



PERÚ

Ministerio de Desarrollo Agrario y Riego

Viceministerio de Desarrollo de Agricultura Familiar e Infraestructura Agraria y Riego

Proyecto Especial Pichis Palcazu



Año de la Recuperación y Consolidación de la Economía Peruana

La Merced, 30 DIC. 2025

OFICIO N.º 580 -2025-MIDAGRI-PEPP-CD/DE

Señora:

Robertina Carlota Martínez Valdivia
Jefe (e) Órgano de Control Institucional
Proyecto Especial Pichis Palcazú
Presente. _



ASUNTO : Subsanación de situación adversa - Implementación de Directiva sobre tratamiento de datos personales y sistema de videovigilancia.

- REFERENCIA:**
- a. Oficio N°054-2025-CG/OCI-PEPP
 - b. Oficio N°065-2025-CG/OCI-PEPP
 - c. Informe de Orientación de Oficio N°001-2025-OCI/3380-SOO
 - d. Informe N°507-2025-MIDAGRI-PEPP/UA

Por medio del presente, y en atención a los documentos de la referencia, me dirijo a usted con el fin de informar que la situación adversa identificada en el Informe de Orientación de Oficio N°001-2025-OCI/3380-SOO ha sido subsanada.

Como es de su conocimiento, mediante Oficio N°054-2025-CG/OCI-PEPP de fecha 21 de julio de 2025, el Órgano de Control Institucional a su cargo remitió el Informe de Orientación referido a la "**Carencia de normativa interna que regule el tratamiento de datos personales y la operación, uso y mantenimiento del sistema de videovigilancia del PEPP**".

En respuesta a dicha observación, la Unidad de Administración del PEPP ha implementado las medidas correctivas correspondientes, habiéndose elaborado y aprobado la "**Directiva Interna que regula el Tratamiento de Datos Personales y la Operación, Uso y Mantenimiento del Sistema de Videovigilancia del Proyecto Especial Pichis Palcazú - PEPP**", mediante Resolución Directoral N° 202-2025-MIDAGRI-PEPP-CD/DE.

Con la aprobación de este instrumento normativo, se garantiza el respeto a los derechos fundamentales de las personas y la operación eficiente y legal del sistema de videovigilancia institucional, subsanándose de manera integral la situación adversa identificada por ese Órgano de Control.

Adjunto al presente, remito copia de la Resolución Directoral N° 202-2025-MIDAGRI-PEPP-CD/DE y de la Directiva aprobada, para su conocimiento y fines pertinentes.

Sin otro particular, aprovecho la oportunidad para expresarle los sentimientos de mi especial consideración y estima

GPC/DE
JGAT/UA -
CC.: UA
Archivo



MINISTERIO DE DESARROLLO AGRARIO Y RIEGO
PROYECTO ESPECIAL PICHIS PALCAZU

M.Sc. GUSTAVO PÉREZ CARREÓN
DIR. 71899
Director Ejecutivo

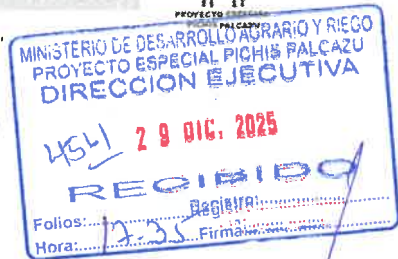
CUT: 1219-2025

Av. Perú s/n Pampa del Carmen – La Merced
Chanchamayo – T: (064) 53-1607
www.pepp.gob.pe – www.midagri.gob.pe

12:27
30/12/2025



"Año de la recuperación y consolidación de la economía peruana"



INFORME N°507-2025-MIDAGRI-PEPP/UA

A : GUSTAVO PEREZ CARREON
Director Ejecutivo – PEPP

DE : Jorge Gerardo Alarcón Tirado
Jefe de la Unidad de Administración
Responsable de la Implementación de Recomendaciones Del Informe De Servicio De Control Posterior

ASUNTO : Implementación y subsanación de situación adversa identificada en Informe de Orientación de Oficio N°001-2025-OCI/3380-SOO - Aprobación de Directiva que regula el tratamiento de datos personales y sistema de videovigilancia.

REFERENCIA : a. Oficio N°065-2025-CG/OCI-PEPP
b. Oficio N°054-2025-CG/OCI-PEPP
c. Resolución Directoral N°202-2025-MIDAGRI-PEPP-CD/DE.

FECHA : La Merced, 29 de diciembre de 2025

Por medio de la presente me dirijo a usted, en atención al documento de la referencia, para informar las acciones adoptadas en respuesta al Informe de Orientación de Oficio N°001-2025-OCI/3380-SOO.

I. Antecedentes

Con fecha 21 de julio de 2025, el Órgano de Control Institucional del PEPP, mediante Oficio N°054-2025-CG/OCI-PEPP, remitió el Informe de Orientación de Oficio N°001-2025-OCI/3380-SOO, referido a la **"Carencia de normativa interna que regule el tratamiento de datos personales y la operación, uso y mantenimiento del sistema de videovigilancia del PEPP"**.

II. Acción Correctiva Ejecutada

Se elaboró y aprobó la **"Directiva Interna que regula el Tratamiento de Datos Personales y la Operación, Uso y Mantenimiento del Sistema de Videovigilancia del Proyecto Especial Pichis Palcazú - PEPP"**, mediante Resolución Directoral N° 202-2025-MIDAGRI-PEPP-CD/DE.

III. Conclusión Y Recomendación

- La situación adversa identificada por el Órgano de Control Institucional ha sido completamente subsanada mediante la aprobación de la Resolución Directoral N° 202-2025-MIDAGRI-PEPP-CD/DE, que formaliza la Directiva Interna mencionada en el numeral II.
- Se recomienda comunicar formalmente mediante oficio al jefe (e) del Órgano de Control Institucional la subsanación de la situación adversa y las acciones correctivas adoptadas, adjuntando copia de la Resolución Directoral N° 202-2025-MIDAGRI-PEPP-CD/DE y la directiva mencionada.

Es cuanto tengo a bien informar para su conocimiento y fines pertinentes.

Atentamente,

JGAT/U. A
C.c DE:

MINISTERIO DE DESARROLLO AGRARIO Y RIEGO
PROYECTO ESPECIAL PICHIS PALCAZU
UNIDAD DE ADMINISTRACIÓN
JORGE GERARDO ALARCÓN TIRADO
Jefe de la Unidad de Administración

PROVEIDO
Para: *Comunicar a OCI*
Fecha: 29 DIC. 2025
CUT: 1219-2025





"Año de la recuperación y consolidación de la economía peruana"

RESOLUCIÓN DIRECTORAL N° 202 -2025-MIDAGRI-PEPP-CD/DE

La Merced, 12 DIC. 2025

VISTO:

El Memorando N° 1308-2025-MIDAGRI-PEPP/UA, de fecha 03 de octubre del 2025, Memorando N° 333-2025-MIDAGRI-PEPP/UUPS de fecha 24 de octubre de 2025, Memorando N° 1668-2025-MIDAGRI-PEPP/UA de fecha 5 de diciembre de 2025, con el cual el jefe de la Unidad de Administración solicita la aprobación mediante Acto Resolutivo de la "Directiva Interna sobre tratamiento de datos personales y gestión del sistema de videovigilancia", Versión 01, Memorando N° 516-2025-MIDAGRI-PEPP/UUPS de fecha 05 de diciembre de 2025 de la Unidad de Programación, Presupuesto y Seguimiento, y;

CONSIDERANDO:

Que, el Proyecto Especial Pichis Palcazú constituye una Unidad Ejecutora del Pliego Ministerio de Desarrollo Agrario y Riego y como tal tiene bajo su responsabilidad organizar, dirigir y ejecutar los proyectos de inversión a su cargo, así como aquellos que le son asignados por el sector de acuerdo a ley, haciendo uso para ello de los recursos financieros, bienes, activos y capacidades humanas con que cuenta, con arreglo a los sistemas de presupuesto y administrativos nacionales;

Que, mediante Memorando N° 1308-2025-MIDAGRI-PEPP/UA de fecha 03 de octubre de 2025, el jefe de la Unidad de Administración solicita la elaboración de la "Directiva interna sobre tratamiento de datos personales y gestión del sistema de videovigilancia", con Memorando N° 333-2025-MIDAGRI-PEPP/UPS de fecha 24 de octubre de 2025 de la Unidad de Programación, Presupuesto y Seguimiento, remite el Proyecto solicitado;

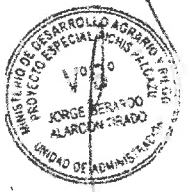
Que, siendo esto así, es necesario establecer procedimientos que regulen el tratamiento de datos personales y gestión del sistema de videovigilancia;

Que, la Directiva General, DI-001-2022-OGPP/OM "Directiva de documentos normativos del Ministerio de Desarrollo Agrario y Riego", Versión 01, aprobado mediante Resolución Ministerial N° 0187-2022-MIDAGRI de fecha 19 de mayo de 2022, tiene como finalidad fortalecer la rectoría sectorial del ministerio de Desarrollo Agrario y Riego, ordenando la producción de documentos normativos, en el marco de su función técnico normativa; y aquellos que se requieran para operativizar el funcionamiento del Ministerio, en el marco de los sistemas administrativos; siendo de aplicación obligatoria para las unidades de organización, programas y proyectos especiales del Ministerio de Desarrollo Agrario y Riego;

Que, mediante Memorando N° 516-2025-MIDAGRI-PEPP/UUPS, de fecha 05 de diciembre de 2025, el jefe de la Unidad de Programación, Presupuesto y Seguimiento realiza el análisis de la propuesta de la "Directiva interna sobre tratamiento de datos personales y gestión del sistema de videovigilancia", Versión 01, solicitado por el jefe de la Unidad Administración, concluyendo que en mérito a la Directiva General, DI-001-2022-OGPP/OM "Directiva de documentos normativos del Ministerio de Desarrollo Agrario y Riego", Versión 01, el proyecto de Directiva cumple con el contenido de la estructura de la directiva;

Estando a lo solicitado y sustentado por el área técnica;

En uso de las facultades contenidas en la Resolución Ministerial N° 230-2025-MIDAGRI de fecha 19 de junio de 2025 y las atribuciones conferidas en el artículo 12° del Manual de Operaciones del Proyecto Especial Pichis Palcazú aprobado





"Año de la recuperación y consolidación de la economía peruana"

RESOLUCIÓN DIRECTORAL N° 202 -2025-MIDAGRI-PEPP-CD/DE

La Merced, 12 DIC. 2025

por Resolución Ministerial N° 0072-2023-MIDAGRI de fecha 02 de marzo del 2023, y visación del jefe de la Unidad de Administración, jefe de la Unidad de Programación, Presupuesto y Seguimiento y jefe de la Unidad de Asesoría Jurídica;

SE RESUELVE:

ARTICULO PRIMERO. – APROBAR la Directiva DI N° 004 -2025-MIDAGRI-PEPP-UA "DIRECTIVA INTERNA SOBRE TRATAMIENTO DE DATOS PERSONALES Y GESTIÓN DEL SISTEMA DE VIDEOVIGILANCIA", VERSIÓN 01, que en X Capítulos y sus anexos forma parte integrante de la presente resolución (en 27 folios); de acuerdo a lo solicitado y sustentado por la Unidad de Administración.

