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

6.1 TÍTULO I. RIESGO OPERACIONAL

En el marco de la implementación de un modelo de Supervisión Basada en Riesgos aplicable a las Cajas de Compensación de Asignación Familiar (C.C.A.F.) se instruye sobre la implementación de la gestión del riesgo operacional, de modo que estas entidades puedan implementar las políticas, procesos y destinar los recursos necesarios para gestionar adecuadamente este tipo de riesgo, sin perjuicio de que las C.C.A.F. puedan adoptar otras medidas complementarias para este propósito.

6.1.1 DEFINICIONES

6.1.1.1 Riesgo operacional

Corresponde al riesgo de pérdida debido a la inadecuación o a la falla de los procesos, del personal y de los sistemas internos y/o de los controles internos aplicables o bien a causa de acontecimientos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.

6.1.1.2 Gestión de riesgo operacional

Corresponde al proceso de identificación, medición y control del riesgo operacional que realiza una Caja de Compensación en el desarrollo de las actividades necesarias para el cumplimiento de sus obligaciones establecidas en el marco legal. Éste debe ser implementado y controlado por la Gerencia General de la C.C.A.F., teniendo presente las responsabilidades del Directorio, de los dueños de los procesos, de la Unidad Especializada de Riesgo Operacional, de las unidades internas de Control Interno y/o Auditoría Interna y en general, del personal de la Caja, el cual debe conocer y participar activamente en la gestión del riesgo operacional.

La gestión del riesgo operacional forma parte integral de la Política de Gestión de Riesgo Operacional, la cual debe ser aprobada por el Directorio.

6.1.1.3 Dueño de procesos

Corresponde a aquel trabajador de la C.C.A.F. designado para hacerse responsable de la administración de un proceso y propiciar las mejoras a implementar en éste.

6.1.1.4 Diagrama de procesos

Corresponde a la representación esquemática de las secuencias de un proceso o subproceso mediante un mapa de procesos y su descripción. El responsable de esta documentación es el dueño del proceso.

6.1.1.5 Matriz de riesgos y controles

Corresponde a una herramienta a través de la cual se identifican los riesgos asociados a un proceso o subproceso, su evaluación cualitativa y/o cuantitativa, los controles asociados junto a su efectividad y el nivel de riesgo residual con el objetivo de priorizar, orientar y focalizar el tratamiento de riesgo.

6.1.1.6 Riesgo inherente

Corresponde a aquel riesgo que por su naturaleza no puede ser separado del proceso o subproceso en que éste se presenta. Lo anterior, en el marco del riesgo que debe asumir cada C.C.A.F., de acuerdo al ámbito de desarrollo de sus actividades establecidas por Ley.

6.1.1.7 Riesgo residual

Corresponde al nivel de riesgo remanente que existe sin perjuicio de haberse implementado las medidas mitigadoras de control.

6.1.1.8 Riesgo aceptado

Corresponde al nivel de riesgo que la Caja de Compensación está dispuesta a aceptar en concordancia con la política de gestión de riesgo operacional y sus responsabilidades establecidas en el marco legal que las rige.

6.1.1.9 Evento de Origen

Corresponde al evento, suceso o acontecimiento que da lugar, o tiene como consecuencia, una o más pérdidas cuantificables, o bien que da lugar a una serie de eventos colaterales que también impliquen pérdidas. En otras palabras, es el primer evento que da origen a una serie de pérdidas y/u otros eventos.

6.1.2 ÁMBITO DE APLICACIÓN DE LA NORMATIVA DE RIESGO OPERACIONAL

La C.C.A.F., en su calidad de entidad de previsión social, otorga y paga prestaciones legales de seguridad social, esto es, asignaciones familiares, subsidios de cesantía y subsidios por incapacidad laboral de origen maternal. Esta administración la realizan con cargo a los fondos financieros de dichos regímenes. También administran el régimen de subsidio por incapacidad laboral respecto de sus trabajadores afiliados pertenecientes al FONASA. El financiamiento de los subsidios pagados proviene de una parte de la cotización de salud que se descuenta de las remuneraciones imponibles de dichos trabajadores.

Además, la C.C.A.F. puede establecer y administrar, con recursos propios, prestaciones de bienestar social, que son beneficios de carácter social y familiar a sus trabajadores y pensionados afiliados, distinguiéndose los regímenes de crédito social (que incluye créditos de consumo, hipotecarios, créditos educacionales y a microempresarios), de prestaciones adicionales y prestaciones complementarias.

