Libro V, Título XVIII, Modelo de Gestión de Seguridad de la Información y Ciberseguridad

Capitulo II. Modelo de Gestión de Seguridad de la Información y Ciberseguridad

---

El Sistema de Gestión de Seguridad y Ciberseguridad definido en la presente norma integra en un modelo de gestión los criterios que se han establecido en el Capítulo I, y está conformado por el grupo de procesos que permiten gestionar la seguridad de la información y ciberseguridad en la Administradora.

La gestión de seguridad es responsabilidad de toda la organización, desde el Directorio, la Administración, los niveles Tácticos y Operacionales.

SISTEMA DE GESTIÓN DE SEGURIDAD Y CIBERSEGURIDAD

A continuación, se definen los componentes del *Sistema de Gestión de Seguridad y Ciberseguridad,* incluyendo para los Procesos Estratégicos, Procesos Tácticos, Procesos Operacionales, los objetivos de control y las buenas prácticas aplicables, como asimismo los requisitos mínimos de cumplimiento tendientes a establecer un ***Sistema de Gestión de Seguridad y Ciberseguridad*** en la Administradora, que promueva estructuras de control y gestión periódica con participación de las tres líneas de defensa, promoviendo también la retroalimentación oportuna y la mejora continua.

Además, se define un grupo de controles técnicos y sus objetivos, los que refuerzan el Sistema de Gestión de Seguridad y Ciberseguridad.

A. PROCESOS ESTRATÉGICOS

1.Cumplimiento de requisitos de las partes interesadas

A través de este proceso la Administradora debe analizar el contexto e identificar a las partes interesadas, es decir, a aquellas partes que son afectadas por la gestión de la seguridad de la información y ciberseguridad.

El Directorio de la Administradora, los afiliados y la Superintendencia de Pensiones son integrantes de las partes interesadas.

Una vez identificadas las partes interesadas se deben inventariar las necesidades de seguridad de la información y ciberseguridad de cada una de ellas, considerando como mínimo estos tres tipos de requisitos: legales y normativos, contractuales y de negocio.

Posteriormente, las necesidades deben ser analizadas y utilizadas como base para definir los objetivos de seguridad de la información y ciberseguridad.

Finalmente, se debe revisar de forma periódica que las necesidades de las partes interesadas sean adecuadas y pertinentes para su debido cumplimiento.

Estándares y buenas prácticas:

a. Analizar el contexto externo e interno.

Se considera buena práctica que el Directorio sea informado del contexto externo e interno desde una perspectiva de seguridad de la información y ciberseguridad.

El contexto externo debe considerar, aspectos políticos, económicos, sociales, tecnológicos, legales, ambientales y sanitarios, entre otros.

El contexto interno debe considerar, aspectos administrativos, de comercialización, de recursos humanos, operacionales, financieros, de investigación e innovación, culturales y tecnológicos, entre otros.

b. Identificar las partes interesadas.

La Administradora debe identificar las partes interesadas que son afectadas por la gestión de la seguridad de la información y ciberseguridad. La identificación de las partes interesadas debe ser el resultado del análisis de contexto y posteriormente, debe ser informado al Directorio para que los objetivos de seguridad de la información y ciberseguridad, formen parte del plan estratégico organizacional.

c. Inventariar las necesidades de las partes interesadas en seguridad de la información y ciberseguridad (SIC).

La Administración debe explicitar y registrar las necesidades de las partes interesadas, considerando al menos aspectos legales y normativos, contractuales y de negocio.

d. Revisar el cumplimiento de las necesidades de las partes interesadas.

La Administración debe verificar que las necesidades de las partes interesadas sean gestionadas de acuerdo con los objetivos del Sistema de Gestión de la Seguridad de la Información y Ciberseguridad.

2. Gobernanza de la seguridad de la información y ciberseguridad

El gobierno de la seguridad de la información y ciberseguridad de la Administradora debe asegurar que las necesidades de las partes interesadas se satisfagan, contribuyendo al mismo tiempo al logro de los objetivos del Sistema de Pensiones. Asimismo, toma decisiones que influyan en la gestión de la seguridad de la información y ciberseguridad. Para ello, establece una política y objetivos de seguridad de la información, proporciona los recursos financieros, establece una estructura organizacional y aprueba los planes de tratamiento de riesgos, así como los criterios y niveles de aceptación de riesgos.

Estándares:

a. Definir el alcance en seguridad de la información y ciberseguridad.

El Directorio debe definir los límites y aplicabilidad del Sistema de Gestión de Seguridad y Ciberseguridad en la Administradora.

b. Definir una política y objetivos de seguridad de la información y ciberseguridad.

El Directorio debe definir una política de seguridad de la información y ciberseguridad que oriente el cumplimiento de los requisitos de las partes interesadas. Asimismo, se deben definir objetivos que permitan medir el cumplimiento de la política y alineada con la estrategia de la Administradora.

Esta política debe ser concisa, precisa y explícita en cuanto a su enunciado, de tal forma que sea viable su difusión al personal de la Administradora y personas externas que presten servicios directamente a la Administradora, a través de medios de comunicación adecuados.

c. Definir estructura organizacional para el Sistema de Gestión de Seguridad y Ciberseguridad.

El Directorio debe establecer una estructura organizacional basada en roles para gestionar la seguridad de la información y ciberseguridad, debiendo definir además las funciones y responsabilidades de cada rol.

La estructura debe comprender los siguientes roles: Directorio, comité de riesgos, comité de seguridad de la información y ciberseguridad, comité de gestión de incidentes de seguridad de la información y ciberseguridad (SIC), oficial o responsable o coordinador de seguridad de la información y/o ciberseguridad, dueños de procesos , propietarios de riesgos de seguridad de la información y ciberseguridad (SIC), custodios de activos de información, entre otros, que se consideren pertinentes para una adecuada gestión de la seguridad de la información y ciberseguridad.