ARTÍCULO SEGUNDO. – DÉJESE sin efecto toda norma que se oponga a la presente.

ARTICULO TERCERO. – ENCARGAR a la Unidad de Administración, efectuar las acciones administrativas que le competen para la difusión y el cumplimiento de lo dispuesto en la Directiva aprobada en el Artículo Primero de la presente resolución.

ARTÍCULO CUARTO. – HÁGASE de conocimiento de la presente Resolución Directoral a la Unidad de Administración, Unidad de Infraestructura Agraria y Riego, Unidad de Programación, Presupuesto y Seguimiento, Unidad de Desarrollo Agroeconómico y demás dependencias del Proyecto Especial Pichis Palcazu, para los fines correspondientes.

ARTICULO QUINTO. - PUBLICAR, la presente disposición en el portal Web de la entidad: www.gob.pe/pepp


Regístrese, Comuníquese y Cúmplase.



MINISTERIO DE DESARROLLO AGRARIO Y RIEGO
 PROYECTO ESPECIAL PICHIS PALCAZU
 M.Sc. GUSTAVO PÉREZ CARREÓN
 D.P. 1895
 Director Ejecutivo


CUT N°:1219-2025

MINISTERIO DE DESARROLLO AGRARIO Y RIEGO



**DIRECTIVA INTERNA QUE REGULE
EL TRATAMIENTO DE DATOS
PERSONALES Y LA OPERACIÓN,
USO Y MANTENIMIENTO DEL
SISTEMA DE VIDEOVIGILANCIA
DEL PROYECTO ESPECIAL PICHIS
PALCAZÚ – PEPP**

2025

 PERU Ministerio de Desarrollo Agrario y Riego	Código	Versión	Ámbito de aplicación
	DI N° -2025-MIDAGRI-PEPP/UA	01	General

DIRECTIVA INTERNA QUE REGULE EL TRATAMIENTO DE DATOS PERSONALES Y LA OPERACIÓN, USO Y MANTENIMIENTO DEL SISTEMA DE VIDEOVIGILANCIA DEL PROYECTO ESPECIAL PICHIS PALCAZÚ – PEPP

I. OBJETIVO

La presente Directiva tiene por objeto establecer las disposiciones para el tratamiento de datos personales captados a través de sistemas de videovigilancia con fines de seguridad, control laboral y otros, de conformidad con lo establecido en la Ley N° 29733 y su reglamento.

II. FINALIDAD

Contar con un documento que establezca lineamientos, procedimientos y unifique criterios para el tratamiento de datos personales y la operación, uso y mantenimiento del sistema de videovigilancia en el PEPP.

III. AMBITO DE APLICACION

La presente Directiva es de obligatorio cumplimiento de las Unidades Funcionales y servidores del Proyecto Especial Pichis Palcazú – PEPP.

IV. BASE LEGAL

- ❖ Constitución Política del Perú.
- ❖ Ley N° 29733, Ley de Protección de Datos Personales (LPDP).
- ❖ Decreto Legislativo N° 1218, que regula el uso de las cámaras de videovigilancia.
- ❖ Decreto Supremo N° 016-2024-JUS, que aprueba el Reglamento de la Ley de Protección de Datos Personales.
- ❖ Decreto Supremo N° 137-80-AA del 10 de octubre de 1980, que crea el Proyecto Especial Pichis – Palcazú.
- ❖ Resolución Ministerial N° 0072-MIDAGRI, que aprueba el Manual de Operaciones del Proyecto Especial Pichis Palcazú – PEPP.
- ❖ Directiva General, DI-001-2022-OGPP/OM, Directiva de documentos normativos del Ministerio de Desarrollo Agrario y Riego, Versión 01.

V. GLOSARIO DE SIGLAS Y TERMINOS

5.1 Para la aplicación de la presente Directiva se utilizan las siglas siguientes:

- DE : Dirección Ejecutiva
- PEPP : Proyecto Especial Pichis Palcazú
- UA : Unidad de Administración
- UAJ : Unidad de Asesoría Jurídica
- UPPS : Unidad de Programación, Presupuesto y Seguimiento

5.2 Para la aplicación de la presente Directiva se utilizan las definiciones siguientes:

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





- **Arquitectura lógica:** Representación gráfica de las conexiones entre los componentes lógicos (software, sistemas, aplicativos, etc.) del sistema de videovigilancia a través del cual se realiza tratamiento de datos personales.
- **Cámara o videocámara:** Dispositivo digital, óptico o electrónico, fijo o móvil que permite captar, grabar o cualquier otro tratamiento de datos personales a través de imágenes, videos o audios.
- **Cámara conectada a internet:** Es aquella 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.
- **Cámara "on board":** Cámara instalada dentro de un vehículo, casco o vestimenta de un conductor, que permite grabar imágenes durante el recorrido que se realiza con el mismo.
- **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.
- **CD:** Disco compacto.
- **Dato personal:** Las imágenes y las voces de una persona constituyen datos personales, ya que permiten identificar o hacer identificable a una persona natural a través de medios que pueden ser razonablemente utilizados.
- **Días:** Días hábiles.
- **Dron:** Aeronave no tripulada.
- **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.
- **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.
- **LPDP:** Ley N° 29733, Ley de Protección de Datos Personales.
- **Máscara de privacidad:** Permite bloquear y/o anonimizar determinadas partes de una imagen que no se visualizará o captará por la cámara o videocámara.
- **Persona identificable:** Persona a la cual se la pueda 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.
- **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 privilegios.

Existen tres tipos de Perfiles:

- 01) **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 encargado del tratamiento.

02) **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.

03) **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.

- **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 deberán ser definidos mediante procesos de identificación y/o autenticación de los usuarios, así como los responsables de realizar dichos procesos.
- **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 tratamiento de datos personales, así como los responsables de realizar el tratamiento de datos personales y de aquellos que llevan a cabo dichos procesos.
- **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.
- **RLPDP:** Reglamento de la Ley de Protección de Datos Personales.
- **RNPDP:** Registro Nacional de Protección de Datos Personales.
- **Sistema de Videovigilancia:** Conjunto de una o más personas y equipos tecnológicos -compuesto por una o varias cámaras de video localizadas estratégicamente e interconectadas entre sí - que permiten el tratamiento de datos personales.
- **Tipos de prestación en contratos de encargo de sistemas de videovigilancia:**

- 01) **Una empresa externa puede prestar servicios consistentes en la instalación y/o mantenimiento técnico de los equipos y sistemas de videovigilancia sin acceso a imágenes y/o audio.** En estos casos estas empresas no tienen la condición de encargados del tratamiento, siendo el titular del banco de datos el obligado a adoptar los sistemas a los requisitos normativos.
- 02) **La empresa externa puede brindar servicios de instalación o mantenimiento de los equipos y sistemas de videovigilancia**



con utilización de los equipos o acceso a las imágenes, videos o audios. En este tipo de relación la empresa se considera encargada del tratamiento y tiene que cumplir las obligaciones que tal condición le otorga la LPDP

- **Tratamiento de datos personales a través de sistemas de videovigilancia:** Es cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de la imagen o voz, captados por medio de un sistema de cámaras fijas o móviles ya sea en tiempo real o en visualización de grabaciones de imágenes, videos o audios.
- **Usuario:** Operador de la plataforma tecnológica a quien se le asignó un perfil determinado.
- **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.
- **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

VI. DISPOSICIONES GENERALES

Ámbito material de aplicación

- 6.1 Se aplica al tratamiento de datos de personas identificadas o identificables captados a través de sistemas de videovigilancia. El tratamiento objeto de esta directiva comprende la grabación, captación, transmisión, conservación o almacenamiento de imágenes o voces, incluida su reproducción o emisión en tiempo real o cualquier otro tratamiento que permita el acceso a los datos personales relacionados con aquellos, para fines de seguridad, control laboral y otros.
- 6.2 No se encuentran dentro del ámbito de aplicación de la presente directiva:
 - 6.2.1 Los tratamientos de datos de personas naturales identificadas o identificables a través de cámaras o videocámaras y sistemas de videovigilancia en el marco de los supuestos de excepción previstos en el artículo 3 de la LPDP
 - 6.2.2 Al tratamiento de imágenes en el ámbito personal y doméstico, que incluye el uso de cámaras "on board" y los sistemas de videoportería, salvo que estos últimos se articulen mediante procedimientos que reproduzcan o graben imágenes de modo constante y que resulten accesibles (mediante internet o emisiones por televisión en circuito cerrado) y, en particular, cuando el objeto de las mismas alcance a las zonas comunes y/o la vía pública colindante.
 - 6.2.3 Al tratamiento de imágenes vinculadas al ejercicio legítimo del derecho a la libertad de información y expresión por los medios de comunicación.