Por otro lado, también se aplican las presentes instrucciones de riesgo operacional al proceso de afiliación de entidades empleadoras, de trabajadores independientes y de pensionados, así como también a las actividades relacionadas con el ahorro para el leasing habitacional que administra la C.C.A.F.

6.1.3 FACTORES QUE ORIGINAN EL RIESGO OPERACIONAL

6.1.3.1 Procesos internos

La Caja de Compensación debe gestionar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, relacionados al diseño inapropiado de los procesos o a políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos, así como su ajuste a la normativa vigente que les es aplicable. Esto incluye a los procesos propios de la C.C.A.F. que se ejecutan de manera externalizada en proveedores de servicios.

6.1.3.2 Personal

La Caja de Compensación debe gestionar apropiadamente los riesgos asociados al personal, relacionados a la inadecuada capacitación, negligencia, conductas inapropiadas de los mismos, seguridad en el puesto de trabajo, error humano, fraude, robo, huelgas, apropiación de información sensible, entre otros.

6.1.3.3 Tecnología de información

La Caja de Compensación debe gestionar los riesgos asociados a la tecnología de información, relacionados a fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, entre otros aspectos.

6.1.3.4 Eventos externos

La Caja de Compensación debe gestionar los riesgos asociados a eventos externos ajenos al control de la entidad, relacionados por ejemplo a fallas en los servicios básicos, la ocurrencia de desastres naturales, atentados y actos delictivos, entre otros.

6.1.4 EVENTOS DE PÉRDIDA POR RIESGO OPERACIONAL

Los eventos de pérdida por riesgo operacional pueden ser clasificados de acuerdo a las siguientes categorías:

6.1.4.1. Fraude interno

Pérdidas derivadas de algún tipo de actuación cuya finalidad sea defraudar, ya sea apropiándose de bienes indebidamente o incumpliendo regulaciones, leyes o políticas internas de la C.C.A.F., con el objeto de obtener un beneficio ilícito, en el que se encuentre implicado, al menos, un representante de la alta administración, cargo directivo, o un empleado de la C.C.A.F.

6.1.4.2. Fraude externo

Pérdidas derivadas de algún tipo de actuación destinada a defraudar, ya sea apropiándose de bienes indebidamente o incumpliendo la legislación, por parte de un tercero, con el fin de obtener un beneficio ilícito.

6.1.4.3. Relaciones laborales y seguridad en el puesto de trabajo

Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, así como las derivadas de reclamaciones por daños personales, físicos o síquicos, incluidas las relativas a casos de acoso y discriminación.

6.1.4.4. Afiliados, productos y prácticas de negocios

Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación con los afiliados de la Caja o de la naturaleza o diseño de un producto y/o servicio ofrecido en el marco de los regímenes sociales administrados por la C.C.A.F.

6.1.4.5. Daños a activos materiales

Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.

6.1.4.6. Interrupción del negocio y fallos en los sistemas

Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas.

6.1.4.7. Ejecución, entrega y gestión de procesos

Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores.

6.1.5 EXIGENCIAS DE GESTIÓN QUE DEBEN CUMPLIR LAS C.C.A.F. PARA IMPLEMENTAR ADECUADAMENTE EL PROCESO DE GESTIÓN DE RIESGO OPERACIONAL

La Caja de Compensación debe contar con procedimientos documentados y debidamente aprobados para implementar el proceso de gestión de riesgo operacional, los que deben considerar al menos los siguientes elementos:

6.1.5.1 Política de Gestión de Riesgo Operacional

El Directorio de la C.C.A.F. debe aprobar y ordenar la implementación de una Política de Gestión de Riesgo Operacional, destinada a establecer las medidas que debe adoptar la administración de la entidad en dicho ámbito.

La Política de Gestión de Riesgo Operacional debe contener al menos los siguientes elementos:

6.1.5.1.1 Roles y responsabilidades

Se deben definir las obligaciones y responsabilidades de quienes participan en el proceso de gestión de riesgo operacional. La Caja debe poseer una unidad especializada en la administración del riesgo operacional y debe disponer de los recursos necesarios, físicos, humanos y tecnológicos para cumplir a cabalidad con su labor. El tamaño de esta unidad especialista en riesgo operacional estará directamente relacionado con la complejidad y volumen de operaciones de la C.C.A.F., y estar en constante coordinación con las otras unidades especializadas que se preocupan de la gestión del riesgo de crédito, liquidez y mercado. Debe existir consistencia entre la estrategia de gestión del riesgo operacional definida por la entidad y el volumen de sus actividades. Adicionalmente, la política debe establecer la función de Auditoría Interna en la gestión del riesgo operacional que realiza la C.C.A.F.