Esta estructura organizacional debe contar con segregación funcional que permita definir roles administradores, ejecutores y de control.

d. Implementar un plan de tratamiento de riesgos y presupuestos para seguridad de la información y ciberseguridad.

La Administradora debe definir e implementar un plan de tratamiento de riesgos de seguridad de la información y ciberseguridad, así como el presupuesto requerido para la implementación de nuevos controles o mejora de controles existentes, los que deben ser aprobados por el Directorio.

e. Aprobar los niveles y criterios de aceptación de riesgos de seguridad de la información y ciberseguridad.

El Directorio debe aprobar los niveles y criterios de aceptación de riesgos de seguridad de la información y ciberseguridad para la Administradora.

B. PROCESOS TÁCTICOS

1. Gestión de riesgos de seguridad de la información y ciberseguridad

Este proceso permite a la Administradora identificar, analizar, evaluar y establecer un plan de tratamiento de los riesgos de seguridad de la información y ciberseguridad.

El análisis de riesgos comprende la revisión de los registros de los incidentes del periodo de análisis.

La evaluación de los riesgos debe efectuarse conforme a los criterios y niveles de aceptación aprobados por el Directorio.

Estándares:

a. Identificar riesgos de seguridad de la información y ciberseguridad (SIC).

Los dueños de los procesos deben identificar, revisar y actualizar los riesgos de seguridad de la información y ciberseguridad de los procesos de la Administradora por lo menos una vez al año (ciclo) o cuando se requiera efectuar un cambio significativo. Se debe asignar un identificador único a cada riesgo e incorporarlo al inventario de riesgos de seguridad de la información y ciberseguridad.

La identificación del riesgo debe contemplar también la identificación de las amenazas y las vulnerabilidades asociadas a cada amenaza.

La identificación del riesgo debe considerar el activo de información o los activos de información que podrían ser afectados por cada amenaza identificada, asimismo, el atributo o los atributos de seguridad de la información y ciberseguridad afectados como la confidencialidad, integridad o disponibilidad de la información, entre otros atributos que la Administradora estime necesarios.

Los riesgos identificados deben comprometer uno o algunos objetivos de seguridad de la información y ciberseguridad establecidos por el Directorio.

b. Analizar riesgos de seguridad de la información y ciberseguridad.

Los propietarios de riesgos deben analizar los riesgos de seguridad de la información y ciberseguridad a fin de estimar la probabilidad de que el riesgo ocurra.

Se debe determinar el nivel de vulnerabilidad a partir de la debilidad o ausencia de controles de seguridad de la información y ciberseguridad del tipo preventivos, detectivos y/o correctivos, así como a partir de la información de los registros de incidentes de seguridad y ciberseguridad.

c. Evaluar riesgos de seguridad de la información y ciberseguridad.

Se deben evaluar los riegos describiendo las consecuencias y estimando el nivel de impacto en caso de que se materialice el riesgo.

El nivel de impacto se debe estimar considerando uno o varios tipos de impacto, pudiendo ser: económico, operativo, legal y normativo, entre otros que la Administradora considere pertinentes a sus procesos.

Se debe estimar el nivel de riesgo residual combinando la probabilidad y el nivel del impacto. Asimismo, debe estimar el nivel de riesgo inherente, de la misma forma que el riesgo residual, pero considerando que no existe ningún tipo de control de seguridad de la información y ciberseguridad.

d. Elaborar o actualizar el plan de tratamiento de riesgos (PTR) de seguridad de la información y ciberseguridad.

Se debe elaborar o actualizar el plan de tratamiento para los riesgos no tolerables de seguridad de la información y ciberseguridad.

e. Elaborar declaración obligatoria de controles (DOC).

La Administradora debe elaborar una Declaración Obligatoria de Controles (DOC), para el Sistema de Gestión de Seguridad y Ciberseguridad, entendiéndose como el conjunto de controles que la Administradora se compromete y obliga formalmente a implementar.

La Declaración Obligatoria de Controles (DOC), debe considerar como mínimo los controles relacionados con:

- Seguridad de la arquitectura.
- Seguridad del personal.
- Seguridad de las áreas y equipos.
- Seguridad de activos.
- Seguridad de los accesos.
- Seguridad de los servicios tecnológicos.
- Seguridad del ciclo de desarrollo del software.
- Seguridad de los proveedores.
- Seguridad de la recuperación de las Tecnologías de la Información y Comunicaciones (TIC).
- Seguridad del cumplimiento.

Para ello, se debe incluir la "Justificación de obligatoriedad de cada control", es decir, el fundamento por el cual la Administradora se compromete o no a implementar un control de seguridad de la información y ciberseguridad. La justificación puede ser por razones normativas, por aspectos contractuales, por respuesta a riesgos, u otra justificación de carácter operativa.

Asimismo, se deben considerar en la Declaración Obligatoria de Controles (DOC), los documentos o herramientas que soportan la operación de cada control de seguridad de la información y ciberseguridad e incluir el estado de implementación de cada uno de ellos.

La Declaración Obligatoria de Controles (DOC), se debe revisar periódicamente y actualizar cuando se requiera efectuar un cambio significativo.

2. Gestión de incidentes de seguridad de la información y ciberseguridad

Este proceso debe permitir a las Administradoras efectuar una adecuada gestión de los incidentes (debilidades, eventos o incidentes) de seguridad de la información y ciberseguridad a fin de que tome las acciones debidas a través del establecimiento de un mecanismo formal que dé respuesta efectiva y oportuna a los incidentes.

La gestión de los incidentes de seguridad de la información y ciberseguridad debe considerar la identificación de los activos de seguridad de la información y ciberseguridad, así como los controles comprometidos en el acontecimiento de un incidente a fin de que se fortalezcan los controles en beneficio de la protección de los activos de información.

