DIRECTIVA DE GERENCIA GENERAL

NORMAS Y PROCEDIMIENTOS PARA LA GESTIÓN DE UN BANCO DE DATOS PERSONALES

DGG N° 20-GG-2021

San Isidro, 28/09/2021

1. FINALIDAD

Establecer las disposiciones, actividades y responsabilidades para realizar la gestión de un banco de datos personales administrado por 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
- Guía de inscripción de Bancos de Datos Personales
- Manual de Organización y Funciones de la Caja de Pensiones Militar Policial
- Manual de Descripción de Cargos 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 16-GG-2021 – Normas y Procedimientos para la Gestión de Incidentes de Protección de los Bancos de Datos Personales

- Directiva de Gerencia General DGG Nº 19-GG-2021 – Normas y Procedimientos para la Gestión de Accesos y Privilegios a los Servicios de Red y Sistemas de Información

3. ALCANCE

Las disposiciones contenidas en la presente directiva comprenden a la Gerencia de Administración y Finanzas, a la Gerencia de Informática, al Departamento de Recursos Humanos y a las unidades orgánicas de la CPMP que gestionen bancos de datos personales.

4. DISPOSICIONES GENERALES

4.1 Identificación de bancos de datos personales existentes

4.1.1 Las unidades orgánicas con apoyo del Oficial de Seguridad de la Información y Ciberseguridad, identifican los bancos de datos personales que gestionan, independientemente de si están inscritos o no, ante la Autoridad Nacional de Protección de Datos Personales.

4.1.2 Las unidades orgánicas con el apoyo del Oficial de Seguridad de la Información y Ciberseguridad, definen si los bancos de datos personales identificados se deben mantener o modificar.

4.1.3 El responsable del registro del banco de datos personales debe inscribir, modificar o cancelar el banco de datos ante la Autoridad Nacional de Protección de Datos Personales.

4.1.4 El Oficial de Seguridad de la Información y Ciberseguridad como responsable de la seguridad de los bancos de datos personales, las solicita al responsable del registro del banco de datos personales, la inscripción de los bancos de datos personales, independientemente de su medio de almacenamiento, incluso cuando solo se utilicen para el tratamiento de datos referidos a la consulta de datos.

4.2 Creación y registro de un banco de datos personales

4.2.1 El Gerente de Administración y Finanzas, como responsable del registro del banco de datos personales debidamente acreditado, presenta la solicitud de inscripción del banco de datos personales ante la Autoridad Nacional de Protección de Datos Personales a fin de iniciar con el proceso de inscripción de la misma.

La solicitud de inscripción es elaborada por el Oficial de Seguridad de la Información, la misma que debe contar con la conformidad del Comité Especializado en Seguridad de la Información y Ciberseguridad.

4.2.2 La solicitud de inscripción, presentada por el responsable del registro del banco de datos personales, debe contener los requisitos exigidos en el Reglamento de la Ley de Protección de Datos Personales, los cuales son:

a) La denominación y ubicación del banco de datos personales, sus finalidades y los usos previstos.

b) La identificación del titular del banco de datos personales, y en su caso, la identificación del responsable del tratamiento de los bancos de datos personales.

c) Tipos de datos personales sometidos a tratamiento en dicho banco.

d) Procedimientos de obtención y el sistema de tratamiento de los datos personales.

e) La descripción técnica de las medidas de seguridad.

f) Los destinatarios de transferencias de datos personales.

4.3 Modificación o cancelación de banco de datos personales

En caso de solicitar una modificación o cancelación de un banco de datos personales; el responsable del registro del banco de datos personales, presenta una solicitud, en la cual indica su código de inscripción en el Registro Nacional de Protección de Datos Personales y declara un domicilio o dirección, a efectos de remitir las notificaciones respectivas.

La solicitud de modificación o cancelación, es elaborada por el Oficial de Seguridad de la Información, la misma que debe contar con la conformidad del Comité Especializado en Seguridad de la Información y Ciberseguridad.

4.4 Subsanación de los requisitos exigidos en el Reglamento de la Ley de Protección de Datos Personales

En caso la solicitud de creación, registro, modificación o cancelación que el responsable del registro del banco de datos personales haya presentado, no cumpla con los requisitos exigidos en el Reglamento de la Ley de Protección de Datos Personales, este debe ser subsanado en un plazo de diez (10) días hábiles.

La elaboración de la solicitud de subsanación de las observaciones es realizada por el Oficial de Seguridad de la Información y Ciberseguridad, en coordinación con las áreas pertinentes, en un plazo interno de seis (6) días hábiles, la misma

que debe contar con la conformidad del Comité Especializado en Seguridad de la Información y Ciberseguridad.

