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



# 6.1.12 CIBERSEGURIDAD

Las presentes instrucciones tienen por objeto establecer un marco regulatorio que comprenda los fundamentos generales y también algunos aspectos de la gestión del riesgo en materia de ciberseguridad, los que deben ser considerados como lineamientos mínimos a cumplir.

Por lo tanto, la Caja debe considerar tanto el análisis del impacto operacional como los riesgos y controles mitigantes, además del ciclo de vida de un ciberincidente. También debe incluir la prevención, detección, análisis, notificación, contención, erradicación, recuperación, documentación a su respecto y escalamiento a las autoridades o entidades pertinentes, según corresponda.

De igual manera, esta norma busca establecer el carácter obligatorio de los reportes sobre ciberincidentes que la C.C.A.F. debe enviar a esta Superintendencia, así como también contar con un reporte anual obligatorio de autoevaluación del estado de la seguridad de la información y ciberseguridad al interior de la organización.

## 6.1.12.1 Definiciones

#### 6.1.12.1.1. 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.

#### 6.1.12.1.2. Autenticidad

Principio de seguridad que permite certificar la veracidad del origen de datos, elementos o sistemas.

#### 6.1.12.1.3. Ciberataque

Cualquier incidente cibernético, provocado deliberadamente y que afecte a un sistema informático.

#### 6.1.12.1.4. 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 estos.

#### 6.1.12.1.5. 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.

#### 6.1.12.1.6. Confidencialidad

Principio de seguridad que requiere que los datos deben únicamente ser accedidos por el personal autorizado a tal efecto.

#### 6.1.12.1.7. Disponibilidad

Capacidad de ser accesible y estar listo para su uso a demanda de una entidad o persona autorizada, incluida la Superintendencia.

#### 6.1.12.1.8. Gestión de incidentes

Procedimiento para la detección, análisis, manejo, contención y resolución de un incidente de ciberseguridad y responder ante éste.

#### 6.1.12.1.9. Incidente

Evento inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes, equipos y sistemas de información.

#### 6.1.12.1.10. Infraestructura crítica

Se refiere a 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 la seguridad, la salud o el bienestar de las personas.

#### 6.1.12.1.11. Integridad

Principio de seguridad que certifica que los datos y elementos de configuración sólo son modificados por personal y actividades autorizadas. La Integridad considera todas las posibles causas de modificación, incluyendo fallos software y

hardware, eventos medioambientales e intervención humana.

#### 6.1.12.1.12. Riesgo

Toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes, equipos y sistemas de información. Se puede cuantificar como la probabilidad de materialización de una amenaza que produzca un impacto en términos de operatividad, de integridad física de personas o material o de imagen corporativa.

#### 6.1.12.1.13. Seguridad de la información

Conjunto de medidas preventivas y reactivas de la C.C.A.F. 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.

## 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.

## 6.1.12.3 Reporte de Ciberincidentes

### 6.1.12.3.1 Mecanismo de reporte

La C.C.A.F. debe reportar oportunamente acerca de todos los ciberincidentes que detecte en sus redes, equipos y sistemas y que alcancen los niveles de peligrosidad e impacto establecidos en los anexos indicados en los números 6.1.12.3.2 y 6.1.12.3.3 del Título I del Libro VI del Compendio de la Ley N°18.833. En caso de que un suceso pueda asociarse con dos o más tipos de incidentes con niveles de peligrosidad o impacto distintos, se le asignará el nivel más alto.

La obligación de reportar se entiende formalmente cumplida luego de que la C.C.A.F. haya informado el ciberincidente a través del sistema GRIS, a través de los formularios habilitados para ello.

Es preciso señalar que los ciberincidentes no deben ser reportados bajo la figura de Evento de Reporte Inmediato, ni como Hecho Relevante según el Título II del Libro V del Compendio de la Ley N°18.833. Sin embargo, sí deben quedar en el Registro de Información de Pérdidas Mensual, en los casos que corresponda, es decir, que impliquen pérdidas operacionales, de acuerdo con lo establecido en el número 6.1.10 del Título I del Libro VI del Compendio de la Ley N°18.833, utilizando el mismo código de evento.