Estándares y buenas prácticas:

a. Establecer mecanismos de comunicación de incidentes de seguridad de la información y ciberseguridad.

La Administradora debe establecer y difundir los mecanismos de comunicación definidos para que los colaboradores internos y externos, proveedores, clientes, entre otras partes interesadas, puedan reportar incidentes de seguridad de la información y ciberseguridad oportunamente.

b. Clasificar el incidente.

La Administradora debe clasificar el incidente para determinar si lo que han reportado constituye una debilidad, evento o incidente de seguridad de la información o ciberseguridad.

Las debilidades se pueden identificar dentro de la Administradora o provenir de fuentes externas o servicios externalizados.

Los eventos se deben analizar para comprender los objetivos y los métodos de ataque empleados. Asimismo, se deben recopilar los datos de los eventos y correlacionarlos con múltiples fuentes.

Los incidentes deben calificarse para determinar su impacto mediante umbrales de significancia. Para la calificación se debe considerar el alcance del daño, así como el tiempo de duración del incidente, entre otros criterios que se consideren adecuados. Cuando el incidente tiene un impacto que deviene en crisis, la Administradora debe activar los procedimientos establecidos en el proceso de continuidad de negocio.

c. Contener, erradicar y recuperar el incidente de seguridad de la información y ciberseguridad.

La Administradora debe efectuar acciones que permitan contener de manera efectiva el incidente e inmediatamente acciones que permitan erradicar el incidente y recuperar oportunamente la operación, entendiéndose que la contención es evitar que el incidente siga produciendo daños. La erradicación es eliminar la causa del incidente, incluyendo todo rastro de daños y la recuperación, volver el entorno afectado a su estado original.

Para ejecutar las acciones de contención, erradicación y/o recuperación es recomendable que se conformen comités o mesas de trabajo que ayuden a la toma de decisiones. Posteriormente, documentar o registrar las acciones, con el objetivo de mantener un registro histórico y lecciones de aprendizaje de las actividades.

d. Identificar la causa del incidente de seguridad de la información y ciberseguridad.

Se espera que la Administradora emplee una técnica o método para identificar la causa raíz del incidente. Durante la identificación de la causa se debe considerar los activos de información, así como los controles de seguridad de la información y ciberseguridad comprometidos o afectados en la ocurrencia del incidente.

Si al identificar la causa raíz del incidente se determina que se requiere mejorar o implementar un control de seguridad de la información y ciberseguridad como respuesta a un riesgo, la Administradora debe realizar las acciones de mejora necesarias para su mitigación.

e. Realizar análisis forense.

Se considera una buena práctica que la Administradora realice análisis forense cuando las consecuencias del incidente así lo ameriten, de acuerdo con la metodología que la AFP haya adoptado para este tipo de análisis. La Administradora deberá denunciar o iniciar acciones legales, cuando corresponda.

f. Determinar acciones correctivas u oportunidades de mejora, con posterioridad al incidente de seguridad de la información y ciberseguridad.

Se espera que la Administradora evalúe si, una vez finalizado el incidente, se genera una Acción Correctiva u Oportunidad de Mejora. Dentro de las consideraciones de evaluación que estime pertinentes también debe considerar la recurrencia del incidente.

g. Registrar el incidente de seguridad de la información y ciberseguridad.

La Administradora debe registrar el incidente (debilidad, evento o incidente) con toda la información de la notificación y clasificación, así como las actividades ejecutadas para su resolución.

3. Auditoría de seguridad de la información y ciberseguridad.

La auditoría debe evaluar el cumplimiento de lo establecido en el Sistema de Gestión de Seguridad y Ciberseguridad por parte de las Administradoras.

La auditoría debe proporcionar una opinión al Directorio respecto del diseño y el cumplimiento de los controles implementados en el Sistema de Gestión de Seguridad y Ciberseguridad.

La Administración debe comprometer acciones correctivas y/u oportunidades de mejora para resolver los hallazgos identificados por Auditoría Interna.

Estándares:

a. Elaborar un plan de auditoría.

La Administradora debe elaborar anualmente un plan de auditoría para la seguridad de la información y ciberseguridad.

El plan debe contener el alcance de la revisión y los tipos de auditoría (internas, externas, seguimiento, control, etc.) que se haya decidido efectuar sobre la seguridad de la información y ciberseguridad.

El plan debe abarcar todos los riesgos de seguridad de la información y ciberseguridad y el cumplimiento de los controles asociados y debe ser aplicado en un lapso o ciclo de auditoría razonable, pudiendo ser en más de un año.

La Administradora debe considerar la evaluación del Sistema de Gestión de Seguridad y Ciberseguridad, por auditores externos al menos una vez al año.

La auditoría debe desarrollarse de acuerdo con normas internacionales de Auditoría Interna y con técnicas ajustadas a los riesgos de seguridad y ciberseguridad que se estén evaluando.

b. Mantener registro de auditores.

La Administradora debe definir el perfil del profesional que auditará la seguridad de la información y ciberseguridad. Asimismo, debe verificar que quien audite la seguridad de la información y ciberseguridad, cumpla con dicho perfil, tanto para auditorías internas como externas. Debe, además, llevar un registro de los profesionales que auditaron la seguridad de la información y ciberseguridad.

c. Implementar acciones correctivas u oportunidades de mejora.

La Administración del área auditada debe comprometer una acción correctiva u oportunidad de mejora para subsanar cada hallazgo o implementar cada recomendación identificada en el informe de auditoría.

d. Elaborar, validar y aprobar plan de acción post auditoría.

Una vez planificadas las actividades para atender las acciones correctivas y oportunidades de mejora solicitadas post auditoría, la Administración del área auditada debe elaborar un plan de acción que consolide las acciones correctivas y oportunidades de mejora. El responsable a cargo de la auditoría debe validar y aprobar el plan de acción post auditoría, luego de lo cual, debe enviar el informe de auditoría y el plan de acción post auditoría para que se comuniquen los resultados de la auditoría al Directorio.

