Compendio de Normas del Seguro Social de Accidentes del Trabajo y Enfermedades Profesionales

A. Generalidades

CAPÍTULO I. Alcance de las instrucciones impartidas

Las presentes instrucciones tienen por objeto establecer un marco regulatorio que comprenda los fundamentos generales de seguridad de la información y ciberseguridad, los que deben ser considerados como buenas prácticas por parte de los organismos administradores del Seguro Social de la Ley N°16.744, con excepción de aquellas instrucciones en las que se indique expresamente su carácter obligatorio.

Adicionalmente, se establece el reporte obligatorio de ciberincidentes que ocurran en sus redes, equipos y sistemas y que alcancen los niveles de peligrosidad e impacto establecidos en esta normativa, así como también un reporte anual obligatorio de autoevaluación del estado de la seguridad de la información y ciberseguridad al interior de la organización.

Las instrucciones contenidas en el presente Título V. Gestión de la Seguridad de la Información serán aplicables a todos los organismos administradores del Seguro de la Ley N°16.744, entendiendo como tales, las mutualidades de empleadores y el Instituto de Seguridad Laboral.

En el caso del Instituto de Seguridad Laboral, estas disposiciones son complementarias a las impartidas por el Estado de Chile, respecto de las instrucciones de seguridad de la información.

CAPÍTULO II. Definiciones

a) Seguridad de la información: Conjunto de medidas preventivas y reactivas de los organismos administradores y sus respectivos sistemas tecnológicos, que tienen por objeto resguardar y proteger la información, asegurando la confidencialidad, integridad, autenticidad y disponibilidad de los datos, continuidad de servicios y protección de activos de información.

b) 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.

c) Ciberincidente: Todo evento que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas o datos informáticos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por dichos sistemas y su infraestructura, que puedan afectar al normal funcionamiento de los mismos.

d) Gestión de incidentes: Procedimiento para la detección, análisis, manejo, contención y resolución de un incidente de ciberseguridad.

e) Protección de los activos de información: Adoptar las medidas que resguarden la seguridad física de los dispositivos, así como los accesos a éstos. Se entenderá por infraestructura crítica las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en los trabajadores protegidos, pensionados, empresas adherentes o afiliadas y en las prestaciones preventivas, médicas y económicas que debe brindar el seguro.

f) Continuidad de servicios: Adoptar las medidas que permitan proveer un nivel mínimo de servicio, entendiendo por esto las prestaciones propias del seguro, reduciendo el riesgo de eventos que puedan crear una interrupción o inestabilidad en las operaciones de la entidad hasta niveles aceptables y planificando la recuperación de los servicios de las tecnologías de la información (TI).

g) Autenticación: Proceso utilizado en los mecanismos de control de acceso con el objetivo de verificar la identidad de un usuario, dispositivo o sistema mediante la comprobación de credenciales de acceso.

h) Confidencialidad: Adoptar las medidas necesarias que impidan la divulgación de información a individuos, entidades o procesos no autorizados. A su vez, asegurar que, en el ambiente interno del organismo administrador, sólo las personas autorizadas dentro de ésta tengan acceso a la información.

i) Integridad: Adoptar las medidas necesarias que aseguren que los datos están protegidos de modificaciones no autorizadas y que dichos datos mantienen exactitud respecto del origen de los mismos.

j) Disponibilidad: Adoptar las medidas necesarias que permitan que la información esté a disposición de quienes la necesitan, entendiendo por esto a trabajadores protegidos, pensionados, trabajadores de los organismos administradores, procesos o aplicaciones, Superintendencia de Seguridad Social y otras entidades con competencia en materias del Seguro de la Ley N° 16.744.