Libro V, Título XVIII Sistema de Gestión de Seguridad y Ciberseguridad de las Administradoras de Fondos de Pensiones

Capítulo I. Aspectos Generales

En el presente Título, se establecen disposiciones basadas en marcos de buenas prácticas, que las Administradoras de Fondos de Pensiones, en adelante "las Administradoras", deben considerar para contar con un Sistema de Gestión de Seguridad y Ciberseguridad, gestionado y resiliente que permita optimizar los procesos y asegurar la confidencialidad, integridad y disponibilidad de la información, protegiendo los datos de carácter personal y sensibles de los afiliados y usuarios del Sistema de Pensiones, con el objeto de lograr un control preventivo de los riesgos en estas materias.

Esta norma considera buenas prácticas sobre la seguridad y ciberseguridad de la información, asimismo establece controles específicos que las Administradoras deberán implementar para reforzar las estructuras de control de seguridad y ciberseguridad.

Lo anterior, complementa el alcance de la evaluación del mitigador transversal referido a la seguridad de la información, de la Resolución N° 153, que contiene el Modelo de Supervisión Basada en Riesgo de la Superintendencia de Pensiones, de fecha 23 de octubre de 2019, o la que la reemplace. Asimismo, los estándares de buenas prácticas y los controles incluidos en el Sistema de Gestión de Seguridad y Ciberseguridad definidos en esta norma complementan las normas de Gestión de Riesgo vigentes y serán considerados como estándares de evaluación de las Administradoras.

La gestión de la seguridad y ciberseguridad es una tarea que comprende a toda la organización y, por lo tanto, para establecer un Sistema de Gestión de la Seguridad y Ciberseguridad, que mitigue los riesgos de disponibilidad, confidencialidad e integridad se debe establecer una estructura de procesos, considerando los objetivos, roles, infraestructura y tecnología de los niveles estratégico, táctico y operacional, de la Administradora.

En tal sentido, será considerado como elemento necesario para un adecuado sistema de gestión, que la alta dirección de la Administradora cumpla un rol esencial dentro del gobierno de la seguridad de la información y ciberseguridad, promoviendo la mejora continua y el liderazgo requerido para que los controles de seguridad y ciberseguridad se establezcan en la organización.

El Sistema de Gestión de Seguridad y Ciberseguridad considera la seguridad de la información como un proceso transversal cuyas actividades deben ser gestionadas, controladas y optimizadas, de forma continua en todos los niveles de la entidad. Asimismo, el sistema de gestión, se perfecciona con la incorporación de controles específicos tendientes a mitigar los riesgos de ciberseguridad.

En Anexo de este Título se incluyen definiciones de los conceptos utilizados en la presente normativa.

ELEMENTOS GENERALES DE GESTIÓN

1. El alcance de la gestión de riesgo de seguridad de la información para las Administradoras se define en la Resolución N° 153, del 23 de octubre de 2019, o la que la modifique o reemplace, en donde se considera el riesgo Inherente Operacional y Tecnológico como: la contingencia de que los afiliados, beneficiarios o usuarios no puedan acceder en tiempo y forma a los servicios, beneficios o a una adecuada rentabilidad y seguridad de los fondos, o que enfrenten problemas derivados de la pérdida de información personal, debido a fallas o insuficiencias de procesos, personas, sistemas o por eventos externos. Se refiere tanto a las operaciones realizadas con medios de la entidad fiscalizada como a las contratadas con proveedores externos a ella. Incluye la pérdida de información sensible y otras contingencias generadas por fallas en las tecnologías de información y comunicaciones.

2. La gobernanza de la seguridad de la información y ciberseguridad es responsabilidad del Directorio. La Administración de la entidad, es responsable de alinear las operaciones diarias con los mandatos estratégicos, aprobados por el Directorio, siendo aplicable a todas las áreas de la entida

3. La Administración debe establecer una estructura organizacional adecuada para mitigar el riesgo de seguridad de la información y ciberseguridad. Para ello, deberá establecer formalmente

actividades de control, líneas de reporte adecuadas y la participación de las áreas de Gestión de Riesgo y Auditoría como mitigadores transversales de este riesgo.

4. Los lineamientos, alcance y límites de la gestión de riesgos de seguridad de la información y ciberseguridad, deben estar contenidos en una política de la Administradora aprobada por el Directorio. Al respecto, el alcance del proceso de la administración de riesgo de seguridad de la información y ciberseguridad debe ser definido considerando todos los activos de información.

5. La política de seguridad de la información y ciberseguridad debe ser revisada anualmente y actualizada siempre que ocurran cambios en los procesos de la Administradora que afecten la seguridad. Debe ser aprobada por el Directorio y en la Administradora de tal forma de garantizar su idoneidad, adecuación y efectividad continua.

6. Respecto de los riesgos de seguridad de la información y ciberseguridad, la Administradora debe mantener un ambiente de control y una estructura organizacional que, cumpliendo con las definiciones estratégicas relacionadas con la seguridad, sean apropiados a sus operaciones y sus riesgos.

7. Este enfoque de gestión de la seguridad de la información y ciberseguridad además de ser adecuado al ambiente de la organización debe estar alineado con la administración de riesgos. De esta forma, los esfuerzos de seguridad deben estar direccionados a los riesgos, de una manera efectiva y oportuna, donde y cuando se necesiten.

8. La administración del riesgo de seguridad de la información y ciberseguridad debe ser una parte integral de las actividades de administración de seguridad y debería ser aplicada tanto en la implementación como en la operación del Sistema de Gestión de Seguridad y Ciberseguridad.

9. La administración de riesgo de seguridad de la información y ciberseguridad debe ser un proceso continuo. El proceso debe evaluar en forma permanente el contexto externo e interno de la Administradora de tal forma de poder prospectar los riesgos y abordarlos con un enfoque preventivo. Asimismo, la Administradora deberá contar con instancias para evaluar y tratar los riesgos en forma oportuna, usando un plan de tratamiento de riesgos para implementar recomendaciones y decisiones que se adopten.

10. El análisis del contexto externo e interno de la administración de riesgo de seguridad de la información y ciberseguridad involucra establecer los criterios necesarios para la administración de riesgos de seguridad de la información, definir alcance y límites y establecer la organización apropiada para la operación de la administración de riesgos de seguridad de la información y ciberseguridad.

11. El proceso de administración de riesgo de seguridad de la información y ciberseguridad debe ser aplicado a la organización de manera integral a todas las áreas que forman parte de la estructura organizacional de la entidad, incluyendo los servicios externalizados. Debe también considerarse el riesgo de seguridad de la información cuando se está diseñando o rediseñando un proceso y cuando se desarrollan sistemas de información.

12. El proceso de administración de riesgo de seguridad de la información y ciberseguridad debe ser un proceso iterativo de evaluación de riesgos e implementación de acciones de tratamiento de riesgos.

13. Los resultados de la evaluación de los riesgos de seguridad de la información y ciberseguridad y las decisiones que se adopten respecto de su tratamiento, deben ser oportunamente comunicados al Directorio, al personal involucrado y a las partes interesadas. Estas materias deberán ser tratadas en la sesión de Directorio más próxima. El detalle de los resultados del proceso de administración de riesgo de seguridad de la información debe ser documentado. Esta base de conocimiento debe ser utilizada para determinar acciones preventivas.

14. El Directorio debe requerir periódicamente información sobre los resultados e indicadores del Sistema de Gestión de Seguridad y Ciberseguridad.

Nota de actualización: Este Capítulo fue creado por la Norma de Carácter General N° 278, de fecha 16 de diciembre de 2020.