4. Gestión de las comunicaciones

La Administradora debe establecer: cómo, cuándo, dónde, a quién y a través de qué medios se entrega la información de las necesidades o requisitos de seguridad de la información y ciberseguridad a las partes interesadas. La información proporcionada debe ser pertinente a las partes interesadas conforme a sus requisitos de seguridad de la información y ciberseguridad.

Estándares:

a. Elaborar matriz de comunicaciones de las partes interesadas.

La Administradora debe definir una matriz que establezca la información que debe comunicar a las partes interesadas, así como la forma, la oportunidad y a través de qué medios.

La matriz debe considerar que la comunicación de incidentes de seguridad y ciberseguridad a la Superintendencia debe efectuarse en forma inmediata, cuando las consecuencias del incidente puedan comprometer los objetivos de seguridad y ciberseguridad, la información de los afiliados y usuarios y la reputación del Sistema de Pensiones.

Asimismo, debe considerar que se debe comunicar, de manera mensual al Directorio, sobre el cumplimiento de las necesidades relacionadas con la seguridad y ciberseguridad de las partes interesadas, identificadas por la Administradora.

b. Elaborar información para las partes interesadas.

La Administradora debe elaborar la información establecida en la matriz de comunicaciones. Debe obtener la información de los procesos según la matriz de comunicaciones, sin embargo, siempre debe obtener información de los procesos que conforman del Sistema de Gestión de Seguridad y Ciberseguridad.

c. Efectuar las comunicaciones a las partes interesadas.

La Administradora debe efectuar las comunicaciones en conformidad con lo establecido en la matriz de comunicaciones para seguridad de la información y ciberseguridad.

La Administradora debe asegurar que las comunicaciones sean efectuadas en la forma, oportunidad y medios establecidos. Entre ellas, la comunicación del informe mensual de cumplimiento de requisitos de sistema de seguridad y ciberseguridad al Directorio.

5. Gestión del conocimiento

Se considera una buena práctica que en la ejecución de los procesos del Sistema de Gestión de Seguridad y Ciberseguridad que se generen registros de información que permitan mejorar las actividades del sistema de gestión. Por esta razón, a través de este proceso se debe lograr organizar, estructurar, recopilar, distribuir y brindar acceso a una base de conocimiento (BC) que facilite y agregue valor a la ejecución de las actividades del sistema en el continuo de su ejecución.

Para lo anterior se espera que la Administradora:

- Defina un medio de almacenamiento de los registros de resultados del proceso de Gestión de Seguridad y Ciberseguridad y una matriz con los privilegios de acceso.

- Defina una estructura de registro de resultados de los procesos, que le permitan sistematizar la información y actualizar una base de conocimientos (BC)

- Implemente la estructura de registro de resultados de los procesos y medios de almacenamiento seguros, para mantener una Base de conocimientos confiable.

- Incorpore los registros para actualizar la base de conocimiento, para que sea usada por los roles definidos en el desempeño de sus funciones.

6. Administración del Sistema de Gestión de Seguridad y Ciberseguridad

Este proceso permite a la Administradora verificar que las actividades de los procesos del Sistema de Gestión de Seguridad y Ciberseguridad se estén llevando a cabo oportunamente, tal como la Administradora lo haya definido.

El Sistema de Gestión de Seguridad y Ciberseguridad adoptado por la Administradora debe ser gestionado a fin de que sea compatible con su estructura organizacional, marcos ya existentes o futuros marcos de seguridad de la información y/o ciberseguridad a adoptar.

Este proceso se diferencia del proceso de auditoría en cuanto al tiempo de su ejecución, dado que verifica las actividades durante su ejecución, mientras que la auditoría es post ejecución del proceso a auditar.

Los procesos de seguridad de la información y ciberseguridad deberían formar parte del mapa de procesos de la Administradora.

Buenas prácticas:

Para la administración del Sistema de Gestión de Seguridad y Ciberseguridad se consideran buena práctica que la Administradora desarrolle un programa de verificación de procesos a cargo de roles responsables, los cuales controlen que las actividades que son parte de los procesos que

conforman el Sistema de Gestión Seguridad y Ciberseguridad se cumplan, genere registros de las actividades de verificación y acuerde acciones correctivas necesarias para el mantenimiento del Sistema de Gestión. Estos roles deben también reportar a la Administración y al Directorio sobre el resultado de sus actividades de evaluación.

C. PROCESOS OPERACIONALES

1. Capacitación y toma de conciencia

La Administradora debe identificar las necesidades de capacitación de cada rol y establecer un programa para desarrollar y mantener las competencias de dichos roles, incluyendo propietarios de riesgo, de activos de información, custodios de información, entre otros.

Cada rol que tiene una función dentro de la gestión de la seguridad de la información y ciberseguridad, debe tener las competencias adecuadas a fin de desempeñar su rol de manera eficiente.

Este proceso debe también contemplar que el personal de los proveedores de servicios cuente con conocimientos básicos de seguridad de la información y ciberseguridad.

La Administradora debe elaborar, ejecutar y registrar un programa de capacitación y toma de conciencia para cada rol que cumpla una función dentro de la gestión de seguridad y ciberseguridad en la Administradora.

2. Medición

La Administradora debería establecer indicadores adecuados para medir el logro de los objetivos de seguridad de la información y ciberseguridad, un programa para medirlos e informar el grado alcanzado de cada objetivo.

La definición de los indicadores debe contemplar la idoneidad de los datos a emplear para efectuar las mediciones, datos que son el resultado de la ejecución de los procesos del Sistema de Gestión de Seguridad y Ciberseguridad y de controles registrados en la Declaración Obligatoria de Controles (DOC). Asimismo, se debe determinar el nivel o grado de cumplimiento de la política de seguridad de la información y ciberseguridad a partir de la combinación de los niveles logrados en los objetivos de seguridad de la información y ciberseguridad.

