DIRECTIVA DE GERENCIA GENERAL

GLOSARIO DEL SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES

DGG N° 13-GG-2021

San Isidro, 28/09/2021

1. FINALIDAD

Establecer los conceptos más trascendentales relacionados al Sistema de Gestión de Protección 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 D.L. 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 y sus modificatorias
- 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 y sus modificatorias
- 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 N° 15-GG-2021 – Normas para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia
- Directiva de Gerencia General DGG N° 14-GG-2021 – Normas para Regular las Transferencias de Datos Personales

3. ALCANCE

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

4. GLOSARIO

4.1 **Arquitectura física:** Representación gráfica de los componentes físicos (servidores, cámaras o videocámaras, monitores, entre otros) del sistema de videovigilancia a través del cual se realiza tratamiento de datos personales.

4.2 **Arquitectura lógica:** Representación gráfica de las conexiones entre los componentes lógicos (software, sistemas, aplicativos, entre otros) del sistema de videovigilancia a través del cual se realiza tratamiento de datos personales.

4.3 **Bloqueo de un dato personal:** Es la medida por la que el responsable de la seguridad de los bancos de datos personales impide el acceso de terceros a los datos personales, asimismo, éstos no pueden ser objeto de tratamiento durante el periodo de bloqueo (físico o lógico). Aplicará durante el periodo en que se esté procesando alguna solicitud de actualización, inclusión, rectificación o supresión, lo cual impide el tratamiento de la información durante dichos periodos.

4.4 **Cámara conectada a Internet:** Cámara o videocámara que se encuentra conectada a internet a través de cualquier identificador (IP u otros) con finalidad de realizar tratamiento de datos personales mediante imágenes, videos o audios.

4.5 **Captación de imágenes y/o sonidos:** Es el proceso técnico que permite la captura de imágenes y/o sonidos en tiempo real mediante cámaras o videocámaras en cualquier medio o soporte tecnológico.

4.6 **Cámara o videocámara:** Dispositivo digital, óptico o electrónico, fijo o móvil, que permita captar, grabar o cualquier otro tratamiento de datos personales a través de imágenes, videos o audios.

4.7 **CD:** Disco compacto.

4.8 **Consentimiento:** Toda manifestación de voluntad, libre, previa, expresa, inequívoca, específica, e informada, mediante la que el interesado acepta el tratamiento de los datos personales que le pertenecen.

4.9 **Consentimiento expreso e inequívoco:** Cuando el consentimiento haya sido manifestado en condiciones que no admitan dudas de su otorgamiento.

Se considera que el consentimiento expreso se otorgó verbalmente cuando el titular lo exterioriza oralmente de manera presencial o mediante el uso de cualquier tecnología que permita la interlocución oral.

Se considera consentimiento escrito a aquel que otorga el titular mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por el ordenamiento jurídico.

La condición de expreso no se limita a la manifestación verbal o escrita.

En sentido restrictivo, se considera consentimiento expreso a aquel que se manifieste mediante la conducta del titular que evidencie que ha consentido inequívocamente.

En el entorno digital también se considera expresa la manifestación consciente en "hacer clic", "cliquear" o "pinchar", u otros similares.

4.10 **Consentimiento informado:** Es la comunicación que se da al Titular de Datos Personales de manera clara, expresa e indubitablemente sobre el tratamiento de sus datos personales, asimismo se le informa sobre la identidad y domicilio del titular del banco de datos personales al que puede dirigirse para revocar su consentimiento o ejercer sus derechos; la finalidad del tratamiento a las que sus datos serán sometidos; la identidad de los que son o pueden ser destinatarios de los datos, la existencia del banco de datos en que se almacenarán; el carácter facultativo u obligatorio de sus respuestas al cuestionario que se le proponga; las consecuencias de proporcionar sus datos personales o de negarse a ello y de ser el caso la transferencia nacional e internacional de datos que se efectúen.

4.11 **Consentimiento libre:** El consentimiento se debe otorgar sin que medie un error, mala fe, violencia o fraude que puedan viciar o afectar la manifestación de voluntad del Titular de Datos Personales.

4.12 **Consentimiento previo:** Debe darse con anterioridad a la recopilación de los datos o en su caso, anterior al tratamiento distinto a aquel por el cual ya se recopilaron.

4.13 **Datos excesivos:** Es aquella información que excede o sale de los límites razonables para lo cual fue solicitado (la finalidad del tratamiento).

4.14 **Datos inadecuados e irrelevantes:** Es aquella información que no es apropiada e importante a las condiciones y objeto de algo (la finalidad del tratamiento).

4.15 **Datos sensibles:** Es aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, hábitos personales que corresponden a la esfera más

íntima e información relativa a la salud física o mental, u otras análogas que afecten su intimidad.

4.16 **Derechos ARCO:** Es el conjunto de facultades a través de los cuales las personas pueden ejercer control sobre sus datos personales, estos son: acceso, rectificación, cancelación y oposición (ARCO).