6.1.5.1.2 Definición de objetivos del proceso de gestión de riesgo operacional

La C.C.A.F. debe establecer los objetivos que persigue la implementación del proceso de gestión de riesgo operacional, los cuales deben estar alineados con sus objetivos estratégicos.

6.1.5.1.3 Definición de riesgos

La C.C.A.F. debe definir con claridad los riesgos operacionales que le corresponde gestionar, con el objetivo de determinar los tipos de riesgos que serán administrados y la forma a partir de la cual, ellos serán gestionados.

6.1.5.1.4 Definición de riesgo aceptado

La C.C.A.F. debe establecer los criterios para determinar el riesgo aceptado, el cual debe ser consecuente con los criterios de evaluación y tratamiento de riesgos y con el marco legal y reglamentario aplicable a la entidad.

6.1.5.1.5 Criterios de evaluación y tratamiento de riesgos

La C.C.A.F. debe definir el criterio de evaluación de riesgo que mejor se adecúe a su contexto organizacional y estratégico. Además, debe especificar los criterios de tratamiento de los riesgos, junto con las variables a considerar en cada una de ellas.

6.1.5.1.6 Criterios de Divulgación de los riesgos a los actores relevantes

La C.C.A.F. debe definir en su política la forma de entrega de información sobre la gestión del riesgo operacional a los actores relevantes (entidades supervisoras, entidades empleadoras, público en general, acreedores, entre otros).

6.1.5.1.7 Periodicidad en la entrega de información al Directorio

La C.C.A.F. debe establecer la forma y periodicidad con la que se informe al Directorio y a la Gerencia General, entre otros, sobre la exposición al riesgo operacional de la Caja y de cada unidad de negocio.

6.1.5.2 Manual de Gestión de Riesgo Operacional

Basándose en la Política, la Caja de Compensación debe establecer procedimientos formales para la gestión de los riesgos que surjan de los procesos asociados a las actividades efectuadas por dichas entidades.

Tales procedimientos deben estar debidamente documentados en un manual de gestión de riesgo operacional que describa las etapas del proceso de gestión de dicho riesgo, junto a los requerimientos de documentación y de informes resultantes, teniendo en consideración lo que se establece en el presente Título I del Libro VI del Compendio de la Ley N°18.833.

En dicho manual, debe estar identificada la unidad responsable de desarrollar, implementar e impulsar la gestión de riesgo operacional en la entidad.

La C.C.A.F. debe contar con un manual de gestión del riesgo operacional que contemple, por lo menos, los siguientes aspectos:

a) Funciones y responsabilidades asociadas con la gestión del riesgo operacional del Directorio, la Gerencia General, el Comité de Riesgos, la Unidad de Riesgos (o la unidad especializada, si corresponde) y las unidades de negocio y de apoyo.

b) Descripción de la metodología aplicada para la gestión del riesgo operacional.

c) El proceso para la aprobación de propuestas de nuevas operaciones, productos y servicios que debe contar, entre otros aspectos, con una descripción general de la nueva operación, producto o servicio de que se trate, los riesgos identificados y las acciones a tomar para su control.

6.1.5.3 Análisis y evaluación de riesgos

La C.C.A.F. debe implementar un proceso estructurado bajo el cual los riesgos son identificados, medidos, monitoreados y controlados, considerando al menos los siguientes aspectos:

6.1.5.3.1 Levantamiento de procesos

La unidad responsable de la gestión de riesgo operacional, debe identificar los procesos y subprocesos en los que se descomponen las actividades efectuadas por la entidad, con total cobertura de sus procesos relevantes, identificando a los respectivos dueños de dichos procesos.

6.1.5.3.2 Diagramas de procesos y matrices de riesgo

Los dueños de procesos deben describir de manera precisa los procesos y/o subprocesos, por medio de diagramas de procesos, matrices de riesgos u otros equivalentes.

6.1.5.3.3 Evaluación de riesgos

La unidad responsable de la gestión de riesgo operacional en conjunto con el dueño de cada proceso debe:

a) Identificar y evaluar los diferentes riesgos y factores que influyen sobre éstos mediante un análisis combinado de riesgo inherente, impacto y probabilidad de materialización, considerando la efectividad de las actividades de control implementadas para mitigar dichos riesgos. A partir de ello, se debe estimar el riesgo residual o nivel de riesgo expuesto. Esta evaluación se debe documentar en una matriz de riesgos y controles.

b) Comparar el resultado de esta evaluación con el nivel de riesgo aceptado, definido en la política de gestión de riesgo operacional.

c) Realizar reevaluaciones de forma periódica de los riesgos de la entidad con el fin de asegurar la visión actualizada de los riesgos a los que se encuentra expuesta la entidad, así como la consideración de un correcto nivel de exposición al riesgo.

d) Mantener actualizada y disponible en todo momento la documentación asociada.