Se espera que la Administradora:

-Defina indicadores para medir los objetivos de seguridad de la información y ciberseguridad.

-Elabore un programa de medición de los indicadores de seguridad de la información y ciberseguridad y efectúe las mediciones.

-Elabore informe de resultados de mediciones de los indicadores y del logro de objetivos de seguridad de la información y ciberseguridad.

-Implemente acciones correctivas u oportunidades de mejora post medición.

3. Implementación de respuestas de seguridad de la información y ciberseguridad

La Administradora debe llevar a cabo el plan de tratamiento de riesgos.

Asimismo, gestionará los controles técnicos de seguridad de la información y ciberseguridad, los que se definen en la letra D de este Capítulo, que se ejecuten y que se encuentran registrados en la Declaración Obligatoria de Controles (DOC).

Por otra parte, los controles a mejorar o implementar, comprometidos en los planes de tratamiento de riesgos, deben también formar parte de la Declaración Obligatoria de Controles (DOC).

A través de este proceso la Administradora llevará el control del estado de implementación de los controles.

Estándares y buenas prácticas:

a. Elaborar planificación y presupuesto del plan de tratamiento de riesgos (PTR).

La Administradora debe planificar y presupuestar el plan de tratamiento de riesgos a fin de implementar las respuestas y conseguir el presupuesto requerido.

La planificación para la implementación de las respuestas incluidas en el plan de tratamiento de riesgos debe considerar al menos la siguiente información: rol responsable de implementación, fechas de inicio y fin de la implementación, recursos necesarios, supuestos y premisas, así como factores críticos para alcanzar la implementación de cada respuesta seleccionada.

El plan de tratamiento de riesgos y el presupuesto deben ser aprobados por el Directorio.

b. Ejecutar planificación y presupuesto del plan de tratamiento de riesgos (PTR).

Los roles responsables de la implementación de las actividades del plan de tratamiento de riesgos, deben ejecutarlas de acuerdo con lo planificado y comprometido en dicho plan.

Se considera una buena práctica que la Administradora, cuente con registros auditables de la operación de los controles de seguridad de la información y ciberseguridad implementados.

c. Elaborar informe mensual de seguimiento del plan de tratamiento de riesgos (PTR).

Se espera que la Administradora comunique mensualmente, el avance de la implementación del plan de tratamiento de riesgos.

d. Actualizar declaración obligatoria de controles (DOC).

La Administradora debe actualizar la Declaración Obligatoria de Controles (DOC) respecto a la justificación de obligatoriedad de los controles y el estado del control, cuando existan respuestas para afrontar el riesgo incluidas en el plan de tratamiento.

4. Acciones correctivas y oportunidades de mejora

La Administradora a través de este proceso debería proporcionar corrección y mejora continua al Sistema de Gestión de Seguridad y Ciberseguridad mediante la implementación de las acciones correctivas y oportunidades de mejora.

Para lo anterior se espera que la Administradora:

-Efectúe el análisis de causa de las acciones correctivas solicitadas para identificar causas raíz y eliminarlas.

-Planifique las actividades de acciones correctivas y oportunidades de mejora, comprometiendo plazos de implementación y roles responsables.

-Ejecute las actividades planificadas de acciones correctivas y oportunidades de mejora.

-Controle y haga seguimiento de las actividades planificadas de acciones correctivas y oportunidades de mejora, dejando registro auditable de esta actividad.

D. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

A continuación, se definen los controles técnicos y sus objetivos, que refuerzan el Sistema de Gestión de Seguridad y Ciberseguridad.

La Administradora debe establecer los controles del Sistema de Gestión de Seguridad y Ciberseguridad para contar con mitigadores de los riesgos técnicos.

Los controles incluidos en esta letra establecen una estructura mínima de seguridad.

La Administradora de acuerdo con la estructura organizacional definida y la complejidad de sus operaciones debe efectuar un análisis de riesgos para incluir controles acordes, que se ajusten al apetito y tolerancia al riesgo definido por el Directorio.

Los controles que se incluyen en esta letra deben estar contenidos en la Declaración Obligatoria de Controles (DOC) de la Administradora.

1. SEGURIDAD DE LA ARQUITECTURA

a. Arquitectura objetivo de seguridad: La Administradora debe desarrollar la arquitectura objetivo de seguridad de la información y ciberseguridad, para permitir que los componentes lógicos, físicos y aplicaciones, corresponda con los requisitos legales, normativos y contractuales de seguridad de la información y ciberseguridad. Se espera que la Administradora realice un análisis de brechas entre la línea base y la arquitectura objetivo.

b. Componentes de la arquitectura de seguridad: La Administradora debe analizar los componentes basándose en las brechas identificadas entre la línea base de la arquitectura de seguridad de la información y ciberseguridad y la arquitectura objetivo. Se debe establecer la estructura y funciones fundamentales para la entrega de servicios críticos; e identificar los riesgos entre la configuración existente y la arquitectura objetivo.

c. Implementación de la arquitectura de seguridad: Se espera que la Administradora asegure la conformidad con la arquitectura objetivo de seguridad de la información y ciberseguridad a través de proyectos de implementación o migración, así como realizar las funciones de gobierno de arquitectura apropiadas para la solución y para las gestiones de cambios.

d. Evaluación de la arquitectura de seguridad: Se espera que la Administradora realice un análisis a nivel de seguridad de la información y ciberseguridad con respecto a los incidentes, amenazas, gestión de las vulnerabilidades, nivel de cumplimiento y riesgos asociados a la arquitectura de seguridad, así como las buenas prácticas y tendencias en seguridad de la información y ciberseguridad; evaluando a nivel de componentes y en conjunto para asegurar la capacidad y cumplimiento de requisitos de seguridad de la información y ciberseguridad, así como de los nuevos requerimientos.

e. Cambios en la arquitectura de seguridad: Se espera que la Administradora asegure que el ciclo de vida de la arquitectura de seguridad de la información y ciberseguridad se mantenga y que la capacidad arquitectónica de seguridad cumpla con los requisitos y requerimientos actuales mediante el procedimiento de la gestión de cambios de la arquitectura de seguridad, establecida por la Administradora.

