Gestión de la seguridad de la información y la ciberseguridad

A fin de que las empresas fortalezcan sus capacidades de ciberseguridad y sus procesos de autenticación, la Superintendencia de Banca, Seguros y AFP ha publicado el presente Reglamento para actualizar la normativa sobre gestión de seguridad de la información, una normativa bastante esperada y necesaria en la actualidad, aún más considerando que el único dispositivo legal sobre la materia era la Circular G-140, del año 2009.

Es complementario al Reglamento para la Gestión del Riesgo Operacional y está en línea con los estándares y buenas prácticas internacionales en esta materia. A continuación, las cuestiones más relevantes:

Sistema de gestión de seguridad de la información y ciberseguridad

El Reglamento define el sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C) como el conjunto de políticas, procesos, procedimientos, roles y responsabilidades diseñados para identificar y proteger los activos de información, detectar eventos de seguridad, así como prever la respuesta y recuperación ante incidentes de ciberseguridad.

Establece que todas las compañías deberán contar con este sistema, que será proporcional al tamaño, la naturaleza y la complejidad de sus operaciones y se basará en los siguientes principios:

Confidencialidad: la información sólo estará disponible para entidades o procesos autorizados, incluyendo las medidas para proteger la misma
Disponibilidad: el acceso y el uso a la información deberán ser oportunos
Integridad: se deberá asegurar la irrenunciabilidad de la información y su autenticidad, y evitar su modificación o destrucción indebida

Medidas mínimas de seguridad

El capítulo II regula el régimen general del SGSI-C: objetivos y requerimientos, alcance, actividades planificadas e intercambio de información de ciberseguridad, así como las medidas mínimas de seguridad de la información a adoptar por las empresas, entre las que se encuentran: seguridad en los recursos humanos, en las operaciones, en las comunicaciones, física y ambiental; controles de acceso físico y lógico; adquisición, desarrollo y mantenimiento de sistemas; gestión de incidentes de ciberseguridad y de activos de información; y criptografía.

Programa de ciberseguridad

El Reglamento contempla que todas las entidades con presencia en el ciberespacio deberán contar, de manera permanente, con un programa de ciberseguridad aplicable a las operaciones, procesos y demás activos de información.

Este programa deberá prever un diagnóstico y un plan de mejora sobre sus capacidades de ciberseguridad, para lo cual tendrá que seleccionar un marco de referencia internacional sobre la materia, que le permita, como mínimo:

Identificar los activos de información

Proteger de las amenazas a los activos de información
Detectar incidentes de ciberseguridad
Responder con medidas que reduzcan el impacto de los incidentes
Recuperar las capacidades o servicios tecnológicos que pudieran ser afectados

Responsabilidades del directorio y de la gerencia

En su artículo 5 recoge que el directorio será responsable de aprobar y facilitar las acciones requeridas para contar con un SGSI-C apropiado a las necesidades de la empresa y su perfil de riesgo, y destaca entre sus funciones:

Aprobar políticas y lineamientos para la implementación del SGSI-C y su mejora continua
Asignar los recursos técnicos, de personal y financieros requeridos para su implementación y adecuado funcionamiento
Aprobar la organización, roles y responsabilidades para el SGSI-C, incluyendo los lineamientos de difusión y capacitación que contribuyan a un mejor conocimiento de los riesgos involucrados

Por otra parte, en el artículo 6 establece que la gerencia general será responsable de tomar las medidas necesarias para implementar el SGSI-C de acuerdo a las disposiciones del directorio y lo dispuesto en el Reglamento.

Además, que los gerentes de las unidades de negocios y de apoyo deberán favorecer el buen funcionamiento del SGSI-C y gestionar los riesgos asociados a la seguridad de la información y Ciberseguridad en el marco de sus funciones.

Responsabilidades del comité de riesgos

Además de las funciones propias del comité de riesgos, el Reglamento le confiere las siguientes responsabilidades relativas a la seguridad de la información y a la ciberseguridad:

Aprobar el plan estratégico del SGSI-C y recomendar las acciones a seguir
Aprobar el plan de capacitación a fin de garantizar que el personal, la plana gerencial y el directorio cuenten con competencias necesarias en seguridad de la información y en ciberseguridad.
Fomentar la cultura de riesgo y conciencia de la necesidad de medidas apropiadas para su prevención

Para su cumplimiento, las empresas podrán constituir un comité especializado en seguridad de la información y ciberseguridad (CSIC). Para aquellas empresas comprendidas en el régimen simplificado que no cuenten con un comité de riesgos o un CSIC, las funciones antes indicadas serán asignadas a la gerencia general.

La función de seguridad de la información y ciberseguridad

El Reglamento exige a las empresas implementar la función de seguridad de la información y ciberseguridad, y contar con un equipo de trabajo multidisciplinario de manejo de incidentes de ciberseguridad que esté capacitado para implementar el plan y los procedimientos para gestionarlos.

Estará conformado por representantes de las áreas que permitan prever los aspectos legales, técnicos y organizacionales, de forma consistente con los requerimientos del programa de ciberseguridad.

Autenticación y régimen simplificado y reforzado

En la regulación también se contemplan otras cuestiones, como la implantación de procesos de autenticación, el enrolamiento del usuario en servicios provistos por canal digital, la autenticación

reforzada para operaciones por canal digital, las exenciones de autenticación reforzada para operaciones por canal digital o el uso de interfaces de programación de aplicaciones para la provisión de servicios en línea.

Asimismo regula la provisión de servicios por terceros y el régimen simplificado y reforzado del SGSI-C.

Otras modificaciones

El Reglamento modifica diversa normativa regulatoria a fin de adecuarla a las disposiciones del presente Reglamento, entre ellos: (i) Reglamentos de Auditoría Interna y Externa a fin de incluir la evaluación al cumplimiento de este sistema; (ii) Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos y Reglamento de Riesgo Operacional, para incluir definiciones y sustituir las disposiciones sobre “Bienes y/o Servicios Provistos por Terceros”; (iii) Reglamento de Tarjetas de Crédito y Débito para modificar la Información mínima, condiciones y vigencia aplicable a las tarjetas de débito; (iv) Reglamento de Operaciones con Dinero Electrónico para sustituir las disposiciones de los Soportes para uso de dinero electrónico.

Aplicación y entrada en vigor

La normativa será de aplicación obligatoria a las empresas de operaciones múltiples, Administradoras de Fondos de Pensiones (AFP), corredoras de seguros, empresas de Seguros y/o Reaseguros (según su promedio de activos), Empresa Emisora de Dinero Electrónico, Banco de la Nación, Banco Agropecuario, COFIDE, Fondo MIVIVIENDA S.A., entre otros.

Entrará en vigor el 1 de junio de 2021, fecha en la que quedará derogada la Circular G 140- 2009, con excepción de las disposiciones listadas en los literales del artículo décimo del Reglamento, sujetos a un plazo de adecuación.