4.5 Seguridad de banco de datos personales

4.5.1 Las medidas de seguridad organizativas son establecidas por los responsables del tratamiento de bases de datos personales de las unidades orgánicas encargadas de recopilar datos:

a) Desarrollar una estructura organizacional con roles y responsabilidades de acuerdo con la proporcionalidad de los datos a proteger.

b) Implementar un documento de compromiso con respecto a los principios de la Ley de Protección de Datos Personales.

c) Llevar un control y registro de los usuarios con acceso al banco de datos personales de la CPMP, con el objetivo de poder identificar al personal con acceso en determinado momento.

d) Revisar periódicamente la efectividad de las medidas de seguridad adoptadas y mantener registros de dicha verificación.

e) Adecuar los sistemas de gestión o aplicaciones existentes que intervengan en el tratamiento de datos personales, conforme a la Ley de Protección de Datos Personales y su reglamento.

f) Adecuar los procesos involucrados y desarrollar los procedimientos documentados para realizar el tratamiento de datos personales a los requisitos establecidos en la Ley de Protección de Datos Personales y su reglamento.

g) Desarrollar un programa de creación de conciencia y entrenamiento en materia de protección de datos personales.

h) Mantener actualizada la directiva de Gerencia General “Normas y Procedimientos para la Gestión de Incidentes de Protección de los Bancos de Datos Personales”.

i) Mantener actualizada la directiva de Gerencia General “Normas y Procedimientos para la Gestión de Accesos y Privilegios a los Servicios de Red y Sistemas de Información”.

4.5.2 Las medidas de seguridad legales son establecidas por el Oficial de Seguridad de la Información y Ciberseguridad en coordinación con el Departamento de Recursos Humanos y la Gerencia Legal y

Cumplimiento:

a) Mantener los formatos de consentimiento para el tratamiento de datos personales, adecuados y de conformidad con la finalidad para lo cual son recolectados.

b) Adecuar los contratos del personal relacionado con el tratamiento de datos personales, al incluir la coherencia con el requisito de confidencialidad establecido en el artículo 17 de la Ley de Protección de Datos Personales.

c) Adecuar los contratos con terceros, al incluir la coherencia con el requisito de confidencialidad establecido en el artículo 17 de la Ley de Protección de Datos Personales.

4.5.3 Las medidas de seguridad técnicas son establecidas por el Oficial de Seguridad de la Información y Ciberseguridad en coordinación con la Gerencia de Informática y las unidades orgánicas:

a) Establecer medidas relacionadas al acceso no autorizado al banco de datos personales.

b) Establecer medidas relacionadas a la alteración no autorizada del banco de datos personales.

c) Establecer medidas relacionadas a la pérdida del banco de datos personales.

d) Establecer medidas relacionadas al tratamiento no autorizado del banco de datos personales.

e) Los ambientes de la CPMP, en donde se procese, almacene o transmita la información esté implementado con controles de seguridad apropiados.

f) Establecer otras medidas complementarias que resulten pertinentes, relacionadas a la seguridad de la información.

4.5.4 Las medidas de seguridad sobre los sistemas informáticos son establecidas por el Oficial de Seguridad de la Información y Ciberseguridad en coordinación con la Gerencia de Informática:

a) El control de acceso a la información de datos personales, además de la gestión de accesos desde el registro de un usuario, la gestión de los privilegios de dicho usuario, la identificación del usuario ante el sistema, entre los que se encuentra usuario-contraseña, entre

otros, y realizar una verificación periódica de los privilegios asignados, los cuales están definidos en un procedimiento documentado a fin de garantizar su idoneidad.

b) Generar y mantener registros que provean evidencia sobre las interacciones con los datos lógicos, los fines de la trazabilidad, la información de cuentas de usuario con acceso al sistema, horas de inicio, cierres de sesión y acciones relevantes. Estos registros deben ser legibles y oportunos, asimismo deben ser custodiados a través de copias de respaldo y tener un destino. Una vez que ya no sean de utilidad, se procede a su destrucción, transferencia, almacenamiento, entre otros.

4.5.5 Las medidas de respaldo de los bancos de datos personales, centralizados en los servidores de la CPMP, son establecidas por la Gerencia de Informática:

La CPMP contempla los mecanismos de respaldo de seguridad de la información del banco de datos personales en el que realiza la verificación de la integridad de los datos almacenados en el respaldo, adicionalmente cuando sea pertinente, la recuperación completa ante una interrupción o daño, al garantizar el retorno al estado en el que se encontraba al momento en que se produjo la interrupción o daño.

4.5.6 Las copias o reproducción autorizada de los documentos con datos personales, son establecidas por los responsables de tratamiento de los bancos de datos personales de las unidades orgánicas:

a) La generación de copias o la reproducción de los documentos con datos personales únicamente puede ser realizada bajo el control del personal designado por la CPMP, con lo cual se restringe la posibilidad de que puedan darse copias no controladas de la documentación con datos especialmente sensibles.

b) La CPMP debe proceder a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior, la misma que puede darse bajo el control de la CPMP o un personal designado por la entidad.

