Superintendencia de Bancos e Instituciones Financieras Chile

CIRCULAR

Bancos N° 3.640

Santiago, 31 de agosto de 2018

RECOPILACIÓN ACTUALIZADA DE NORMAS. Capítulos 1-13 y 20-8.

Lineamientos para la gestión de la Ciberseguridad y reporte de incidentes operacionales. Actualiza instrucciones.

Como es de su conocimiento, durante los últimos años esta Superintendencia ha puesto un fuerte énfasis en el fortalecimiento de la gestión de la Ciberseguridad por parte de las instituciones fiscalizadas. En efecto, a través de diversas iniciativas, se ha destacado la necesidad que los bancos tomen medidas para fortalecer la gestión interna de los riesgos asociados a las tecnologías de la información y la continuidad de negocio.

En dicho contexto, mediante la Circular N° 3.633 de 24 de enero de 2018, se impartieron normas tendientes a establecer lineamientos mínimos y buenas prácticas que deben observar los bancos para la gestión de la Ciberseguridad, siendo estos parte de los elementos que se consideran en el ámbito de la evaluación de gestión que realiza este Organismo. Además, se estableció la exigencia de generar y mantener una base de incidentes que sistematice la identificación, registro y posterior gestión de los mismos, la que debe mantenerse a disposición de esta Superintendencia para cuando sea requerida.

Luego de la evaluación realizada por este Organismo a la forma en que se han estado implementando las referidas disposiciones, y en atención a los recientes incidentes que han afectado a la industria, se ha resuelto progresar en el desarrollo de los protocolos y sistemas de información pertinentes, mediante la adopción de las medidas que se exponen a continuación y que se materializan mediante los correspondientes ajustes a los Capítulos 1-13 y 20-8 de la Recopilación Actualizada de Normas.

1. Capítulo 20-8

a) Se modifican las disposiciones del N° 1, precisando conceptualmente el tipo de incidentes operacionales que deben ser comunicados a la Superintendencia.

b) Se introduce un numeral 1.1, donde se establece la oportunidad, contenido mínimo y mecanismo de comunicación de los incidentes operacionales.

En particular, cabe destacar que se define un plazo máximo de 30 minutos para remitir los primeros antecedentes de que dispongan a través de la Extranet de la Superintendencia, a partir de la fecha que se indica en las disposiciones transitorias de esta Circular. Asimismo, se establece la obligación de designar un encargado de nivel ejecutivo para establecer permanente comunicación con la Superintendencia y la asignación automática de un número único de identificación de los incidentes reportados, con la finalidad de identificarlos y mantener un adecuado seguimiento en su desarrollo, tratamiento y resolución.

c) Se agregan los numerales 1.2 y 1.3, donde se define el tipo de información que debe ser proporcionada a los clientes y a la industria, respectivamente.

En el primer caso, corresponde informar a los usuarios y clientes sobre aquellos incidentes que afecten la calidad o continuidad de los servicios, la seguridad de sus datos personales o se trate de un hecho de público conocimiento.

Por su parte, en el caso de la información para la industria, se establece la obligación de mantener un sistema de alerta de incidentes de Ciberseguridad, con la finalidad de que los bancos compartan información que permita a las demás entidades tomar los resguardos pertinentes para la detección, respuesta y recuperación de sus servicios, y así disminuir la probabilidad de que impactos negativos se propaguen en el sistema. El desarrollo de dicho sistema de información también tiene como propósito que las instituciones fiscalizadas puedan, bajo un estándar común, desarrollar instancias de colaboración para enfrentar aquel tipo de amenazas, tal como lo han venido haciendo otras jurisdicciones que sirven como referentes en la materia.

d) Se elimina el N° 2 del Capítulo 20-8, traspasando al Capítulo 1-13 de la Recopilación Actualizada de Normas, los elementos que se evalúan en el ámbito de riesgo operacional.

Por otro lado, las variables mínimas que se deben considerar para la elaboración de una base de incidentes ahora serán parte de un archivo del Manual de Sistema de Información, que sistematiza la información requerida por este Organismo y que próximamente se publicará para comentarios del público.

2. Capítulo 1-13

De acuerdo a lo indicado previamente, en cuanto a las condiciones y elementos relacionados a los sistemas de información de Ciberseguridad que se evalúan en el ámbito del riesgo operacional, en el séptimo párrafo de la letra C) del numeral 3.2 del título II del Capítulo 1-13, se introducen las siguientes modificaciones:

a) En la décimo primera viñeta, a continuación de la palabra "actividades", se intercala entre comas la siguiente frase: "entre estas las políticas de actualización y parche de software".

b) A continuación de la citada viñeta, se intercala lo siguiente:

"- 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."

c) En la décimo segunda viñeta, que pasó a ser décimo sexta, se elimina la expresión "y en el capítulo 20-8, número 2 de esta Recopilación".

3. Disposiciones transitorias

El envío de información sobre incidentes operacionales a través de la Extranet de esta Superintendencia rige a partir del 16 de octubre próximo. En el intertanto, se seguirá utilizando el correo electrónico habilitado para dichos efectos. Por su parte, los bancos deberán tener habilitado su sistema de intercambio de información, según lo indicado en el numeral 1.3 del Capítulo 20-8, a más tardar el 5 de noviembre del presente año.

Se adjuntan las hojas de la Recopilación Actualizada de Normas que contienen el texto actualizado del Capítulo 20-8 y las que reemplazan las hojas N°s 14, 15, 16, 17, 18, 19 y 20 del Capítulo 1-13.

Saludo atentamente a Ud.,

MARIO FARREN RISOPATRÓN
Superintendente de Bancos e Instituciones Financieras