- 6.2.4 Aquellos sistemas que involucren cámaras o videocámaras simuladas o desactivadas. A estas últimas, si les resultará aplicable la directiva en lo que respecta a las medidas de seguridad del sistema.

Legitimación para el tratamiento de datos mediante cámaras o sistemas de videovigilancia

- 6.3 Existe legitimidad para el tratamiento de datos personales mediante sistemas de videovigilancia cuando se cuente con alguno de los siguientes supuestos:
- 6.3.1 Se cuente con el consentimiento del titular de los datos personales.
 - 6.3.2 Una norma con rango de ley habilite a captar los datos sin el consentimiento de los titulares.
 - 6.3.3 Se dé alguna de las circunstancias previstas en el artículo 14 de la LPDP.

Principios

6.4 **Principio de proporcionalidad:**

El tratamiento de los datos personales debe ser adecuado, pertinente y no excesivo en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.

Debe existir una relación de proporcionalidad entre la finalidad perseguida y el modo en que se traten los datos. Una adecuación medio —fin.

El uso de instalaciones de cámaras o videocámaras es legítimo cuando no exista un medio menos invasivo o igual de eficaz, para alcanzar la finalidad perseguida

6.5 **Principio de seguridad:**

El responsable del tratamiento debe adoptar las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Aquellos sistemas de videovigilancia de personas jurídicas conectados o que vayan a ser conectados con una central receptora de alarmas o un centro de control, deben cumplir con lo previsto en el Decreto Legislativo N° 1213, que regula los servicios de seguridad privada. Estos servicios únicamente pueden ser realizados por empresas de seguridad, en virtud de sus condiciones y cualificación, debiendo estas ser consideradas encargadas del tratamiento

6.6 **Principio de calidad:**

El tratamiento de los datos deberá ser necesario, pertinente y adecuado respecto a la finalidad para la que fueron recopilados, y deberán conservarse solo por el tiempo necesario para cumplir con la finalidad que motivó su tratamiento, tomando en cuenta el plazo señalado en el punto 6.13 de la presente directiva.

Derecho de información

- 6.7 Debe informarse sobre la captación y/o grabación de las imágenes, para tal fin se debe colocar en las zonas videovigiladas al menos un distintivo

informativo ubicado en un lugar suficientemente visible, tanto en espacios abiertos como cerrados.

Si la información prevista en el artículo 18 de la LPDP no puede ser colocada en su integridad en el cartel informativo, en el espacio videovigilado debe tenerse a disposición de los interesados, ya sea a través de medios informáticos, digitalizados o impresos, la información mínima requerida para garantizar sus derechos, regulada en el punto 6.12 de la presente directiva.

Si el lugar vigilado dispone de varios accesos, el cartel se coloca en todos ellos, en un lugar visible, para que la información contenida en el mismo también lo sea.

Respeto a los derechos fundamentales de terceros

6.8 Debe prevenirse la captación de imágenes de terceros ajenos a los fines de la captación. El titular del banco de datos personales o quien realice el tratamiento de los datos a través de los sistemas de videovigilancia es responsable por la implementación de mecanismos o medidas adecuadas para no afectar los derechos de terceros que aparezcan en las grabaciones.

Las cámaras o videocámaras instaladas en espacios privados no deben obtener imágenes de espacios públicos, salvo que resulte imposible evitarlo. En este último caso, la cámara debe captar únicamente la sección de vía pública que resulte imprescindible para cumplir con los fines de vigilancia que se pretende con la instalación del sistema.

Registro de banco de datos de videovigilancia

6.9 La persona natural, jurídica o entidad pública que utilice un sistema de videovigilancia o cualquier dispositivo que permita el tratamiento de datos para dicho fin, debe solicitar la inscripción del banco de datos personales respectivo a la Dirección de Protección de Datos Personales, unidad orgánica de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos, encargada de la administración del Registro Nacional de Protección de Datos Personales.

6.10 Los sistemas que no almacenan imágenes, sino que consisten exclusivamente en la reproducción y emisión de imágenes en tiempo real, no son considerados bancos de datos. Sin embargo, esto no los exime del cumplimiento de las demás obligaciones contenidas en la LPDP, su reglamento y la presente directiva, en lo que resulte aplicable.

Características del cartel informativo

6.11 Cada acceso a la zona videovigilada debe tener un cartel o anuncio visible con fondo amarillo o cualquier otro que contraste con el color de la pared y que lo haga suficientemente visible. Su contenido mínimo debe indicar (Anexo 1):

6.11.1 La identidad y domicilio del titular del banco de datos personales.

6.11.2 Ante quién y cómo se pueden ejercitar los derechos establecidos en la LPDP.

- 6.11.3 Lugar dónde puede obtener la información contenida en el artículo 18 de la LPDP.
- 6.11.4 En lo que se refiere a las dimensiones, los elementos gráficos podrán tener, como mínimo, las siguientes: 297 x 210 mm. Cuando el espacio en que se vaya a ubicar el cartel informativo no lo permita, este debe adecuarse al espacio disponible, de tal forma que cumpla su finalidad informativa.

Características del informativo adicional del sistema de videovigilancia

- 6.12 El informativo adicional del sistema de videovigilancia (Anexo 2) debe estar disponible, ya sea a través de medios informáticos, digitalizados o impresos, y debe contener la información requerida para garantizar el derecho reconocido en el artículo 18 de la LPDP:
- 6.12.1 La identidad y domicilio del titular del banco de datos personales y del encargado del tratamiento, de ser el caso.
- 6.12.2 La finalidad.
- 6.12.3 Las transferencias y destinatarios de los datos personales.
- 6.12.4 El plazo durante el cual se conservarán los datos personales.
- 6.12.5 El ejercicio de los derechos de información, acceso, cancelación y oposición de los datos

Plazo de conservación o almacenamiento de la información grabada

- 6.13 Las imágenes y/o voces grabadas se almacenan por un plazo de treinta (30) días y hasta un plazo máximo que dependerá de la capacidad de almacenamiento del DVR. Durante ese plazo, el titular del banco de datos o encargado del tratamiento de los datos debe asegurar la reserva y confidencialidad de la información, no permitiendo la difusión, copia o visualización de imágenes por terceros no autorizados.
- 6.14 El registro de las imágenes, videos o audios que presenten indicios razonables de la comisión de un delito o falta debe ser informado haciendo entrega del soporte que contiene el mismo de manera inmediata a la Policía Nacional del Perú o al Ministerio Público, según corresponda.

Cancelación definitiva de la información

- 6.15 Transcurrido el plazo de conservación de la información referido en el punto 6.13, y no habiendo requerimiento de alguna autoridad competente para entregar o visualizar el contenido de la grabación, se deben eliminar los archivos de manera automática en el DVR, salvo disposición distinta en norma sectorial.
- 6.16 plazo máximo previsto para la eliminación de la información no será aplicable cuando exista alguna finalidad o interés legítimo que justifique su conservación, así como la concurrencia de alguna contingencia de orden técnico que justifique razonablemente el aplazamiento de la eliminación de la misma por un período determinado o determinable.

Formalidades que debe seguir el encargado del tratamiento

- 6.17 Cuando una persona natural, jurídica o entidad pública ha instalado o pretende instalar un sistema de cámaras de videovigilancia, pero encarga a otra la gestión del sistema con utilización de los equipos o acceso a las imágenes o voces, debe de suscribirse un contrato, convenio o documento similar en el que se establezca el objeto, la duración, la naturaleza y

finalidad del tratamiento, el tipo de datos y categorías de interesados, las obligaciones y derechos que correspondan, así como el destino de los datos al finalizar la prestación.

- 6.18 El contrato, convenio o documento similar atiende a las circunstancias concretas de la prestación del servicio. El encargado está obligado, en mérito de él, a cumplir con las condiciones técnicas y organizativas necesarias para respetar las obligaciones establecidas en la LPDP; a observar los requisitos legales que lo habilitan para prestar el servicio; a seguir las instrucciones del responsable del tratamiento o del titular del banco de datos; a realizar las acciones necesarias para asistir al responsable o titular del banco de datos en el cumplimiento de su deber de responder frente el ejercicio de los derechos señalados en la LPDP; y, en general, de colaborar en el cumplimiento de las obligaciones del titular del banco de datos.
- 6.19 El encargado del tratamiento debe garantizar al responsable que el acceso a los datos sólo se realizará por personas debidamente autorizadas debiendo adoptar las medidas de seguridad necesarias para asegurar el adecuado uso del sistema y tratamiento de los datos personales.
- 6.20 El encargado del tratamiento del sistema de videovigilancia debe notificar, sin dilación, al responsable del tratamiento acerca de la existencia de una violación o brecha de seguridad.
- 6.21 De acuerdo a lo establecido en el artículo 32 del RLPDP, es posible la subcontratación con terceros, debiendo asumir la persona natural o jurídica subcontratada las mismas obligaciones que se establezcan para el titular del banco de datos, responsable o encargado del tratamiento, según corresponda, de acuerdo a lo establecido en el artículo 33 del RLPDP.

Principales obligaciones sobre medidas de seguridad.

- 6.22 La persona que opera o tiene acceso a cualquier sistema de cámaras de videovigilancia, en razón de sus funciones, debe cumplir con lo siguiente:
- 6.22.1 Tener procedimientos de identificación y autenticación de usuarios que den cuenta del funcionamiento del centro de control y monitoreo del sistema de cámaras o videocámaras de videovigilancia, de las partes que lo componen y los equipos.
- 6.22.2 Conocer el funcionamiento correcto del sistema de videovigilancia.
- 6.22.3 Contar con un inventario documentado de las cámaras u otros dispositivos de videovigilancia.
- 6.22.4 Contar con un esquema y/o diagrama documentado de la arquitectura física y lógica del sistema de videovigilancia. La arquitectura física es la representación gráfica de las conexiones físicas entre los diversos componentes del sistema. Entiéndase por componentes: los servidores, cámaras de videovigilancia, computadoras, etc.

