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 Comisión 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 Comisión los incidentes operacionales que afecten o pongan en riesgo la continuidad del negocio, los fondos o recursos de la entidad o de sus clientes, la calidad de los servicios o la imagen de la institución. El banco, en caso de incidentes, será responsable de mantener informada a esta Comisión de la situación en desarrollo y de las medidas o acciones de detección, respuesta y recuperación del incidente. A modo de ejemplo, 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 Comisión.

1.1 Envío de la información a la Comisión

La información deberá ser enviada, 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 Comisión, 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 Comisión a la información compartida.
