COMUNICADO DE PRENSA

En Bancos e Instituciones Financieras:

CMF publica normativa para la Gestión de la Seguridad de la Información y Ciberseguridad

La normativa, que comenzará a regir el 1 de diciembre de este año, establece los lineamientos y mejores prácticas que deben cumplir las entidades en la gestión de la seguridad de la información y ciberseguridad.

Entre ellos, destaca la responsabilidad que tendrán los Directorios en la aprobación de las estrategias de ciberseguridad de sus instituciones.

7 de julio de 2020. La Comisión para el Mercado Financiero (CMF) informa que luego de concluido el proceso de consulta pública, emitió la normativa para la Gestión de la Seguridad de la Información y Ciberseguridad. Esta se aplicará a Bancos, Filiales Bancarias, Sociedades de Apoyo al Giro Bancario y Emisores y Operadores de Tarjetas de Pago.

De manera creciente las instituciones financieras han migrado al mundo de las operaciones digitales, situación que si bien ofrece una serie de oportunidades a las instituciones fiscalizadas y a sus clientes, también implica mayores riesgos operacionales que deben ser adecuadamente administrados, a fin de lograr un equilibrio entre el uso de las tecnologías de la información y el control de los riesgos subyacentes.

Esta normativa, en busca de contribuir a ese objetivo, establece una serie de lineamientos y mejores prácticas que deben ser consideradas por las entidades en su proceso de gestión de la seguridad de la información y ciberseguridad.

La Comisión espera que esta normativa sea un marco de referencia para futuros cambios en esta materia para otras instituciones, como las cooperativas de ahorro y crédito y entidades de la industria de valores y seguros.

El nuevo Capítulo 20-10 de la Recopilación Actualizada de Normas (RAN), contiene una serie de disposiciones, basadas en las mejores prácticas internacionales, que deben ser consideradas para la gestión de la seguridad de la información y ciberseguridad.

La adopción de esta nueva normativa permitirá que las entidades se encuentren mejor preparadas para prevenir y actuar frente a eventos operacionales relacionados a la seguridad de la información y ciberseguridad.

Los principales elementos que abordan las nuevas directrices se resumen a continuación:

• Se otorgan lineamientos específicos respecto del rol que debe tener el Directorio para la adecuada gestión, tanto de seguridad de la información como de ciberseguridad, otorgándole como responsabilidad la aprobación de la estrategia institucional en esta materia.

Además, los Directorios deberán asegurar que la entidad mantenga un sistema de gestión de la seguridad de la información y ciberseguridad, que contemple la administración específica de estos riesgos en consideración a las mejores prácticas internacionales existentes, entre otros aspectos.

• Los bancos e instituciones financieras a quienes les aplican las presentes disposiciones deberán definir las etapas mínimas de un proceso de gestión de riesgos de seguridad de la información y ciberseguridad, considerando al menos: la identificación, análisis, valoración, tratamiento y la aceptación de los riesgos a que están expuestos los activos de información, así como su monitoreo y revisión permanente.

• Se establece la necesidad de que las entidades definan sus activos críticos, así como las funciones de protección de éstos, la detección de las amenazas y vulnerabilidades, la respuesta ante incidentes y la recuperación de la operación normal de la entidad.

• Las entidades deberán contar además, con políticas y procedimientos para la identificación de aquellos activos que componen la infraestructura critica de la industria financiera y del sistema de pagos, y para el adecuado intercambio de información técnica de incidentes que afecten o pudieran afectar la ciberseguridad de la entidad.

Este nuevo Capítulo de la RAN complementa lo señalado en distintas normativas de la CMF, como aquellas establecidas en el Capítulo 1-13 sobre la evaluación de gestión del riesgo operacional; el Capítulo 20-7 en lo que se refiere a los riesgos que las entidades asumen en la externalización de servicios; el Capítulo 20-8 sobre información de incidentes operacionales; y el Capítulo 20-9 sobre gestión de la continuidad del negocio.

La norma entrará en vigencia el 1 de diciembre de 2020. Mientras esto no ocurra, los bancos deberán seguir cumpliendo las disposiciones del actual Capítulo 1-13 en el ámbito del riesgo operacional y, particularmente, en lo relacionado con seguridad de la información y ciberseguridad, incluido lo dispuesto en el Anexo N°3.

Junto con el detalle de la Normativa, se pone a disposición de los interesados una Presentación y un documento de Preguntas Frecuentes que resumen los alcances de la modificación.

Área de Comunicación, Educación e Imagen - Comisión para el Mercado Financiero (CMF)
Contacto: prensa@cmfchile.cl | sala de prensa
@cmfchile_