Libro V, Título XIV Instrucciones sobre Administración de Riesgo en las Administradoras de Fondos de Pensiones

Capítulo V. Gestión de Incidentes

1. La Administradora deberá disponer de sistemas, procedimientos y mecanismos de gestión para identificar, registrar, evaluar, controlar, mitigar y monitorear incidentes. Para lo anterior, deberá registrar y actualizar en una Base de Datos de Incidentes, cada uno de los incidentes materializados que afecten o pongan en riesgo la continuidad de las operaciones, los objetivos de los Fondos de Pensiones, la entrega eficiente y oportuna de los servicios, beneficios y prestaciones que la ley establece en favor de sus afiliados y beneficiarios.

La Administradora deberá transmitir dicha información a esta Superintendencia vía transferencia electrónica, de acuerdo a las instrucciones que se establecen para cada etapa.

La Administradora deberá disponer de mecanismos de comunicación para reportar incidentes a los afiliados, los usuarios, partes interesadas, a la industria y a la Superintendencia de Pensiones, cuando estos incidentes afecten la disponibilidad o calidad del servicio o exista el riesgo de afectar a afiliados, empleadores, AFP u otras entidades del sistema previsional.

Para la gestión o tratamiento de los incidentes por parte de la Administradora, deberá aplicar el siguiente procedimiento:

Etapa I - Registro y clasificación

Corresponde a la identificación, registro y clasificación de un incidente.

En esta etapa la Administradora debe informar en forma muy general a la Superintendencia sobre la materialización de un incidente.

a. Base de Datos de Incidentes:

En esta etapa la Administradora deberá registrar en una Base de Datos de Incidentes la siguiente información:

i. N° único de identificación del incidente (código y número del incidente).

ii. Fecha y hora de la identificación del incidente.

iii. Descripción del incidente (descripción general).

iv. Causa(s) probable(s) o identificada(s).

v. Clasificación del incidente: Asignación preliminar o definitiva del tipo de incidente de acuerdo a lo siguiente:

Tipo de incidente:

- Operacional.

- Seguridad de la Información.

- Ciberseguridad.

Definición de tipos de incidentes:

Código y N°	Descripción
INCO - 01	**Incidente operacional:** Relacionados con los procesos de: administración de cuentas, beneficios, inversiones, servicios a los afiliados y tecnológicos. Ejemplos: Indisponibilidad de sistemas, indisponibilidad de sitio Web, indisponibilidad de los sistemas de atención de público, indisponibilidad de Contact Center, realización de transacciones operacionales con error, problemas operacionales en los procesos de administración de cuentas, traspasos de cuentas personales, recaudación, acreditación, cobranza, contabilidad de los fondos, prevención de lavado de activos y financiamiento del terrorismo, inversión de los fondos, decisión de inversión, ejecución de inversiones, perfeccionamiento de inversiones, control de inversiones, valorización, registro y emisión de reportes a la Superintendencia de Pensiones, medición y reporte de los riesgos financieros, evaluación inversión de los fondos, concesión pensiones contributivas, información para concesión beneficios no contributivos, pago pensiones, conciliación fondos estatales de beneficios no contributivos, otros beneficios (Cuota Mortuoria, Herencia, Excedente Libre Disposición), pago de prima del Seguro de Invalidez y Sobrevivencia, evaluación beneficios, etc.
INCSI - 01	**Incidente de seguridad de la información:** Incidente que afecta directamente la disponibilidad, confidencialidad e integridad de la información referida a la administración de los Fondos de Pensiones. Ejemplos: Modificación no autorizada a información, daño físico a Data Center o Centro de Datos, mal uso de cuentas privilegiadas, fuga de información, etc.
INCCI - 01	**Incidente de ciberseguridad:** Uso de información indebida y/o pérdida parcial o total de los sistemas de información que comprometa la operación referida a la administración de los Fondos de Pensiones. Ejemplos: Interrupción de las operaciones o efecto en los sistemas de administración de cuentas o de servicios a los afiliados y clientes como efecto de: Phishing, código malicioso, intentos de intrusión, denegación de servicios, DoS, infección por malware, suplantación de identidad, etc.

