ECIJA OTERO
Av. Apoquindo 3669, Piso 13,
Las Condes, Santiago - Chile
Tel: +562 2361 8900
www.ecija.com

# Normativa CMF para la Gestión de la Seguridad de la Información y Ciberseguridad

**El 1 de diciembre de 2020 comenzó a regir el Capítulo 20-10 de la Recopilación Actualizada de Normas (RAN) emitida por la Comisión para el Mercado Financiero (CMF), norma que toma como base las mejores prácticas internacionales en la materia y que está destinada a los bancos y se hace extensiva a filiales y sociedades de apoyo al giro bancario.**

Su finalidad es establecer buenas prácticas y entregar lineamientos que faciliten una adecuada gestión de los riesgos en seguridad de la información y ciberseguridad, siendo la misma parte integrante de la evaluación en la gestión que la propia CMF hace a los bancos en el ámbito de los riesgos que enfrentan en sus operaciones.

La norma considera a este tipo de entidades como actor relevante de la infraestructura crítica del país al ser parte de la industria financiera y del sistema de pagos, infraestructura que, según la definición establecida en 2015 por las Bases para una Política Nacional de Ciberseguridad elaborada por la Subsecretaría del Interior y la Subsecretaría de Defensa Nacional, comprende *"las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, interrupción o destrucción pueden tener una repercusión importante en la seguridad, la salud, el bienestar de los ciudadanos y el efectivo funcionamiento del Estado y del sector privado"*.

### Evaluación de la CMF a los bancos

El rol que cumple el Directorio de este tipo de entidades es esencial respecto al análisis al que le somete la CMF para evaluar los riesgos que enfrentan en sus operaciones, ya que será su responsabilidad para mitigarlos la aprobación de una estrategia institucional y la autorización de los recursos presupuestarios suficientes para mantener un sistema de gestión de la seguridad de la información y ciberseguridad.

Por seguridad de la información se entiende el ámbito de medidas implementadas por una entidad para proteger la confidencialidad, integridad y disponibilidad de la información que trata, mientas que la ciberseguridad se ocupa de prever, evitar o mitigar los riesgos que la información enfrenta en el ciberespacio.

Entre las medidas que la norma de la CMF considera como necesarias para establecer un adecuado sistema de gestión se encuentran las siguientes:

- El Directorio debe definir una estructura organizacional con personal especializado y con atribuciones y competencias que permitan gestionar la seguridad de la información y ciberseguridad.

- La estructura organizacional definida debe encargarse del diseño y mantención de un adecuado sistema de identificación, seguimiento, control y mitigación de los riesgos de seguridad de la información y ciberseguridad.

- El Directorio debe disponer de una estructura de alto nivel, con atribuciones administrativas reales, para la administración de las crisis que pudieran afectar los activos de información, propios o de sus clientes, estructura que se encargará de establecer un plan de actuación e informar oportunamente a las autoridades y a las partes interesadas.

- El Directorio debe aprobar políticas para la gestión de los riesgos de seguridad de la información y ciberseguridad, las cuales deben ser ampliamente difundidas al interior de la organización, y revisadas y aprobadas al menos anualmente.

- El Directorio debe informarse periódica y adecuadamente respecto de los riesgos a que está expuesta la entidad en términos de seguridad de la información y ciberseguridad, así como del cumplimiento de sus políticas internas, con el fin de mejorar su gestión y prevención.

- El Directorio debe aprobar políticas de conducta interna dirigidas a todos sus empleados, así como planes formales de difusión, capacitación y concientización.

- La entidad debe revisar los riesgos asociados que pueda implicar la introducción de nuevos productas o actividades en la compañía.

- Asimismo, debe asegurarse que cumple con las leyes y normativas vigentes en materias como la protección de los datos de carácter personal y los derechos de propiedad intelectual, así como deberá exigirlo a los proveedores que utilicen sus plataformas.

**Implementación del proceso de gestión de los riesgos**

Construir un sistema de seguridad interno como base para proteger la información de la entidad implica que se considere la identificación, el análisis, la valoración o el tratamiento de los riesgos a que están expuestos los activos de la entidad, así como su monitoreo y revisión permanente.

Para ello, la norma aprobada por la CMF establece una serie de aspectos que ayudan a la consecución de estos fines, entre los que destacan los siguientes:

- Identificarlos activos de información de la entidad que pueden enfrentar riesgos.

- Identificar las amenazas que puedan dañar los activos, así como de sus vulnerabilidades.

- Identificar las consecuencias que puedan tener en los activos de información las pérdidas de confidencialidad, integridad y disponibilidad.

- Realizar análisis de riesgos, una valoración y un plan de tratamiento de los mismos.

