



Superintendencia
de Bancos
e Instituciones
Financieras
Chile

Cuestionario: Normativa para la gestión de Ciberseguridad (En consulta)

www.sbif.cl



1. Descripción general de las normas

Cuestionario: Normas sobre
la Emisión y operación
de tarjetas de pago



¿Qué aborda esta publicación?

El presente cambio normativo que se pone en consulta establece diversos aspectos para la gestión de la seguridad de los activos de información sujetos a riesgo en el ciberespacio que serán parte de la evaluación de gestión sobre la Administración del Riesgo Operacional.

Por otra parte esta normativa, también considera la necesidad de generar una base de incidentes de Ciberseguridad bajo un estándar común, que tiene por objeto establecer un lenguaje y nivel de información mínimo y homogéneo en la industria.

¿A quiénes está dirigida esta norma?

La norma está dirigida a los bancos fiscalizados por esta Superintendencia, en el marco de las disposiciones establecidas en el Capítulo 1-13 de la Recopilación Actualizada de Normas, específicamente la letra C) del numeral 3.2 del Título II sobre la Administración del Riesgo Operacional.

¿Cuál es el contexto de la emisión de esta normativa?

A partir de la constante evolución de la industria financiera en materias tecnológicas se hace necesario incorporar aspectos específicos en materia de riesgos, como lo es la Ciberseguridad.

En abril de 2017 se publicó la Política Nacional de Ciberseguridad, marco específico en materias de seguridad de la información en el ciberespacio. Y además, esta Superintendencia considera que es el momento de establecer esta visión y este lenguaje de manera específica dentro su normativa.



2. Conceptos aplicables a la normativa

Cuestionario: Normas sobre
la Emisión y operación
de tarjetas de pago



¿Qué es 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.

¿Qué es ciberespacio?

Es el entorno que permite la interacción lógica, es decir, no física, mediante la conexión de redes tecnológicas.

3. Infraestructura para la gestión de Ciberseguridad

¿Qué elementos nuevos considera la normativa?

La normativa se enmarca en la evaluación que esta Superintendencia realiza sobre la Administración del Riesgo Operacional.

En este contexto, se presentan orientaciones para la adecuada definición, caracterización e identificación de los principales activos de información de la institución y de la infraestructura física que los soporta y los resguarda, como también aspectos asociados a la gestión de riesgos en el ciberespacio. Con este fin se agrega a la normativa actual un nuevo anexo, titulado "Anexo n° 3. Gestión de la Ciberseguridad".

¿Qué contempla el anexo n° 3 sobre Gestión de la Ciberseguridad?

El anexo n°3 de la normativa establece aspectos mínimos a tener en cuenta en la definición y gestión de la infraestructura crítica y la generación y gestión de la base de incidentes de Ciberseguridad.



¿Qué contempla la infraestructura crítica de Ciberseguridad?

La infraestructura crítica contempla a aquellos activos de información lógicos que son considerados críticos para el funcionamiento del negocio. Asimismo, considera la infraestructura física, 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.

¿Cuál es el objetivo de la base de incidentes de Ciberseguridad?

El objetivo de que las entidades fiscalizadas por la SBIF generen una base de incidentes de Ciberseguridad es establecer un lenguaje y nivel de información mínimo y homogéneo en la industria, como también permitir la gestión integral de los incidentes generados al interior de las entidades fiscalizadas.

¿Por qué se requiere de estas infraestructuras?

Por una parte, la gestión de la infraestructura crítica de Ciberseguridad es fundamental para el adecuado funcionamiento del sistema financiero, en el caso de eventuales ataques. Por otra, 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.



4. Plazo y modo de la consulta pública

Cuestionario: Normas sobre
la Emisión y operación
de tarjetas de pago



¿Cuál es el plazo que estableció la SBIF para la recepción de comentarios a la normativa en consulta?

La normativa sobre gestión de Ciberseguridad estará en consulta desde hoy, 13 de diciembre de 2017, hasta el 08 del 01 de 2018, inclusive.

Cómo se podrán realizar comentarios a la normativa?

Los comentarios deben ser ingresados en la sección Normativa en Trámite del sitio web institucional www.sbif.cl.