INTENDENCIA DE BENEFICIOS SOCIALES
DEPARTAMENTO NORMATIVO

AU08-2021-00468

SANTIAGO, 26 DE MAYO DE 2021.

CIRCULAR N°3.594.

CAJAS DE COMPENSACIÓN DE ASIGNACIÓN FAMILIAR MODIFICA Y COMPLEMENTA CIRCULAR Nº2.821, DE 2012, SOBRE GESTIÓN DEL RIESGO OPERACIONAL EN MATERIAS DE CIBERSEGURIDAD

La Superintendencia de Seguridad Social, en uso de las atribuciones que le confieren los artículos 1°, 2°, 3° y 23 de la Ley N°16.395 y el artículo 3° de la Ley N°18.833, ha estimado pertinente impartir instrucciones a las Cajas de Compensación de Asignación Familiar y que tienen por finalidad modificar y complementar lo dispuesto en su Circular N°2.821, de 2012, relacionadas con la gestión del riesgo operacional en materias de ciberseguridad.

I. AGRÉGASE A LA CIRCULAR N°2.821 DE 2012, EL SIGUIENTE NÚMERO "XIII. CIBERSEGURIDAD":

1. Generalidades

1.1. Alcance de las instrucciones impartidas

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 las C.C.A.F. deben 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.

2. Definiciones

a) **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.

b) **Autenticidad:** Principio de seguridad que permite certificar la veracidad del origen de datos, elementos o sistemas.

c) **Ciberataque:** Cualquier incidente cibernético, provocado deliberadamente y que afecte a un sistema informático.

d) **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.

e) **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.

f) **Confidencialidad**: Principio de seguridad que requiere que los datos deben únicamente ser accedidos por el personal autorizado a tal efecto.

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

h) **Gestión de incidentes**: Procedimiento para la detección, análisis, manejo, contención y resolución de un incidente de ciberseguridad y responder ante éste.

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

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**: 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.

l) **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.

m) **Seguridad de la información:** Conjunto de medidas preventivas y reactivas de las 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.

3. Gestión de la seguridad de la información

3.1. Medidas de gestión.

La Caja de Compensación de Asignación Familiar deberá 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 podrá 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. determinará 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 de que la ciberseguridad pueda ser abordada con un sentido de entorno dinámico que debe ajustarse a las necesidades regulatorias y tecnológicas se establecerá 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. deberá 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 deberán ser actualizados anualmente y sometidos a aprobación del directorio e implementados y difundidos por la alta gerencia. Estos planes deberán 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. deberá establecer planes de capacitación y formación para su personal en materia de ciberseguridad.

Por otro lado, la Caja deberá 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. deberá 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.

3.2. **Sistema de gestión de seguridad de la información de la C.C.A.F.**
La Caja deberá 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.

3.3. Elementos de la gestión del sistema de seguridad de la información:

3.3.1. 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.

3.3.2 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. gestionará 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) Considerar 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.

4. Reporte de Ciberincidentes

4.1. Mecanismo de reporte

La C.C.A.F. deberá 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 4.2 y 4.3 siguientes. 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 entenderá formalmente cumplida luego de que la C.C.A.F. haya informado el ciberincidente a través del sistema GRIS, por lo que esta Superintendencia habilitará en dicha plataforma los formularios especiales para el reporte de este tipo de eventos.

Es preciso señalar que los ciberincidentes no deberán ser reportados bajo la figura de Evento de Reporte Inmediato, ni como Hecho Relevante según la Circular Nº2.980. 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 XI. "Sobre el envío de Registro de Información de Pérdidas", utilizando el mismo código de evento.

4.2. 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 5.

4.3. 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 6.

4.4. 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. deberá 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 de que la C.C.A.F. lo considere necesario, podrá solicitar la colaboración de entidades especializadas en materia de ciberseguridad, para la resolución de un ciberincidente.

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

4.5. Contenido de los reportes de Ciberincidentes

La C.C.A.F. deberá 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 deberá 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. deberá mantener una bitácora con el registro de todos los ciberincidentes identificados.

a) **Reporte de alerta de Ciberincidente**

Dentro del plazo de **1 hora**, contado desde la toma de conocimiento del ciberincidente, la C.C.A.F. deberá reportar a través del formulario "Reporte de alerta 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) **Informe parcial de Ciberincidente**

Posteriormente, antes de **6 horas** desde la toma de conocimiento del ciberincidente, la C.C.A.F. deberá reportar a través del formulario "Informe parcial 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 de Ciberincidente**

Finalmente, en un plazo máximo de **10 días hábiles** desde la toma de conocimiento del ciberincidente, la C.C.A.F. deberá reportar a través del formulario "Informe de resolución 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 deberán ser remitidos a través del "Sistema GRIS" ubicado en el sitio web de la Superintendencia.