- Revisar, al menos anualmente, el proceso de gestión de riesgos de seguridad de la información y ciberseguridad, para así identificar la necesidad de efectuar ajustes en las metodologías y/o herramientas utilizadas.

**Gestión de la ciberseguridad de la entidad**

Además de las medidas que permiten el diseño y la implementación de un sistema que resguarde la información de la compañía, la norma aprobada por la CMF considera los riesgos cibernéticos como fundamentales, estableciendo una serie de aspectos que es importante considerar para determinar, por un lado, cuales son los activos críticos para el funcionamiento del negocio de una entidad financiera, y por otro, cuales son las medidas que permiten proteger esos activos.

Entre estos aspectos a tener en cuenta por una organización la CMF establece:

- Contar con un inventario de activos de ciberseguridad críticos clasificados desde una perspectiva de confidencialidad, integridad y disponibilidad.

- Disponer de un proceso de gestión del cambio que permite que las modificaciones realizadas a la infraestructura de Tecnologías de la Información (TI) sean efectuadas de manera segura y controlada.

- Contar con un apropiado proceso de gestión de capacidades, que le permite asegurar que la infraestructura TI cubre las necesidades presentes y futuras, de acuerdo al volumen y complejidad de las operaciones de la entidad.

- Disponer de un proceso de gestión de la obsolescencia tecnológica que le permita mantener una infraestructura TI con estándares de desempeño de seguridad apropiados a los objetivos y necesidades de la entidad.

- Proteger adecuadamente las redes informáticas de ataques provenientes de Internet o de otras redes externas, a través de la implementación de herramientas.

- Contar con adecuadas herramientas para controlar, registrar y monitorear las actividades realizadas por los usuarios en general sobre los activos críticos, así como de aquellos con privilegios especiales.

- Disponer de apropiados mecanismos de control de accesosa los canales electrónicos dispuestos por la entidad, con los que interactúan los clientes y usuarios.

- Contar con herramientas de monitoreo continuo que permitan en forma proactiva identificar, recolectar y analizar información interna y externa respecto de nuevas amenazas y vulnerabilidades que puedan afectar los activos de ciberseguridad.

- Realizarde forma regular, con el suficiente alcance y profundidad, pruebas de seguridad a su infraestructura tecnológica para detectar las amenazas y vulnerabilidades que pudieran existir, tales como pentesting y/o ethical hacking.

Por último, se establecen de igual forma una serie de medidas para valorar el nivel de respuesta ante incidentes de ciberseguridad, así como de recuperación de las actividades afectadas. Para ello, los bancos o las entidades que son destinatarios de la normativa de la CMF deben:

- Probar, al menos anualmente, los planes necesarios para enfrentar adecuadamente los escenarios que puedan afectar la ciberseguridad, así como los equipos para dar respuesta a los ciberincidentes que se pudieran materializar.

- Contar con un plan definido de actuación para, dependiendo de la gravedad del incidente de ciberseguridad, escalar la situación a la alta administración para la toma de decisiones.

- Contar con un plan de comunicaciones para casos de incidentes de ciberseguridad de alto impacto, que alcance a todas las partes interesadas, ya sea internas o externas, a fin de mantenerlas adecuadamente informadas.

- Llevar a cabo un proceso independiente de análisis forense para los ciberincidentes relevantes que se ocupe de analizar todos los aspectos relevantes del mismo.

- Contar con una base de incidentes de ciberseguridad de los activos de información presentes en el ciberespacio suficientemente detallada para perfeccionar su capacidad de respuesta, así como para realizar pruebas que permitan detectar las amenazas y vulnerabilidades propias.

- Realizar autoevaluaciones en esta materia, al menos anualmente, para determinar el grado de cumplimiento de las políticas internas, normativa regulatoria y la adherencia a las mejores prácticas en ciberseguridad.

La aplicación de la nueva norma de la CMF pone de manifiesto que, en la actualidad, las instituciones del sector financiero están migrando sus operaciones y actividades al entorno digital, lo que aumenta las oportunidades, pero también los riesgos de ciberataques, fraudes o robos masivos de datos. Con esta norma lo que se pretende es paliar los efectos

negativos a los que están expuestos las entidades que operan en este sector en materia de seguridad de la información y ciberseguridad, pero que en general afectan también a cualquier persona jurídica que opera en el entorno digital. Por ello, se encuentran actualmente en trámite dos proyectos de ley del Gobierno, uno de ley marco en materia de ciberseguridad e infraestructura crítica, y otro proyecto que adecua los delitos informáticos al Convenio de Budapest suscrito por Chile.

Javier Sabido.: jsabido@ecija.com