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



## 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.