5. Reporte de Autoevaluación

La C.C.A.F. deberá realizar una autoevaluación anual en cuanto a su desempeño y nivel de madurez. Para esto, deberá elaborar un informe de autoevaluación de gestión de ciberseguridad, conforme a lo establecido en el Anexo 7: "Informe de autoevaluación de la gestión de ciberseguridad", de esta Circular. El proceso de autoevaluación será responsabilidad de la respectiva C.C.A.F., para lo cual podrá contratar a una entidad especialista para estos efectos. El reporte de autoevaluación podrá contener pruebas de "ethical hacking" en la medida que dichas pruebas permitan mejorar el ambiente de ciberseguridad de la Caja.

El informe de autoevaluación deberá 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. El primer reporte deberá ser remitido en marzo de 2023.

II. **Agréganse** los siguientes Anexos: "Anexo 5: Niveles de peligrosidad de los ciberincidentes", "Anexo 6: Niveles de impacto de los ciberincidentes", y "Anexo 7: Informe de autoevaluación de la Gestión de Ciberseguridad".

III. Vigencia

La presente Circular entrará en vigencia a partir del 1° de enero de 2022.

IV. IV: Anexos

ANEXO 5
NIVELES DE PELIGROSIDAD DE LOS CIBERINCIDENTES

Nivel	Clasificación	Tipo de incidente
Crítico	Amenaza Avanzada Persistente	APT: Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.
Muy alto	Código dañino	Distribución de malware: Ej: recurso de una organización empleada para distribuir malware.
		Configuración de malware: Recurso que aloje ficheros de configuración de malware. Ej: ataque de webinjects para troyano.

	Intrusión	Acceso no autorizado a un sistema informático con el fin de conocer sus datos internos, apoderarse de ellos o utilizar sus recursos, acceso no autorizado a Centro de Proceso de Datos.
		Destrucción, inutilización de un sistema de tratamiento de información, la destrucción, alteración de datos contenidos en un sistema de tratamiento de información, cortes de cableados de equipos o incendios provocados.
	Disponibilidad del servicio	Interrupciones: Ej: ataque informático, en qué consiste

Nivel	Clasificación	Tipo de incidente
Alto	Contenido abusivo	Pornografía infantil, contenido sexual o violento inadecuado: Ej: Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
	Código Dañino	Sistema infectado: Ej: Sistema, computadora o teléfono móvil infectado con un rootkit.
		Servidor C&C (Mando y Control): Ej: Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.
	Intrusión	Compromiso de aplicaciones: Ej: Compromiso de una aplicación mediante la explotación de vulnerabilidades de software, como por ejemplo a través de una inyección de SQL.
		Compromiso de cuentas con privilegios: Ej: Compromiso de un sistema en el que el atacante ha adquirido privilegios.
	Intento de Intrusión	Ataque desconocido: Ej: Ataque empleando exploit desconocido.

	Disponibilidad del servicio	DoS (Denegación de servicio): Ej: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
		DDoS (Denegación distribuida de servicio): Ej: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
	Compromiso de la información	Acceso no autorizado a información: Ej: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
		Modificación no autorizada de información: Ej: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.
	Fraude	Pérdida de datos: Ej: pérdida por fallo de disco duro o robo físico.
		Phishing.

Nivel	Clasificación	Tipo de incidente
Medio	Contenido abusivo	Discurso de odio: Ej: ciberacoso, racismo, amenazas a una persona o dirigida contra colectivos.
	Obtención de información	Ingeniería social: Ej: mentiras, trucos, sobornos, amenazas.
		Explotación de vulnerabilidades conocidas: Ej: desbordamiento de buffer, puertas traseras, cross site scripting (XSS).
	Intrusión	Intento de acceso con vulneración de credenciales: Ej: intentos de ruptura de contraseñas, ataque por fuerza bruta.