Por su parte, la arquitectura lógica es la representación gráfica de las conexiones entre los componentes lógicos (software, sistemas aplicativos, etc.) de una red o sistema de videovigilancia, en el cual se debe detallar nombre del sistema y funciones específicas



- 6.22.5 Contar con documentación respecto a la gestión de accesos, privilegios y verificación periódica de privilegios asignados.
- 6.22.6 Cuando corresponda, contar con mecanismos de respaldo de seguridad de la información de carácter personal obtenida a través de sistemas de videovigilancia, así como con un procedimiento que contemple la verificación de la integridad de los datos almacenados en el respaldo.
- 6.22.7 Implementar las medidas de seguridad en el caso de que resulte necesario transportar los sistemas o cámaras de videovigilancia que contengan información de carácter personal. El transporte debe ser autorizado por el titular del banco de datos personales.
- 6.22.8 Otras obligaciones que las leyes o normativa sobre la materia dispongan.

6.23 Para efectos de un cumplimiento adecuado de las medidas de seguridad dentro del sistema de videovigilancia, es necesaria la implementación de los perfiles definidos en el glosario de la presente directiva, a fin de limitar accesos y gestión de privilegios de los usuarios. En el caso de personas jurídicas o naturales que cuenten con un número no superior de ocho cámaras y dos operadores de las mismas, sólo será necesario la determinación del perfil administrador y habilitarse un ambiente aislado o apropiado con mecanismo de control de acceso asignado para el mismo.

Deber de confidencialidad

- 6.24 El deber de confidencialidad podrá materializarse a través de un documento en el que se determine la obligación de secreto entre las partes, a efectos de no divulgar una determinada información. En este documento se establece la prohibición de reproducir, modificar, publicar o difundir o transferir a terceros la información sin autorización expresa de la otra parte.
- 6.25 El documento debe ser suscrito entre las personas que en razón de sus funciones operan o tienen acceso a cualquier sistema de videovigilancia, con el titular del banco de datos personales o con el encargado del tratamiento, dependiendo de a quien presta sus servicios directamente, siendo la empresa empleadora la propietaria del sistema de videovigilancia o del establecimiento en donde este se realiza.

Responsabilidades de las personas que operan sistemas o centros de videovigilancia por operaciones no autorizadas

- 6.26 Las personas que operan o tienen acceso a cualquier sistema de videovigilancia, en razón de sus funciones, son responsables de la facilitación, comercialización, difusión, copia o entrega no autorizadas del contenido de las grabaciones.

Prestaciones de servicio sin acceso a datos personales

- 6.27 El responsable o encargado del tratamiento de los datos personales adopta las medidas adecuadas para limitar el acceso del personal distinto al especialmente designado para acceder y gestionar el sistema de videovigilancia.

6.28 El personal que no tiene entre sus funciones realizar tratamiento de datos personales se encuentra prohibido de tratar los datos personales, debiendo consignarse esta prohibición:

6.28.1 En el contrato de trabajo o prestación de servicios que suscriban con el titular del banco de datos o encargado de su tratamiento, o,

6.28.2 En el contrato que suscriba la empresa tercerizadora o intermediaria y el titular del banco de datos o el encargado de su tratamiento, debiendo la empresa tercerizadora o intermediadora hacer de conocimiento de quien vaya a prestar directamente el servicio de tal obligación de confidencialidad.

6.29 Asimismo, deberá consignarse la obligación de secreto respecto a los datos que este personal hubiera podido conocer con motivo de la prestación de su servicio.

Derechos de los titulares de los datos

6.30 Los derechos establecidos en la LPDP pueden ser ejercidos por los titulares de los datos personales con motivo de su captación a través de un sistema de videovigilancia. Por las particularidades propias de los sistemas de videovigilancia podrán ejercitarse los siguientes derechos:

6.30.1 Derecho acceso.

6.30.2 Derecho de cancelación.

6.30.3 Derecho de oposición (en algunos supuestos).

Derecho de Acceso

6.31 Dadas las particularidades propias de los sistemas de videovigilancia, el derecho de acceso reviste características singulares:

6.31.1 El titular del dato personal debe precisar la fecha, rango de horas, lugar o cualquier otra información que permita facilitar la ubicación de la imagen requerida. Asimismo, de ser necesario, aportará una imagen actualizada de sí mismo que permita al titular o encargado del tratamiento verificar su presencia en el registro.

6.31.2 Con la finalidad de no afectar la protección de datos personales de terceros, el titular del dato personal puede escoger entre las siguientes alternativas para acceder a su información:

a) Acceso mediante un escrito:

El titular del dato personal presentará una solicitud escrita a la dirección física o electrónica que aparece en el cartel o documento informativo, adjuntando e indicando lo señalado en el numeral 6.31.1.

La respuesta emitida por el titular del banco de datos personales o por el encargado del tratamiento debe detallar los datos requeridos que son objeto de tratamiento, sin afectar derechos de terceros.

b) Entrega de las imágenes, videos o audios:

El titular del dato personal debe entregar un CD en blanco o dispositivo análogo al titular del banco de datos personales o al encargado de tratamiento con el fin de que este grabe su información. En este supuesto, el titular o encargado del tratamiento debe utilizar máscaras de privacidad para difuminar la imagen o cualquier otro medio que impida la afectación de

terceros, así como implementar un mecanismo de protección para el archivo (cifrado, contraseña u otros).

c) Visualización en sitio:

El titular del dato personal debe acercarse físicamente a las instalaciones del titular del banco de datos o responsable del tratamiento para acceder directamente a su información.

Para ello, debe presentar previamente una solicitud en la dirección física o electrónica que aparece en el cartel o documento informativo, indicando fecha, rango de horas, lugar o cualquier otra información que permita facilitar la ubicación de la imagen; así como una imagen actualizada de sí mismo que permita al titular del banco de datos personales o responsable del tratamiento advertir su presencia en el registro.

Se debe dejar constancia de lo visualizado y entregar la misma al titular del dato personal, una vez culminada la visualización

- 6.31.3 Adicionalmente, se entrega al titular de los datos personales información precisa sobre la finalidad de la recolección de los datos, sobre la inscripción del banco de datos, el lugar donde se produjo el registro o captación de su imagen, el tiempo en que la misma se produjo y el destino de los datos.
- 6.31.4 Si se ejerce el derecho de acceso ante el responsable de un sistema que únicamente reproduce imágenes sin registrarlas, debe ponerse esta situación a conocimiento del titular del dato personal.
- 6.31.5 No procede la difuminación de imágenes o aplicación de máscaras de seguridad de terceras personas cuando se acredite el legítimo interés del titular del dato personal que lo solicita. Se entiende por legítimo interés, el acopio de información para ejercer el derecho de defensa, formular denuncia administrativa o penal o similares.
- 6.31.6 En el supuesto que el responsable o encargado del tratamiento no aplicara la máscara de seguridad o algún mecanismo de difuminación de imágenes que impidiera la afectación de terceros, aduciendo falta de capacidad técnica o económica, será la autoridad administrativa que valorará este alegato en cada caso en concreto.
- 6.31.7 Si el titular del banco de datos o responsable del tratamiento es declarado un activo crítico nacional conforme a la normativa de la materia o si se tratara de áreas de alto riesgo para la seguridad, se deberá acordar con el titular del dato personal otro mecanismo idóneo para dar acceso a su información. De no existir ningún medio posible, podrá ser denegada su solicitud por el titular del banco de datos personales o el responsable del tratamiento, debiendo hacerlo de forma motivada

Derechos de Cancelación y Oposición

- 6.32 Los derechos de cancelación y oposición se ejercen atendiendo a lo dispuesto en el numeral 6.31.1. de la presente directiva, a los artículos 20 y 22 de la LPDP y los artículos 61, 69 y 86 del RLPDP. Asimismo, procederá la atención en aquellos supuestos donde sea materialmente posible y responda a criterios fundamentados y motivados.



Imposibilidad de ejercicio del derecho de rectificación

6.33 No es posible el ejercicio del derecho de rectificación en el tratamiento mediante sistemas de videovigilancia, dado que, por su naturaleza, las imágenes captadas reflejan un hecho objetivo que no puede ser modificado a petición del titular del dato personal.

Denegación de los derechos de acceso, cancelación y oposición

6.34 En caso de denegación de alguno de los derechos deberá indicarse expresamente en el escrito de denegación, la posibilidad de reclamar su tutela ante la Autoridad Nacional de Protección de Datos Personales.

Comunicación sin consentimiento de los titulares de los datos

6.35 Es legítima la transferencia de los datos personales captados por los sistemas de videovigilancia sin el consentimiento de los titulares de los datos, cuando:

- 6.35.1 La comunicación de lo captado deba ser entregada por orden judicial o a una entidad pública en cumplimiento de sus funciones.
- 6.35.2 Cuando deba ser puesto a disposición o sea requerido por la Policía Nacional del Perú o el Ministerio Público, en razón del ejercicio de las competencias asignadas por ley, en aquellos supuestos necesarios para la prevención, investigación, detección o represión de infracciones penales o delitos. La petición de las grabaciones debe realizarse de forma motivada y el tratamiento de las mismas debe responder a la finalidad del requerimiento realizado.

VIDEOVIGILANCIA PARA EL CONTROL LABORAL

Excepción al consentimiento en torno de la finalidad

6.36 En virtud del poder de dirección del empleador, este se encuentra facultado para realizar controles o tomar medidas para vigilar el ejercicio de las actividades laborales de sus trabajadores, entre las que se encuentra la captación y/o tratamiento de datos a través de sistemas de videovigilancia.

Deber de informar

6.37 El empleador se encuentra obligado a informar a sus trabajadores de los controles videovigilados, a través de carteles (o en su defecto de los avisos informativos mencionados en la presente directiva); ello, sin perjuicio de informar de manera individualizada a cada trabajador, si se considera pertinente.

Finalidad de los sistemas de videovigilancia

6.38 El tratamiento de los datos de los trabajadores se limita a las finalidades propias del control y supervisión de la prestación laboral, de tal forma que no pueden utilizarse los medios o el sistema de videovigilancia para fines distintos, salvo que se cuente con el consentimiento del trabajador o se trate de alguna de las excepciones señaladas en el artículo 14 de LPDP.

