

CASOS PRÁCTICOS SOBRE LA APLICACIÓN DE LOS PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES



Olga María Escudero Vílchez
Directora de la Dirección de Fiscalización e Instrucción
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
Autoridad Nacional de Protección de Datos Personales

¿QUÉ ES UN...

...dato personal?

Toda Información
que te identifica o te
hace identificable.



...dato sensible?

Son datos que tienen
especial protección.
Están constituidos por:



¿De quien son los datos personales?

De la persona titular, como lo son los clientes de una entidad crediticia, los alumnos de una institución educativa, o el personal de una empresa.

¿Qué se entiende por tratamiento de datos personales?

En la práctica, cualquier actividad en la que estén presentes datos personales constituirá un tratamiento, se realice de manera manual o automatizada. Como la **recopilación**, **registro**, **almacenamiento**, **consulta**, **utilización**, **bloqueo**, **difusión**, **interconexión**....

Los Principios en protección de datos

El responsable del tratamiento será responsable del cumplimiento de estos principios:

- Principio de legalidad
- Principio de consentimiento
- Principio de finalidad
- Principio de proporcionalidad
- Principio de calidad
- Principio de seguridad

Principio de Legalidad

Artículo 4° de la LPDP

El tratamiento de los datos personales se hace conforme a lo establecido en la ley. Se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.



CASUÍSTICA: TRATAMIENTO DE ANTECEDENTES

A través de un sistema web ofertado por una “empresa de verificación”, se expedía un informe respecto al perfil del postulante a una plaza laboral a cambio de una contraprestación económica.

La información que proporcionaba esta empresa contenía datos referidos a **antecedentes y denuncias policiales** (comisaría), **requisitorias** (RQ), **antecedentes judiciales**, **antecedentes penales**, **detenciones policiales** (RENADESPPLE), **denuncias ante el Ministerio Público** - Fiscalía; datos que únicamente podría entregar la persona titular de los mismos o la entidad legalmente autorizada para ello.

Por lo cual, quedó claro que el tratamiento de datos personales referidos a antecedentes realizado por la empresa, al ser una entidad privada sin competencia para ello, deviene en desleal e ilícito, ya que el acceso a la misma está restringido únicamente para las entidades públicas con competencia para ello.

Infracción: **literal b, numeral 3, artículo 132° del RLPDP**, esto es, *“Recopilar datos personales mediante medios fraudulentos, desleales o ilícitos”*, dicha infracción es **muy grave**, **sanción de +50 UIT hasta 100 UIT**.



Principio de Consentimiento

Artículo 5° de la LPDP

Los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo que la ley lo autorice.

El consentimiento debe ser:

Libre

Expreso

Previo

Informado

Datos sensibles:
por escrito

¿Puedo revocar
mi consentimiento
en cualquier
momento?



CASUÍSTICA: Llamadas para publicidad sin consentimiento

La denunciante venía recibiendo constantes llamadas de prospección comercial de una empresa de seguros oncológicos, pese a no contar con su consentimiento. Adicional a ello, la denunciante había ejercido su derecho de oposición al uso de sus datos, por lo cual, la empresa la había registrado en una lista de no contactabilidad, sin embargo, la continuaban llamando telefónicamente.

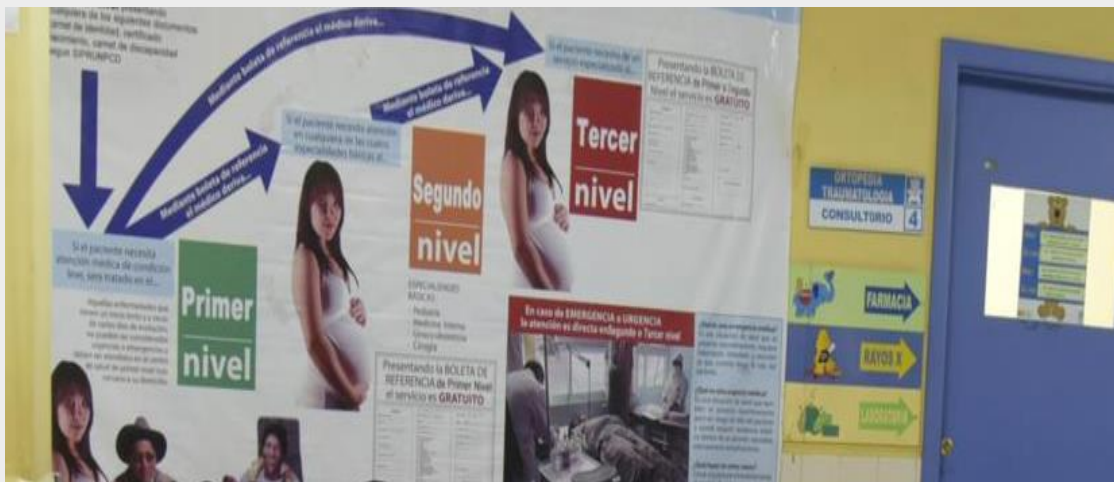
Se debe precisar que las llamadas recibidas vulneran el derecho a la protección de los datos personales de la denunciante, máxime si la propia afectada había manifestado a la administrada su negativa para que continúen contactándola vía comunicaciones telefónicas, no obstante, estas persistieron.



