CIRCULAR N°

Correlativo Interno N° O-148761-2024

MODIFICA INSTRUCCIONES EN MATERIA DE CIBERSEGURIDAD MODIFICA EL LIBRO VI DEL COMPENDIO DE NORMAS QUE REGULAN A LAS CAJAS DE COMPENSACIÓN DE ASIGNACIÓN FAMILIAR

Esta Superintendencia, en uso de las atribuciones que le confieren los artículos 1, 2, 3, 23, 38 letra d) de la Ley N° 16.395, Orgánica de este Servicio, y el artículo 3 de la Ley N° 18.833, que contiene el Estatuto Orgánico de las Cajas de Compensación de Asignación Familiar (C.C.A.F.), ha estimado necesario modificar el Compendio de Normas que Regulan a las C.C.A.F. en materia de ciberseguridad luego de la dictación de la Ley N°21.663 o Ley Marco de Ciberseguridad.

En conformidad con su artículo 1° de la Ley N°21.663, ésta tiene por objeto establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre éstos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones determinadas en el artículo 4°, y los mecanismos de control, supervisión y de responsabilidad ante infracciones.

De acuerdo con lo establecido en el artículo 4° siguiente, la referida Ley se aplicará a las instituciones que presten servicios calificados como esenciales según lo contemplado en los incisos segundo y tercero de este artículo y a aquellas que sean calificadas como operadores de importancia vital, de conformidad con lo dispuesto en los artículos 5° y 6°.

Continúa el artículo 4° indicando que son servicios esenciales, entre otros, la administración de prestaciones de seguridad social.

En consecuencia, la Ley N°21.663 resulta aplicable a las Cajas de Compensación de Asignación Familiar -C.C.A.F.-, toda vez que en conformidad a lo establecido en el artículo 1° de la Ley N°18.833, las C.C.A.F. son entidades de previsión social y cuyo objeto es la administración de prestaciones de seguridad social.

Por su parte, establece el artículo 26 de la Ley N°21.663 que las autoridades sectoriales podrán emitir normativas generales, técnicas e instrucciones necesarias para fortalecer la ciberseguridad en las instituciones de su sector, en conformidad con la regulación respectiva y siguiendo lo dispuesto en el artículo 24 de esa Ley, cuando corresponda.

Las instituciones supervisadas, continúa el artículo 26, deberán cumplir obligatoriamente con estas normas e instrucciones en la gestión de sus riesgos, de acuerdo con la autoridad sectorial que las haya emitido. La fiscalización y sanción relacionadas con estas disposiciones se regirán por las leyes respectivas de dicha autoridad sectorial.

En consecuencia, encontrándose las C.C.A.F. sujetas a la supervigilancia y fiscalización de la Superintendencia de Seguridad Social, tal como lo establece el artículo 3° de la Ley N°18.833 y lo dispuesto en el artículo 4° de la Ley N°21.663, se imparten las siguientes instrucciones a las C.C.A.F. en materia de ciberseguridad.

I. MODIFÍCASE EL COMPENDIO DE NORMAS QUE REGULAN A LAS CAJAS DE COMPENSACIÓN DE ASIGNACIÓN FAMILIAR DE LA SIGUIENTE FORMA:

1. SUSTITÚYENSE las instrucciones contenidas en el numeral 6.1.12 Ciberseguridad, del Libro VI, por las siguientes:

"**6.1.12 Ciberseguridad**

Las C.C.A.F. son entidades de previsión social que administran prestaciones de seguridad social, por lo que se les considera instituciones que prestan servicios esenciales de acuerdo con lo dispuesto en el artículo 4° de la Ley N°21.663.

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 la Caja de Compensación.

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.

La Caja debe aplicar, de manera permanente, medidas para prevenir, reportar y resolver incidentes de ciberseguridad. Estas medidas podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso.

El cumplimiento de estas obligaciones exige la debida implementación de los protocolos y estándares establecidos por la Agencia Nacional de Ciberseguridad o Agencia, así como de los estándares particulares de ciberseguridad dictados por la Superintendencia de Seguridad Social.

El objeto de estos protocolos y estándares será la prevención y gestión de los riesgos asociados a la ciberseguridad, así como la contención y mitigación del impacto que los incidentes puedan tener sobre la continuidad operacional del servicio prestado o la confidencialidad y la integridad de la información o de las redes o sistemas informáticos, de conformidad con lo prescrito en la Ley N°21.663.