6.39 Son fines legítimos para el control y la supervisión de la prestación laboral, la protección de bienes y recursos del empleador; la verificación de la adopción de medidas de seguridad en el trabajo; y, aquellos otros que la legislación laboral y sectorial prevea.

Principio de proporcionalidad

- 6.40 El control laboral a través de sistemas de videovigilancia sólo se realiza cuando sea pertinente, adecuado y no excesivo para el cumplimiento de tal fin.
- 6.41 Asimismo, la instalación de las cámaras o, en todo caso, su ámbito de captación debe restringirse a los espacios indispensables para satisfacer las finalidades de control laboral.
- 6.42 En ningún caso se admite la instalación de sistemas de grabación o captación de sonido ni de videovigilancia en los lugares destinados al descanso o esparcimiento de los trabajadores, como vestuarios, servicios higiénicos, comedores o análogos.

- 6.43 La grabación videovigilada con sonido en el lugar de trabajo sólo se admitirá cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad y finalidad.

Prohibición de uso de las imágenes para fines comerciales o publicitarios

- 6.44 Las imágenes captadas a través de los sistemas de videovigilancia laboral no pueden ser utilizadas con fines comerciales o publicitarios, salvo que se cuente con el consentimiento de los trabajadores.

Cancelación de imágenes y/o voces

- 6.45 Las imágenes y/o voces grabadas se almacenan por un plazo de treinta (30) días y hasta un plazo máximo que dependerá de la capacidad de almacenamiento del DVR, salvo disposición distinta en las normas laborales. Durante ese plazo, el titular del banco de datos o encargado del tratamiento debe cuidar que la información sea accesible sólo ante las personas que tengan legítimo derecho a su conocimiento y manteniendo así la reserva necesaria respecto a las imágenes y/o voces.
- 6.46 Transcurrido el plazo señalado en numeral anterior y no habiendo requerimiento de alguna autoridad competente para entregar o visualizar el contenido de la grabación, se deben eliminar los archivos de manera automática en el DVR, salvo disposición distinta en norma sectorial.
- 6.47 El plazo máximo previsto para la eliminación de la información, no será aplicable cuando exista alguna finalidad o interés legítimo que justifique su conservación, así como la concurrencia de alguna contingencia de orden técnico que justifique razonablemente el aplazamiento de la eliminación de la misma por un período determinado o determinable.
- 6.48 Las imágenes y/o voces sin editar que den cuenta de la comisión de presuntas infracciones laborales y/o accidentes de trabajo deben ser conservadas por el plazo de ciento veinte (120) días, contados a partir de su conocimiento, salvo la existencia de alguna finalidad que justifique su conservación o de interés legítimo, tiempo dentro del cual el empleador podrá iniciar las acciones legales pertinentes.

6.49 El trabajador podrá solicitar el acceso a las grabaciones o a una copia digital de las mismas que contengan información sobre una conducta o incumplimiento laboral que se le haya imputado, pudiendo utilizar esta grabación como medio de prueba. El empleador deberá resguardar el derecho de terceros que, sin estar involucrados con la conducta o incumplimiento, de manera directa o indirecta, puedan aparecer en registros captados; ello se hará adoptando las medidas técnicas necesarias para difuminar su imagen e impedir su identificación.

6.50 En el caso de que el empleador, en base a lo captado por los sistemas de videovigilancia, decida imputar una falta grave a un trabajador, deberá proceder de conformidad con lo establecido en las normas laborales. Asimismo, el empleador deberá proceder a resguardar el derecho de terceros que puedan aparecer en los registros captados, de la forma establecida en el párrafo anterior.

Tutela Directa de los trabajadores

6.51 Los trabajadores deben estar informados por los medios establecidos en la directiva sobre el procedimiento implementado por el empleador para ejercer sus derechos de acceso, cancelación y oposición.

Transferencia de datos personales

6.52 Si el empleador debe transferir los datos personales de sus trabajadores captados mediante videovigilancia a un tercero por motivos no laborales, debe informar de ello a los trabajadores, conforme la LPDP y su reglamento. De igual modo, cuando corresponda, debe solicitar su consentimiento.

Tratamiento con fines científicos o de investigación

6.53 En el caso de tratamiento de datos personales con fines científicos o de investigación se deberá cumplir con los principios y reglas establecidas en la LPDP, su reglamento y la presente directiva, en particular los principios de consentimiento, proporcionalidad y finalidad, así como las medidas técnicas y organizativas para garantizar la seguridad de la información de los datos personales, hasta donde resulte aplicable razonablemente.

TRATAMIENTO DE DATOS CON OTRAS TECNOLOGÍAS

Cámaras conectadas a internet

Deberes adicionales del titular del banco de datos personales o encargado del tratamiento

6.54 Revisar si las funciones de identificación y autenticación se encuentran activadas con el fin de evitar accesos de terceros a las imágenes y de garantizar que sólo acceden los usuarios autorizados.

6.55 Garantizar la seguridad en el acceso a través de redes públicas de comunicaciones.

Mediante drones

Especialidad en el manejo de los drones con fines de videovigilancia

6.56 Las personas que, con fines de seguridad privada, por razón de sus funciones, tengan a su cargo el sistema de videovigilancia a través de drones, deben contar con formación especializada en el manejo de estos equipos, garantizando reserva, confidencialidad y cumpliendo las demás obligaciones dispuestas en esta directiva para los sistemas de videovigilancia, así como la normativa especial o sectorial de la materia.

Responsabilidad del titular y/o encargado del tratamiento

6.57 El titular del banco de datos personales, responsable o el encargado del tratamiento debe informar de acuerdo a lo señalado en el punto 6.8 de esta directiva a las personas que serán controladas mediante los sistemas de videovigilancia a través de drones. Este deber alcanza también a aquellas personas o entidades que brinden el servicio de videovigilancia a través de drones de forma complementaria a la que preste el servicio principal. Dicha información debe entregarse en formato físico o electrónico, al momento de suscribir el contrato de videovigilancia con la entidad o persona que brinde este servicio a través de drones o de forma singularizada en el documento de contratación; además, debe estar a disposición de quien lo requiera.

6.58 Debe utilizarse los sistemas de carteles o folletos cuando sea factible. En caso de utilizar el cartel o el folleto se debe indicar gráficamente (dibujo) el medio utilizado (Anexo 3), aplicándose, en lo que resulte pertinente, de forma mínima lo establecido en el punto 6.11 de esta directiva.

6.59 Los titulares de bancos de datos personales, responsables o encargados de tratamiento, en caso cuenten con una página web, deben publicar información que permita conocer los diferentes tipos de operaciones realizadas o las que se proponen realizar en el futuro cercano con los datos captados.

VII. DISPOSICIONES ESPECIFICAS

El Sistema de Videovigilancia del Proyecto Especial Pichis Placazú - PEPP

7.1 El sistema de videovigilancia del PEPP se implementa como una herramienta de vigilancia, identificación, observación y, registro, que en algunos casos también puede ser usado como una herramienta de productividad para la institución.

7.2 El sistema de videovigilancia cumple con las acciones siguientes:

- ❖ Ayudar en la detección de riesgos, amenazas y daños.
- ❖ Fortalecer la seguridad interna y externa de las diferentes sedes de la entidad.
- ❖ Facilitar la indagación y detección de infracción y/o presuntos delitos.
- ❖ Apoyar en las investigaciones disciplinarias, donde se requiera el registro de información (videos) como medios probatorios.
- ❖ Monitorear el registro de las imágenes las veinticuatro (24) horas al día, durante todo el año.
- ❖ Grabar imágenes, videos y audio en caso excepcional según normativa.

De la instalación y operatividad del Sistema de Videovigilancia.

- 7.3 El sistema de videovigilancia prioriza la cobertura de ambientes físicos, tales como pasadizos y puertas de accesos de las sedes del Proyecto Especial Pichis Palcazú – PEPP.
- 7.3.1 Se encuentra prohibida la instalación de cámaras en baños y vestuarios.
- 7.3.2 La Unidad de Administración del PEPP, coloca señaléticas en las zonas videovigiladas. Las señaléticas comunican las zonas vigiladas.

Del acceso al monitoreo mediante el software y control de los servidores

- 7.4 La Unidad de Administración designa a servidores de su Unidad Orgánica como responsables autorizados del manejo de los equipos e información para el acceso a la visualización en tiempo real de imágenes a través de las cámaras o del software de monitoreo:

7.4.1 **Servidor designado como perfil administrador:** quien debe haber juramentado en mantener la confidencialidad y la reserva de la información que tramita; así como también, haber presentado su "Declaración Jurada de Confidencialidad" (Anexo N° 04). Realiza la administración de dispositivos, configuraciones, visualización, descarga y otros de competencia técnica como el inventario y la seguridad física del sistema de videovigilancia.

7.4.2 **Servidor designado como perfil básico:** quien debe haber juramentado en mantener la confidencialidad y la reserva de la información que tramita; así como también, haber presentado su "Declaración Jurada de Confidencialidad" (Anexo N° 04). Realiza el monitoreo, mediante visualización en tiempo real a través de estación de monitoreo, las cámaras de determinada localización, sede o área física.

- 7.5 Al cesar en el cargo (el servidor designado como perfil administrador y el servidor designado como perfil básico) realizan la entrega de cargo respectiva en concordancia con la normatividad vigente, bajo responsabilidad. Esto incluye la entrega de claves y contraseñas a la jefatura de la Unidad de Administración.
- 7.6 El jefe de la Unidad de Administración designa al servidor designado como perfil administrador, y dispone al servidor designado el cambio de las claves y contraseñas del sistema (servidores y equipos de videovigilancia) en periodos máximo de tres (3) meses.

