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

6.1.12.2 Gestión de la seguridad de la información

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.

6.1.12.2.2 Sistema de gestión de seguridad de la información de la C.C.A.F.

La Caja debe contar con un sistema de gestión de seguridad de la información que considere, al menos, lo siguiente:

a) Contar con una política de seguridad de la información y ciberseguridad definida al interior de la organización y aprobada por el directorio.

b) Realizar un levantamiento de los activos de información críticos existentes en la C.C.A.F., asegurando que la información reciba el nivel de protección adecuado de acuerdo con su importancia para la organización. En particular aquellos sistemas relevantes para el soporte de las operaciones y procesos críticos que involucran el adecuado otorgamiento de las

prestaciones de seguridad social, con el fin de resguardar la información interna, así como también la de carácter externa relacionada con sus afiliados y no afiliados.

c) Conocer los riesgos críticos de las tecnologías de la información identificando los que afecten la seguridad de la información y ciberseguridad.

d) Establecer anualmente el nivel de riesgos aceptado por la C.C.A.F. en materia de tecnologías de información, considerando además los niveles de disponibilidad mínimos para asegurar la continuidad operacional.

e) Informar al Directorio y a toda la organización respecto a los lineamientos principales de la entidad frente a la seguridad de la información.

f) Adoptar las recomendaciones entregadas por auditores externos e internos respecto de esta materia.

g) Contar con el apoyo del área de riesgos existente, procurando que dicha área se involucre en materia de valorización, identificación, tratamiento y tolerancia de los riesgos propios del ambiente de tecnologías de la información a los que se expone la C.C.A.F. por los distintos factores en que se desenvuelve.

h) Identificar las amenazas más relevantes a las que se expone la C.C.A.F. ante eventuales ciberataques y evaluar el impacto organizacional que conlleva la vulnerabilidad e indisponibilidad de estos activos de información.

i) Mantener un registro formalmente documentado de los sistemas de información existentes al interior de la organización, señalando el proceso de negocio que gestiona el área usuaria, identificación de la base de datos y sistema operativo que soporta el aplicativo.

6.1.12.2.3 Elementos de la gestión del sistema de seguridad de la información

6.1.12.2.3.1. Consideraciones

Para una efectiva gestión del sistema de seguridad de la información, éste se debe integrar a los procesos de las C.C.A.F., considerando sus aspectos en el diseño de los procesos y controles establecidos, en base a las obligaciones y responsabilidades derivadas del cumplimiento de las Leyes N°s.16.395 y 18.833.

El sistema de gestión de la seguridad de la información debe ser consistente con las definiciones y objetivos de la política de gestión integral de riesgos.

6.1.12.2.3.2. Política de Seguridad de la Información

Para una eficiente gestión del sistema de seguridad de la información, se estima necesario establecer la política interna que entregue el marco en que la C.C.A.F. gestiona la seguridad de la información.

En dicho contexto, esta política debiese considerar al menos los siguientes aspectos:

a) Definición de la seguridad de la información, objetivos generales, alcance y la importancia de ésta como un mecanismo que permita compartir y gestionar información de forma segura.

b) Una declaración de la intención de la alta administración, que apoye los objetivos y principios de la seguridad de la información, en concordancia con las metas y estrategias del organismo administrador.

c) Una explicación de los principios, estándares y requisitos de cumplimiento más relevantes para la Caja, tales como, el adecuado otorgamiento de las prestaciones de la Ley N°18.833, cumplimientos normativos de la seguridad social, gestión de la continuidad de negocio, consecuencia de una violación de la política de seguridad de la información, entre otros aspectos.

d) Una definición clara respecto de las responsabilidades generales y específicas de la alta gerencia y demás estamentos relevantes dentro del organismo administrador.

e) Un registro de incidentes de seguridad de la información.

f) Referencia de documentos complementarios a la política de seguridad de la información, si corresponde, tales como procedimientos o manuales detallados con reglas o estándares asociados a actividades específicas.

La política de seguridad de la información debiese ser comunicada y difundida a toda la organización, de forma clara y comprensible para el usuario final. Se recomienda considerar, como parte de este proceso que, al momento de la contratación de un colaborador, éste firme que ha tomado conocimiento de dicha política.

La política de seguridad de la información debe ser revisada y actualizada anualmente, para asegurar que se encuentre en concordancia con las metas y estrategias de los organismos administradores. Este hecho debe quedar documentado con la correspondiente firma en el control de cambios del referido documento.