Infracción: **literal b, numeral 2 del artículo 132° del RLPDP**: “Dar tratamiento a datos personales sin el consentimiento libre, expreso, inequívoco, revió e informado del titular, cuando el mismo sea necesario conforme a los dispuesto en la ley n.º 29733 y su Reglamento”, dicha infracción es **grave, sanción de 5 UIT hasta 50 UIT**.

CASUÍSTICA

Un Hospital público difunde imágenes en su sitio web, así como al interior de las instalaciones del mismo (existen periódicos murales y cuadros donde se exhiben imágenes de personas menores de edad y adultos). Si bien la administrada presentó un documento denominado “Autorización Cesión de Derechos de Imagen” para acreditar la obtención del consentimiento, se verificó que el consentimiento obtenido no era válido al no cumplir con la característica de ser informado



Infracción: **literal b, numeral 2, artículo 132° del RLPDP**, esto es, “*Dar tratamiento a los datos personales sin el consentimiento, libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la Ley n.º 29733 y su Reglamento*”, dicha infracción es **grave**, sanción de **+5 UIT hasta 50 UIT**.

Principio de Finalidad

Artículo 6° de la LPDP

Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita.

Los datos personales no deben ser tratados para una finalidad distinta a la establecida al momento de su recopilación.

Hay que tener establecido claramente el motivo por el cual se recopilan los datos personales.



CASUÍSTICA

Una institución educativa utilizó los datos personales de los alumnos para transferirlos a una Universidad para que les ofrezcan los planes educativos, sin contar con el consentimiento.

Los datos solicitados por la institución educativa, de acuerdo a la inscripción de su banco de datos personales denominado “Alumnos”, tiene como finalidad: *“Recopilar los datos personales para prestar el servicio educativo”*.

Si se recopilaron los datos para realizar la matrícula, no se podrán utilizar para finalidades diferentes de la prestación del servicio educativo, como la publicación de fotografías de los alumnos en la web del centro o la comunicación de sus datos a museos o empresas para organizar visitas, salvo que se haya recabado el consentimiento.

Infracción: **literal e, numeral 2, del artículo 132° del RLPDP**, *“Utilizar los datos personales obtenidos lícitamente para finalidades distintas de aquellas que motivaron su recopilación, salvo que medie procedimiento de anonimización o disociación”*, dicha infracción es **grave**, **sanción de +5 UIT hasta 50 UIT**.

CASUÍSTICA

Se presentó una denuncia contra una entidad financiera por realizar llamadas constantes para publicidad sin contar con el consentimiento del afectado.

La entidad financiera indicó que los datos del denunciante los recopiló de la base de datos de la **Central de Riesgos de la SBS** que constituye una fuente de acceso al público y los transfirió a un *call center* para que realicen la prospección comercial

La caja municipal realizó el tratamiento (recopilación, almacenamiento y uso) de los datos personales del denunciante obtenidos de forma lícita de la base de datos de la SBS, para una **finalidad distinta** de aquella que motivó su recopilación, como es la evaluación del historial crediticio en el caso que el interesado solicite un crédito, y en su lugar los utilizó para enriquecer su banco de datos personales de potenciales clientes, a fin de contactarlos para ofrecerles publicidad.

Infracción grave: **literal e, numeral 2, del artículo 132° del RLPDP**, “Utilizar los datos personales obtenidos lícitamente para finalidades distintas de aquellas que motivaron su recopilación, salvo que medie procedimiento de anonimización o disociación”, dicha infracción es **grave**, sanción de **+5 UIT hasta 50 UIT**.

Principio de Proporcionalidad

Artículo 7° de la LPDP

El tratamiento de los datos debe ser adecuado, relevante y no excesivo respecto de la finalidad de su recopilación.