		Compromiso de cuentas sin privilegios.
	Disponibilidad del servicio	Mala configuración: Ej: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto.
		Uso no autorizado de recursos: Ej: uso de correo electrónico para participar en estafas piramidales.
	Fraude	Derechos de autor: Ej: uso, instalación, distribución de software sin la correspondiente licencia.
		Suplantación: Ej: suplantación de una entidad por otra para obtener beneficios ilegítimos.
	Vulnerable	Criptografía débil: Ej: servidores web susceptibles de ataques POODLE/FREAK.
		Amplificador DDoS: Ej: DNS openresolvers o Servidores NTP con monitorización monlist.
		Servicios con acceso potencial no deseado: Ej: Telnet, RDP o VNC.
		Revelación de información: Ej: SNMP o Redis.
		Sistema vulnerable: Ej: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.

Nivel	Clasificación	Tipo de incidente
Bajo	Contenido abusivo	Spam.
		Escaneo de redes: Ej: peticiones DNS, ICMP, SMTP, escaneo de puertos.

	Obtención de información	Análisis de paquetes (sniffing).
	Otros	Otros: Todo aquel incidente que no tenga cabida en ninguna categoría anterior.

ANEXO 6
NIVELES DE IMPACTO DE LOS CIBERINCIDENTES

Nivel	Descripción
Crítico	Afecta a sistemas clasificados como confidenciales o que contengan información calificada como datos sensibles de acuerdo a la ley.
	Afecta a más del 50% de los procesos que soportan los sistemas de la C.C.A.F.
	Interrupción de la prestación del servicio igual o superior a 12 horas o superior al 40% de los beneficiarios.
	Afecta a más del 50% de sus agencias o centros de atención a nivel nacional.
	Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) afectando a la reputación de terceros.

Nivel	Descripción
Muy Alto	Afecta a la seguridad ciudadana con potencial peligro para bienes materiales.
	Afecta la vida privada y/o la honra de la persona y su familia, y asimismo, la protección de sus datos personales.
	Afecta a más del 40% de los procesos que soportan los sistemas de la C.C.A.F.
	Interrupción de la prestación del servicio igual o superior a 8 horas o superior al 30% de los afiliados.

	Afecta a más del 40% de sus agencias o centros de atención a nivel nacional.
	Daños reputacionales, con eco mediático (amplia cobertura en los medios de comunicación) afectando a la reputación de terceros.
Alto	Afecta a más del 30% de los procesos que soportan los sistemas de la C.C.A.F.
	Interrupción de la prestación del servicio igual o superior a 6 horas o superior al 20% de los afiliados.
	Afecta a más del 30% de sus agencias o centros de atención a nivel nacional.
	Daños reputacionales, con eco mediático (amplia cobertura en los medios de comunicación) que no afecta la reputación de terceros.
Medio	Afecta a más del 20% de los procesos que soportan los sistemas de la C.C.A.F.
	Interrupción de la prestación del servicio igual o superior a 4 horas y superior al 10% de los afiliados.
	Afecta a más del 20% de sus agencias o centros de atención a nivel nacional.
Bajo	Daños reputacionales sin eco mediático.
	Afecta al 10% o más de los sistemas de la C.C.A.F.
	Interrupción de la prestación del servicio igual o superior a 2 horas y superior al 5% de los afiliados.
	Afecta al 10% o más, de sus agencias o centros de atención a nivel nacional.
Sin impacto	No hay ningún impacto apreciable.

ANEXO 7
INFORME DE AUTOEVALUACIÓN DE LA GESTIÓN DE CIBERSEGURIDAD

Para informar acerca de la autoevaluación de Gestión de la Ciberseguridad, establecida en la presente Circular, se ha definido este Anexo "Autoevaluación de la Gestión de la Ciberseguridad", que a continuación se especifica.

La C.C.A.F. podrá anexar información que considere pertinente para dar mayor nivel de detalle a lo informado.

Los campos específicos para reportar son los siguientes:

a) Resultado de autoevaluación: deberá indicar para cada pregunta, el estado en el que se encuentra el cumplimiento de acuerdo con las siguientes opciones:

   i. Cumple: La C.C.A.F. cumple con la implementación de las acciones definidas para el tema especificado.

   ii. Cumple parcialmente: La C.C.A.F. cumple parcialmente con la implementación y ejecución del tema especificado.

   iii. No cumple: La C.C.A.F. no ha implementado ni ejecutado el tema especificado.

b) Descripción del fundamento de la Autoevaluación: incluir el fundamento que explique y justifique la evaluación establecida por la C.C.A.F.