4.17 **Derecho de acceso:** Es la facultad del titular de solicitar información de sus datos personales incluidos en los bancos de datos de la entidad, la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación y a solicitud de quién se realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos.

4.18 **Derecho de rectificación:** Es la facultad del Titular de Datos Personales de solicitar la modificación de datos en forma de actualización, rectificación e inclusión de los datos personales materia de tratamiento.

4.19 **Derecho de cancelación o supresión:** Es la facultad del Titular del Banco de Datos Personales de eliminar o suprimir los datos personales de un banco de datos, cuando los mismos han dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recopilados, cuando hubiera vencido el plazo establecido para su tratamiento o cuando el Titular de Datos Personales haya revocado su consentimiento para el tratamiento y en los demás casos en los que no están siendo tratados conforme a la Ley de Protección de Datos Personales y a su Reglamento.

4.20 **Derecho de oposición:** Es la potestad del Titular de Datos Personales de oponerse al tratamiento de sus datos o de solicitar el cese del mismo, cuando no hubiera prestado su consentimiento por haber sido tomados de fuente de acceso al público o de haber prestado el consentimiento, acredite la existencia de motivos fundados y legítimos relativos a una concreta situación personal que justifique el cese del ejercicio de este derecho, siempre que, por ley, no se disponga lo contrario.

4.21 **Días:** Días hábiles.

4.22 **Encargo de tratamiento:** Entrega por parte del Titular del Banco de Datos Personales al responsable del tratamiento de los bancos de datos personales en virtud de una relación jurídica que los vincula. Dicha relación jurídica delimita el ámbito de actuación del responsable del tratamiento del banco de los datos personales.

4.23 **Flujo transfronterizo de datos personales:** Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.

4.24 **Gestor del tratamiento de datos personales:** Es el encargado de liderar el cumplimiento de la Ley de Protección de Datos Personales.

4.25 **Grabación:** Es el proceso técnico a través del cual se registra imágenes, videos o audios en cualquier medio o soporte tecnológico, con la finalidad de almacenar o reproducir con posterioridad lo registrado.

4.26 **Inventario documentado:** Lista ordenada de la totalidad de las cámaras u otros dispositivos de videovigilancia, en la cual se debe precisar la ubicación física de los dispositivos, ya sea interna o externa, así como su estado de operatividad.

4.27 **LPDP:** Ley 29733 – Ley de Protección de Datos Personales.

4.28 **Participantes del tratamiento de los bancos de datos personales:** Personal de las diferentes unidades orgánicas que apliquen el tratamiento de uno o varios bancos de datos personales.

4.29 **Perfil:** Conjunto de facultades que se le atribuyen a los usuarios del sistema de videovigilancia que permiten determinar la atribución de sus funciones, en razón de sus posibilidades de accesos al sistema y de gestión de privilegios. Se han definido tres tipos de perfiles.

4.29.1 Perfil administrador: Es la persona que tiene a cargo todas las obligaciones contenidas en la LPDP, su reglamento y la presente directiva. Toda persona natural, jurídica o entidad pública que cuente con sistemas de videovigilancia, para los fines establecidos en esta directiva, debe designar, mediante documento, a la persona que estará a cargo de estas atribuciones, pues será quien responda específicamente por el tratamiento de datos personales que se realice a través del sistema, sin perjuicio de la responsabilidad atribuida al responsable del tratamiento de los bancos de datos personales.

4.29.2 Perfil intermedio: Es aquel a quien el perfil administrador puede delegar determinadas funciones o responder, en defecto del perfil administrador, por ellas. Las funciones que le pueden ser asignadas, mediante documento, están reguladas en esta directiva. El perfil intermedio se encuentra bajo la dirección del perfil administrador.

4.29.3 Perfil básico: Es aquel a quien, de acuerdo al documento de asignación, le compete únicamente las funciones de monitoreo de las cámaras de videovigilancia, seguridad lógica y física del ambiente de videovigilancia y mantener actualizado el inventario documentado de cámaras. Ello, sin perjuicio que estas actividades puedan ser realizadas también por el perfil intermedio y administrador, pudiéndose encontrar incluso bajo su mando o dirección.

4.30 **Persona identificable:** Persona a la cual se le puede identificar mediante tratamientos a los que se refiere la directiva. Se identifica a una persona natural con la captación de su imagen, voz o cualquier otro tratamiento de sus datos que permita hacerlo.

4.31 **Principios:** Es el conjunto de reglas que indican como recoger, tratar y ceder los datos de carácter personal para garantizar la intimidad y demás derechos fundamentales de los ciudadanos. Los principios de la protección de datos personales son: calidad, consentimiento, finalidad, legalidad, proporcionalidad y seguridad.

4.32 **Principio de calidad:** Los datos contenidos en un banco de datos personales, deben ajustarse con precisión a la realidad, ser veraces, exactos y adecuados.