En caso de ausencia del encargado, el jefe de la Unidad de Administración conserva las claves y contraseñas en sobre lacrado

- 7.7 La Unidad de Administración atiende las solicitudes de información.
- 7.8 La Unidad de Administración administra los medios de grabación del sistema, propiedad del Proyecto Especial Pichis Palcazú – PEPP.
- 7.9 El PEPP a través de la Unidad de Administración está comprometido con el uso legal y responsable de la información registrada en el sistema e

videovigilancia. No se utiliza el sistema para la vigilancia encubierta y acciones contrarias al marco legal vigente.

7.10 El PEPP a través de la Unidad de Administración garantiza la seguridad interna y externa de las instalaciones, a través de las cámaras de videovigilancia que son instaladas, y las que monitorean solo los accesos y zonas comunes de las instalaciones del PEPP.

7.11 El PEPP garantiza la privacidad y el derecho a la intimidad personal en el marco de la norma de la materia. Dicha disposición cesa cuando existe una resolución judicial de la materia.

Visualización de imágenes o copia de las grabaciones

7.12 Para solicitar videos o fotografías que obran en el archivo del sistema de videovigilancia y con el fin de cumplir con las normativas vigentes del PEPP, se debe cumplir con las disposiciones siguientes:

7.12.1 Solicitud de copia de registro de grabaciones.

7.12.1.1 Las solicitudes para la atención de copias de registros de grabaciones del sistema de videovigilancia son dirigidas a la Dirección Ejecutiva.

Solo para casos excepcionales de visualización mas no de entrega de copias de registros de grabaciones contenida en el sistema de videovigilancia, es autorizada directamente por el jefe de la Unidad de Administración.

7.12.2 La Dirección Ejecutiva a través de la Unidad de Administración tramita las solicitudes para las atenciones de copias de registros de grabaciones contenida en el sistema de videovigilancia, previa opinión técnica legal de la Unidad de Asesoría Jurídica

7.12.3 Las solicitudes de copia de grabación deben corresponder a situaciones claramente descritas y limitadas a un periodo de tiempo de acuerdo con la disponibilidad, indicando:

- ❖ El detalle específico de la solicitud y las razones del requerimiento.
- ❖ La fecha y hora aproximada, de ser el caso, para facilitar la Ubicación de las imágenes.

7.12.4 No está permitida la entrega de información que afecte la intimidad personal y que expresamente este excluida por Ley o por razones de Seguridad Nacional

Del solicitante

7.13 El solicitante, puede ser una persona natural, jurídica o entidades del estado que en el marco de una investigación penal y/o administrativa requiera copias de grabaciones contenidas en el sistema de videovigilancia del PEPP.

7.14 Las solicitudes presentadas por funcionarios y/o servidores del PEPP se realizan cumpliendo lo descrito en el segundo párrafo del numeral 7.12.3 de la presente directiva.

7.15 Asimismo, el Ministerio Público, autoridades judiciales y la Policía Nacional por la naturaleza de sus funciones, podrán solicitar el acceso a las imágenes del sistema de videovigilancia en poder del PEPP, mediante la visualización de estas ingresando a los ambientes del sistema de

videovigilancia (cumpliendo lo dispuesto en el numeral 7.12.11) o solicitar de manera formal copia de las imágenes.

- 7.16 La Unidad de Administración remite las respuestas a los solicitantes (personas jurídicas o natural), concluyendo con el proceso de atención, al pedido.

De la atención de la solicitud

- 7.17 La Unidad de Administración dispone las atenciones de las solicitudes de entrega de las imágenes, teniendo en consideración lo siguiente:

Servidor designado como perfil administrador

- 7.17.1 Verificar que las imágenes solicitadas se encuentren almacenadas en los discos duros de las grabadoras digitales.
- 7.17.2 Determinar si las imágenes de terceros (es decir, imágenes de personas que no sean el interesado en intención) están contenidas dentro de las imágenes.
- 7.17.3 Determinar si la solicitud debe ser atendida informando de manera oportuna al jefe de la Unidad de Administración, para que, a través de este, se informe a la Dirección Ejecutiva el motivo de la no entrega de imágenes.
- 7.17.4 Verificar el proceso de búsqueda y descarga, y solicitar a la Unidad de Administración a través del Especialista en Abastecimiento los medios de almacenamiento para la entrega de la información (USB, discos externos, otros) al solicitante.
- 7.17.5 Confirmar la autenticidad de las grabaciones y se encarga de la correcta grabación y procesamiento de imágenes.

Servidor designado como perfil básico

- 7.17.6 Localizar las imágenes en los equipos de grabación de acuerdo con lo solicitado.
- 7.17.7 En caso no se ubiquen las imágenes solicitadas debido a motivos técnicos verificables (falta de capacidad de disco duro, falla de equipo, solicitud extemporánea u otro razonable) debe informar en forma detallada, especificando las razones por las que no se pueden facilitar las imágenes solicitadas, debiendo coordinar las incidencias y acciones a seguir.
- 7.17.8 Procede a descargar en un medio físico de almacenamiento.
- 7.17.9 Verificar que el video emitido es copia fiel del archivo del sistema de videovigilancia.

- 7.18 El servidor designado como perfil administrador emite a la Unidad de Administración el informe en atención a lo solicitado adjuntando el medio de almacenamiento (en caso existan imágenes grabadas), para su derivación al solicitante.

De la confidencialidad

- 7.19 El PEPP protege en todo uso el ciclo de vida de la información, para lo cual vela por la confidencialidad, la cual es garantizar que la información sea accesible solo a aquellas personas autorizadas a tener acceso a la misma.
- 7.20 La Unidad de Administración debe velar porque todo el personal designado, previo al inicio de las funciones, debe haber registrado la "Declaración Jurada de Confidencialidad" (Anexo N° 04).

- 7.21 La administración, grabación y descarga de videos solo se llevará a cabo en el ambiente del sistema de video vigilancia por los servidores debidamente autorizados.
- 7.22 El jefe de la Unidad de Administración y/o el servidor designado como perfil administrador, aseguran que todo el personal que labora en el sistema de videovigilancia se encuentre plenamente informado y capacitado sobre la operación y uso de la información recopilada a través del sistema de videovigilancia.
- 7.23 El jefe de la Unidad de Administración debe velar por el cumplimiento de las disposiciones siguientes:
- 7.23.1 Guardar secreto y confidencialidad sobre la información a la que tienen acceso, con ocasión del ejercicio de sus funciones, preservando la integridad de la información en relación con los videos e imágenes que se graban.
- 7.23.2 Solo ingresará al interior del sistema de videovigilancia los servidores autorizados por el jefe de la Unidad de Administración a través del servidor designado como perfil administrador, debiendo registrarse toda persona que ingrese en el sistema de videovigilancia en el formato de "Registro de Ingreso a los ambientes del sistema de videovigilancia" (Anexo N° 05), sin excepción incluyendo a los servidores designados (encargado y/o operadores), durante las veinticuatro (24) horas del día los siete (7) días de la semana.
- 7.23.3 Está totalmente prohibida la difusión o entrega de videos que se guardan en el sistema de videovigilancia, su extracción y copiado por otros medios portátiles (celulares, videograbadoras portátiles, dispositivos USB u otros similares); así como de permitir el ingreso a los ambientes del sistema de videovigilancia a "personas no autorizadas" y/o atenciones de "solicitudes no autorizadas".
- 7.23.4 Está prohibido la divulgación total o parcial de un video de propiedad y custodia del PEPP, sin la autorización del jefe de la Unidad de Administración.

De las grabaciones y custodia de la información

- 7.24 El acceso a las imágenes grabadas durante los sesenta (30) días anteriores a la fecha de recepción del requerimiento, es de responsabilidad del personal que labora en el sistema de videovigilancia de la Unidad de Administración, los cuales serán almacenados en los servidores del sistema de videovigilancia en resguardo y custodia del Especialista en Informática y Sistemas.
- 7.25 El sistema de grabación digital del sistema de videovigilancia, en resguardo y custodia por el Especialista en Informática y Sistemas almacena las imágenes y videos por espacio de treinta (30) días.
- 7.26 Todo requerimiento solicitado por el Ministerio Público que ha sido atendido será transferido a un archivo digital y debe permanecer en custodia por espacio de un (1) año para futuras solicitudes de investigación. Para tal efecto, la Unidad de Administración planificará las adquisiciones de dispositivos de almacenamiento de información.

De las incidencias

- 7.27 Actos fortuitos: Ante un evento de corte de energía (cortes de luz) y tras la reposición del servicio de energía los servidores del sistema de videovigilancia (encargados y operador) deben verificar que los componentes del sistema se encuentran operativos.
- 7.28 De equipos y software: Los encargados y operador deberán informar y coordinar el servicio de mantenimiento y reparación para la solución de la incidencia.

