

Diciembre, 2019

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:

- 1. 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.
- 2. 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.
- 3. Principales disposiciones:** La Nueva Regulación introduce las siguientes innovaciones regulatorias principales:
 - a.** 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.
 - b.** Define las etapas mínimas que deben comprender los procesos de gestión de seguridad de la información y riesgos de ciberseguridad.
 - c.** 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
 - d.** 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.



Si tiene consultas respecto de los temas comentados en esta alerta, puede contactar a los siguientes abogados o a su contacto regular en Carey.

Diego Peralta

Socio

+56 2 2928 2216
dperalta@carey.cl

Paulina Silva

Directora

+56 2 2928 2665
psilva@carey.cl

Carlo Benussi

Asociado

+56 2 2928 2665
cbenussi@carey.cl

Diego Lasagna

Asociado

+56 2 2928 2216
dlasagna@carey.cl

La información contenida en esta alerta fue preparada por Carey y Cía. Ltda. sólo para fines educativos e informativos y no constituye asesoría legal.

Carey y Cía. Ltda.
Isidora Goyenechea 2800, Piso 43.
Las Condes, Santiago, Chile.
www.carey.cl

- 4. 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 operacionales; 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.
- 5. 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.