# DIRECTIVA DE GERENCIA GENERAL

**NORMAS Y PROCEDIMIENTOS PARA LA GESTIÓN DE INCIDENTES DE PROTECCIÓN DE LOS BANCOS DE DATOS PERSONALES**

**DGG N° 16-GG-2021**

**San Isidro, 28/09/2021**


## 1. FINALIDAD

Establecer las disposiciones, actividades y responsabilidades para notificar y gestionar de manera estándar los incidentes que puedan comprometer la seguridad de los bancos de datos personales en posesión de la Caja de Pensiones Militar Policial (CPMP).

## 2. REFERENCIA LEGAL Y NORMATIVA

- Decreto Ley Nº 21021 – Ley de Creación de la Caja de Pensiones Militar-Policial y sus modificatorias
- Decreto Supremo Nº 005-75-CCFA – Reglamento del Decreto Ley Nº 21021 y sus modificatorias
- Ley Nº 29733 – Ley de Protección de Datos Personales y sus modificatorias
- Decreto Supremo Nº 003-2013-JUS – Reglamento de la Ley de Protección de Datos Personales y sus modificatorias
- Constitución Política del Perú artículo 2, numeral 6
- Ley Nº 27806 – Ley de Transparencia y Acceso a la Información Pública
- Decreto Supremo Nº 072-2003-PCM – Reglamento de la Ley de Transparencia y Acceso a la Información Pública y sus modificatorias
- Decreto Legislativo Nº 1353 – Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la Regulación de la Gestión de Intereses
- Manual de Organización y Funciones de la Caja de Pensiones Militar Policial
- Directiva de Consejo Directivo DCD Nº 13-2019 – Políticas y Objetivos de Protección de Datos Personales
- Directiva de Gerencia General DGG Nº 01-GG-2020 – Normas y Procedimientos del Sistema de Gestión de Protección de Datos Personales
- Directiva de Gerencia General DGG Nº 13-GG-2021 – Glosario del Sistema de Gestión de Protección de Datos Personales

## 3. ALCANCE

Las disposiciones contenidas en la presente directiva comprenden a las unidades orgánicas de la CPMP que gestionen los bancos de datos personales.

## 4. DISPOSICIONES GENERALES

**4.1** Es aplicable ante cualquier incidente que afecte a la seguridad de los bancos de datos personales.

**4.2** En cualquier caso, se llevan a cabo las acciones descritas en los numerales 5.1, 5.2 y 5.3 de la presente directiva.

**4.3** Se ejecutan las acciones descritas en el numeral 5.4 en los casos en que el incidente de seguridad suponga un riesgo alto para los derechos y libertades de los afectados.

**4.4 Responsabilidades**

Se detalla la matriz de asignación de responsabilidades (RACI) dentro del proceso de gestión de incidentes de seguridad sobre datos de carácter personal. En esta matriz se asigna en cada una de las tareas, una o más responsabilidades representadas por una letra:

**a)** R (responsable): Este rol corresponde a quien efectivamente realiza la tarea.

**b)** A (encargado): Este rol se responsabiliza de que la tarea se realice y es el que debe rendir cuentas sobre su ejecución.

**c)** C (consultado): Este rol posee alguna información o capacidad necesaria para realizar la tarea.

**d)** I (informado): Este rol implica que se debe informar sobre el avance y los resultados de la ejecución de la tarea.

| Tareas / Recurso | Comité de Riesgos | Responsable del tratamiento de los bancos de datos personales | Gestor del tratamiento de los datos personales | Responsable de la seguridad de los bancos de datos personales | Participante del tratamiento de los bancos de datos personales |
|---|---|---|---|---|---|
| Comunicar el incidente | I | I | I | I | R / A |
| Registrar el incidente | I | R / A | I / C | I | |
| Evaluar el incidente | I / C | R / A | I / C | I / C | |
| Notificar a la Autoridad Nacional de protección de datos personales | I | R / A | I | I | |
| Notificar a los afectados | A | R | I | I | |

### 4.5 Comunicación del incidente

**4.5.1** Todo el personal está obligado a comunicar cualquier incidencia de seguridad relativa a los datos de carácter personal al Gestor del tratamiento de datos personales.

**4.5.2** Las incidencias pueden aparecer en todas las actividades relacionadas con el manejo y gestión de información en formato físico o bases de datos lógicos que almacenen datos de carácter personal, así como en el desarrollo de las actividades que afecten a la seguridad de los datos contenidos en las mismas.

