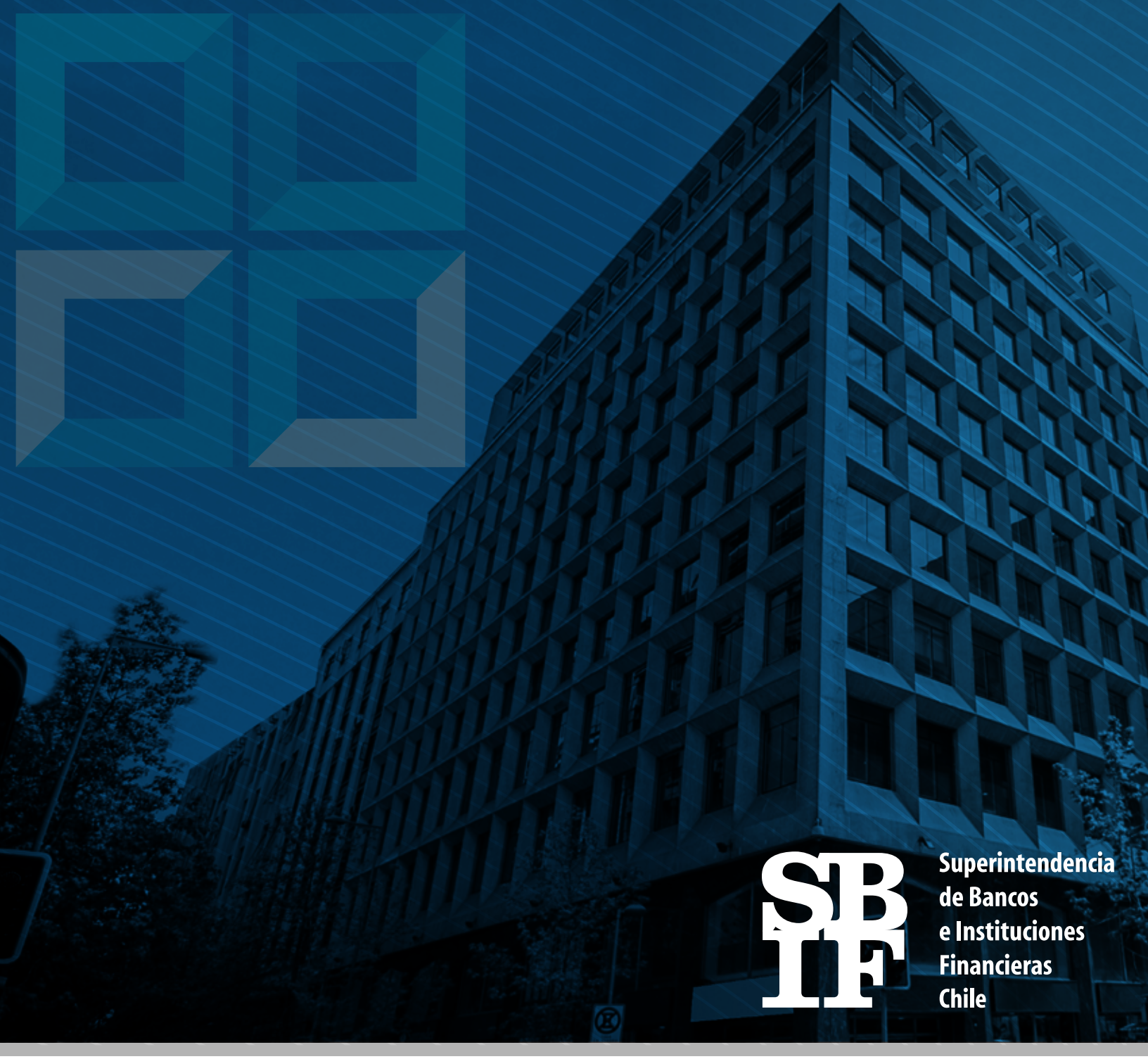

Cuestionario: Normativa para la gestión de Ciberseguridad

www.sbif.cl

1. Descripción general de las normas

¿Qué aborda esta publicación?

El presente cambio normativo 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 en los procesos de fiscalización que desarrolla la Superintendencia de Bancos e Instituciones Financieras (SBIF) a las entidades bancarias.

En particular, se establece la definición y gestión de una infraestructura crítica y la generación de 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 bancaria.

Además, se establece que el contenido de Ciberseguridad debe estar incluido en los programas e iniciativas de educación financiera de bancos, cooperativas de ahorro y crédito, sociedades de apoyo al giro y emisores de tarjetas de pago.

¿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 los capítulos 1-13 y 20-8 de la Recopilación Actualizada de Normas.

A su vez, se agrega el concepto de Ciberseguridad en la Carta Circular 2017 n°4 de Bancos, n°2 de Cooperativas, n° 2 de Sociedades de Apoyo al Giro y n°3 de Emisores de Tarjetas de Pago.

¿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.
En ese contexto, 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

¿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?

Para los bancos, la normativa establece 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, colocando especial atención en aquellos activos de información que componen la infraestructura crítica. Con este fin se agrega al Capítulo 1-13 de la RAN un nuevo anexo, titulado "Anexo n° 3. Gestión de la Ciberseguridad".

A su vez, incorpora un nuevo requerimiento de registro y gestión de una base de incidentes de ciberseguridad, el que se establece en el Capítulo 20-8 de la RAN.
En tanto, para otros fiscalizados, se incorpora la Ciberseguridad como contenido de educación financiera, en la Carta Circular 2017 n°4 de Bancos, n°2 de Cooperativas, n° 2 de Sociedades de Apoyo al Giro y n°3 de Emisores de Tarjetas de Pago que establece lineamientos de educación financiera.

¿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 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, 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.

¿Qué contempla el requerimiento de una 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.

¿Qué establece el contenido de ciberseguridad en la Circular sobre lineamientos de educación financiera?

Se establece que en los programas de educación financiera deben considerarse los riesgos y ventajas en el uso de tecnologías asociados a los productos y servicios financieros.

4. Inicio vigencia de la normativa

La normativa de Ciberseguridad entrará en vigencia el día **24 de enero de 2018.**