Para la entrega de productos adquiridos vía online, las empresas solo deben solicitar la información personal necesaria.



No debes permitir que le tomen una foto a tu DNI

CASUÍSTICA

Recibimos una denuncia contra una institución educativa por haber colocado cámaras de videovigilancia dentro de los **salones de clase**, ante ello, la institución educativa manifestó que la finalidad de la instalación de las cámaras de videovigilancia radicaba en la prevención y rápido actuar frente a casos de violencia escolar de manera efectiva, así como, preservar los bienes de los estudiantes.

La instalación de cámaras de videovigilancia en las aulas de una institución educativa sería viable únicamente ante una **circunstancia excepcional**, donde la necesidad de tal medida se pueda demostrar o justificar claramente por la presencia de un riesgo objetivo y previsible para la seguridad de los menores.

En el caso analizado, el uso de cámaras de videovigilancia en las aulas resultaría ser una medida excesiva y **desproporcionada**, ya que no se demostró que sea indispensable para prevenir casos de violencia escolar o para preservar los bienes de los estudiantes.



Infracción: **literal b, numeral 1 del artículo 132° del RLPDP:** *“Recopilar datos personales que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos”*, dicha infracción es **leve**, **sanción de 0,5 UIT hasta 5 UIT**.



¿Qué es la Videovigilancia?

Es el monitoreo y captación de imágenes, videos o audios de lugares, personas u objetos.

¿Cuándo se da un tratamiento de datos personales a través de los sistemas de videovigilancia?

La imagen de una persona en la medida que identifique o pueda identificar a la misma constituye un dato personal, que puede ser objeto de tratamiento para diversas finalidades.

La instalación de sistemas de videovigilancia con la finalidad de garantizar la seguridad de personas e instalaciones es una realidad en un importante número de espacios y cuya tendencia va en aumento.

¿Se debe informar de la existencia de un sistema de videovigilancia?

Una de las obligaciones que conlleva el uso de la videovigilancia con fines de seguridad, en relación con la protección de datos, es cumplir con el **derecho de información**, mediante un distintivo informativo.

También se deberá disponer de una **cláusula informativa** que incluya los extremos exigidos por el art. 18 de la LPDP.

Ubicación de los carteles

- ✓ Lugar visible.
- ✓ En cada acceso.

DIRECTIVA N° 01-2020-JUS/DGTAIPD



gob.pe

<https://www.gob.pe/institucion/anpd/informes-publicaciones/1938476-directiva-para-el-tratamiento-de-datos-personales-mediante-sistemas-de-videovigilancia>

Principio de Calidad

Artículo 8° de la LPDP

Los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados.



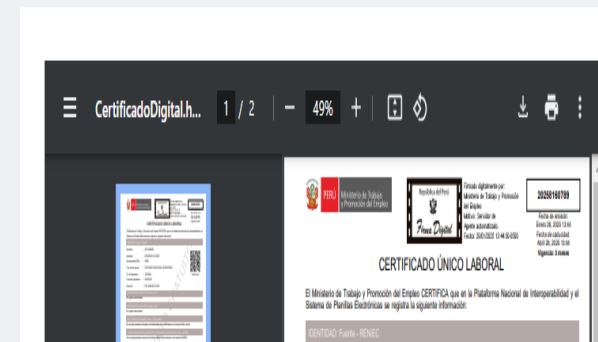
CASUÍSTICA

Ingresó una denuncia donde una ciudadana evidenció que en el **Certificado Único Laboral** (CUL), en el apartado de experiencia laboral figuraba como trabajadora de una empresa desde el año 2017 hasta la actualidad, pese a no haber mantenido vínculo laboral alguno.

El Ministerio encargado refirió que la información de la experiencia laboral la obtiene de la planilla electrónica proporcionada por la SUNAT, no obstante, al ser el titular del banco de datos, debe contar con filtros y mecanismos que permitan verificar la **veracidad** y **exactitud** de los datos personales que suministra a través del certificado único laboral en relación a la experiencia laboral de los trabajadores que registran las entidades en la planilla electrónica, y así evitar que figuren trabajadores relacionados con empresas con las que no tienen ningún vínculo laboral. Evidenciándose que el tratamiento de datos no cumple con el **PRINCIPIO de CALIDAD** lo cual generó el tratamiento inadecuado de los datos personales de la denunciante.



Certificado



Infracción: **literal f, numeral 1, del artículo 132° del RLPDP**: “Dar tratamiento a los datos personales contraviniendo las disposiciones de la Ley y su Reglamento”, dicha infracción es **leve**, **sanción de 0,5 UIT hasta 5 UIT**.

