Resolución Directoral
N° 02-2020-JUS/DGTAIPD

Lima, 10 de enero de 2020

CONSIDERANDO:

Que, el inciso 6 del artículo 2 de la Constitución Política del Perú señala que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar;

Que, la Ley N° 29733, Ley de Protección de Datos Personales, tiene por objeto garantizar el derecho fundamental a la protección de datos personales, previsto en el numeral 6 del artículo 2 de la Constitución Política del Perú;

Que, la mencionada norma legal, creó la Autoridad Nacional de Protección de Datos Personales como el órgano competente para realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones de dicha Ley y su Reglamento;

Que, la Autoridad Nacional de Protección de Datos Personales ejerce funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras de acuerdo con lo establecido en el artículo 33° de la Ley N° 29733, Ley de Protección de Datos Personales;

Que, en mérito a sus competencias normativas, la Autoridad Nacional de Protección de Datos Personales de conformidad con lo dispuesto en el inciso 12 artículo 33 de la Ley N° 29733, puede emitir las directivas que correspondan para la mejor aplicación de lo previsto en la Ley y su reglamento;

Que, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales como órgano de línea del Despacho Viceministerial de Justicia del Ministerio de Justicia y Derechos Humanos, de conformidad con lo establecido en el inciso a) del artículo 71 del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado por Decreto Supremo N° 013-2017-JUS, ejerce la Autoridad Nacional de Protección de Datos Personales;

Que, actualmente es innegable el aumento de instalación de sistemas videovigilancia en el país para la seguridad, control laboral, así como otras finalidades, por lo que resulta necesario contar con una directiva que establezca las disposiciones para que el tratamiento de los datos personales que se efectúe a través de dichas

cámaras u otros dispositivos similares se realice acorde con lo establecido en la normativa de protección de datos personales;

Que, habiéndose recabado los comentarios, sugerencias y observaciones de los interesados conforme lo dispuesto en la Resolución Directoral N° 54-2019-JUS/DGTAIPD de 16 de agosto de 2019, corresponde aprobar el texto definitivo de la Directiva para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia;

De conformidad con la Constitución Política del Perú; Ley N° 29733, Ley de Protección de Datos Personales; Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado por Decreto Supremo Nº 013-2017-JUSR y el Reglamento que establece disposiciones relativas a la publicidad, publicación de Proyectos Normativos y difusión de normas legales de carácter general, aprobado por Decreto Supremo Nº 001-2009-JUS;

SE RESUELVE:

Artículo 1.- Aprobación de la Directiva para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia

Aprobar la Directiva para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia, así como sus anexos, los mismos que forman parte de la presente Resolución Directoral.

Artículo 2.- Publicidad

La presente Resolución Directoral se publica en el Diario Oficial El Peruano. La Directiva aprobada en el artículo 1 y sus Anexos, se publican en el portal institucional del Ministerio de Justicia y Derechos Humanos – MINJUSDH (https://www.gob.pe/minjus), en la misma fecha de publicación de esta norma.

Artículo 3.- Resultados del período de consulta pública

Publicar en el Portal Institucional del Ministerio de Justicia y Derechos Humanos – MINJUSDH (https://www.gob.pe/minjus) la Matriz que sistematiza y absuelve los comentarios, observaciones y sugerencias recibidas por la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales durante el período de prepublicación de la propuesta de Directiva.

Regístrese, comuníquese y publíquese.

EDUARDO LUNA CERVANTES
Director General de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
Ministerio de Justicia y Derechos Humanos

DIRECTIVA N° 01-2020-JUS/DGTAIPD
TRATAMIENTO DE DATOS PERSONALES MEDIANTE SISTEMAS DE VIDEOVIGILANCIA

FORMULADA POR: Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
Dirección de Protección de Datos Personales

