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

Anexo

DEFINICIONES

Actividad: Unidad mínima funcional que forma parte del proceso y debe ser ejecutada por un rol perteneciente a la estructura organizacional que gestiona la seguridad de la información y ciberseguridad de la Administradora. Las actividades deben ser incorporadas a los procesos de la Administradora.

Acción correctiva: Acciones correctivas sobre hallazgos o desviaciones de actividades de control.

Activo de información: Conceptualización de un conjunto de componentes, recursos, datos o bienes económicos, con significado, que tienen valor para la administración de los fondos de pensiones y que se deben proteger.

Amenaza: Causa interna o externa con motivación y potencial para vulnerar un activo de información de la Administradora.

Análisis de riesgos de seguridad de la información y ciberseguridad: Mecanismo a través del cual se determina la probabilidad de que un riesgo pueda ocurrir.

Base de Conocimiento: Repositorio o base de datos que permite almacenar información, desde políticas, manuales, instructivos, papeles de trabajo, entre otra documentación que sea relevante para gestionar el conocimiento de los equipos de trabajo y el desarrollo de competencias para mejorar su rendimiento y del proceso que administran.

Categoría de proceso: Un conjunto de procesos que guardan relación dentro de una misma área general de actividades de las Administradoras.

Ciberamenaza: Tipo de amenaza especial que dirige vectores de ataque aprovechando el ciberespacio.

Ciberataque: Cualquier incidente cibernético, provocado deliberadamente y que afecte a un sistema informático.

Ciberespacio: Dominio global y dinámico dentro del entorno de la información que corresponde al ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información, los datos (almacenados, procesados o transmitidos) que abarcan los dominios físico, virtual y cognitivo y las interacciones sociales que se verifican en su interior.

Ciberseguridad: Conjunto de acciones posibles para la prevención, mitigación, investigación y manejo de las amenazas e incidentes sobre los activos de información, datos y servicios, así como para la reducción de los efectos de los mismos y del daño causado antes, durante y después de su ocurrencia.

Confidencialidad: Principio de seguridad que requiere que la información solo pueda ser accedida por quien tiene el privilegio y emplearla únicamente para los fines concedidos, evitándose su divulgación no autorizada.

Control de información documentada del proceso: Aborda las siguientes actividades sobre la información documentada del proceso: a) distribución, acceso, recuperación y uso; b) almacenamiento y preservación; c) control de cambios y; d) conservación y disposición.

Control de seguridad de la información y ciberseguridad: Mecanismo que apoya a la preservación de la confidencialidad, integridad o disponibilidad de los activos de información.

Control específico de seguridad de la información y ciberseguridad: Instrumento (política, plan, instructivo, procedimiento, etc.) que emplea la Administradora dentro de sus procesos para implementar un control de seguridad de la información y ciberseguridad.

Criterio de aceptación del riesgo: Regla o parámetro a través del cual la Administradora establece las condiciones bajo las cuales acepta un riesgo.

Declaración obligatoria de controles DOC: Conjunto de controles, a través del cual la Administradora se compromete y obliga a cumplir con todos o un conjunto de controles.

Debilidad de seguridad de la información y ciberseguridad: Ineficacia de un control de seguridad de la información y ciberseguridad, destinado a contener riesgos de los activos de información.

Disponibilidad: Principio de seguridad que requiere que la información deba estar dispuesta en su punto de uso para quienes tienen el acceso concedido.

Evaluación del riesgo: Mecanismo a través del cual se determinan las consecuencias e impactos de un riesgo determinándose el nivel efectivo del riesgo.

Evento de seguridad de la información y ciberseguridad: Materialización de un riesgo de seguridad de la información y ciberseguridad no deseado con efectos negativos poco relevantes para la administradora.

Gestión de seguridad de la información y ciberseguridad: Conjunto de procesos mutuamente cohesionados e interrelacionados para llevar a cabo la planificación, ejecución, verificación y mejora de la seguridad de la información y ciberseguridad en la Administradora.

Incidente de seguridad de la información y ciberseguridad: Materialización de un riesgo de seguridad de la información y ciberseguridad no deseado con efectos negativos considerables para la Administradora.

Indicador: Mecanismo que permite darle significancia, con evidencia, del logro de metas de los procesos. Los procesos tienen métricas para medir el logro de sus metas.

Integridad: Principio de seguridad que requiere que la información debe permanecer exacta y completa. Los datos y elementos de configuración sólo son modificados por personal y actividades autorizadas. La integridad considera todas las posibles causas de modificación, incluyendo fallos software y hardware, eventos medioambientales e intervención humana.

Nivel de aceptación del riesgo: Indicador numérico que significa que el riesgo es aceptable por la Administradora, por lo tanto, puede convivir con dicho riesgo. El nivel de aceptación del riesgo constituye un criterio de aceptación del riesgo.

Objetivo de seguridad de la información y ciberseguridad: Fin de la gestión de la seguridad de la información.

Oportunidad de mejora: Acciones destinadas optimizar las actividades desarrolladas por la Administradora.

Parte interesada: Son todas las personas naturales y jurídicas que interactúan con la Administradora, que afectan o se podrían ver afectadas por la gestión de la seguridad de la información y ciberseguridad.

Proceso: Conjunto de actividades interrelacionadas mutuamente cuya ejecución agregan valor a la Administradora y permite alcanzar los propósitos y resultados. Son ejecutados por roles, que pertenecen a la estructura organizacional que gestiona la seguridad de la información y ciberseguridad.

Requisito de seguridad de la información y ciberseguridad: Deber de la Administradora de abordar y cumplir aspectos de seguridad de la información y ciberseguridad contenidos en normas, contratos y de negocio (riesgos de seguridad de la información y ciberseguridad), que afectan a las partes interesadas.

Resiliencia: Capacidad de los sistemas, equipos o redes para seguir operando pese a estar sometidos a un incidente o ciberataque, aunque sea en un estado degradado, debilitado o segmentado. Así como, incluye la capacidad de restaurar con presteza sus funciones esenciales después de un incidente o ataque de modo de recuperarse con presteza de una interrupción, por lo general con un efecto reconocible mínimo.

Riesgo de seguridad de la información y ciberseguridad: Probabilidad de que una amenaza o ciberamenaza explote una vulnerabilidad de los activos de información impactando el logro de los objetivos de seguridad de la información y ciberseguridad de la Administradora.

Riesgo inherente: Nivel de riesgo considerando que no existe ningún tipo de control.

Riesgo residual: Nivel de riesgo resultante después de implementar la respuesta de tratamiento seleccionada.

Seguridad de la información: Conjunto de controles organizados que ayudan a preservar la confidencialidad, integridad y disponibilidad de los activos de información, protegiéndolos de las amenazas.

Tratamiento del riesgo: Mecanismo a través del cual se elige un tipo de respuesta para los riesgos no tolerables o no aceptables. La respuesta puede ser: afrontar, evitar, transferir o aceptar el riesgo.

Verificación: Determinar objetivamente que las actividades de los procesos se ejecutan en el momento y forma establecido por la Administradora. La verificación puede dar lugar a correcciones y/ o mejoras de las actividades.

Vulnerabilidad: Debilidad de un activo o ausencia de un control de seguridad de la información y ciberseguridad, que puede ser explotado por una o más amenazas informáticas.

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