5. DESCRIPCIÓN DE PROCEDIMIENTOS

5.1 Identificación de bancos de datos personales nuevos

5.1.1 Cada unidad orgánica (a través de los participantes del tratamiento de los bancos de datos personales) con apoyo del Oficial de Seguridad de

la Información y Ciberseguridad, identifica los procesos de la entidad, que involucran la identificación de bancos de datos personales.

5.1.2 Posteriormente los participantes del tratamiento de los bancos de datos personales, con apoyo del responsable del tratamiento de los bancos de datos personales y el Oficial de Seguridad de la Información y Ciberseguridad, ejecutan una prueba de recorrido sobre cada proceso, para lo cual identifican los activos de información que contengan información y que puedan contener datos personales, por ejemplo: documentos físicos, archivos digitales, hojas de cálculo, correos electrónicos, mensajes, sistemas, entre otros.

5.1.3 El responsable del tratamiento de los bancos de datos personales, para cada activo de información identificado, realiza las siguientes preguntas:

a) ¿Contiene información sobre "una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados"?

b) ¿Esta información es parte de los procesos formales o ya se encuentra alojada en los activos de información de la CPMP por intermediación de un colaborador (fotografías de índole personal, grabaciones, exámenes médicos propios, direcciones)?

c) ¿Esta información ha sido recabada por medios regulares o podría tener carácter ilícito?

5.1.4 El responsable del tratamiento de los bancos de datos personales, en base a las respuestas obtenidas, evalúa si cada activo de información identificado, tiene información personal sujeta al tratamiento formal de la entidad.

5.1.5 En caso el activo de información identificado, tiene información personal sujeta al tratamiento formal de la entidad, es tratada en el proceso de inventario de banco de datos personales.

5.2 Inventario de banco de datos personales nuevos

5.2.1 El responsable del tratamiento de los bancos de datos personales con apoyo del Oficial de Seguridad de la Información y Ciberseguridad, define los siguientes atributos en el formato inventario de bancos de datos personales:

a) Código: Identificador del banco, inicia en BDP001 y continúa secuencialmente.

b) Nombre: Nombre general del banco de datos personales.

c) Finalidad: Detalla el contenido de la información personal que contiene el banco de datos personales y el fin para el cual es compilado y usado.

d) Instancias**:** Lista la instancia donde se identificó el activo de información, así como cualquier otra donde se tenga conocimiento de que existe una copia de la información:

- Activo de información**:** Nombre del activo de información contenedor (documento, sistema, archivo).
- Tipo**:** Física o digital.
- Ubicación**:** Ubicación real o virtual donde es posible encontrar el activo de información.
- Custodios: Personal con acceso y uso del activo de información que contiene la información personal.

e) Sensible: Se indica si el activo de información contiene información sensible o no, según establece la Ley, se dice que un dato es sensible si son datos: *"…constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual".*

5.2.2 Posteriormente, el responsable del tratamiento de los bancos de datos personales, con apoyo del Oficial de Seguridad de la Información y Ciberseguridad, orientan a los participantes del tratamiento de los bancos de datos personales del proceso para que completen las categorías de datos personales alojadas en el banco, usando la Guía de inscripción de Bancos de Datos Personales de la Autoridad Nacional de Protección de Datos Personales, las cuales son:

a) Datos de carácter identificativo.

b) Datos de características personales.

c) Datos económicos-financieros y de seguros.

d) Datos de carácter social.

e) Datos sensibles.

5.3 Compilación, distribución y validación de los inventarios

5.3.1 El responsable del tratamiento de los bancos de datos personales, con apoyo del Oficial de Seguridad de la Información y Ciberseguridad recopila e integra los distintos bancos de datos personales identificados (debido a que es posible que dos -2- unidades orgánicas declaren un mismo banco), para evitar que exista duplicidad.

5.3.2 Finalmente, el responsable del tratamiento de los bancos de datos personales, distribuye el inventario resultante a las unidades orgánicas declarantes, para su validación.

5.4 Registro del banco de datos personales

5.4.1 El responsable del registro del banco de datos personales presenta ante la Autoridad Nacional de Protección de Datos Personales, una solicitud para la inscripción, modificación o cancelación de un banco de datos personales.

Dicha solicitud es elaborada por el Oficial de Seguridad de la Información y Ciberseguridad, la misma que debe contar con la conformidad del Comité Especializado en Seguridad de la Información y Ciberseguridad.

5.5 Difusión de banco de datos personales

El Oficial de Seguridad de la Información y Ciberseguridad, en coordinación con el responsable del registro del banco de datos personales, publica información referida a la Ley de Protección de Datos Personales y de los bancos de datos personales que la CPMP ha creado, a través del Portal Previsional.

CAJA DE PENSIONES MILITAR POLICIAL

RICARDO MEDINA PALOMINO
Gerente General (e)