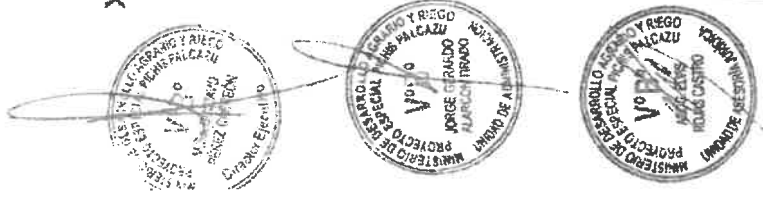
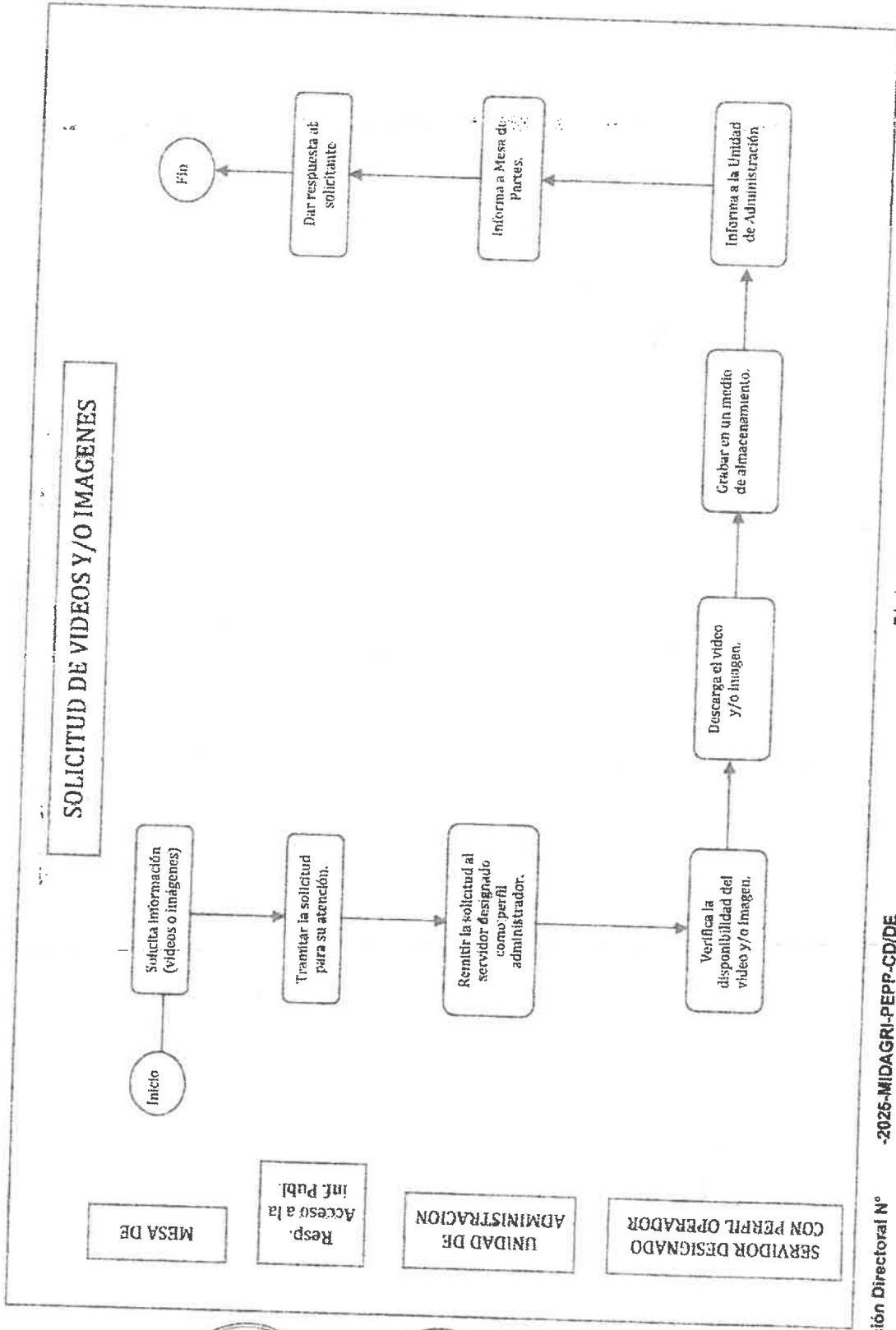
VIII. RESPONSABILIDADES

- 8.1 El responsable de esta directiva, a efectos de su difusión, exigibilidad y cumplimiento, es la Unidad de Administración.
- 8.2 La Unidad de Administración, dispone las medidas que sean necesarias para el cumplimiento de las disposiciones señaladas en la presente Directiva, en el marco de sus competencias y funciones.
- 8.3 La Unidad de Administración, autoriza la atención de solicitudes de información relacionadas al sistema de videovigilancia del PEPP, previa opinión técnica legal de la Unidad de Asesoría Jurídica.
- 8.4 La Unidad de Asesoría Jurídica, es responsable de emitir opinión técnica legal respecto a las solicitudes de acceso de información pública, con relación al sistema de videovigilancia del PEPP.
- 8.5 La Unidad de Administración a través del Especialista en Informática y Sistemas es responsable de brindar el soporte y apoyo técnico necesario a la operatividad de los equipos informáticos (estaciones de monitoreo, equipos DVR, redes y equipos de comunicación) del sistema de videovigilancia; mediante la supervisión de los mantenimientos preventivos y correctivos a ser realizados y supervisión, monitoreo y configuración de los equipos de redes y comunicaciones usados por el sistema de videovigilancia; así como de evaluar y asesorar en el uso de nuevas tecnologías de información y de comunicaciones, promoviendo medidas de seguridad en cumplimiento de la normativa en materia de protección de datos personales.
- Asimismo, a través del Especialista en Sistemas tiene a cargo el resguardo y custodia de los servidores del sistema de videovigilancia instalado en el PEPP.
- 8.6 Las unidades orgánicas y servidores del PEPP, son responsables de dar cumplimiento a lo dispuesto en la presente directiva.

IX. DISPOSICIONES COMPLEMENTARIAS FINALES

- 9.1 Difusión de la normativa.
La Unidad de Administración, es la encargada de las actividades de difusión de la normativa aplicable al tratamiento de datos mediante sistemas de videovigilancia, así como de la promoción para su progresiva implementación en el ámbito del PEPP, brindando servicios de información y orientación.
- 9.2 La presente Directiva tendrá vigencia al día siguiente de notificada su aprobación mediante acto resolutivo.

X. FLUJOGRAMA



XI. ANEXOS

ANEXO 1



ZONA VIDEOVIGILADA



LEY DE PROTECCIÓN DE DATOS PERSONALES - Ley N° 29733

PUEDA EJERCITAR SUS DERECHOS ANTE:

TITULAR DEL BANCO DE DATOS Y DIRECCIÓN

LUGAR DÓNDE PUEDE OBTENER LA INFORMACIÓN CONTENIDA EN EL ARTÍCULO 18 DE LA LPDP

ANEXO 2

HOJA INFORMATIVA SOBRE EL TRATAMIENTO DE DATOS PERSONALES

1. **IDENTIDAD Y DOMICILIO DEL TITULAR DEL BANCO DE DATOS PERSONALES O ENCARGADO DEL TRATAMIENTO:** El titular del presente banco de datos en el que se almacenarán los datos personales facilitados mediante sistema de videovigilancia es con domicilio en

La existencia de este banco de datos personales ha sido declarada a la Autoridad Nacional de Protección de Datos Personales, mediante su inscripción en el Registro Nacional de Protección de Datos Personales con la denominación y el código: RNPDP N°

Se informa al usuario que, cualquier tratamiento de datos personales, se ajusta a lo establecido por la legislación vigente en PERÚ en la materia (Ley N° 29733 y su reglamento).

2. **FINALIDAD:**
El titular del Banco de datos tratará sus datos con la finalidad de

3. **TRANSFERENCIAS Y DESTINATARIOS:** Cuando los datos personales recabados vayan a ser enviados a otras instituciones/empresas (incluido cuando éstas pertenezcan a la misma institución o mismo grupo empresarial) deberá informarse de manera detallada al usuario, de tal forma que éste pueda conocer explícitamente las finalidades determinadas a las que se destinarán los datos. De la siguiente forma:

Los datos personales se transferirán a nivel nacional a: (detalle de la(s) instituciones/empresas destinatarias de los datos) con la finalidad de (finalidad de la transferencia)

Si no realiza transferencia de datos personales, esta información se debe de indicar de la siguiente manera:

Los datos personales no se transferirán a terceros, salvo obligación legal.

4. **PLAZO DURANTE EL CUAL SE CONSERVARAN LOS DATOS PERSONALES:** los datos personales proporcionados se conservarán (durante un plazo de días).
5. **EJERCICIO DE LOS DERECHOS DE INFORMACION, ACCESO, CANCELACION Y OPOSICION DE LOS DATOS:**
Como titular de sus datos personales el usuario tiene el derecho de acceder a sus datos en posesión de (indicar al titular del banco de datos personales); conocer las características de su tratamiento; solicitar sean suprimidos o cancelados al considerarlos innecesarios para las finalidades previamente expuestas o bien oponerse a su tratamiento de ser el caso.

El usuario podrá dirigir su solicitud de ejercicio de los derechos a la siguiente dirección: o a la siguiente dirección de correo electrónico:

A fin de ejercer los derechos antes mencionados, el usuario deberá presentar en el domicilio especificado previamente, la solicitud respectiva en los términos que establece el Reglamento de la Ley N° 29733 (incluyendo: nombre del titular del dato personal y domicilio u otro medio para recibir respuestas; documentos que acrediten su identidad o la representación legal; descripción clara y precisa de los datos respecto de los que busca ejercer sus derechos y otros elementos o documentos que faciliten la localización de los datos).

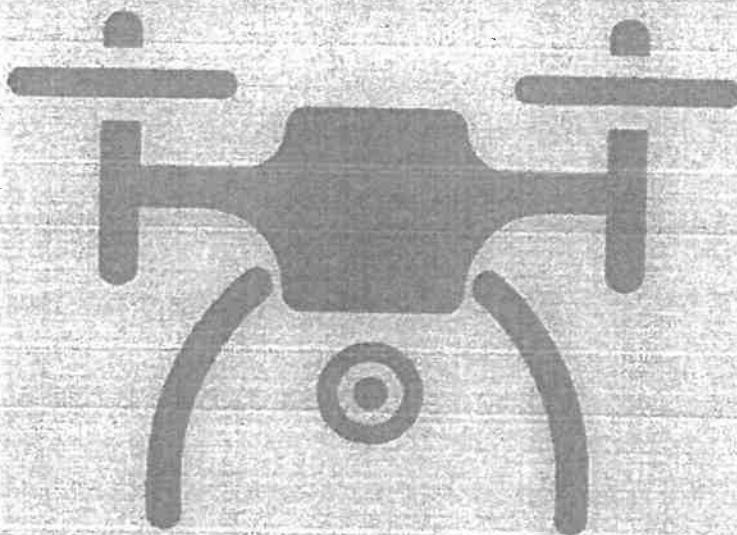
De considerar el usuario que no ha sido atendido en el ejercicio de sus derechos puede presentar una reclamación ante la Autoridad Nacional de Protección de Datos Personales, dirigiéndose a la Mesa de Partes del Ministerio de Justicia y Derechos Humanos:

(Indicar al titular del banco de datos personales) será responsable del banco de datos personales (reiterar denominación del banco de datos, señalados en el numeral 1) y de los datos personales contenidos en éste. Con el objeto de evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de los datos personales o información confidencial facilitados por titulares de datos personales, (Indicar al titular del banco de datos personales) ha adoptado los niveles de seguridad y de protección de datos personales legalmente requerido, y ha instalado todos los medios y medidas técnicas a su alcance.