#	Pregunta	Resultado de auto evaluación	Descripción del fundamento de la autoevaluación
1	La Caja ha implementado medidas técnicas y de organización para gestionar los riesgos de seguridad de la información y ciberseguridad de las redes, equipos y sistemas que utilizan para el otorgamiento de las prestaciones. Detallar las medidas.		
2	La Caja ha determinado las medidas de gestión que garanticen la disponibilidad, integridad y confidencialidad de la información. Detallar las medidas.		
3	La Caja cuenta con una política de seguridad de la información y ciberseguridad, establecida por el Directorio.		
4	La Caja ha realizado un levantamiento de los activos de información críticos. Adjuntar documento con el levantamiento de los activos de información.		

5	La Caja ha identificado los riesgos críticos de las tecnologías de la información, individualizando aquellos que afecten la seguridad de la información y ciberseguridad. Adjuntar los riesgos identificados.		
6	La Caja ha establecido formalmente el nivel de riesgos aceptado en materia de tecnologías de Información, considerando además los niveles de disponibilidad mínimos para asegurar la continuidad operacional. Aportar documento de respaldo.		
7	La Caja ha designado a un responsable del diseño, mantención y seguimiento de los riesgos de seguridad de la información y ciberseguridad. Señalar al designado responsable (nombre y cargo).		
8	La Caja ha creado un registro formalmente documentado de los sistemas de información existentes al interior de la organización, señalando qué proceso de negocio gestiona, el área usuaria, identificación de la base de datos y sistema operativo que soporta el aplicativo. Aportar documento de respaldo.		
9	Los criterios de tratamiento del riesgo se encuentran especificados y formalmente documentados. Adjuntar documento correspondiente.		
10	La Caja ha implementado medidas asociadas a la seguridad de acceso físico tanto a los servidores como a la inmediación o a cualquier centro sobre el que se encuentre información sensible. Detallar medidas.		
11	La Caja ha implementado reglas de accesos (identificación y autenticación) a los sistemas de información mediante usuarios individualizados y contraseñas encriptadas.		
12	Las cuentas de usuarios con privilegios de administrador se encuentran formalmente definidas e identificadas, tanto en la base de datos, sistema operativo que soporta el aplicativo y el aplicativo en sí. Aportar detalle.		
13	Existe un procedimiento formalmente documentado que considere las autorizaciones necesarias y perfiles de accesos para los sistemas de información. Aportar documento.		
14	Se ha implementado un monitoreo de accesos periódicos sobre los sistemas con el objeto de identificar accesos no autorizados o sospechosos a los sistemas de información. Aportar informe de resultados.		
15	Se han implementado ambientes de desarrollo y prueba separados del ambiente productivo para los sistemas de información que soportan procesos críticos de la Caja.		

16	Se encuentran formalizados y documentados los hitos de conformidad y autorización frente a un cambio en los sistemas, tanto del área dueña del proceso, así como también la contraparte técnica.		
17	Se considera como parte del proceso de cambios a los sistemas, la documentación de las pruebas de usuario y la respectiva conformidad. Aportar un documento de ejemplo.		
18	Existe un procedimiento formalmente documentado de control y gestión de cambio a los sistemas y datos. Aportar documento.		
19	Existe un procedimiento formalmente documentado de procedimiento de respaldo y restauración de los sistemas críticos. Aportar documento.		
20	Existe un plan formalmente documentado de administración de ciberincidentes. Aportar documento.		
21	La Caja ha considerado en el plan anual de auditoría interna la revisión sobre la consistencia de los datos reportados a los sistemas de información de administración de esta Superintendencia. Aportar informe de resultados.		
22	La Caja ha definido la ejecución de un hacking ético periódicamente. Aportar si aplica.		

ANA PATRICIA Soto Altamirano

Firmado digitalmente por ANA PATRICIA Soto Altamirano
Fecha: 2021.05.26 11:51:17 -04'00'

ANA PATRICIA SOTO ALTAMIRANO
SUPERINTENDENTA DE SEGURIDAD SOCIAL (S)

GOP/CRR/CLLR/RMG/NMM/JAS/JMC/DBG/FMV/LMG
DISTRIBUCIÓN
CAJAS DE COMPENSACIÓN DE ASIGNACIÓN FAMILIAR
INTENDENTE DE BENEFICIOS SOCIALES
DEPARTAMENTO DE FISCALIZACIÓN Y SUPERVIGILANCIA IBS
DEPARTAMENTO DE TECNOLOGÍA Y OPERACIONES
DEPARTAMENTO NORMATIVO IBS