# Lineamientos y buenas prácticas para la gestión de la ciberseguridad

El pasado 31 de agosto la Superintendencia de Bancos e Instituciones Financieras de Chile publicó la circular Nº 3.640 que modifica el Capítulo 1-13 de la RAN relativo a la clasificación de gestión y solvencia con el fin de establecer los lineamientos y buenas prácticas para la gestión de la ciberseguridad, y el Capítulo 20-8 relativo a la Información de incidentes operacionales precisando aquéllos que deben ser comunicados al órgano regulador.

## Capítulo 1-13. Clasificación de gestión y solvencia.

Tal y como define el nuevo Anexo que se introduce con motivo de la modificación, la ciberseguridad ha de entenderse como el *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*.

Los aspectos más relevantes que incluye la Circular son los siguientes:

### Evaluación de la gestión de los Bancos: administración del riesgo operacional.

La norma señala la importancia de contar con una definición e identificación de los principales activos de información así como de la infraestructura física que soporta y resguarda la seguridad de los mismos. A estos efectos, se exige expresamente la gestión de la seguridad de los activos de información expuestos a riesgos en el ciberespacio.

### Buena gestión.

Es necesario la disposición de estructuras dedicadas a la gestión de la ciberseguridad que contemplen los aspectos descritos en el nuevo Anexo 3 de la Circular en el que se regula en primer lugar, la gestión de la infraestructura crítica de ciberseguridad, y en segundo, la base de los incidentes de la misma.

### Gestión de la infraestructura crítica de ciberseguridad.

El Directorio debe establecer un marco de gestión que contemple la estrategia de administración específica de este riesgo, el nivel de tolerancia, las responsabilidades de los participantes y las metodologías a utilizar para su gestión teniendo en cuenta las mejores prácticas y características de su actividad de negocio.

### Base de incidentes de ciberseguridad.

En este sentido, se incluyen unas condiciones mínimas para el desarrollo y mantenimiento de una Base de Incidentes entre las que destaca la periódica toma de conocimiento de este tipo de incidentes por parte del Directorio y el consiguiente pronunciamiento sobre los mismos. Asimismo contempla las variables mínimas a considerar para la elaboración de esta base.

## Capítulo 20-8. Información de incidentes operacionales

La norma también introduce modificaciones al Capítulo 20-8 motivadas por los nuevos riesgos operacionales que conlleva la evolución de la industria financiera, particularmente la incorporación de la tecnología en la forma de generar, procesar y administrar sus activos de información. Los aspectos más significativos que establece son:

Requisitos relativos a la información que se debe enviar a la SBIF cuando ocurran incidentes operacionales
Obligación de mantener adecuadamente informados a los clientes en determinados eventos
Deber de los bancos de compartir información de ataques relacionados a Ciberseguridad.

* Entorno que permite la interacción lógica, es decir no física, mediante la conexión de redes tecnológicas