficientemente independiente para permitir una adecuada cobertura y profundidad de las revisiones que se efectúen sobre la materia y la adopción oportuna de medidas correctivas por parte de las áreas auditadas.

A modo de ejemplo, revelan una buena gestión sobre la materia, los siguientes aspectos:

- Políticas y procedimientos formalmente establecidos de transparencia de la información referida a los atributos de los productos y sus tarifas, de modo que cumplan las condiciones necesarias para una adecuada toma de decisiones por parte de los clientes. Lo anterior comprende la información entregada tanto al inicio de la relación comercial con el cliente, como durante todo el período que dure la relación contractual con este.

- Políticas y procedimientos formalmente establecidos, que consideren aspectos tales como la gestión de los reclamos, la existencia de canales formales de recepción de reclamos, la atención de consultas y solicitudes del público, la existencia de código de buenas prácticas comerciales, la capacitación al personal, la entrega de normas y procedimientos para la administración de los fraudes y de otros hechos delictuosos.

- La existencia y funcionamiento de unidades especializadas que cuenten con las herramientas y los recursos humanos y tecnológicos adecuados al tamaño del banco para administrar eficientemente las consultas y los reclamos del público.

- La existencia de informes de gestión que permitan identificar los tipos de reclamos, consultas y solicitudes, los productos involucrados en las presentaciones, los canales de recepción y el cumplimiento de estándares de respuesta, los que periódicamente deben ser dados a conocer al Directorio o a quién haga sus veces.

- La participación del Directorio en la aprobación de políticas y procedimientos; y de alguna de las instancias de la alta administración, en la definición de estándares de calidad, resolución de controversias y promoción de acciones correctivas.

- La adecuada divulgación, cuando corresponda, de las políticas, procedimientos y estándares de calidad hacia las filiales y sociedades de apoyo del banco, y su posterior control.

- La presencia de la función de auditoría interna en la revisión del proceso de atención de clientes y administración de reclamos.

H) Gestión de la función de auditoría interna y rol del comité de auditoría.

La existencia de una sólida función de auditoría interna se caracteriza por entregar una opinión independiente respecto de la calidad de los sistemas de control interno y del cumplimiento de las políticas y procedimientos, de manera de identificar, medir y controlar razonablemente los riesgos presentes y potenciales que pueden existir.

A continuación se describen algunos elementos que constituyen una buena gestión en relación al rol de la auditoría interna:

- La función de auditoría, previamente definida por el Directorio, presenta independencia de las áreas que desarrollan la negociación, operación y control de los negocios, y cuenta con adecuados recursos humanos y tecnológicos para el logro de sus objetivos, en concordancia con el tamaño y complejidad de las operaciones del banco.

- Todos los procesos y áreas de mayor riesgo en el banco son examinados por la auditoría interna, al menos en forma anual.

- La función de auditoría posee un enfoque de carácter proactivo e integral, es decir, se incorporan en sus revisiones aspectos operativos, de riesgos y de gestión, entregando una opinión global de la unidad, producto o materia auditada.