Principio de Seguridad

Artículo 9° de la LPDP

Se deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales.

Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar.

Gestión de accesos: Asignación de cuentas usuario y contraseñas de los sistemas.

Gestión de privilegios: Determinar los perfiles de usuario.

Verificación periódica de privilegios asignados: Control o monitoreo de los privilegios (permisos) otorgados a los titulares de las cuentas de usuario de los sistemas.

Generar y mantener registros de interacción lógica: Registro de trazabilidad (¿Quién ingresó?, ¿Cuándo ingresó?, ¿Qué hizo?), es el dejar una huella de lo que se realiza.

Seguridad en ambientes donde se almacene, procese y transmita información: Los centros de datos deben contar con las medidas de seguridad adecuadas (ambiente exclusivo, puerta con llave, UPS, control de temperatura, extintor).

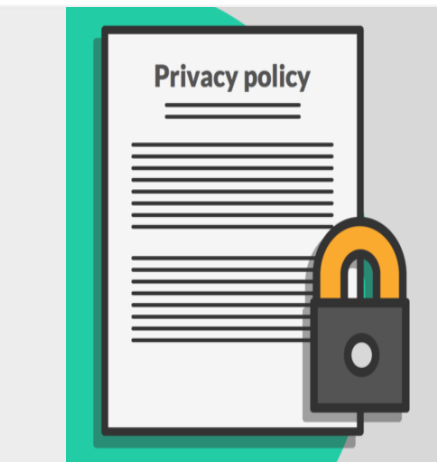
Realizar copias de respaldo seguras y continuas de los bancos de datos personales: Se deben realizar copias de la información con el fin de disponer de un medio para recuperarla en caso de su pérdida.

Almacenar la documentación que conforma el banco de datos personales no automatizado en ambientes o muebles que se encuentren debidamente protegidos: La documentación física debe estar clasificada y almacenada en ambientes o muebles que cuenten con cerradura y cuyo mecanismo de acceso debe estar debidamente asignado a un personal responsable.

Establecer procedimientos que restrinjan la generación de copias o reproducción de documentación y/o información (bloqueo de puertos USB y grabador de discos; fotocopadoras y/o multifuncionales con contraseña; restringir el uso de cuentas de correo personales, redes sociales, aplicaciones de mensajería -entre otros- y establecer acuerdos de confidencialidad).

Derecho de Información: Artículo 18 de la LPDP

- Previa
- Detallada
- Sencilla
- Expresa
- Inequívoca



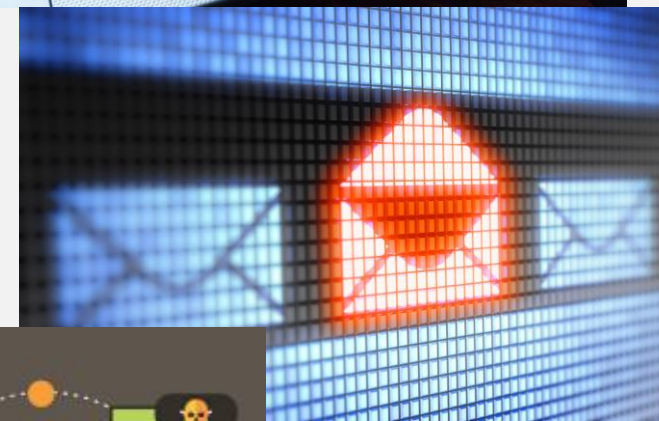
E INSTRU

Todos los sitios web deben incluir en algún lugar visible la política de privacidad

<https://www.gob.pe/institucion/minjus/informes-publicaciones/353793-guia-practica-para-la-observancia-del-deber-de-informar>

Consejos y recomendaciones

- ✓ Usar contraseñas seguras y no compartirlas.
- ✓ Evitar conectarse a redes *Wi-Fi* públicas y realizar transacciones financieras.
- ✓ Navegar en sitios seguros y oficiales. 
- ✓ Mantener los dispositivos actualizados.
- ✓ No compartir información personal, videos o audios en modo público.
- ✓ No ingresar a enlaces sospechosos.
- ✓ Rechazar contactos desconocidos en redes sociales.
- ✓ Leer las políticas de privacidad.
- ✓ Realiza copias de seguridad de tu información.



GRACIAS

Para consultas nos pueden escribir a:

protegetusdatos@minjus.gob.pe

o llamar al:

2048020 anexo 2410



Autoridad Nacional de Protección de Datos Personales