6.1.5.4 Tratamiento de Riesgos

De acuerdo con las prioridades establecidas en la etapa de análisis y evaluación de riesgos, la unidad responsable de la gestión de riesgo operacional, en conjunto con el dueño de cada proceso, debe analizar las distintas opciones para el tratamiento de los riesgos, definidas en la política de gestión de riesgo operacional, preparar planes de acción para su tratamiento y definir la forma en que estos últimos se implementarán.

Esta decisión debe estar documentada en la matriz de riesgos y controles, la cual, en este ámbito, debe indicar para cada proceso o subproceso revisado, a lo menos lo siguiente:

a) Descripción del riesgo.

b) Nivel de riesgo o riesgo inherente.

c) Descripción de la acción a tomar.

d) Responsable de la implementación.

e) Plazo y estado de la implementación.

f) Apoyo de otras áreas de la entidad.

6.1.5.5 Responsabilidades y Estructura Organizacional

La C.C.A.F. debe mantener una estructura organizacional apta para la definición, administración y el control del riesgo operacional, derivado del desarrollo de sus actividades. La estructura organizacional de las entidades debe considerar, al menos:

6.1.5.5.1 Directorio

El Directorio tiene las siguientes responsabilidades específicas respecto a la gestión del riesgo operacional:

a) Definir la política general para la gestión del riesgo operacional.

b) Asignar los recursos necesarios para la adecuada gestión del riesgo operacional, a fin de contar con la infraestructura, metodología y personal apropiados.

c) Pronunciarse sobre la conveniencia de establecer un sistema de incentivos, tanto pecuniarios como no pecuniarios, que fomente la adecuada gestión del riesgo operacional y que no favorezca la toma inapropiada de riesgos.

d) Aprobar el manual de gestión del riesgo operacional.

e) Conocer los principales riesgos operacionales afrontados por la entidad, estableciendo adecuados niveles de riesgo aceptado.

f) Establecer un sistema adecuado de delegación de facultades y de segregación de funciones a través de toda la organización.

g) Obtener aseguramiento razonable que la Caja cuenta con una efectiva gestión del riesgo operacional, y que los principales riesgos identificados se encuentran bajo control dentro de los límites que han establecido.

h) Velar por el cumplimiento de las instrucciones contenidas en este Título I del Libro VI del Compendio de la Ley N°18.833.

6.1.5.5.2 Gerencia General

La gerencia general tiene la responsabilidad de implementar la gestión del riesgo operacional conforme a las disposiciones del Directorio. Por su parte, los gerentes de las unidades organizativas de negocios o de apoyo tienen la responsabilidad de gestionar el riesgo operacional en su ámbito de acción, dentro de las políticas, límites y procedimientos establecidos.

6.1.5.5.3 Comité de Riesgos

La C.C.A.F. debe contar con un Comité de Riesgos, que sesione en forma periódica, instancia en la que se debe abordar de manera adecuada el riesgo operacional. En estos comités deben participar miembros del Directorio y de la Alta Gerencia de la C.C.A.F. Las decisiones y aspectos relevantes tratados en la sesión del Comité deben quedar registrados formalmente.

6.1.5.5.4 Comité de Auditoría

La Caja de Compensación debe contar con un órgano de decisión o Comité de Auditoría, que analice los resultados e informes de auditoría y de control, en términos de riesgo operacional, con el fin de obtener conclusiones y tomar acuerdos que trasladará a las Unidades y Direcciones competentes. El Comité de Auditoría debe debatir materias relativas a Riesgo Operacional en aquellos casos en los cuales a partir del proceso de auditoría interna realizado sobre las metodologías de medición y gestión del Riesgo Operacional surjan aspectos relevantes a discutir en dicha instancia. Las decisiones y aspectos relevantes tratados en la sesión del Comité deben quedar registrados formalmente.