También debe incluirse la 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 y al Equipo Nacional de Respuesta a Incidentes de Seguridad Informática -CSIRT- de la Agencia, 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, de acuerdo a lo instruído en el numeral 6.1.12.11 de este Libro VI.

6.1.12.1 Definiciones

a) **Activo informático:** toda información almacenada en una red y sistema informático que tenga valor para una persona u organización.
b) **Auditorías de seguridad:** procesos de control destinados a revisar el cumplimiento de las políticas y procedimientos que se derivan del Sistema de Gestión de la Seguridad de la Información.
c) **Autenticación:** propiedad de la información que da cuenta de su origen legítimo.
d) **Ciberataque:** intento de destruir, exponer, alterar, deshabilitar, o exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático.
e) **Ciberseguridad**: preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad.
f) **Confidencialidad:** propiedad que consiste en que la información no es accedida o entregada a individuos, entidades o procesos no autorizados.
g) **Disponibilidad:** propiedad que consiste en que la información está disponible y es utilizable cuando es requerida por un individuo, entidad o proceso autorizado.
h) **Equipo de Respuesta a Incidentes de Seguridad Informática o CSIRT:** centros multidisciplinarios que tienen por objeto prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme a procedimientos y políticas predefinidas, ayudando a mitigar sus efectos.
i) **Incidente de ciberseguridad o ciberincidente:** todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos.
j) **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.
k) **Integridad:** propiedad que consiste en que la información no ha sido modificada o destruida sin autorización.
l) **Red y sistema informático:** conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales.

m) **Resiliencia:** capacidad de las redes y sistemas informáticos para seguir operando luego de un incidente de ciberseguridad, aunque sea en un estado degradado, debilitado o segmentado, y la capacidad de las redes y sistemas informáticos para recuperar sus funciones después de un incidente de ciberseguridad.
n) **Riesgo:** posibilidad de ocurrencia de un incidente de ciberseguridad; la magnitud de un riesgo es cuantificada en términos de la probabilidad de ocurrencia del incidente y del impacto de las consecuencias de este.
o) **Vulnerabilidad:** debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.

6.1.12.2 Principios rectores

Se consideran principios rectores en ciberseguridad los siguientes:

a) **Principio de control de daños:** frente a un ciberataque o a un incidente de ciberseguridad siempre se deberá actuar coordinada y diligentemente, y adoptar las medidas necesarias para evitar la escalada del ciberataque o del incidente de ciberseguridad y su posible propagación a otros sistemas informáticos.
b) **Principio de cooperación con la autoridad:** para resolver los incidentes de ciberseguridad se deberá prestar la cooperación debida con la autoridad competente y, si es necesario, cooperar entre diversos sectores, teniendo en cuenta la interconexión y la interdependencia de los sistemas y servicios.
c) **Principio de respuesta responsable:** la aplicación de medidas para responder a incidentes de ciberseguridad o ciberataques en ningún caso podrá significar la realización o el apoyo a operaciones ofensivas.
d) **Principio de seguridad informática:** toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática que considere necesarias, incluyendo el cifrado.
e) **Principio de racionalidad:** las medidas para la gestión de incidentes de ciberseguridad, las obligaciones de ciberseguridad y el ejercicio de las facultades de la Agencia y de la Superintendencia de Seguridad Social deberán ser necesarias y proporcionales al grado de exposición a los riesgos, y al eventual impacto social y económico.
f) **Principio de seguridad y privacidad por defecto y desde el diseño:** los sistemas informáticos, aplicaciones y tecnologías de la información deben diseñarse, implementarse y gestionarse teniendo en cuenta la seguridad y la privacidad de los datos personales que procesan.

6.1.12.3. Sistema de Gestión de la seguridad de la información

a) La Caja debe implementar un sistema de gestión de seguridad de la información continuo con el fin de determinar aquellos riesgos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y la continuidad operacional de los servicios que presta a sus afiliados y no afiliados, cuando corresponda, indistintamente si tal gestión estuviere o no externalizada. Este sistema deberá permitir evaluar tanto la probabilidad como el potencial impacto de un incidente de ciberseguridad.