**4.5.3** A continuación, se cita algunos ejemplos de incidencias:

**a)** Crear una base de datos de carácter personal sin realizar la solicitud de registro en la Autoridad Nacional de Protección de Datos Personales.
**b)** Recabar datos de carácter personal sin la autorización del afectado y sin informarle de sus derechos.
**c)** Uso de los datos de carácter personal con una finalidad diferente a la registrada en la Autoridad Nacional de Protección de Datos Personales.
**d)** Intento o violación del control de acceso físico y de las bases de datos.
**e)** Alterar bases de datos (borrado, modificación o inclusión de datos que atente contra la calidad de las bases de datos).
**f)** Sacar datos en soportes sin la autorización pertinente.
**g)** Sacar datos en soportes diferentes a los autorizados en el registro de la base de datos.
**h)** Incumplir los plazos establecidos para resolver y contestar las solicitudes para ejercer los derechos del interesado.
**i)** Usar ilícitamente datos de carácter personal.
**j)** Ejecutar el proceso de recuperación de datos.
**k)** Gestionar incorrectamente los *backups*.
**l)** Pérdida de activo material (teléfono de trabajo, portátiles, entre otros).
**m)** Imposibilidad de acceder al sistema con nuestro usuario/contraseña habitual.
**n)** Contraseña de acceso posiblemente comprometida.
**o)** Comportamiento anormal del sistema (información incompleta o irreal, fallos inesperados, entre otros).

**4.5.4** Las incidencias relativas a datos de carácter personal no se limitan al tratamiento automatizado, sino que también incluyen los medios de tratamiento no automatizado. Así pues, las incidencias que afecten a dichos medios, como por ejemplo la pérdida de listados en papel con datos de carácter personal, deben ser también obligatoriamente reportadas.

**4.6 Evaluación del incidente**

**4.6.1** La categoría o nivel de criticidad del incidente respecto a la seguridad de la información afectada, sigue la clasificación genérica, en la que se puede distinguir entre:

**a)** Crítico: Afecta a datos sensibles de gran volumen y en poco tiempo.

**b)** Muy alto: Cuando dispone de capacidad para afectar a información valiosa, en cantidad apreciable.

**c)** Alto: Cuando dispone de capacidad para afectar a información valiosa.

**d)** Medio: Cuando dispone de capacidad para afectar a un volumen apreciable de información.

**e)** Bajo: Escasa o nula capacidad para afectar a un volumen apreciable de información.

**4.6.2** Adicionalmente pueden existir escenarios técnicos que pueden dar lugar a un incidente:

**a)** 0-day (vulnerabilidad no conocida): Vulnerabilidad que permite a un atacante el acceso a los datos en la medida en que es una vulnerabilidad desconocida. Esta vulnerabilidad estará disponible hasta que el fabricante o desarrollador la resuelva.

**b)** APT (ataque dirigido): Se refiere a diferentes tipos de ataques dirigidos normalmente a recabar información fundamental que permita continuar con ataques más sofisticados. En esta categoría se encuadraría, por ejemplo, una campaña de envío de correo electrónico con *software* malintencionado a empleados de una empresa hasta conseguir que alguno de ellos lo instale en su equipo y proporcione una puerta de entrada al sistema.

**c)** Denegación de servicio (DoS/DDoS): Ciberataque que consiste en inundar de tráfico un sistema teniendo como objetivo inhabilitar el

uso de un sistema, una aplicación o una máquina, con el fin de bloquear el servicio para el que está destinado.

**d)** Acceso a cuentas privilegiadas: El atacante consigue acceder al sistema mediante una cuenta de usuario con privilegios avanzados, lo que le confiere libertad de acciones. Previamente deberá haber conseguido el nombre de usuario y contraseña por algún otro método, por ejemplo, un ataque dirigido.

**e)** Código malicioso: piezas de software cuyo objetivo es infiltrase o dañar un ordenador, servidor u otro dispositivo de red con finalidades muy diversas. Una de las posibilidades para que el código dañino alcance a una organización es que un usuario lo instale de forma involuntaria.

**f)** Compromiso de la información: Recoge todos los incidentes relacionados con el acceso y fuga, modificación o borrado de información no pública.

**g)** Robo y/o filtración de datos: Se incluye en esta categoría la pérdida/robo de dispositivos de almacenamiento con información.

