/Carey

5 de diciembre de 2019

ALERTA LEGAL

CMF publica en consulta nueva normativa sobre seguridad de la información y ciberseguridad para entidades financieras

El día 25 de noviembre de 2019, la Comisión para el Mercado Financiero publicó en consulta, una propuesta de modificación a su Recopilación Actualizada de Normas ("RAN"), mediante la dictación de un nuevo Capítulo 20-10, sobre "Gestión de Seguridad de la Información y Ciberseguridad" (la "Nueva Regulación")

Las principales características de esta Nueva Regulación pueden sintetizarse como sigue:

- **Perímetro Regulatorio:** La Nueva Regulación será aplicable a bancos, filiales de bancos, sociedades de apoyo al giro bancario y a emisores y operadores de tarjetas de pago.
- **Estructura de la Nueva Regulación:** La Nueva Regulación está dividida en cuatro secciones. La primera de ellas establece reglas generales sobre gestión de seguridad de la información y ciberseguridad. La segunda fija lineamientos obligatorios que deben considerarse al tiempo de implementar un proceso de gestión de riesgos, para apoyar el sistema de seguridad de la información y ciberseguridad. La tercera parte establece requisitos de due diligence específicos para el manejo de riesgos cibernéticos, y la última sección establece ciertas consideraciones que deben ser observadas por la entidad respectiva, como parte la infraestructura local crítica, en conformidad con la Política Nacional de Ciberseguridad.
- **Principales disposiciones:** La Nueva Regulación introduce las siguientes innovaciones regulatorias principales:

  - Establece directrices específicas en gestión de seguridad de la información y ciberseguridad, haciendo al Directorio responsable de aprobar y supervisar la estrategia de la correspondiente entidad a este respecto. Estas directrices establecen que el proceso de gestión de seguridad de la información debe garantizar el cumplimiento con la ley, incluyendo aquellas normas relativas a la protección de datos personales y derechos de propiedad intelectual.

- Define las etapas mínimas que deben comprender los procesos de gestión de seguridad de la información y riesgos de ciberseguridad.
- Establece requisitos de due diligence específicos para la gestión de riesgos cibernéticos, tales como la determinación de activos críticos de ciberseguridad y sus mecanismos de protección, y
- Establece que las entidades deberán contar con políticas y procedimientos para la identificación de activos que comprenden la infraestructura crítica de la industria, y para el intercambio de información sobre incidentes con entidades que son parte de dicha infraestructura.

- **Vinculación con otras normas de la RAN:** La Nueva Regulación complementará las actuales regulaciones sobre seguridad de la información, tales como aquellas referidas en el Capítulo 1-13, sobre evaluación de la gestión de riesgos operaciones; el Capítulo 20-7, sobre riesgos asumidos por las entidades que externalizan servicios; Capítulo 20-8, sobre información de incidentes operacionales, y el Capítulo 20-9, sobre gestión de continuidad del negocio.
- **Vigencia:** La Nueva Regulación entrará en vigor el día 1 de marzo de 2020.

El período de consulta se mantendrá abierto hasta el día 27 de diciembre de 2019.

Autores: Diego Peralta