   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, la C.C.A.F. debe adoptar las medidas adecuadas para prevenir y reducir al mínimo los efectos de los ciberataques o incidentes de ciberseguridad 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.

   La 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 incidentes de ciberseguridad y planes de acción de mejoras implementadas.

Junto a lo anterior, los planes de gestión de riesgos deben incluir medidas para la protección de los datos personales y sensibles, en cumplimiento con lo establecido en la Ley N°19.628.

b) La Caja debe mantener un registro de las acciones ejecutadas que compongan el sistema de gestión de seguridad de la información.

c) La C.C.A.F. debe elaborar e implementar planes de continuidad operacional y ciberseguridad, los cuales deberán certificarse en ciberseguridad, y someterse a revisiones periódicas, con una frecuencia mínima de dos años. Con todo, la Superintendencia podrá instruir fundadamente y por motivos sobrevinientes graves, la certificación de sus planes de continuidad operacional o ciberseguridad en un plazo menor al indicado en el párrafo precedente; sin embargo, la Superintendencia sólo podrá ejercer esta facultad siempre que la certificación tenga, al menos, un año de vigencia.

d) La C.C.A.F. debe realizar continuamente operaciones de revisión, ejercicios, simulacros y análisis de las redes, sistemas informáticos y sistemas para detectar acciones o programas informáticos que comprometan la ciberseguridad y comunicar la información relativa a dichas acciones o programas a la Superintendencia y al CSIRT Nacional, en la forma que determinen estas instrucciones y el reglamento de la Ley N°21.663.

e) Adoptará la Caja de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad, incluida la restricción de uso o el acceso a sistemas informáticos, si fuera necesario.

Para estos efectos, 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 incidentes de ciberseguridad.

f) La Caja debe contar con la certificación de ciberseguridad a que se refiere el artículo 28 de la Ley N°21.663.

g) Informará la Caja a los potenciales afectados, en la medida que puedan identificarse y cuando así lo requiera la Superintendencia, sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y

sistemas informáticos, especialmente cuando involucren datos personales y no exista otra disposición legal que requiera su notificación; o cuando sea necesario para prevenir la ocurrencia de nuevos incidentes o para gestionar uno que ya hubiera ocurrido.

h) Contará la Caja con programas de capacitación, formación y educación continua de sus trabajadores y colaboradores, que incluyan campañas de ciberhigiene.

i) La Caja de Compensación debe designar un delegado de ciberseguridad y su respectivo suplente, quien actuará como contraparte ante la Superintendencia de Seguridad Social, la Agencia y el CSIRT Nacional y quien será el responsable en 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 informáticos de la organización, incluyendo las nuevas formas de trabajo a distancia o teletrabajo.

j) La Caja debe contar con una política de seguridad de la información y ciberseguridad definida al interior de la organización y aprobada por el directorio.

k) Debe la Caja efectuar un levantamiento de los activos de información o informáticos críticos existentes, 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.

l) La Caja debe reconocer los riesgos críticos de las tecnologías de la información identificando los que afecten la seguridad de la información y ciberseguridad.

m) Debe establecerse 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.

n) El Gerente General informará al Directorio y a toda la organización respecto a los lineamientos principales de la entidad frente a la seguridad de la información.

o) Adoptará la Caja las recomendaciones entregadas por auditores externos e internos respecto de esta materia.

p) En materia de ciberseguridad se debe 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.

q) Se deben 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.

r) 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.

6.1.12.4 Consideraciones de la gestión del sistema de seguridad de la información

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.

6.1.12.5. 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 rectores en ciberseguridad, 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.
g) 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.
h) 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 la Caja. Este hecho debe quedar documentado con la correspondiente firma en el control de cambios del referido documento.

6.1.12.6. Reporte de Ciberataques

La C.C.A.F. debe reportar oportunamente acerca de todos los ciberataques que detecte en sus redes, equipos y sistemas y que puedan tener efectos significativos, tan pronto les sea posible.

Se considerará que un incidente de ciberseguridad tiene efecto significativo si es capaz de interrumpir la continuidad de un servicio esencial o afectar la integridad física o la salud de las personas, así como en el caso de afectar sistemas informáticos que contengan datos personales. Para determinar la importancia de los efectos de un incidente, se tendrán especialmente en cuenta los siguientes criterios:

a) El número de personas afectadas.
b) La duración del incidente.
c) La extensión geográfica con respecto a la zona afectada por el incidente.