I. OBJETIVO

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. BASE LEGAL

- Constitución Política del Perú.
- Ley N° 27153, Ley que regula la explotación de juegos de casinos y máquinas tragamonedas.
- Ley N° 27933, Ley del Sistema de Seguridad Ciudadana.
- Ley N° 29733, Ley de Protección de Datos Personales (LPDP)
- Ley N° 27972, Ley Orgánica de Municipalidades.
- Ley N° 30120, Ley de Apoyo a la Seguridad Ciudadana con Cámaras de Videovigilancia Públicas y Privadas.
- Ley N° 30037, Ley que Previene y Sanciona la Violencia en los Espectáculos Deportivos.
- Ley N° 30740, Ley que regula el uso y las operaciones de los sistemas de aeronaves pilotadas a distancia (RPAS).
- Decreto Legislativo N° 1218, que regula el uso de las cámaras de videovigilancia.
- Decreto Supremo Nº 003-97-TR, que aprueba el Texto Único Ordenado de la Ley de Productividad y competitividad laboral.
- Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley de Protección de Datos Personales.
- Decreto Supremo N° 011-2014-IN, que aprueba el Reglamento de la Ley N° 27933, Ley del Sistema Nacional de Seguridad Ciudadana.
- Decreto Supremo N° 007-2016-IN, que aprueba el Reglamento de la Ley N° 30037, Ley que previene y sanciona la violencia en los espectáculos deportivos.
- Decreto Supremo N° 013-2017-JUS, que aprueba el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.
- Decreto Supremo N° 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley de Procedimiento Administrativo general, Ley N° 27444.
- Decreto Supremo N° 018-2013-MINJUS, que aprueba el Texto Único Ordenado de la Ley Orgánica del Ministerio de Justicia y Derechos Humanos, modificado por Resolución Ministerial N° 065-2017-JUS.
- Decreto Supremo N° 009-2002-MINCETUR, que aprueba el Reglamento de la Ley N° 27153, que regula la explotación de juegos de casinos y máquinas tragamonedas,
- Resolución Directoral N° 709-2005-MINCETUR/VTM/DNT: "Normas complementarias a la instalación del sistema de video en la sala de juego y máquinas tragamonedas".

F. LUNA C.

O. ESCUDERO V.

M. GONZALEZ L.

III. ALCANCE

Las disposiciones contenidas en la presente directiva se aplican a toda persona natural y jurídica que realice tratamiento de datos personales a través de sistemas de videovigilancia y, en general, mediante cualquier dispositivo que permita el tratamiento de datos para dicho fin.

Las entidades de la Administración Pública señaladas en el artículo I de la Ley N° 27444, Ley del Procedimiento Administrativo General, se sujetarán a aquellas disposiciones de la presente directiva que resulten aplicables conforme a las normas comunes de derecho público.

IV. RESPONSABLE:

El responsable de esta directiva, a efectos de su difusión, exigibilidad y cumplimiento, es la Autoridad Nacional de Protección de Datos Personales que es ejercida por el Ministerio de Justicia y Derechos Humanos a través de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

PERÚ
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

V. DEFINICIONES Y/O SIGLAS

5.1 **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.

PERÚ
Dirección de Fiscalización e Instrucción
ESCUDERO V.

5.2 **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.

5.3 **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.

PERÚ
Dirección de Protección de Datos Personales
M. GONZALEZ I.

5.4 **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.

5.5 **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.

5.6 **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.

5.7 **CD:**
Disco compacto.

5.8 **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.

5.9 **Días:** Días hábiles.

5.10 **Dron:**
Aeronave no tripulada.

5.11 **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.

5.12 **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.

5.13 **LPDP**:
Ley N° 29733, Ley de Protección de Datos Personales.

5.14 **Máscara de privacidad:**
Permite bloquear y/o anonimizar determinadas partes de una imagen que no se visualizará o captará por la cámara o videocámara.

5.15 **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.

5.16 **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:

5.16.1 **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 encargado del tratamiento.

5.16.2 **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

PERÚ
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

PERÚ
Dirección de Fiscalización e Instrucción
O. ESCUDERO V.

PERÚ
Dirección de Protección de Datos Personales
M. GONZALEZ L.

reguladas en esta directiva. El perfil intermedio se encuentra bajo la dirección del perfil administrador.

5.16.3 **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.

5.17 **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 autentificación de los usuarios, así como los responsables de realizar dichos procesos.

PERU
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

5.18 **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.

PERU
Dirección de Fiscalización e Instrucción
J. ESCUDERO V.

5.19 **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.

