Normativa de Ciberseguridad

Superintendencia
de Bancos
e Instituciones
Financieras
Chile

Principales objetivos

- Especificar que la gestión del Riesgo Operacional de los bancos debe incorporar materias de Ciberseguridad.
- Establecer la generación y gestión de una base de incidentes sobre la materia.
- Incorporar el contenido de Ciberseguridad en los lineamientos de educación financiera requeridos para gran parte de las entidades fiscalizadas.

Contexto regulatorio

Abril de 2017

Se publica la Política Nacional de Ciberseguridad, que entrega un marco específico en materias de seguridad de la información en el ciberespacio.

SBIF considera que es el momento de establecer esta visión y este lenguaje de manera específica dentro su normativa.

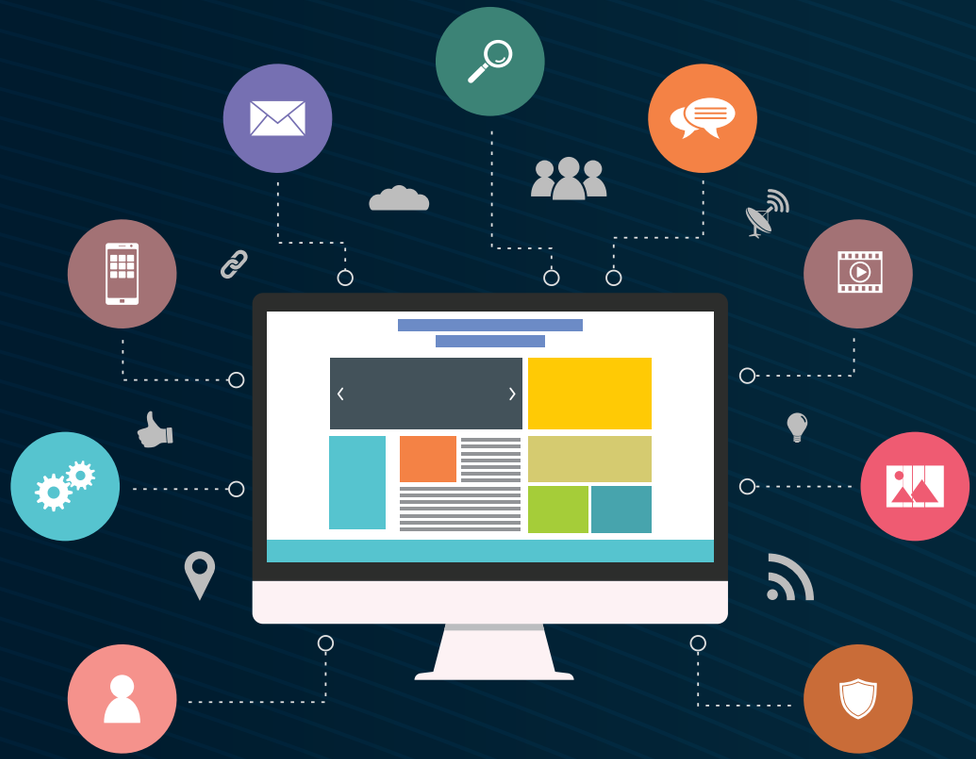
Normativa de Ciberseguridad | SBIF Superintendencia de Bancos e Instituciones Financieras Chile

La normativa incorpora la gestión de la Ciberseguridad como aspecto clave del Riesgo Operacional

La normativa incorpora la gestión de temas de Ciberseguridad en el capítulo 1-13 de la Recopilación Actualizada de Normas (RAN), colocando especial atención en la gestión de la Infraestructura Crítica, como parte de la Evaluación de Riesgo Operacional dirigida a bancos.