Definición de tipos de incidentes

vi. Proceso(s) afectado(s): Nombre del o de los procesos afectados por la incidencia.

vii. Dependencia(s) afectada(s): Nombre de la Gerencia, Subgerencia o áreas que han sido afectadas por la incidencia.

viii. Activo(s) de información: Nombre del o los activos de información afectados.

ix. Proveedor involucrado: en caso de que el incidente haya sido provocado por el proveedor en el que se ha externalizado el servicio, indicar el nombre y RUT del o los proveedores involucrados y datos de su contacto dentro de la Administradora.

x. Identificación del responsable de reportar la incidencia a la Superintendencia: Nombre, apellidos, cargo, teléfono y correo electrónico de la persona que reporta la incidencia a la Superintendencia de Pensiones.

b. Envío de reporte de incidentes a la Superintendencia

Una vez identificado el incidente, la Administradora deberá transmitir a esta Superintendencia vía transferencia electrónica un primer informe, de acuerdo a lo descrito en la letra a. Base de Datos de Incidentes, de esta etapa.

El mencionado informe deberá ser enviado en cualquier horario, tanto en días hábiles como inhábiles, en el plazo máximo de 30 minutos de identificado el incidente.

El no contar con toda la información no debe ser impedimento para el envío del informe dentro del plazo antes definido. La información no reportada deberá ser completada y comunicada en la medida que disponga de ella.

Etapa II - Evaluación y análisis

Corresponde a la descripción de las características del incidente, y a la realización de acciones o actividades de evaluación y análisis del incidente con el objeto de evitar su propagación y disminuir los daños o consecuencias potenciales.

Esta corresponde a una etapa más avanzada en la evolución del incidente, en la cual la Administradora debe reportar a la Superintendencia información de su origen y efectos.

a. Base de Datos de Incidentes:

En esta etapa la Administradora deberá completar o actualizar la información de la Base de Datos de Incidentes, considerando los siguientes campos:

i. Causa(s) probable(s) o identificada(s): Describir de forma breve las causas probables que podrían haber originado la incidencia. Se actualiza o complementa lo registrado en la letra a. Base de Datos de Incidentes, de la Etapa I de este Capítulo.

ii. Indicar canales de atención y servicios y/o productos afectados ya sea por su disponibilidad o calidad en su funcionamiento. Tales como:

- Servicios a los afiliados: Sitio web, aplicaciones móviles, correo electrónico, sucursales y centros de servicios, cambio de fondos, simulación de pensiones, traspasos, retiros de fondos, entre otros.

- Procesos operacionales: Traspasos, cambio de fondo, recaudación, acreditación, actualización de cuentas personales, pago de pensiones, entre otros.

iii. N° estimado de afiliados o clientes afectados directamente por la incidencia.

iv. N° estimado de cuentas personales afectadas.

v. Tipo estimado de cuentas personales afectadas, según la siguiente clasificación:

Código	Descripción
CCICO	Cuenta de capitalización individual de cotizaciones obligatorias
CAV	Cuenta de ahorro voluntario
CAI	Cuenta de ahorro de indemnización
CCICV	Cuenta de capitalización individual de cotizaciones voluntarias
CCIDC	Cuenta de capitalización individual de depósitos convenidos
CCIAV	Cuenta de capitalización individual de afiliado voluntario
CAPVC	Cuenta individual de ahorro previsional voluntario colectivo

b. Envío de reporte de incidentes a la Superintendencia

La Administradora deberá enviar un informe de actualización de la Base de Datos de Incidentes, con la información descrita en la letra a. Base de Datos de Incidentes, de esta etapa.

El mencionado informe se deberá enviar en el plazo máximo de 72 horas, luego de identificado el incidente.

El no contar con toda la información no debe ser impedimento para el envío del informe dentro del plazo antes definido. La información no reportada deberá ser completada y comunicada en la medida que disponga de ella.

Etapa III - Resolución, reparación y cierre

Corresponde a las medidas adoptadas para corregir el incidente de forma oportuna, debiendo incluir planes, actividades o proyectos que haya determinado para adoptar medidas tendientes a prevenir o mitigar la ocurrencia del incidente.

En consecuencia, se requiere que una vez que se haya analizado el incidente la Administradora remita un informe final a la Superintendencia en el que se analice el incidente, sus efectos y las medidas preventivas de control que se adopten.

a. Base de Datos de Incidentes:

En esta etapa la Administradora deberá completar o actualizar la información de la Base de Datos de Incidentes, considerando los siguientes campos:

i. Tipo de mitigación realizada: Categorizar el tipo de mitigación, de acuerdo a la siguiente escala:

01: Total, solución definitiva del incidente.