2. SEGURIDAD DEL PERSONAL

a. Alineamiento de recursos humanos y responsabilidades de la Administración: La seguridad de la información y ciberseguridad deben estar incluidas en los procesos de recursos humanos desde la contratación hasta el término del vínculo contractual. La Administración debe requerir a todos los empleados, proveedores y socios que apliquen la seguridad de la información y ciberseguridad de acuerdo con las políticas, procedimientos y controles establecidos por la Administradora.

b. Verificación de las identidades y antecedentes del candidato: La Administradora debe llevar a cabo la verificación de las identidades, los antecedentes y perfiles públicos de los candidatos para cada empleo, de acuerdo a las leyes, regulaciones y normas vigentes, aspectos de seguridad de la información y ciberseguridad y a la ética; esta verificación debe ser proporcional a los requisitos de la Administradora, la clasificación de la información a la que tendrá acceso y los riesgos que se perciban.

c. Acuerdos contractuales, responsabilidades, sanción disciplinaria y término del empleo: Los acuerdos contractuales entre la Administradora y el personal deben fijar sus responsabilidades y las de la Administradora con respecto a la seguridad de la información y ciberseguridad; dentro de los acuerdos se debe informar respecto de las sanciones disciplinarias en caso de que se detecte alguna infracción contra la seguridad de la información y ciberseguridad; así como las responsabilidades que permanecerán válidas después del término del empleo, tales como la no divulgación de la información y devolución de todos los activos de la Administradora que estén en su posesión una vez terminado su empleo, contrato o acuerdo.

3. SEGURIDAD DE LAS ÁREAS Y EQUIPOS

a. Perímetro, controles y protección de seguridad física: La Administradora debe diseñar, determinar y utilizar los perímetros de seguridad y aplicar mecanismos de control físico de ingreso para proteger las áreas que contienen o procesan información de carácter personal, sensible y crítica. El

diseño debe contemplar mecanismos de mitigación de riesgos operacionales, tecnológicos e incidentes de seguridad de la información y ciberseguridad.

Asimismo, se debe monitorear el entorno físico para detectar riesgos de seguridad de la información y ciberseguridad, en cumplimiento de las disposiciones legales y normativas, y las políticas con respecto al entorno operativo físico para los activos de información de la Administradora.

b. Determinación de zonas seguras, de carga y descarga: La Administradora debe diseñar y aplicar procedimientos de control para el trabajo en zonas seguras, acceso, distribución, carga, descarga y otros puntos por los que podría ingresar personal y equipamiento a la Administradora. El diseño debe contemplar distancias, recorridos y mecanismos para evitar el acceso no autorizado, así como para evitar la filtración de información de carácter personal, sensible y crítica, en cualquiera de sus medios.

c. Ubicación y protección de los equipos y cableado: Los equipos deben ser ubicados y protegidos de tal forma que se reduzcan los riesgos como resultado de las amenazas a la seguridad de la información y ciberseguridad, los peligros del medio ambiente, y las oportunidades de acceso no autorizado físico o digital. Se debe proteger de cualquier interferencia, intercepción o daño al cableado de energía o telecomunicaciones que transfiere datos o que sirve de apoyo en los servicios de información.

d. Soporte y mantenimiento de los equipos para atención a público: Los equipos deben ser protegidos contra las fallas de energía y otras alteraciones causadas por interrupciones no programadas, adicionalmente se debe asegurar el correcto mantenimiento de los equipos para garantizar su disponibilidad, integridad y confidencialidad de la información.

e. Retiro de activos y seguridad fuera de las instalaciones: El equipo, la información o el software no puede ser retirado de su lugar sin previa autorización, verificación de inventario y registro respectivo de salida; en caso de retiro aprobado se debe aplicar medidas para los activos utilizados fuera de las instalaciones, tomando en cuenta los diferentes riesgos de seguridad de la información y ciberseguridad al trabajar fuera de las instalaciones de la Administradora. Los medios de comunicación que contienen información deben ser protegidos contra el acceso no autorizado, mal uso o corrupción durante su transporte.

4. SEGURIDAD DE LOS ACTIVOS

a. Inventario y propiedad de los activos: La Administradora debe identificar los activos de la información, tales como, instalaciones, herramientas y componentes asociados a la información y al procesamiento de ésta dentro y fuera de la Administradora, para lo cual se debe diseñar y mantener un inventario de dichos activos considerando los aspectos de seguridad de la información y ciberseguridad.

b. Clasificación y etiquetado de la información: La información debe ser clasificada en términos de los requisitos y valores legales, de acuerdo a cuán crítico y sensible sea su divulgación y modificación no autorizada.

c. Uso aceptable y manejo de los activos: Se espera que la Administradora documente e implemente las reglas para el uso aceptable de los activos y las instalaciones de procesamiento de la información. Estos mecanismos deberían considerar el esquema de clasificación de la información adoptado por la Administradora y las protecciones contra las filtraciones de información.

d. Reutilización y eliminación de equipos y medios de comunicación: Todos los equipos que contienen información deben ser gestionados formalmente con respecto a la seguridad de la información y ciberseguridad, durante la reutilización, transferencias y eliminación.

Los medios de comunicación deben ser eliminados de manera segura a nivel físico y digital cuando ya no son necesarios, de acuerdo con las políticas de la Administradora.