PERU
Dirección de Protección de Datos Personales
M. GONZALEZ I.

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

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

5.22 **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.

5.23 **Tipos de prestación en contratos de encargo de sistemas de videovigilancia**:

5.23.1 **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.

5.23.2 **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.

5.24 **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, vídeos o audios.

Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

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

5.26 **Videoportería**:
Sistema autónomo que sirve para gestionar las llamadas que se hacen en la puerta de un edificio (sea complejo residencial, vivienda unifamiliar, centros de trabajo, etc.), controlando el acceso al mismo mediante la comunicación audiovisual entre el interior y el exterior. La característica principal de la videoportería es que permite que la persona que ocupa el interior identifique a la visita, pudiendo, si lo desea, entablar una conversación y/o abrir la puerta para permitir el acceso de la persona que ha activado un timbre o dispositivo de comunicación.

Dirección de Fiscalización e Instrucción
J. ESCUDERO V.

5.27 **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.

5.28 **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.

Dirección de Protección de Datos Personales
M. GONZALEZ L.

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.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

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, sí 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:

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Fiscalización e Instrucción
ESCUDERO V.

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.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

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.

PERU Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

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.

PERU Dirección de Fiscalización e Instrucción
O. ESCUDERO V.

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.

PERU Ministerio de Justicia y Derechos Humanos Dirección de Protección de Datos Personales
M. GONZALEZ L.

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.

PERU Ministerio de Justicia y Derechos Humanos
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

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.

PERU
Dirección de Fiscalización e Instrucción
Q. ESCUDERO V.

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.

PERU Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

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 de sesenta (60), salvo disposición distinta en normas sectoriales. 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 en el plazo máximo de dos (02) días hábiles, salvo disposición distinta en norma sectorial.

PERÚ Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

6.16 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.

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.

PERÚ Dirección de Fiscalización e Instrucción
O. ESCUDERO V.

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.

PERÚ Dirección de Protección de Datos Personales
M. GONZALEZ L.

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 37 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 38 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 autentificación 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.

PERU
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

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.

PERU
Dirección de Fiscalización e Instrucción
O. ESQUIVERO V.

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.

PERU
Dirección de Protección de Datos Personales
M. GONZALEZ L.

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.

PERU
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

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.

PERU
Dirección de Fiscalización e Instrucción
O. ESCUDERO V.

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.

PERU
Dirección de Protección de Datos Personales
M. GONZALEZ L.

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, vídeos 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.

Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

Dirección de Fiscalización e Instrucción
O. ESCUDERO V.

Dirección de Protección de Datos Personales
M. GONZALEZ L.

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.

PERU
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

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.

PERU
Dirección de Fiscalización e Instrucción
O. ESCUDERO V.

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 solitud 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 67 y 71 del RLPDP. Asimismo, procederá la atención en aquellos supuestos donde sea materialmente posible y responda a criterios fundamentados y motivados.

PERU
Dirección de Protección de Datos Personales
M. GONZALEZ L.

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.

PERÚ Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

VII. DISPOSICIONES ESPECÍFICAS

TRATAMIENTOS ESPECÍFICOS CON FINES DE SEGURIDAD

Espacios públicos de uso privado

Prohibiciones de uso de sistemas de videovigilancia en determinados espacios.

7.1 En espacios públicos de uso privado, como establecimientos comerciales, restaurantes, lugares de ocio, entre otras, se deberá cumplir en estricto con el principio de proporcionalidad, de esta forma a título enunciativo se tiene que:

PERÚ Dirección de Fiscalización e Instrucción
. ESCUDERO V.

7.1.1 Se encuentra prohibida la instalación de cámaras en baños y vestuarios.

7.1.2 En los lugares de ocio:

a) El sistema de videovigilancia sólo puede ser visual, está prohibida la grabación de las conversaciones. Además, deberá utilizarse sólo cuando no exista otro método de seguridad menos invasivo e igual de eficaz que cumpla con la finalidad legítima determinada.

b) No se pueden utilizar las imágenes captadas por sistemas de videovigilancia con fines comerciales o promocionales, salvo consentimiento de las personas cuyas imágenes han sido grabadas.

PERÚ Dirección de Protección de Datos Personales
M. GONZALEZ L.