6.1.5.5.5 Unidad Especializada en Riesgo Operacional

La C.C.A.F. debe contar con una unidad especializada de gestión del riesgo operacional que cumpla, entre otras, con las siguientes funciones:

a) Proponer políticas para la gestión del riesgo operacional.

b) Participar en el diseño y permanente actualización del Manual de gestión del riesgo operacional.

c) Desarrollar la metodología para la gestión del riesgo operacional.

d) Apoyar y asistir a las demás unidades de la Caja para la aplicación de la metodología de gestión del riesgo operacional.

e) Evaluación del riesgo operacional, de forma previa al lanzamiento de nuevos productos y ante cambios importantes en el ambiente operativo o informático.

f) Consolidación y desarrollo de reportes e informes sobre la gestión del riesgo operacional por proceso, o unidades de negocio y apoyo.

g) Identificación de las necesidades de capacitación y difusión para una adecuada gestión del riesgo operacional.

h) Otras necesarias para el desarrollo de la función.

i) Informar al Directorio y a la Alta Gerencia periódicamente sobre el cumplimiento de las políticas y procedimientos de la gestión del riesgo operacional.

Esta unidad puede delegar determinadas funciones de evaluación, tales como la realización de pruebas a los procedimientos y controles, a otras personas o entidades calificadas externas. No obstante, dicha unidad seguirá siendo responsable de aquellas funciones, las cuales se efectuarán bajo su propia supervisión.

La C.C.A.F. debe asegurar que la función o unidad especializada de gestión del riesgo operacional cuente con recursos suficientes para el pleno desarrollo de sus actividades, así como independencia suficiente en la toma de decisiones.

6.1.5.5.6 Cultura de Riesgo Operacional

Los funcionarios de la C.C.A.F. deben conocer y dar cumplimiento cabal a la política de gestión de riesgo operacional. Además, debe existir evidencia de la toma de conocimiento de la política.

Asimismo, la C.C.A.F. debe promover la capacitación en la gestión del riesgo operacional de su personal, considerando sus diferentes casuísticas en las responsabilidades de los distintos roles.

6.1.5.5.7 Auditoría Interna

La Unidad y/o Gerencia de Auditoría Interna debe evaluar el cumplimiento de los procedimientos utilizados para la gestión del riesgo operacional de acuerdo con las exigencias contenidas en el presente Título I del Libro VI de este Compendio de la Ley N°18.833.

El rol de la Auditoría Interna debe ser independiente del área encargada de la gestión del riesgo operacional, y debe contar con los recursos necesarios, independencia y objetividad para entregar información para la toma de decisiones al Directorio sobre la calidad de la gestión de los riesgos que realiza la C.C.A.F.

De forma específica, la función de Auditoría Interna debe:

a) Verificar que el sistema de medición del riesgo está correctamente integrado en la gestión de la Caja de Compensación.

b) Analizar la adecuación de las infraestructuras tecnológicas y la captura y mantenimiento de los datos.

c) Verificar el correcto funcionamiento de los procedimientos y herramientas de la gestión del Riesgo Operacional, validando:

- Los datos internos cargados en la Base de Datos de Pérdidas por Riesgo Operacional.
- El rigor en la cumplimentación de cuestionarios.
- La coherencia entre ambas metodologías.
- El adecuado seguimiento de los Planes de Acción.
- Los procedimientos para revisar y actualizar el Marco de Gestión de Riesgo Operacional.
- Los procedimientos de reporte de la información de gestión.

6.1.5.6 Base de datos de pérdida

6.1.5.6.1 Registro de información de pérdidas

La Caja debe contar con una base de datos de los eventos de pérdida por riesgo operacional. Debe tenerse en cuenta que un evento puede tener como efecto una o más pérdidas y que podrían existir recuperaciones directas o indirectas sobre las mismas, por lo cual la C.C.A.F. debe estar en capacidad de agrupar las pérdidas ocurridas por evento. La base de datos debe cumplir con los siguientes criterios:

a) Deben registrarse los eventos de pérdida originados en toda la C.C.A.F., para lo cual la entidad debe contar con políticas, procedimientos de captura, identificación y asignación de roles y responsabilidades y entrenamiento al personal que interviene en el proceso.

b) Deben registrarse de forma diferenciada cada uno de los impactos económicos y recuperaciones, tanto directas como

por seguros, asociadas al evento de pérdidas. Para cada uno de ellos, se deben registrar las categorizaciones, fechas y valores que permitan su completa caracterización sin netear.

c) Debe adelantarse, en lo posible, el reconocimiento y registro por parte de la Caja sobre aquellos eventos de que se tiene conocimiento o certeza razonable que acabarán generando pérdidas por riesgo operacional en la Entidad. Esto incluye a los eventos provisionados.

d) Debe registrarse, como mínimo, la siguiente información referida al evento y a las pérdidas asociadas:

- Código único de identificación del evento.
- Tipo de evento de pérdida, según tipos de eventos señalados en el Anexo N°1: Tipos de evento riesgo operacional nivel I y nivel II del Título I del Libro VI del Compendio de la Ley N°18.833.
- Línea de negocio asociada, según líneas señaladas en el Anexo N°2: Líneas de negocio genéricas para C.C.A.F. del Título I del Libro VIdel Compendio de la Ley N°18.833. Estos cuadros pueden ser actualizados por la Superintendencia. En el caso de que la C.C.A.F. cuente con líneas de negocio internas, éstas deben encontrarse mapeadas a las líneas de negocio definidas en este Título I del Libro VI del Compendio de la Ley N°18.833 y sus procedimientos de asignación documentados.
- Descripción del evento.
- Fecha de ocurrencia o de inicio del evento.
- Fecha de descubrimiento o toma de consciencia del evento.
- Fecha de registro contable del evento.
- Monto(s) bruto(s) de la(s) pérdida(s).
- Monto total recuperado.
- Cuenta(s) contable(s) asociadas.
- Identificación si el evento está asociado con el riesgo de crédito.

6.1.5.6.2 Conciliación contable

La C.C.A.F. debe establecer y ejecutar procedimientos robustos que le permitan asegurar la conciliación de la información registrada en la Base de Pérdidas con el registro contable y que la información de pérdidas por riesgo operacional reflejada en la contabilidad se encuentre debidamente registrada en la Base de Pérdidas.

Dichos procedimientos de conciliación se deben encontrar formalizados y validados.

La C.C.A.F. debe mantener registro de las pruebas periódicas realizadas sobre la conciliación, así como los resultados obtenidos y las acciones mitigantes o correctoras desarrolladas.

6.1.5.6.3 Pruebas de Calidad de Datos

La C.C.A.F. debe desarrollar de forma periódica, por lo menos una vez al año, pruebas específicas que le permitan asegurar la calidad de los datos registrados en la Base de Pérdidas, incluyendo razonabilidad de montos y fechas, así como la concentración o distribución de eventos.

Los procedimientos y el detalle de las pruebas deben estar formalizados en documentos validados.

La C.C.A.F. debe mantener registro de las pruebas periódicas realizadas sobre la calidad de los datos de la Base de Pérdidas, así como los resultados obtenidos y las acciones mitigantes o correctoras desarrolladas.

6.1.5.6.4 Documentación de eventos

La C.C.A.F. debe mantener registro físico, a disposición de la Superintendencia de Seguridad Social, del expediente con los eventos en los cuales la pérdida asociada sea mayor o igual a 40 U.F., o que cumplan con las demás características indicadas en la letra d) del número 1 del Anexo N°3: Formato y diccionario de archivos planos y formulario web del Título I del Libro VI del Compendio de la Ley N°18.833.

6.1.5.7 Planes de contingencia para asegurar capacidad operativa continua de la C.C.A.F.

Como parte de una adecuada gestión del riesgo operacional, las Cajas deben implementar un sistema de gestión de la continuidad del negocio que tenga como objetivo implementar respuestas efectivas para que la operatividad del negocio de la C.C.A.F. continúe de una manera razonable, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la entidad. El plan debe considerar tanto aquellos procesos de soporte o negocio que desarrolle de forma interna la entidad, como aquellos que se encuentren externalizados en proveedores de servicios.

La C.C.A.F. debe realizar de forma periódica, por lo menos una vez al año, pruebas sobre la efectividad de los planes de continuidad de negocio a nivel de la entidad. El plan de dichas pruebas debe quedar documentado, así como los resultados obtenidos y las posibles medidas correctoras identificadas.

Asimismo, la Caja debe contar con un sistema de gestión de la seguridad de la información, orientado a garantizar la integridad, confidencialidad y disponibilidad de la información. En el diseño del sistema de seguridad de la información se debe tener en cuenta qué hay que proteger y por qué, de qué (o quién) se debe proteger y cómo protegerlo. Además, la Caja puede adherir a alguno de los estándares conocidos y aceptados de Seguridad de la Información, de acuerdo al nivel, complejidad y particularidades de las operaciones de cada Caja.