02: Parcial, solución alternativa del incidente, para que posteriormente, se implemente una solución total.

03: Nula, no se ha determinado una solución parcial o total del incidente.

ii. Descripción de la solución implementada para reparar el incidente.

iii. Individualización del o los proveedores involucrados directamente en la causa del incidente, registrando su nombre y RUT, y datos de su contacto dentro de la Administradora.

iv. Individualización del responsable de la solución: Indicar el responsable de la reparación del incidente, señalando nombre, cargo y datos de contacto.

v. Causa final de origen: Describir la razón de ocurrencia final de la incidencia.

vi. Duración incidente: Indicar el tiempo total en que el incidente materializado, se mantuvo desde su identificación hasta su reparación o solución.

vii. Cuentas personales afectadas: Indicar el impacto patrimonial en pesos y cuotas que la incidencia ha tenido en los Fondos de Pensiones y en las cuentas personales involucradas.

viii. N° de afiliados o clientes afectados directamente por la incidencia.

ix. N° de cuentas personales afectadas.

x. Tipo de cuentas personales afectadas, según definición en el numeral v., de la letra a. Base de Datos de Incidentes, de la Etapa II, del presente Capítulo.

xi. Costos del incidente: Indicar los costos del daño ocasionado por el incidente en pesos.

xii. Costos de mitigación y/o solución: Indicar los costos totales que significó para la Administradora efectuar actos de mitigación, recuperación, puesta en marcha y reparación total de los daños causados por el incidente.

xiii. Experiencia adquirida: describir la experiencia adquirida, incluyendo el establecimiento de medidas preventivas o planes de acción para mitigar el impacto o evitar la ocurrencia de incidentes similares.

xiv. Fecha y hora de la mitigación del incidente.

xv. Fecha y hora de cierre del incidente.

b. Envío de reporte de incidentes a la Superintendencia

Una vez cerrado el incidente y en un tiempo máximo de 48 horas, la Administradora deberá enviar un informe de actualización de la Base de Datos de Incidentes, con la información descrita en la letra a. Base de Datos de Incidentes, de esta etapa.

El no contar con toda la información no debe ser impedimento para el envío del informe dentro del plazo antes definido. La información no reportada deberá ser completada y comunicada en la medida que disponga de ella.

2. Difusión hacia los afiliados y otros

Al tratarse de incidentes que afecten la calidad o continuidad de los servicios a los afiliados o se trate de un hecho de público conocimiento, la Administradora, será responsable de comunicar oportunamente a sus afiliados y usuarios, y partes interesadas sobre la ocurrencia de dicho incidente. En relación con los afiliados y usuarios, las comunicaciones deberán realizarse a través de sus canales presenciales, digitales, remotos y otros medios que disponga la Administradora dejando registro auditable de su envío.

3. Difusión a las entidades del sistema previsional

Con el objetivo de lograr sinergias y mitigar el riesgo de propagación de un incidente a las entidades que conforman el Sistema Previsional, sobre todo en aquellos casos en que un hecho pudiera afectar a otras Administradoras de Fondos de Pensiones o a la Administradora de Fondos de Cesantía, la AFP involucrada será responsable de comunicarles oportunamente el incidente, a través del mecanismo que acuerden entre ellas.

La información debe ser comunicada en el más breve plazo posible.

La Superintendencia deberá tener acceso a estas comunicaciones para efectos de fiscalización.

Las comunicaciones entre entidades deben mantenerse hasta que el incidente haya sido superado o cerrado, dejando registro auditable de su envío. Las Administradoras deberán acordar e implementar las medidas necesarias para resguardar la reserva de la información intercambiada.

La comunicación entre las Administradoras debe contemplar a lo menos una breve descripción de los hechos que permitan determinar claramente el tipo de incidente, indicando los canales o servicios afectados, observando las disposiciones de la Ley N° 19.628, sobre Protección de la Vida Privada o aquella que la modifique o reemplace.

4. Organización

La Administradora deberá designar un responsable y un suplente para realizar los reportes y efectuar las comunicaciones con esta Superintendencia.

Con la finalidad de determinar acciones correctivas u oportunidades de mejora respecto de la Gestión de Incidentes y análisis de la Gestión de Incidentes, la AFP deberá presentar sus causas y planes de acción en un comité para su revisión y seguimiento.

Nota de actualización: Este Capítulo fue incorporado por la Norma de Carácter General N° 298, de fecha 6 de junio de 2022.