### 6.1.12.3.2 Niveles de peligrosidad

El nivel de peligrosidad determina la potencial amenaza que supondría la materialización de un incidente en las redes, equipos y sistemas de la C.C.A.F., así como su efecto en la calidad o continuidad en el otorgamiento de las prestaciones.

Conforme a sus características, las amenazas son clasificadas con los siguientes niveles de peligrosidad: Crítico, Muy Alto, Alto, Medio y Bajo.

El nivel asignado se determinará según lo que se señala en el Anexo N°5: Niveles de peligrosidad de los ciberincidentes del Título I del Libro VI del Compendio de la Ley N°18.833.

### 6.1.12.3.3 Niveles de impacto

Los posibles niveles de impacto de un ciberincidente se clasifican en Crítico, Muy Alto, Alto, Medio, Bajo o Sin Impacto. El nivel de impacto correspondiente se asignará usando como referencia lo señalado en el Anexo N°6: Niveles de impacto de los ciberincidentes del Título I del Libro VI del Compendio de la Ley N°18.833.

### 6.1.12.3.4 Resolución de Ciberincidentes

Una vez detectado un ciberincidente que afecte a una red, equipo o sistema utilizado en el otorgamiento de prestaciones, la C.C.A.F. debe efectuar, de manera oportuna, todas las gestiones que sean necesarias para su resolución y restaurar la normal provisión de los servicios afectados, dando primera prioridad a aquellas medidas que permitan evitar o, en su defecto, minimizar el impacto a los grupos de interés.

En caso que la C.C.A.F. lo considere necesario, puede solicitar la colaboración de entidades especializadas en materia de ciberseguridad, para la resolución de un ciberincidente.

La C.C.A.F. debe proporcionar la información adicional que le sea requerida para analizar la naturaleza, causas y efectos de los incidentes notificados, así como para elaborar estadísticas y reunir los datos necesarios para elaborar informes de resultados.

Asimismo, sin perjuicio de las medidas inmediatas conducentes a la mitigación de los efectos y al restablecimiento de los servicios afectados por un ciberincidente, la C.C.A.F. debe subsanar, en la medida que sea técnicamente posible, las vulnerabilidades de sus sistemas, equipos y redes que hubieran permitido o facilitado el ciberincidente.

En caso de que una C.C.A.F. detecte que sus redes, equipos y sistemas fueron utilizados como medio para la comisión de algún delito informático, debe efectuar las denuncias ante los órganos competentes, ejercer las acciones judiciales pertinentes e informar a la Superintendencia de Seguridad Social.

La C.C.A.F. debe establecer los protocolos de recuperación de la información, en caso de pérdida de ésta por manipulación, ciberincidentes u otras causas de su responsabilidad.

### 6.1.12.3.5 Contenido de los reportes de Ciberincidentes

La C.C.A.F. debe reportar toda aquella información relativa al evento de un ciberincidente, cuyo nivel de impacto o peligrosidad, se encuentra definido en los niveles Alto, Muy Alto o Crítico, según lo establecido en los números precedentes.

Esta información debe ser recopilada con la rapidez que amerita, sin afectar la estrategia de contención del incidente y los mecanismos desplegados para evitar la propagación de este en la red interna, en la red externa y la interoperación con los beneficiarios y grupos de interés.

Además de la rapidez para obtener la información, se recomienda seguir las buenas prácticas de primera respuesta forense internacionalmente aceptadas o que hayan sido validadas nacionalmente por el Instituto Nacional de Normalización, con el objetivo de contaminar lo menos posible las evidencias que permitan investigaciones avanzadas por parte de equipos de ciberseguridad altamente especializados o los entes persecutores que correspondan.

