Compendio de Normas que regulan a las Cajas de Compensación de Asignación Familiar

6.1.12.2.1 Medidas de gestión

La Caja de Compensación de Asignación Familiar debe implementar medidas técnicas y de organización para gestionar los riesgos de ciberseguridad de las redes, equipos y sistemas que utiliza para la prestación de los servicios a sus afiliados y no afiliados, cuando corresponda, indistintamente si tal gestión estuviere o no externalizada.

Lo anterior implica identificar, analizar, evaluar, tratar, monitorear y comunicar el impacto de los riesgos de ciberseguridad sobre los procesos de la C.C.A.F.

De igual forma, se recomienda que la C.C.A.F. adopte las medidas adecuadas para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten la seguridad de sus redes, equipos y sistemas, con el objeto de garantizar su continuidad operativa, así como la continuidad de la seguridad de la información. En todos los casos se puede diseñar, implementar, practicar y evaluar un plan de respuesta que otorgue adecuada cobertura a sus redes, equipos y sistemas, en conformidad con estándares internacionales o nacionales, de amplia aplicación y, a su vez, desde el punto de vista de los grupos de interés, de modo de garantizar la integridad, disponibilidad y confidencialidad de la información.

Cada C.C.A.F. debe determinar las medidas de gestión que garanticen la disponibilidad, integridad y confidencialidad que en definitiva adopte, de conformidad con el tipo de organización, la naturaleza y contexto de los servicios prestados, los riesgos asociados y la tecnología disponible.

Con el objetivo que la ciberseguridad pueda ser abordada con un sentido de entorno dinámico que se ajuste a las necesidades regulatorias y tecnológicas se debe establecer un Sistema de Gestión de Seguridad de la Información (SGSI) cuya operación y funcionamiento, respecto de los procesos de negocio centrales y críticos, puedan ser certificados por entidades externas a la Caja y especialistas en el tema.

Asimismo, la C.C.A.F. debe establecer planes de gestión de riesgos de ciberseguridad, formulados de acuerdo con 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.

Los planes de gestión de riesgos deben ser actualizados anualmente y sometidos a aprobación del directorio e implementados y difundidos por la alta gerencia. Estos planes deben señalar el estado de los riesgos de ciberseguridad, indicadores claves y su medición asociada, descripción de los ciberincidentes y planes de acción de mejoras implementadas.

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

La C.C.A.F. debe establecer planes de capacitación y formación para su personal en materia de ciberseguridad.

Por otro lado, la Caja debe contar con un equipo de respuesta inmediata para la adecuada gestión de la ciberseguridad, con el objeto de identificar los riesgos de afectación de los servicios por causas de ciberincidentes, verificar el cumplimiento eficaz de los respectivos planes de gestión y reporte de los ciberincidentes.

A su vez, la C.C.A.F. debe designar, al interior de la organización, a un profesional en calidad de titular y su respectivo suplente, como contraparte formal de la Superintendencia de Seguridad Social, el cual será el responsable de la Caja de las políticas de 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 para ello 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.