Entidades financieras

Características especiales

7.2 Dado los servicios que presta la entidad financiera deberá tenerse en cuenta lo siguiente:

7.2.1 Que lo captado a través de los sistemas de videovigilancia y contenido en los soportes informáticos tiene que ser utilizado exclusivamente para fines de seguridad.

7.2.2 Las imágenes que registren la supuesta comisión de un acto delictivo o falta, deben ser puestas a conocimiento de la Policía Nacional del Perú o del Ministerio Público de forma inmediata, como medio de identificación de los presuntos autores de delitos.

7.2.3 Si la entidad financiera decide no encargar el tratamiento de los sistemas de videovigilancia a una empresa especializada en sistemas de seguridad videovigilada, debe contar con un responsable de la propia entidad especializado en sistemas de seguridad videovigilada.

7.2.4 Si una cámara se ubica en la puerta de entrada de una entidad bancaria debe orientarse de modo que la parte de vía pública que capte se limite al acceso vigilado, sin recoger más proporción de la vía pública que la imprescindible para efectos de la labor de vigilancia, no debiendo captar imágenes del resto de la acera o la calle.

7.2.5 Otras disposiciones de acuerdo a las normas específicas sobre la materia.

PERU Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

Entornos escolares

Requisitos de los sistemas de videovigilancia en entornos escolares

7.3 En el caso de uso de sistemas de videovigilancia, se debe instalar un distintivo o cartel informando a los miembros de la comunidad educativa de la existencia de cámaras u otros dispositivos análogos, en un lugar completamente visible, tanto si los dispositivos están en el interior como en espacios abiertos. En dicho distintivo o cartel debe también indicarse dónde se puede obtener la información que regula el artículo 18 de la LPDP.

PERU Dirección de Fiscalización e Instrucción
D. ESCUDERO V.

7.4 La zona objeto de videovigilancia será la mínima imprescindible para el fin de vigilancia trazado, pudiendo abarcar espacios públicos o comunes como accesos y pasillos, patio de recreo, comedores, y siempre con miras a la protección y defensa del interés superior del niño, niña y adolescente.

7.5 En ningún caso deben instalarse cámaras de videovigilancia en espacios privados como baños, vestuarios o aquellos en los que se desarrollen actividades cuya captación pueda afectar la imagen o la intimidad de forma desproporcionada.

PERU Dirección de Protección de Datos Personales
M. GONZALEZ L.

7.6 Los usos de sistemas de videovigilancia con fines de seguridad en aulas y otros ámbitos en los que se desarrolla la personalidad de los niños, niñas y adolescentes podrán grabar imágenes si existen circunstancias excepcionales, justificadas por la presencia de un riesgo objetivo y previsible para la seguridad y los derechos fundamentales de los menores.

7.7 El acceso a las imágenes de los sistemas de videovigilancia queda restringido al director del centro o a la persona designada como responsable del tratamiento. No puede ser de libre acceso para cualquier personal docente o administrativo no autorizado para ello.

Cancelación de las imágenes

7.8 Las imágenes se conservarán por un plazo máximo de treinta (30) días desde su captación. Transcurrido dicho plazo, el titular del banco de datos o responsable del tratamiento únicamente podrá conservar aquellas imágenes que revelen algún

hecho trascendente que deba ser puesto en conocimiento de los padres de familia o tutores, quienes de acuerdo a sus facultades pueden actuar velando por los intereses de sus menores hijos en defensa y protección de sus derechos o, de ser el caso, frente a la comisión de presuntos actos delictivos poniendo en conocimiento los hechos a la Policía Nacional o del Ministerio Público.

TRATAMIENTO DISTINTO A LOS FINES DE SEGURIDAD

Videovigilancia para el control laboral

Excepción al consentimiento en torno de la finalidad

7.9 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.

PERÚ Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

Deber de Informar

7.10 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.

En el caso de trabajadores del hogar, para acreditar el cumplimiento del deber de informar, bastará con que los empleadores acrediten de forma razonable que han cumplido con el deber de informar contenido en el artículo 18 de la LPDP.

PERÚ Dirección de Fiscalización e Instrucción
O. ESCUDERO V.