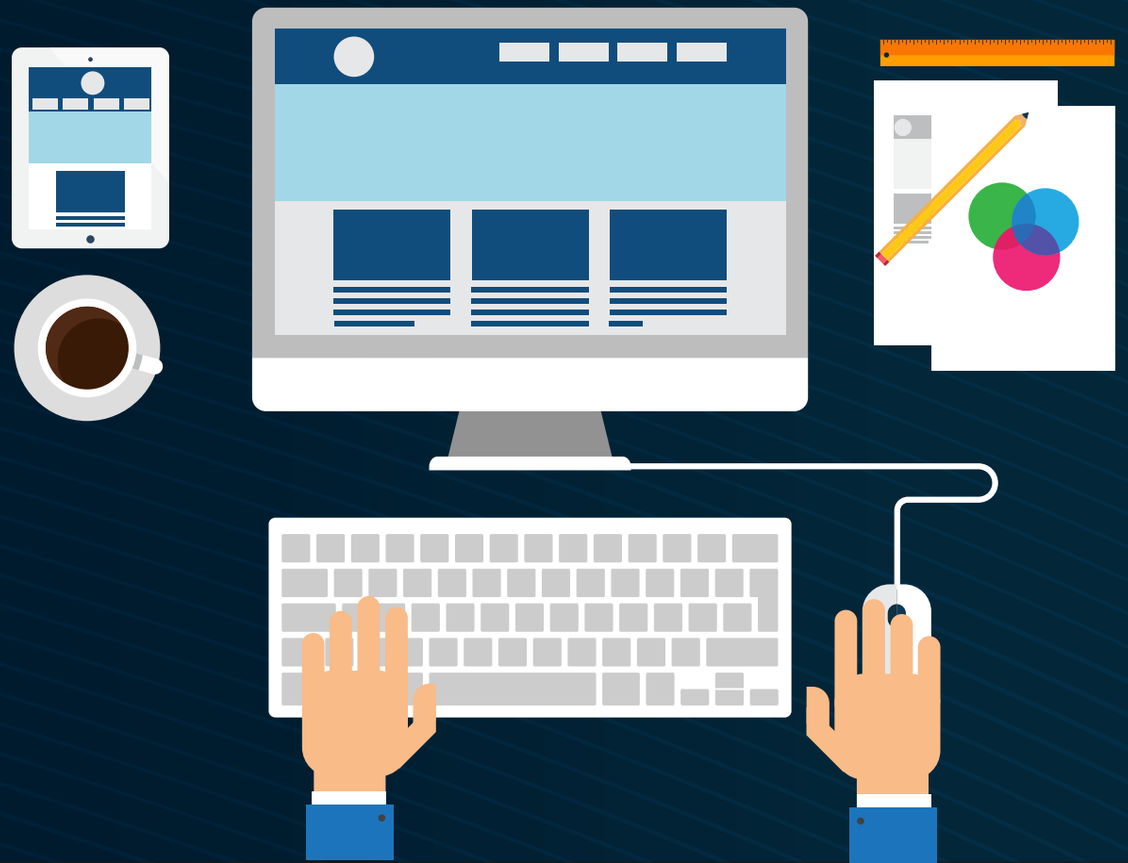
La normativa incorpora la gestión de una base de incidentes

Se incorpora un nuevo requerimiento a los bancos, de registro y gestión de una base de incidentes de Ciberseguridad, el que se incorpora en el Capítulo 20-8 de la RAN.



Se incorpora el contenido de Ciberseguridad en los lineamientos de educación financiera

Además, en el contexto del cambio normativo, se incorpora la ciberseguridad dentro de los lineamientos de educación financiera para bancos, cooperativas de ahorro y crédito, sociedades de apoyo al giro, y emisores de tarjetas de pago.



Novedades de la normativa

Administración de riesgo operacional

A este ítem de la normativa actual, se añaden:

- ✓ Consideraciones para una adecuada definición, caracterización e identificación de los principales activos de información y de la seguridad de los mismos. Gestión de la seguridad de sus activos de información expuestos a riesgos en el ciberespacio.

Novedades de la normativa

Nuevo anexo de Ciberseguridad (Anexo Nº3)

1. Incorpora aspectos de gestión de la infraestructura crítica de Ciberseguridad. Esto es:

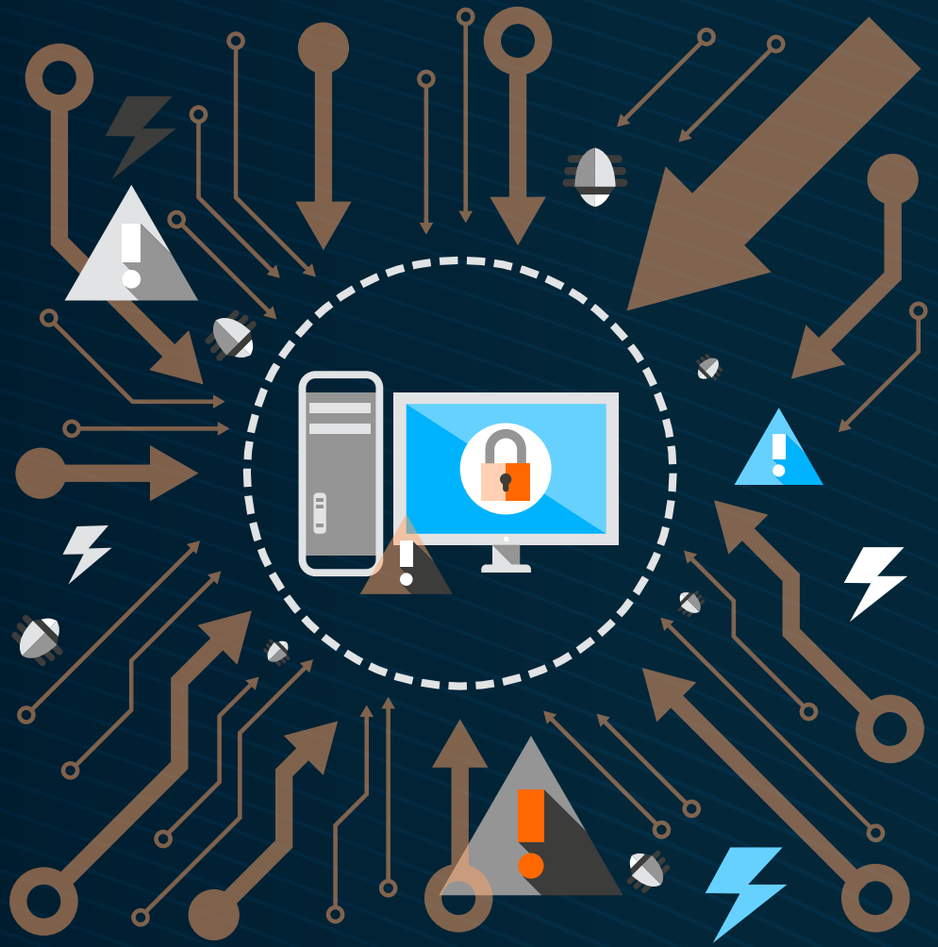
- ✓ Aquellos activos de información lógicos que son considerados críticos para el funcionamiento del negocio.
- ✓ La infraestructura física, hardware y sistemas tecnológicos que almacenan, administran y soportan estos activos y que de no operar adecuadamente, exponen a la entidad a riesgos de integridad, disponibilidad y confidencialidad de la información.