**h)** Desfiguración (*Defacement*): Es un tipo de ataque dirigido que consiste en la modificación de la página web de la CPMP con la intención de colgar mensajes reivindicativos de algún tipo o cualquier otra intención. La operativa normal de la página web queda interrumpida, produciéndose además daños reputacionales.

**i)** Explotación de vulnerabilidades de aplicaciones: Cuando un posible atacante logra explotar con éxito una vulnerabilidad existente en un sistema o producto consiguiendo comprometer una aplicación de la organización.

**j)** Ingeniería social: Son técnicas basadas en el engaño, normalmente llevadas a cabo a través de las redes sociales, que se emplean para dirigir la conducta de una persona u obtener información sensible. Por ejemplo, el usuario es inducido a pulsar sobre un enlace haciéndole pensar que es lo correcto.

### 4.7 Notificación del incidente

#### 4.7.1 Notificación a la Autoridad Nacional de Protección de Datos Personales

**a)** Cuando se tenga conocimiento de que se ha producido una brecha de la seguridad de los datos personales sin dilación y, a más tardar

en los tres (3) días hábiles siguientes a tener constancia se debe realizar la correspondiente notificación a la Autoridad Nacional de Protección de Datos Personales.

**b)** Se considera que se tiene constancia de una brecha de seguridad cuando hay una certeza de que se ha producido y se tiene conocimiento suficiente de su naturaleza y alcance.

**c)** Cuando la notificación inicial no sea posible en el plazo de tres (3) días hábiles, la notificación deberá realizarse igualmente a posteriori, y en ella deberán constar y justificarse los motivos de la dilación.

**d)** Las notificaciones deben ser sean claras, concisas y que incluyan la información necesaria para que puedan ser analizadas adecuadamente.

### 4.7.2 Notificación al Titular de datos personales

Se notifica a los afectados a más tardar a los tres (3) días hábiles siguientes de ocurrido el incidente, con el objetivo de permitir a estos la toma de medidas para protegerse de las consecuencias del incidente.

### 4.7.3 Excepción a la notificación / comunicación

**a)** No será necesaria la notificación a Autoridad Nacional de Protección de Datos Personales cuando el responsable de la seguridad de los bancos de datos personales pueda demostrar, de forma fehaciente, que la brecha de la seguridad de los datos personales no entraña un riesgo para los derechos y las libertades de las personas físicas.

**b)** Por ejemplo, si los datos ya se encontraban públicamente disponibles y su revelación no entraña ningún riesgo hacia el titular de los datos.

**c)** Asimismo, no será necesaria la comunicación a los afectados cuando:

- El responsable de la seguridad de los bancos de datos personales ha tomado medidas técnicas y organizativas adecuadas, como que los datos no sean inteligibles para personas o máquinas no autorizadas con anterioridad a la brecha de seguridad de datos personales, mediante el uso de: cifrados de datos de última generación, minimización,

disociación de datos, acceso a entornos de prueba sin datos reales, entre otros.

- Por ejemplo, es probable que no sea necesaria la notificación si se pierde un dispositivo móvil y los datos personales que contiene están cifrados. Sin embargo, sí que es posible que se requiera de notificación si esta fuera la única copia de los datos personales o, por ejemplo, la clave de cifrado en posesión del responsable estuviera comprometida.

- El responsable de la seguridad de los bancos de datos personales ha tomado con posterioridad a la brecha de seguridad de datos personales las medidas de protección que mitiguen total o parcialmente el posible impacto para los afectados y garanticen que ya no hay posibilidad de que el alto riesgo se materialice. Por ejemplo, mediante la identificación y puesta en marcha inmediatamente de las medidas contra la persona que ha accedido a los datos personales antes de que pudieran hacer algo con ellos.

- Cuando la notificación a los afectados suponga un esfuerzo desproporcionado a nivel técnico y organizativo. Por ejemplo, cuando los detalles de contacto se hayan perdido como resultado de la brecha, o aquellos casos en los que se tenga que desarrollar un nuevo sistema o proceso para realizar la notificación, o se requiera la dedicación excesiva de recursos internos para la identificación de los afectados. Ante esta situación, se realizará la notificación de manera pública a través de los canales establecidos por el responsable.