4.33 **Principio de consentimiento:** Para el tratamiento de los datos personales debe mediar el consentimiento de su titular.

4.34 **Principio de finalidad:** El tratamiento de los datos personales no debe extenderse a otro fin que no haya sido establecido de manera inequívoca como tal al momento de su recopilación; se excluyen los casos de actividades de valor histórico, estadístico o científico, o cuando se utilice un procedimiento de disociación o anonimización de datos personales.

4.35 **Principio de legalidad:** El tratamiento de los datos personales se hace conforme a lo establecido en la Ley de Protección de Datos Personales. Se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.

4.36 **Principio de proporcionalidad:** Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que se han recopilado.

4.37 **Principio de seguridad:** El Titular del Banco de Datos Personales y el responsable del tratamiento de los bancos de datos personales deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales que se trate.

4.38 **Principio de disposición de recurso:** La CPMP difunde a sus usuarios, mediante el portal previsional y la Intranet, los diversos mecanismos internos en los cuales pueden ejercer sus derechos a la protección de datos personales; y de considerarlo pertinente, pueden acudir a la Autoridad Nacional de Protección de Datos Personales.

4.39 **Principio de nivel adecuado de protección:** Los datos personales de los usuarios poseen un nivel adecuado de protección, para el flujo transfronterizo de datos personales, con un mínimo de protección equiparable a lo previsto por la Ley Nº 29733 o por los estándares internacionales de la materia, en caso exista flujo transfronterizo.

4.40 **Procedimiento documentado de gestión de acceso:** Documento en el que se establecen los procedimientos y políticas de seguridad a fin de garantizar el acceso seguro a los sistemas, aplicativos y/o equivalentes que realizan tratamiento de datos personales. Dichos accesos son deberán ser definidos mediante procesos de identificación y/o autenticación de los usuarios, así como los responsables de realizar dichos procesos.

4.41 **Procedimiento documentado de gestión de privilegios:** Documento mediante el cual se establecen los procedimientos formales de definición y de aprobación de los perfiles de los usuarios que realizan tratamiento de datos personales, teniendo en cuenta las autorizaciones de acceso y las restricciones del banco de datos automatizado que realiza el tratamiento de datos personales, así como los responsables de realizar el tratamiento de datos personales y de aquellos que llevan a cabo dichos procesos.

4.42 **Procedimiento documentado de verificación periódica de privilegios asignados:** Documento a través del cual se establecen los procedimientos, políticas formales y la periodicidad de revalidación, y la verificación de los privilegios a los usuarios que tienen acceso a datos personales, así como a los responsables de dichos procesos.

4.43 **RLPDP:** Reglamento de la Ley de Protección de Datos Personales.

4.44 **RNPDP:** Registro Nacional de Protección de Datos Personales.

4.45 **Responsable del registro de banco de datos personales**: Es aquél que se encarga de inscribir, modificar o cancelar el banco de datos ante la Autoridad Nacional de Protección de Datos Personales.

4.46 **Responsable del tratamiento de los bancos de datos personales:** Es aquél que decide sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos personales.

4.47 **Responsable de la seguridad de los bancos de datos personales:** Es quien comprende la administración de los controles de seguridad respecto a la información física y digital alojada en los bancos de datos personales.

4.48 **Responsable de la atención del ejercicio de los derechos y contestación:** Es a quien la entidad le otorga la autorización para realizar el trámite de la atención y contestación de las solicitudes del ejercicio de los derechos ARCO.

4.49 **Sistema de videovigilancia:** Conjunto de personas y equipos tecnológicos compuestos por una o varias cámaras de video localizadas estratégicamente e interconectadas entre sí, que permiten el tratamiento de datos personales.

4.50 **Solicitud:** Es el documento por el cual el Titular de Datos Personales realiza un pedido en el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición al Titular del Banco de Datos Personales o Responsable del Tratamiento del Banco de Datos Personales.

4.51 **Solicitud no presentada:** Calidad que se le da a una solicitud remitida a la entidad que contiene defectos no subsanados en los plazos establecidos, por lo que es un requerimiento sobre el cual no se realiza acción.

4.52 **Usuario:** Operador de la plataforma tecnológica a quien se le asignó un perfil determinado.

4.53 **Videovigilancia:** Monitoreo y captación de imágenes, videos o audios de lugares, personas u objetos. La información captada puede o no ser objeto de almacenamiento a través de su grabación.

4.54 **Violación o brecha de seguridad de los datos personales:** Se produce cuando los datos contenidos en sistemas de videovigilancia sufren un incidente de seguridad que da lugar a la violación de la confidencialidad, disponibilidad o integridad de los mismos.

Dichos incidentes de seguridad pueden ser: la destrucción, pérdida o alteración accidental o ilícita de los datos personales transmitidos, conservados y tratados, o la comunicación y/o accesos no autorizados a dichos datos.

CAJA DE PENSIONES MILITAR POLICIAL

RICARDO MEDINA PALOMINO
Gerente General (e)