Novedades de la normativa

Nuevo requerimiento en Capítulo 20-8 de la RAN

2. Establece contenidos para la generación y gestión de una adecuada base de incidentes de Ciberseguridad:

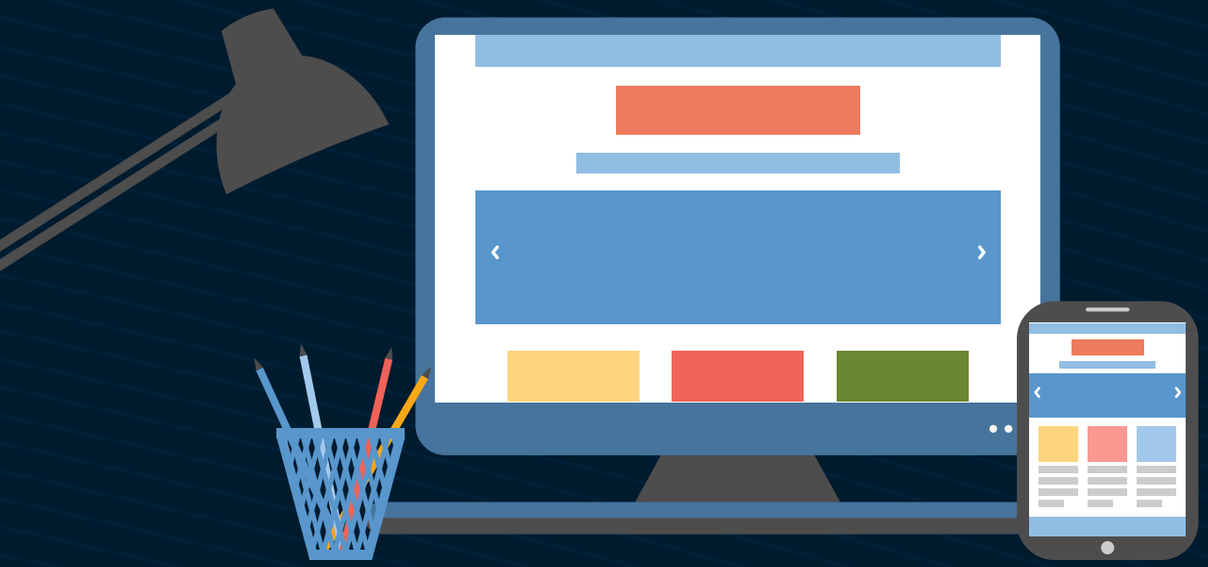
- ✓ Las entidades disponen de sistemas, procedimientos y mecanismos de gestión que permiten identificar, registrar, evaluar, controlar, mitigar, monitorear y reportar incidentes operacionales relacionados con la Ciberseguridad.



Novedades de la normativa

Carta Circular 2017 n°4 (Bancos), n°2 (Cooperativas), n° 2 (Sociedades de Apoyo al Giro) y n°3 (Emisores de Tarjetas de Pago)

3. Incorpora la Ciberseguridad como contenido de educación financiera:



- ✓ Riesgos y ventajas en el uso de tecnologías asociados a los productos y servicios financieros.

Entrada en vigencia de la norma

La nueva normativa entrará en vigencia desde el
miércoles 24 de enero de 2018

Superintendencia
de Bancos
e Instituciones
Financieras
Chile

Para mayores detalles visite www.sbif.cl