6.1.5.8 Política para administrar el riesgo asociado a actividades externalizadas

Con el fin de gestionar los riesgos operacionales asociados a la subcontratación, la Caja debe establecer políticas y procedimientos apropiados para evaluar, administrar y monitorear los procesos subcontratados, siendo la Caja la responsable última de dichos procesos. Dichas políticas y procedimientos deben considerar:

a) La evaluación del riesgo, que considere a todas las partes involucradas, previa decisión de externalización. Dicha evaluación debe considerar criterios tales como: los montos pagados, el volumen de transacciones y la frecuencia de trato con el proveedor del servicio.

b) El proceso de selección del proveedor del servicio.

c) La elaboración del acuerdo de subcontratación.

d) La gestión y monitoreo de los riesgos asociados con el acuerdo de subcontratación.

e) La identificación de la criticidad del proveedor.

f) La implementación de un entorno de control efectivo.

g) Establecimiento de planes de continuidad, así como sus pruebas periódicas y reporte de resultados.

h) Acceso a la información por parte del Regulador.

Los acuerdos de subcontratación deben formalizarse mediante contratos firmados entre las partes, los cuales deben incluir acuerdos de niveles de servicio, cláusulas de penalizaciones y definir claramente las responsabilidades del proveedor y de la C.C.A.F., así como establecer los mecanismos de control y seguimiento que se consideren necesarios.

6.1.6 MONITOREO Y EVALUACIÓN INTERNA

La C.C.A.F. debe monitorear de forma permanente sus principales riesgos, junto a la efectividad de las actividades de control implementadas.

Los resultados de los monitoreos deben ser informados periódicamente a los miembros del directorio, a la gerencia general y a los dueños de procesos, a través de reportes periódicos. Para tales efectos, la unidad responsable de la gestión de riesgo operacional, debe implementar indicadores para realizar los monitoreos sobre:

a) Los riesgos de la entidad y su evolución

b) La evolución de las pérdidas

c) Los factores de riesgo asociados

d) La efectividad de medidas de control implementadas o existentes

Adicionalmente dicha unidad debe mantener la documentación y el registro de al menos los incidentes más significativos ocurridos y las medidas de mitigación aplicadas los cuales deben permanecer disponibles para su consulta por un periodo de tiempo de al menos cinco años. La documentación señalada anteriormente debe estar disponible para las revisiones que realice esta Superintendencia. Además, la C.C.A.F. debe enviar a esta Superintendencia un informe anual sobre la gestión del riesgo operacional, a más tardar, el último día hábil del mes de marzo del año siguiente. Dicho informe debe contener, al menos, la siguiente información:

a) Pérdidas operacionales y su evolución, diferenciadas por las distintas líneas de negocio y tipología de riesgos

b) Inventario con detalle de las pérdidas más relevantes registradas por la C.C.A.F.

c) Nivel de su exposición a los riesgos operacionales y su distribución a través de las líneas de negocio y categorías de riesgo

d) Hechos relevantes acaecidos dentro de la C.C.A.F. en términos de riesgo operacional

6.1.7 INFORMACIÓN Y COMUNICACIÓN

La unidad responsable de la gestión de riesgo operacional debe mantenerse en constante comunicación con el resto de las unidades de la C.C.A.F. Para ello debe diseñar y emitir reportes periódicos a los diferentes interesados (internos o externos a la entidad). Corresponde considerar a lo menos los siguientes aspectos:

a) La gerencia general debe informar, a lo menos, cada tres meses al directorio, al comité de riesgos y/o de auditoría sobre los principales riesgos de la Caja y los planes de tratamiento adoptados; en este aspecto, incluyendo los planes de tratamiento que se implementarán. De la presentación que se efectúe, su discusión y aprobación, debe quedar constancia en las actas de sesión de directorio correspondientes.

b) La unidad responsable de la gestión de riesgo operacional debe informar oportunamente, o a lo menos trimestralmente, a la gerencia general sobre los procesos revisados, los resultados sobre la efectividad de los controles revisados, el estado de avance de los planes de mitigación acordados con los dueños de procesos, los incidentes registrados y la evolución de los indicadores diseñados para el monitoreo.

c) La unidad responsable de la gestión de riesgo operacional debe informar a los dueños de procesos sobre el resultado de la evaluación de gestión de riesgo operacional relativo a sus procesos, y adicionalmente, debe informar sobre el estado de avance mensual de los planes de acción comprometidos.

d) La unidad responsable de evaluar de forma permanente e independiente la efectividad de las políticas y procedimientos de la gestión de riesgo operacional, debe informar, a lo menos, una vez al año al directorio sobre el cumplimiento de la política y del manual de gestión de riesgo operacional.

e) La gerencia general debe informar a toda la organización, como también al público en general, los lineamientos principales de la gestión de riesgo operacional, al menos a través de la Memoria Anual y la página web, así como cualquier otro medio que la C.C.A.F. estime pertinente.

