

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

/ 6 LIBRO VI. GESTIÓN DE RIESGOS / 6.1 TÍTULO I. RIESGO OPERACIONAL / 6.1.12 CIBERSEGURIDAD / 6.1.12.2 Gestión de la seguridad de la información / 6.1.12.2.3 Elementos de la gestión del sistema de seguridad de la información

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.