Sin perjuicio de lo anterior, la C.C.A.F. debe mantener una bitácora con el registro de todos los ciberincidentes identificados.

#### 6.1.12.3.5.1. Reporte de alerta de Ciberincidente

Dentro del plazo de 1 hora, contado desde la toma de conocimiento del ciberincidente, la C.C.A.F. debe reportar a través del formulario "Reporte de alerta de Ciberincidente" del sistema GRIS, la siguiente información:

a) Código del evento.

b) Fecha ocurrencia del evento.

c) Hora de Detección del evento.

d) Resumen ejecutivo del Ciberincidente.

e) Recursos tecnológicos afectados.

f) Tipo de Ciberincidente (tabla de nivel de peligrosidad)

#### 6.1.12.3.5.2. Informe parcial de Ciberincidente

Posteriormente, antes de 6 horas desde la toma de conocimiento del ciberincidente, la C.C.A.F. debe reportar a través del formulario "Informe parcial de Ciberincidente" del sistema Gris, la siguiente información:

a) Código de evento.

b) Fecha Ocurrencia Evento.

c) Fecha Detección Evento.

d) Resumen ejecutivo del ciberincidente.

e) Recursos tecnológicos afectado.

f) Tipo de ciberincidente.

g) Descripción detallada de lo sucedido, señalando los activos de información afectados y su nivel de sensibilidad y afectación (confidencialidad/integridad/disponibilidad).

h) Alcance del problema local, regional o nacional, si se conoce.

i) Sistemas de información afectados actuales y potenciales.

j) Grupos de interés afectados actuales y potenciales, identificando sobre todo los afiliados afectados.

#### 6.1.12.3.5.3. Informe de resolución de Ciberincidente

Finalmente, en un plazo máximo de 10 días hábiles desde la toma de conocimiento del ciberincidente, la C.C.A.F. debe reportar a través del formulario "Informe de resolución de Ciberincidente" del sistema GRIS, la siguiente información:

a) Código de evento.

b) Resumen ejecutivo del ciberincidente.

c) Origen o causa identificable del ciberincidente.

d) Total de sistemas de información afectados.

e) Total de grupos de interés afectados.

f) Infraestructura crítica afectada.

g) Descripción de los niveles de compromiso: indicadores de compromiso de nivel IP, indicadores de compromiso de nivel de dominios y subdominios, indicadores de compromiso de correos, indicadores de compromiso a nivel HASH (MD5/SHA1/SHA256 o el que los reemplace), vulnerabilidades facilitadoras del incidente y posibles vectores de ingreso/egreso de los artefactos, y en general los datos técnicos del incidente, entre otros similares.

h) Descripción del plan de acción y medidas de resolución y mitigación.

i) Medios necesarios para la resolución calculados en horas hombre (HH) / persona.

j) Monto impacto estimado.

k) Daños reputacionales, aun cuando sean eventuales.

l) Descripción cronológica de los hechos asociados del ciberincidente.

Los reportes requeridos deben ser remitidos a través del "Sistema GRIS" ubicado en el sitio web de la Superintendencia.

## 6.1.12.4 Reporte de Autoevaluación

La C.C.A.F. debe realizar una autoevaluación anual en cuanto a su desempeño y nivel de madurez. Para esto, deben elaborar un informe de autoevaluación de gestión de ciberseguridad, conforme a lo establecido en el Anexo N°7: Informe de autoevaluación de la gestión de ciberseguridad del Título I del Libro VI del Compendio de la Ley N°18.833.

El proceso de autoevaluación es responsabilidad de la respectiva C.C.A.F., para lo cual puede contratar a una entidad especialista para estos efectos. El reporte de autoevaluación puede contener pruebas de "ethical hacking" en la medida que dichas pruebas permitan mejorar el ambiente de ciberseguridad de la Caja.

El informe de autoevaluación debe ser conocido por el directorio y remitido a la Superintendencia a más tardar el último día hábil de marzo de cada año, referido a la evaluación del año calendario anterior.