Finalidad de los sistemas de videovigilancia

7.11 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.

7.12 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.

PERÚ Dirección de Protección de Datos Personales
M. GONZALEZ L.

Principio de proporcionalidad

7.13 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.

7.14 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.

7.15 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.

7.16 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.

7.17 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

7.18 Las imágenes y/o voces grabadas se almacenan por un plazo de treinta (30) días y hasta un plazo máximo de sesenta (60) días, 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.

PERÚ Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

7.19 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 en el plazo máximo de dos (02) días hábiles, salvo disposición distinta en norma sectorial.

7.20 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.

PERÚ Dirección de Fiscalización e Instrucción
O. ESCUDERO V.

7.21 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.

7.22 El trabajador podrá solicitar el acceso a las grabaciones o a una copia digital de las mismas que contengan información sobre una inconducta 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 inconducta 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.

PERÚ Dirección de Protección de Datos Personales
M. GONZALEZ L.

7.23 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

7.24 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

7.25 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

7.26 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.

PERU Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales E. LUNA C.

TRATAMIENTO DE DATOS CON OTRAS TECNOLOGÍAS

Cámaras conectadas a internet

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

7.27 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.

PERU Dirección de Fiscalización e Instrucción ESCUDERO V.

7.28 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

7.29 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.

PERU Dirección de Protección de Datos Personales M. GONZALEZ L.

Responsabilidad del titular y/o encargado del tratamiento

7.30 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.

7.31 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.

PERÚ
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

7.32 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.

VIII. DISPOSICIONES COMPLEMENTARIAS FINALES

PERÚ
Dirección de Fiscalización e Instrucción
O. ESCUDERO V.

8.1 **Difusión de la normativa**
La Autoridad Nacional de Protección de Datos Personales ejercida por el Ministerio de Justicia y Derechos Humanos a través de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, 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 privado y público, brindando servicios de información y orientación.

8.2 **Vigencia**
La presente Directiva entrará en vigencia a los sesenta (60) días calendario siguientes de la publicación de la Resolución que la aprueba en el Diario Oficial "El Peruano".

PERÚ
Dirección de Protección de Datos Personales
M. GONZALEZ L.

ANEXO 1

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Fiscalización e Instrucción
O. ESCUDERO V.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

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 empresas (incluso cuando éstas pertenezcan al 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 las empresas destinatarias de los datos) con la finalidad de ..... (finalidad de la transferencia).

   Los datos personales se transferirán a nivel internacional a: .....(indicar denominación de la empresa, país y finalidad de la transferencia).

PERÚ Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales E. LUNA C.

PERÚ Dirección de Fiscalización e Instrucción O. ESCUDERO V.

PERÚ Ministerio de Justicia y Derechos Humanos Dirección de Protección de Datos Personales M. GONZALEZ

La ENTIDAD contrata los servicios en la nube (computación en la nube) a través de: .....(detalle el nombre de la empresa y ubicación geográfica del servidor en el que se puedan almacenar los datos personales).

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

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

4. **PLAZO DURANTE EL CUAL SE CONSERVARAN LOS DATOS PERSONALES:** Los datos personales proporcionados se conservaran (durante un plazo de ... días).

5. **EJERCICIO DE LOS DERECHOS DE INFORMACION, ACCESO, CANCELACIÓN Y OPOSICIÓN 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 respuesta; 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

PERU Direccion General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

PERU Dirección de Fiscalización e Instrucción
O. ESCUDERO

PERU Dirección de Protección de Datos Personales
M. GONZALEZ

Personales, dirigiéndose a la Mesa de Partes del Ministerio de Justicia y Derechos Humanos: Calle Scipion Llona 350, Miraflores, Lima, Perú.