ANEXO 3

ZONA VIDEOVIGILADA



**LEY DE PROTECCIÓN DE DATOS
PERSONALES - Ley N° 29733**

PUEDE EJERCITAR SUS DERECHOS ANTE:

TITULAR DEL BANCO DE DATOS Y DIRECCIÓN

**LUGAR DÓNDE PUEDE OBTENER LA INFORMACIÓN
CONTENIDA EN EL ARTÍCULO 16 DE LA LPDP**



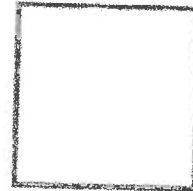
ANEXO 4

DECLARACIÓN JURADA DE CONFIDENCIALIDAD

Yo identificado con DNI N°, servidor del Proyecto Especial Pichis Palcazú – PEPP, en mi condición de Servidor designado como perfil administrador o Servidor designado como perfil básico, me comprometo a mantener confidencialidad de la información que se encuentra en el sistema de videovigilancia instaladas en ambientes físicos del Proyecto Especial Pichis Palcazú - PEPP; asimismo me comprometo a mantener en reserva el usuario, contraseña y otros elementos que el Proyecto Especial Pichis Palcazú - PEPP ponga a mi disposición en el cumplimiento a mis funciones.

..... de del 202....

Firma del Servidor designado como perfil administrador
o Servidor designado como perfil básico
Nombres:
DNI:



Impresión digital
Índice derecho

"Decenio de igualdad de Oportunidades para Mujeres y Hombres"
"Año de la recuperación y la consolidación de la economía peruana"

Chanchamayo, 1 de octubre de 2025.

OFICIO N° 065-2025-CG/OCI-PEPP

Señor:
Gustavo Pérez Carreón
Director Ejecutivo
Proyecto Especial Pichis Palcazú
Av. Perú s/n – Pampa del Carmen
Junín/Chanchamayo/Chanchamayo

MINISTERIO DE DESARROLLO AGRARIO Y RIEGO
PROYECTO ESPECIAL PICHIS PALCAZU
UNIDAD DE ADMINISTRACION

38440 2 OCT. 2025

CUT: FOLIO:
HORA: 4:35 FIRMA:

MINISTERIO DE DESARROLLO AGRARIO Y RIEGO
PROYECTO ESPECIAL PICHIS PALCAZU
DIRECCION EJECUTIVA

3510 01 OCT. 2025

RECIBIDO

Folios: Registro:
Hora: 12:41 Firma:

Asunto : Requerimiento de acciones adoptadas respecto al Informe de Orientación de Oficio n.° 001-2025-OCI/3380-SOO.

Referencia : a) Oficio n.° 054-2025-CG/OCI-PEPP de 18 de julio de 2025.
b) Oficio n.° 365-2025-MIDAGRI-PEPP-CD/DE de 13 de agosto de 2025.
c) Directiva n.° 013-2022-CG/NORM "Servicio de Control Simultáneo", aprobada mediante Resolución de Contraloría n.° 218-2022-CG de 30 de mayo de 2022 y modificatorias.

Tengo el agrado de dirigirme a usted, en relación al documento de la referencia a), mediante el cual, la Jefatura del Órgano de Control Institucional del Proyecto Especial Pichis Palcazú, hizo entrega al titular de la Entidad el Informe de Orientación de Oficio n.° 001-2025-OCI/3380-SOO de 17 de julio de 2025, relacionada a la carencia de normativa interna que regule el tratamiento de datos personales y la operación, uso y mantenimiento del sistema de videovigilancia del PEPP.

Sobre el particular, con documento de la referencia b), vuestro Despacho remitió a este Órgano de Control Institucional el Informe n.° 329-2025-MIDAGRI-PEPP/JA de 11 de agosto de 2025, documento con el cual el Jefe de la Unidad de Administración del Proyecto Especial Pichis Palcazú comunica compromiso para la implementación de medidas correctivas sobre normativa interna para tratamiento de datos personales y sistema de videovigilancia.

En adición a lo antes señalado, en consideración que el precitado informe de control fue remitido a su despacho el 18 de julio de 2025, se verifica que el seguimiento que realiza este Órgano de Control a las acciones que adopte la Entidad, respecto al mencionado informe de control, **venció el 3 de setiembre de 2025.**

Por lo que, estimaré se sirva **remitir la información o documentación sobre las acciones adoptadas en torno a la situación adversa** "La Entidad carece de un documento normativo interno que regule el tratamiento de los datos personales y la operación, uso y mantenimiento del sistema de videovigilancia, o que afectaría la legalidad del tratamiento de la información, así como la continuidad, el uso adecuado y el funcionamiento del sistema de cámaras", debiendo para tal caso acompañar la documentación sustentante.

En ese sentido, estimare que la información solicitada sea remitida a este Órgano de Control Institucional a más tardar el **lunes 6 de octubre de 2025.**

Es propicia la oportunidad para manifestarle las seguridades de mi mayor consideración.

Atentamente,

Robertina Carlosa Martínez Valdivia

Robertina Carlosa Martínez Valdivia
Jefe (e) del Órgano de Control Institucional
Proyecto Especial Pichis Palcazú
Ministerio de Desarrollo Agrario y Riego

URGENTE

PROVEIDO

Pase a: *UA*

Para: *Se cumplimiento de la responsabilidad*

Fecha: *01 OCT. 2025*

MINISTERIO DE DESARROLLO AGRARIO Y RIEGO
PROYECTO ESPECIAL PICHIS PALCAZU
GUSTAVO PÉREZ CARREÓN
Director Ejecutivo

Cc: Archivo OCI
/lrcmv

Cut. 12/10-2025

PROVEIDO

Para:

Fecha:

MINISTERIO DE DESARROLLO AGRARIO Y RIEGO
PROYECTO ESPECIAL PICHIS PALCAZU
JORGE GERARDO ALARCON TIRADO

02 OCT 2025



Chanchamayo, 18 de julio de 2025

OFICIO N° 054-2025-CG/OCI-PEPP

Señor:
Gustavo Pérez Carreón
Director Ejecutivo
Proyecto Especial Pichis Palcazú
Av. Perú s/n Pampa del Carmen
Chanchamayo/Chanchamayo/Junín

MINISTERIO DE DESARROLLO AGRARIO Y RIEGO
PROYECTO ESPECIAL PICHIS PALCAZU
DIRECCION EJECUTIVA
2560 18 JUL. 2025
RECIBIDO
Folios: Registro:
Hora: 12:30 Firma:

- Asunto** : Notificación de Informe de Orientación de Oficio n.° 001-2025-OCI/3380-SOO
- Referencia** : a) Artículo 8° de la Ley n.° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República y sus modificatorias.
b) Directiva n.° 013-2022-CG/NORM "Servicio de Control Simultáneo", aprobada con Resolución de Contraloría n.° 218-2022-CG publicada el 31 de mayo de 2022 y modificatorias.

Me dirijo a usted en el marco de la normativa de la referencia, que regula el Servicio de Control Simultáneo y establece la comunicación al Titular de la entidad o responsable de la dependencia, y de ser el caso a las instancias competentes, respecto de la existencia de situaciones adversas que afectan o podrían afectar la continuidad del proceso, el resultado o el logro de los objetivos del proceso en curso, a fin de que se adopten oportunamente las acciones preventivas y correctivas que correspondan.

Sobre el particular, de la revisión de la información y documentación vinculada a la "Carencia de normativa interna que regule el tratamiento de datos personales y la operación, uso y mantenimiento del sistema de videovigilancia del PEPP", comunicamos que se ha identificado una (1) situación adversa contenida en el Informe de Orientación de Oficio n.° 001-2025-OCI/3380-SOO, que se adjunta al presente documento.

En tal sentido, solicitamos comunicar al Órgano de Control Institucional del Proyecto Especial Pichis Palcazú, en el plazo máximo de cinco (5) días hábiles desde la comunicación del presente Informe, las acciones preventivas o correctivas adoptadas y por adoptar respecto a la situación adversa identificada en el citado Informe, adjuntando la documentación de sustento respectiva.

Es propicia la oportunidad para expresarle las seguridades de mi consideración.

Atentamente,

PROVEIDO
Pase a: UA
Para: Alvarado
..... JCI/OCI
Fecha: 12/19-2025



MINISTERIO DE DESARROLLO AGRARIO Y RIEGO
PROYECTO ESPECIAL PICHIS PALCAZU
MG. JESÚS COLQUINGA
Jefe (e) Órgano de Control Institucional

PROVEIDO
Pase a: UA
Para: Su implementación
Digo Responsabilidad
Fecha: 18 JUL. 2025



21 JUL. 2025

**ÓRGANO DE CONTROL INSTITUCIONAL
PROYECTO ESPECIAL PICHIS PALCAZÚ**

**INFORME DE ORIENTACIÓN DE OFICIO
N° 001-2025-OCI/3380-SOO**

**ORIENTACIÓN DE OFICIO
PROYECTO ESPECIAL PICHIS PALCAZÚ
CHANCHAMAYO, CHANCHAMAYO, JUNÍN**

**“CARENCIA DE NORMATIVA INTERNA QUE REGULE EL
TRATAMIENTO DE DATOS PERSONALES Y LA
OPERACIÓN, USO Y MANTENIMIENTO DEL SISTEMA DE
VIDEOVIGILANCIA DEL PEPP”**

**PERÍODO DE EVALUACIÓN:
DEL 12 DE JUNIO AL 17 DE JULIO DE 2025**

TOMO I DE I

CHANCHAMAYO, 17 DE JULIO DE 2025