6.1.8 ACTUALIZACIÓN DE POLÍTICAS Y PROCEDIMIENTOS

Las políticas y procedimientos de gestión de riesgo operacional deben ser constantemente revisados, monitoreados y mantenerse actualizados, de forma tal que se asegure una efectiva identificación de los riesgos y se cuente con los controles adecuados para su mitigación. Estas revisiones deben ser realizadas con una periodicidad de a lo menos de una vez al año.

6.1.9 AUTOEVALUACIÓN

La C.C.A.F. deben efectuar una vez al año, una autoevaluación del cumplimiento de los requisitos del presente Título I del Libro VI del Compendio de la Ley N°18.833, para lo cual debe establecer sus propios indicadores de medición en relación a lo instruido en las presentes instrucciones, los cuales deben ser claros, objetivos y verificables por parte de esta Superintendencia. Dicha pauta debe confeccionarse teniendo en cuenta los diferentes tópicos contemplados en las presentes instrucciones. La autoevaluación que realice una Caja constituye un insumo para las labores de fiscalización que realice esta Superintendencia.

El sistema de gestión y evaluación del riesgo operacional debe ser objeto de una revisión periódica, al menos anual, por parte de la Unidad de Auditoría Interna.

6.1.10 SOBRE EL ENVÍO DE INFORMACIÓN DE REGISTRO DE PÉRDIDAS

La Caja de Compensación debe remitir a esta Superintendencia los días 15 de cada mes (o el día hábil siguiente si éste fuese sábado, domingo o festivo) el registro de información de pérdidas indicado en el número 6.1.5.6.1 del Título I del Libro VI del Compendio de la Ley N°18.833, correspondiente a los archivos planos de: Evento, Impacto y Recuperación, de acuerdo a lo señalado en los Anexo N°3: Formato y diccionario de archivos planos y formulario web y Anexo N°4: Instrucciones generales, ambos del Título I del Libro VI del Compendio de la Ley N°18.833. La información remitida debe corresponder a la registrada al cierre del mes anterior hasta su último día (ya sea sábado, domingo o festivo).

Además del envío de registro de información de pérdidas, las Cajas de Compensación deben informar a esta Superintendencia cada vez, y en el momento que se produzca o llegue a su conocimiento un evento de riesgo, ya sea o no de pérdida, o un conjunto de eventos bajo una misma tipología de riesgo, que tengan un impacto estimado igual o superior a las 40 U.F., o que cumplan con las demás características indicadas en la letra d) del número 1 del Anexo N°3: Formato y diccionario de archivos planos y formulario web del Título I del Libro VI del Compendio de la Ley N°18.833, y que no sean reportados acorde a las

definiciones estipuladas en el numeral 5.2.3. del Título III del Libro V del Compendio de la Ley N°18.833. Para estos efectos, deben realizar el envío de Eventos de Reporte Inmediato, utilizando el sistema de formularios web que proveerá esta Superintendencia para dichos fines, de acuerdo a lo indicado en el Anexo N°3: Formato y diccionario de archivos planos y formulario web del Título I del Libro VI del Compendio de la Ley N°18.833.

La información requerida por el presente Título I del Libro VI del Compendio de la Ley N°18.833, debe ser remitida siguiendo las instrucciones señaladas en la página web de esta Superintendencia (www.suseso.cl) en el link denominado "Proyecto GRIS".

6.1.11 AUTORIZACIÓN DE USUARIOS

Para proceder a la creación de los usuarios autorizados a enviar los reportes detallados en el número 6.1.10 del Titulo I del Libro VI del Compendio de la Ley N°18.833, se requiere que los Gerentes Generales de cada Caja de Compensación envíen el nombre completo, cargo, correo electrónico y teléfono de contacto de dos usuarios que serán los autorizados a reportar.

La información para la creación de usuarios debe ser remitida mediante la plataforma PAE, opción "Otros-Ingresos", debiendo proceder de igual forma para la eliminación de usuarios.

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.

6.1.13 ANEXOS

Anexo N°1: Tipos de evento riesgo operacional nivel I y nivel II

Anexo N°2: Líneas de negocio genéricas para C.C.A.F.

Anexo N°3: Formato y diccionario de archivos planos y formulario web

Anexo N°4: Instrucciones generales

Anexo N°5: Niveles de peligrosidad de los ciberincidentes

Anexo N°6: Niveles de impacto de los ciberincidentes

Anexo N°7: Informe de autoevaluación de la gestión de ciberseguridad