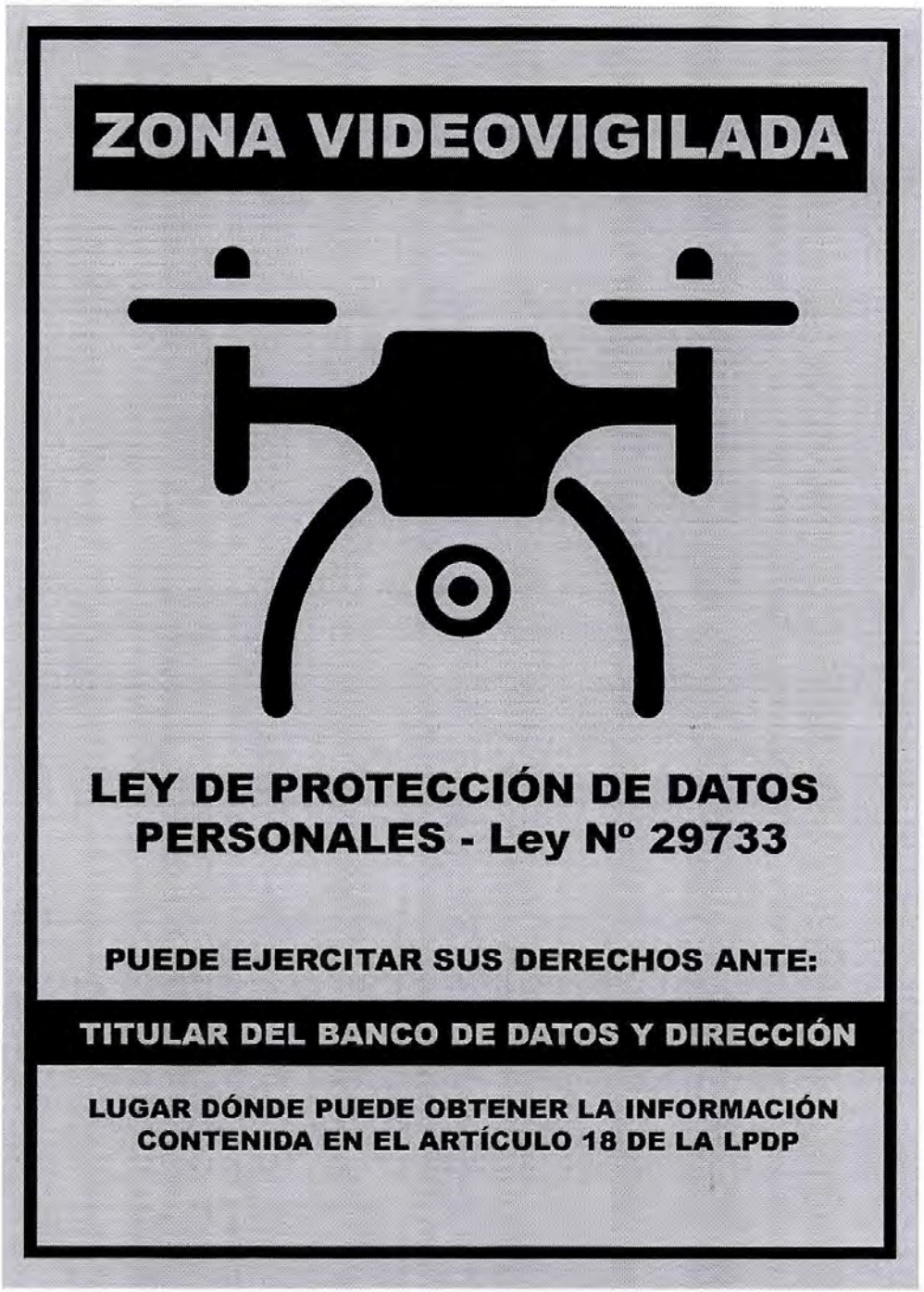
(Indicar al titular del banco de datos personales)..... será responsable del banco de datos personales .....(reiterar denominación del banco de datos, señalado en el numeral 1) y de los datos personales contenidos en éste. Con el objeto de evitar la pérdida, mal uso, alteración, acceso no autorizado 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 requeridos, y ha instalado todos los medios y medidas técnicas a su alcance.

PERÚ
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA

PERÚ
Dirección de Fiscalización e Instrucción
ESCUDERO V.

PERÚ
Dirección de Protección de Datos Personales
M. GONZALEZ

ANEXO 3



PERÚ
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
E. LUNA C.

PERÚ
Dirección de Fiscalización e Instrucción
ESCUDERO V.

PERÚ
Dirección de Protección de Datos Personales
M. GONZALEZ L.