Deberá omitirse en los reportes de incidentes de ciberseguridad todo dato o información personal, conforme a lo dispuesto en el artículo 2°, letra f), de la ley N° 19.628, sobre protección de la vida privada. Para efectos de lo dispuesto en este inciso, no se considerará que la dirección IP sea un dato o información personal.

El procedimiento específico para notificar un incidente de ciberseguridad al CSIRT Nacional, la forma, así como las condiciones de anonimato, la taxonomía del informe y la periodicidad, serán establecidos en el reglamento de la Ley 21.663.

La obligación de reportar se entiende formalmente cumplida respecto de la Superintendencia luego de que la C.C.A.F. haya informado el ciberataque a través del sistema GRIS, por medio de los formularios habilitados para ello y al CSIRT Nacional de acuerdo con los mecanismos dispuestos por el reglamento a que se refiere el párrafo anterior.

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 Tïtulo I del Libro VI del Compendio de la Ley N°18.833, utilizando el mismo código de evento.

6.1.12.7 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.

6.1.12.8 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.

6.1.12.9 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, debiendo aplicar al efecto el principio de control de daños descrito en el numeral 6.1.12.2.

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.

6.1.12.10 Contenido de los reportes de Ciberincidentes

a) Reporte de alerta temprana

Dentro del plazo de 3 horas, contado desde la toma de conocimiento del ciberincidente, la C.C.A.F. debe reportar a través del formulario "Reporte de alerta temprana de Ciberincidente" del sistema GRIS, la siguiente información:

i. Código del evento.
ii. Fecha ocurrencia del evento.
iii. Hora de Detección del evento.
iv. Resumen ejecutivo del Ciberincidente.
v. Recursos tecnológicos afectados.
vi. Tipo de Ciberincidente (tabla de nivel de peligrosidad)

b) Actualización de la información

Posteriormente, a más tardar dentro de las 72 horas desde la toma de conocimiento del ciberincidente, la C.C.A.F. debe reportar a través del formulario "Informe de actualización de Ciberincidente" del sistema Gris, la siguiente información:

i. Código de evento.
ii. Fecha Ocurrencia Evento.

iii. Fecha Detección Evento.
iv. Resumen ejecutivo del ciberincidente.
v. Recursos tecnológicos afectado.
vi. Tipo de ciberincidente.
vii. Descripción detallada de lo sucedido, señalando los activos de información afectados y su nivel de sensibilidad y afectación (confidencialidad/integridad/disponibilidad).
viii. Alcance del problema local, regional o nacional, si se conoce.
ix. Sistemas de información afectados actuales y potenciales.
x. Grupos de interés afectados actuales y potenciales, identificando sobre todo los afiliados afectados.

c) Informe de resolución final de Ciberincidente

Finalmente, en un plazo máximo de 15 días corridos contado desde el envío de la alerta temprana, la C.C.A.F. debe reportar a través del formulario "Informe de resolución final de Ciberincidente" del sistema GRIS, la siguiente información:

i. Código de evento.
ii. Resumen ejecutivo del ciberincidente.
iii. Origen o causa identificable del ciberincidente.
iv. Total de sistemas de información afectados.
v. Total de grupos de interés afectados.
vi. Infraestructura crítica afectada.
vii. 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.
viii. Descripción del plan de acción y medidas de resolución y mitigación.
ix. Medios necesarios para la resolución calculados en horas hombre (HH) / persona.
x. Monto impacto estimado.
xi. Daños reputacionales, aun cuando sean eventuales.
xii. 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.

6.1.12.11 Reporte de Autoevaluación

La C.C.A.F. debe realizar una autoevaluación anual en cuanto a su desempeño y nivel de madurez. Para esto, debe 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."

II. VIGENCIA

Las presentes instrucciones comenzarán a regir a contar de la entrada en vigencia de la Ley N°21.663, de acuerdo con lo dispuesto en el numeral 2 del artículo primero transitorio de esa misma Ley.

PAMELA GANA CORNEJO
SUPERINTENDENTA DE SEGURIDAD SOCIAL