# 5. DESCRIPCIÓN DE LOS PROCEDIMIENTOS

## 5.1 Comunicación del incidente

El personal comunica cualquier incidencia de seguridad relativa a los datos de carácter personal al Gestor del tratamiento de los datos personales, mediante el buzón de correo electrónico datospersonales@lacaja.com.pe o bien a través del formulario ubicado en el Portal Previsional.

## 5.2 Registro del incidente

**5.2.1** Una vez que se ha comunicado el incidente de seguridad, el responsable del tratamiento de los bancos de datos personales registra formalmente dicho incidente de seguridad. En este sentido, se detalla al menos la siguiente información:

**a)** Tipo de incidencia.

**b)** Descripción de la incidencia.

**c)** Fecha y hora de la notificación.

**d)** Usuario que reporta la incidencia.

**5.2.2** En el caso de que sea necesario, el responsable del tratamiento de los bancos de datos personales coordina con el responsable del tratamiento de datos personales para el análisis del incidente de seguridad. Adicionalmente, el responsable del tratamiento de los bancos de datos personales puede solicitar soporte técnico del participante del tratamiento de los bancos de datos personales durante la fase de análisis del incidente.

## 5.3 Evaluación del Incidente

**5.3.1** Una vez registrado el incidente de seguridad, el responsable de la seguridad de los bancos de datos personales evalúa el incidente de seguridad.

**5.3.2** En caso de que el responsable de la seguridad de los bancos de datos personales lo considere oportuno, con base a la criticidad del incidente, convoca al Comité de Riesgos con el fin de evaluar el impacto del incidente en el grupo.

## 5.4 Notificación del incidente

### 5.4.1 Notificación a la Autoridad Nacional de Protección de Datos Personales

**a)** Una vez que el responsable del tratamiento de los bancos de datos personales tenga conocimiento de que se ha producido una brecha de la seguridad de los datos personales efectúa la correspondiente notificación a la Autoridad Nacional de Protección de Datos Personales sin dilación y, a más tardar a los tres (3) días hábiles siguientes a tener constancia. Se considera que se tiene constancia de una brecha de seguridad cuando hay una certeza de que se ha producido y se tiene conocimiento suficiente de su naturaleza y alcance.

Esta comunicación debe contener la siguiente información:

- Datos identificativos y de contacto de:

**i.** Entidad / Responsable del tratamiento de los bancos de datos personales.
**ii.** Titular de banco de datos personales (si está designado) o persona de contacto.
**iii.** Indicación de si se trata de una notificación completa o parcial. En caso de tratarse de una notificación parcial indicar si se trata de una primera notificación o una notificación complementaria.

- Información sobre la brecha de seguridad de datos personales:

**i.** Fecha y hora en la que se detecta.
**ii.** Fecha y hora en la que se produce el incidente y su duración.
**iii.** Circunstancias en que se haya producido la brecha de seguridad de datos personales (por ejemplo, pérdida, robo, copia, entre otros).
**iv.** Naturaleza y contenido de los datos personales en cuestión.
**v.** Resumen del incidente que ha causado la brecha de seguridad de datos personales (con indicación de la ubicación física y del soporte de almacenamiento).
**vi.** Posibles consecuencias y efectos negativos en los afectados.
**vii.** Categoría de los datos afectados y número de registros afectados.
**viii.** Categoría y número de individuos afectados.
**ix.** Posibles cuestiones de carácter transfronterizo, indicando la posible necesidad de notificar a otras autoridades de control.

**b)** Si en el momento de la notificación, no fuese posible facilitar toda la información, el responsable del tratamiento de los bancos de datos personales realiza una primera notificación en la que informa que proporcionará más información a posteriori. Así como aportar información adicional mediante comunicaciones intermedias a la Autoridad Nacional de Protección de Datos Personales bajo petición de esta, o cuando el responsable del tratamiento de los bancos de datos personales considere adecuado actualizar la situación de esta.

### 5.4.2 Notificación al Titular de datos personales

En el caso de que se produzca un incidente de seguridad que suponga un riesgo alto para los derechos y libertades de los afectados, el Gestor

del tratamiento de datos personales comunica a los afectados mediante correo electrónico o por teléfono e incluye como mínimo la siguiente información:

- Naturaleza del incidente.
- Datos personales comprometidos.
- Recomendaciones al Titular de datos personales.
- Medidas correctivas implementadas.

**CAJA DE PENSIONES MILITAR POLICIAL**

RICARDO MEDINA PALOMINO
Gerente General (e)