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

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.