5. SEGURIDAD DE LOS ACCESOS

a. Control de acceso en los servicios: La Administradora debe establecer, documentar y revisar la política de control del acceso en base a los requisitos del Sistema de Gestión de Seguridad de la Información y Ciberseguridad. Los usuarios deben tener acceso únicamente a los servicios, manteniendo los principios de menor privilegio y separación de funciones.

b. Gestión de información de las credenciales: La Administradora debe controlar la asignación de la información de credenciales de usuarios mediante un proceso de gestión formal. La autenticación debería considerar más de un factor de autenticación, acorde con los riesgos de seguridad de la información y ciberseguridad, determinados por la Administradora.

c. Ciclo de vida de las credenciales: La Administradora debe implementar un mecanismo que contemple el ciclo de vida de las credenciales, la autorización, emisión, verificación, revocación de los derechos de acceso **y credenciales o privilegios** a todos los tipos de usuarios en todos los servicios. Asimismo, debe considerar los derechos de acceso a la información e instalaciones de procesamiento de la información.

d. Verificación de accesos y credenciales: Los propietarios de los activos deben verificar los derechos de acceso y credenciales de acuerdo a la periodicidad que se defina la Administradora.

e. Gestión de accesos privilegiados: La Administradora debe restringir y controlar la asignación, así como el uso de los derechos de acceso privilegiado. Los derechos de acceso privilegiado deben ser gestionados con mayores exigencias a nivel de política, gestión de credenciales, ciclo de vida y verificación de los derechos de acceso.

f. Restricción del acceso a información, herramientas con privilegios y al código fuente: Se debe restringir el acceso a la información y a las funciones de administración de aplicación de los sistemas, de acuerdo con la política de control de acceso de la Administradora, considerando la separación de funciones y distintos niveles de privilegio, según corresponda a cada función definida a los roles y responsabilidades de las personas.

6. SEGURIDAD DE LOS SERVICIOS TECNOLÓGICOS

a. Gestión de la configuración y documentación: Se espera que la Administradora implemente un sistema que permita registrar e identificar las configuraciones (elementos de configuración) y documentación operativa de los servicios tecnológicos que proporcionan soporte a los procesos de la Administradora.

La base de datos de gestión de configuración y de documentación (CMDB por sus siglas en inglés Configuration Management Database), debe permitir la identificación, control, mantenimiento y verificación de los distintos elementos de configuración que componen los servicios en Tecnologías de la Información y Comunicación, así como la documentación de sus registros.

b. Gestión de eventos de tecnologías de la información y comunicaciones: Se espera que la Administradora planifique los requisitos y actividades correspondientes a la gestión de eventos y la auditoría de los servicios de tecnologías de la información y comunicaciones que soportan los procesos de la Administradora.

Se debería elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, operador y administrador, considerando los accesos, excepciones, fallas y eventos de seguridad de la información y ciberseguridad. Estos registros deben de estar protegidos en su origen y almacenamiento contra la alteración y acceso no autorizado.

c. Gestión de la capacidad: La Administradora debe disponer y mantener una capacidad adecuada de recursos de cómputo y de procesamiento para la disponibilidad de los servicios de tecnología de la información y comunicaciones. La gestión de la capacidad debe incluir el registro, monitoreo y mejora del uso de los recursos, así como las proyecciones a realizar sobre los requisitos

de capacidad que garanticen el desempeño de los servicios en tecnologías de la información y comunicaciones.

d. Gestión de las vulnerabilidades técnicas: Las vulnerabilidades de seguridad de la información y ciberseguridad deben ser gestionadas por la Administradora mediante un plan. Este plan debe comprender el análisis y comprobación de las vulnerabilidades, las pruebas de intrusión de ser el caso y la investigación y evaluación de remediaciones. Asimismo, la gestión debe incluir la revisión periódica de parches de seguridad en los servicios de Tecnologías de Información y Comunicaciones. La Administradora debería contar con equipos dedicados a la gestión de vulnerabilidades, para obtener, de manera oportuna, la información sobre las vulnerabilidades técnicas de los servicios de Tecnologías de Información y Comunicaciones y evaluar la exposición de la Administradora a dichas vulnerabilidades y tomar las medidas adecuadas para manejar los riesgos asociados.

e. Gestión de la criptografía: De acuerdo con los requisitos de seguridad de la información y ciberseguridad, la Administradora debe hacer uso de controles criptográficos en cumplimiento con los acuerdos, las leyes y las regulaciones correspondientes.

f. Gestión de cambios: La Administradora debe mantener una gestión integrada sobre los cambios en todos los servicios mediante procedimientos formales de cambios, para lo cual debe considerar la criticidad, tiempos de ejecución, recursos necesarios, impacto, pruebas de seguridad y aceptación, marcha atrás y los requisitos de seguridad de la información y ciberseguridad.

Luego de realizados los cambios, se debe revisar y verificar la funcionalidad y nivel de seguridad de la información y ciberseguridad, para garantizar que no haya un impacto adverso sobre las operaciones.

g. Control de "endpoints": La Administradora debe determinar los tipos de dispositivos permitidos (incluye los medios extraíbles) que sirvan de soporte a los procesos. Se deben implementar procedimientos y mecanismos para controlar los dispositivos de acuerdo con sus políticas de seguridad de la información y ciberseguridad.

h. Control del "malware": La Administradora debe implementar mecanismos de control para la detección, prevención, eliminación y cuarentena de "malware" o código malicioso. Debe implementar procedimientos para la recuperación de la información, acorde con los niveles de servicios definidos por la Administradora.

i. Respaldo de la información y pruebas de restauración: La Administradora debe definir una política de respaldo de información y pruebas de restauración. Se debe contar con un plan de respaldos y pruebas, acordes con la política de seguridad de la información y ciberseguridad de la Administradora.

j. **Controles en las redes y comunicaciones:** Se debe administrar, controlar y proteger la integridad de las redes, sistemas y las aplicaciones que soportan los procesos de la Administradora. Para ello, se deben identificar los mecanismos de seguridad, los niveles del servicio y los requisitos de todos los servicios de redes e incluirlos en los acuerdos de servicios de redes.

