

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

/ LIBRO VII. ASPECTOS OPERACIONALES Y ADMINISTRATIVOS / TÍTULO V. Gestión de la Seguridad de la Información / D. Ciberseguridad / CAPÍTULO I. Gestión de la ciberseguridad

CAPÍTULO I. Gestión de la ciberseguridad

Se considera buena práctica la designación al interior de la organización de un profesional en calidad de titular y su respectivo suplente, como contraparte formal de la Superintendencia de Seguridad Social, y que sea el responsable de la seguridad de la información y la ciberseguridad, así como del diseño, mantención, seguimiento y notificación de los riesgos de seguridad de la información y ciberseguridad, considerando controles de segregación de deberes y áreas de responsabilidad para reducir las oportunidades de modificación o uso indebido no autorizado o no intencional de los activos de la organización, incluyendo las nuevas formas de trabajo a distancia o teletrabajo.

Es recomendable que el organismo administrador cuente con un equipo de respuesta para la adecuada gestión de la ciberseguridad, con el objeto de identificar los riesgos de afectación de los servicios por causa de ciberincidentes, verificar el cumplimiento eficaz de los respectivos planes de gestión y reportar los ciberincidentes.

Asimismo, los organismos administradores debiesen establecer planes de gestión de riesgos de ciberseguridad, formulados de acuerdo a estándares y directrices que guarden la debida coherencia con las características de las redes, equipos y sistemas críticos utilizados para el otorgamiento de las prestaciones de Seguro de la Ley N°16.744.

Se recomienda que los planes de gestión de riesgo sean actualizados y sometidos a aprobación del directorio o dirección institucional y conocidos por la alta gerencia de los organismos administradores, junto con señalar el estado de los riesgos de ciberseguridad, indicadores claves, principales ciberincidentes y planes de acción de mejoras.

Junto a lo anterior, se recomienda que los planes de gestión de riesgo incluyan medidas para la protección de los datos personales y sensibles, en cumplimiento con lo establecido en la Ley N°19.628.
