COMISIÓN
PARA EL MERCADO
FINANCIERO

Preguntas Frecuentes:
Norma para la Gestión de la Seguridad de la Información y Ciberseguridad

Julio 2020

Comisión para el Mercado Financiero – Chile

¿Qué aborda esta publicación?

La norma establece nuevos lineamientos de sanas prácticas para una adecuada gestión de la seguridad de información y ciberseguridad. Este nuevo Capítulo refunde además las disposiciones actualmente vigentes en ciberseguridad del Capítulo 1-13 de la Recopilación Actualizada de Normas.

¿Por qué se introducen estos nuevos lineamientos normativos?

En los últimos años las instituciones financieras han migrado de manera creciente al mundo de las operaciones digitales, situación que si bien ofrece una serie de oportunidades 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.

¿A quiénes están dirigidas las normas?

La norma que se presenta está dirigida a los Bancos, sus filiales, Sociedades de Apoyo al Giro Bancario y Emisores y Operadores de Tarjetas de Pago, quienes deberán dar cumplimiento a ésta atendiendo al volumen y complejidad de sus operaciones.

¿Cuando entra en vigencia la norma?

Las instrucciones establecidas en la presente Norma de Carácter General regirán a contar del 1 de diciembre de 2020.

¿Cuál es la estructura de la norma?

La norma se divide en 4 secciones. La primera trata de aspectos generales de gestión para las materias de seguridad de la información y ciberseguridad. La segunda señala lineamientos que deben considerar las instituciones en la implementación de un proceso de gestión de los riesgos para apoyar el sistema de seguridad de la información y ciberseguridad. La tercera, atendiendo la relevancia de los riesgos cibernéticos, define una especial diligencia para gestionarlos. La última sección, indica consideraciones que deben tener las instituciones al formar parte relevante de la infraestructura crítica del país.

¿Cuáles son los principales lineamientos que establece esta nueva normativa?

Los principales elementos que se abordan con las nuevas directrices en consulta 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, así como 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.

- Definición de las etapas mínimas de un proceso de gestión de riesgos de seguridad de la información y ciberseguridad, considerando al menos, la identificación, el análisis, la valoración, el tratamiento y la aceptación de los riesgos a que están expuestos los activos de información de la entidad, así como su monitoreo y revisión permanente.
- Considerando la relevancia de los riesgos cibernéticos, se establece que las entidades deben realizar una especial diligencia para gestionarlos. Para esto se indica la necesidad de definir los 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.
- Se establece que las entidades como parte de la industria financiera deben contar con políticas y procedimientos para el intercambio de información en esta materia de alertas e incidentes de ciberseguridad, identifiquen los activos que componen la infraestructura critica de la industria financiera y del sistema de pago y procuren la realización de pruebas conjuntas de determinados escenarios de riesgo.

  En este sentido resulta importante que las entidades cuenten con políticas y procedimientos para la identificación de aquellos activos que componen la infraestructura critica de la industria financiera y del sistema de pago, así como para el adecuado intercambio de información de incidentes, con otros integrantes que son parte de esta infraestructura crítica. Considerando lo anterior, a fin de detectar y gestionar las amenazas y vulnerabilidades que pudieran afectar el funcionamiento del sistema financiero, las distintas entidades deben procurar la realización de pruebas conjuntas de determinados escenarios de riesgo