Se considera una buena práctica que los controles de redes y comunicaciones incluyan herramientas y/o mecanismos para monitorear y detectar eventos de seguridad de la información y ciberseguridad.

k. Protección de las transacciones y los servicios en las redes públicas: Se debe proteger la información que pasa a través de las redes públicas de las actividades fraudulentas, controversias contractuales y divulgación y modificaciones no autorizadas, así mismo se debe proteger la información que provenga de las transacciones de los servicios de aplicación, para evitar las transmisiones incompletas, desvíos, duplicado o reproducción no autorizados de mensajes.

l. Control para la transferencia de la información: La Administradora debe implementar políticas, procedimientos y controles formales para la transferencia de información a través del uso de todo tipo de equipos de comunicación; para lo cual se deben emplear mecanismos de transferencia segura de la información del Sistema de Pensiones entre la Administradora y terceros. Este nivel se seguridad de la información y ciberseguridad incluye todos los medios de comunicación aprobados por la Administradora, pudiendo ser correo electrónico, aplicaciones de transferencia, herramientas colaborativas, chats y otros servicios.

7. SEGURIDAD DEL CICLO DE DESARROLLO DEL SOFTWARE

a. Seguridad en ingeniería del software: La Administradora debe establecer y aplicar reglas de seguridad de la información y ciberseguridad durante el proceso de desarrollo del software, para cumplir con la arquitectura de seguridad y las políticas de seguridad que aplican a los servicios de tecnologías de la información y comunicaciones.

b. Protección de entornos de desarrollo y pruebas: La Administradora debe establecer y proteger adecuadamente los entornos de desarrollo, calidad y pruebas.

c. Revisión de la seguridad y aceptación: Antes de pasar a producción, la Administradora debe de llevar a cabo revisiones de la funcionalidad, seguridad de la información y ciberseguridad durante el desarrollo, para lo cual se debe establecer programas de verificación de la aceptación y de los criterios relacionados con respecto a los nuevos desarrollos, renovaciones y nuevas versiones.

8. SEGURIDAD DE LOS PROVEEDORES

a. Política de seguridad sobre las relaciones con los proveedores: La Administradora debe identificar, establecer, evaluar, gestionar y acordar los mecanismos de gestión del riesgo de la cadena de suministro de seguridad de la información y ciberseguridad. Dentro de la política de seguridad de la información se deben establecer lineamientos de seguridad sobre las relaciones con los proveedores.

b. Acuerdos y cadena de suministro de seguridad: Los contratos con proveedores deben contener medidas apropiadas para cumplir con la política de seguridad de la información y ciberseguridad, incluyendo la gestión de riesgos de la cadena de suministro con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proveer con elementos de infraestructura tecnológica, información de la Administradora.

c. Evaluación de servicios del proveedor: Se considera una buena práctica la evaluación periódica de los proveedores para confirmar que cumplen con las obligaciones contractuales con la Administradora, acordes a la política de seguridad de la información y ciberseguridad.

d. Gestión de cambios en el servicio de los proveedores: Se espera que la Administradora gestione los cambios en la provisión de los servicios prestados por los proveedores, por lo cual debe aprobar, registrar y verificar que se realice en cumplimiento con la política de seguridad de la información y ciberseguridad.

9. SEGURIDAD DE LA RECUPERACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES.

a. Determinación de requisitos de resiliencia tecnológica y de seguridad: La Administradora debe establecer los requisitos de resiliencia tecnológica, seguridad de la información y ciberseguridad, para respaldar la entrega de servicios críticos de tecnologías de la información y comunicaciones.

Los eventos que pueden causar interrupciones deben ser identificados, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información y ciberseguridad.

b. Implementación de los planes de recuperación: La Administradora debe establecer, documentar, implementar y mantener procedimientos y controles para asegurar el nivel necesario de

recuperación de los servicios críticos de tecnología de la información y comunicaciones considerando los requisitos de resiliencia tecnológica, seguridad de la información y ciberseguridad, para asegurar la disponibilidad de los servicios críticos de tecnología de la información y comunicaciones al nivel y en las escalas de tiempo requeridas. Estos planes deben ser concordantes con el Plan de Continuidad de Negocio o BCP (Business Continuity Planning).

c. Mantenimiento, prueba y mejora de los planes de recuperación: La Administradora debe verificar los controles para la recuperación de los servicios críticos en tecnologías de la información y comunicaciones establecidos y probar los planes de recuperación implementados, periódicamente con la finalidad de asegurar su validez y efectividad ante distintos escenarios de indisponibilidad, incluyendo los servicios externalizados.

d. Redundancias e instalaciones de contingencia: La Administradora debe implementar instalaciones de contingencia para los servicios críticos de tecnologías de la información y comunicaciones y/o redundancias a nivel de cada capa con una capacidad suficiente para cumplir con los requisitos de resiliencia tecnológica, de seguridad de la información y ciberseguridad, en situaciones normales y ante distintos escenarios de indisponibilidad.

10. SEGURIDAD DEL CUMPLIMIENTO

a. Propiedad intelectual, privacidad y protección de los registros: La Administradora debe garantizar la propiedad intelectual, la privacidad y la protección de la información de carácter personal, sensible y crítica. Los registros deben ser protegidos contra la pérdida, destrucción, falsificación, divulgación y/o acceso no autorizado, de acuerdo con las disposiciones legales y normativas, y la política de seguridad de la información y ciberseguridad de la Administradora.

b. Revisión de cumplimiento técnico: La Administradora debe establecer un programa de revisión de cumplimiento de controles y ejecutar la revisión de la política y procedimientos de seguridad de la información y ciberseguridad. Esta revisión debe abarcar todos los aspectos técnicos descritos en la política y procedimientos.

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