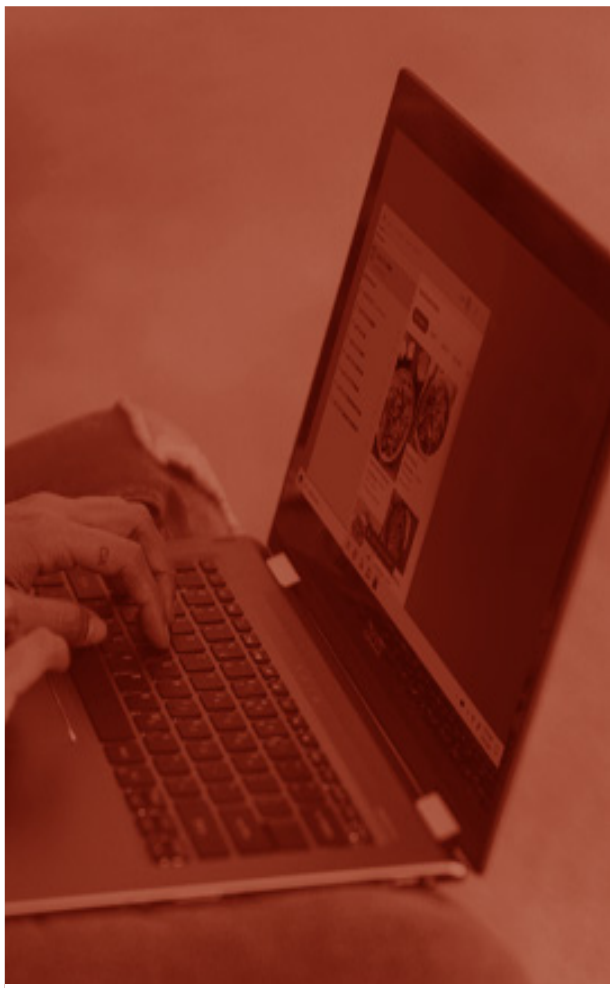
Uruguay Presidencia | agesic

# GUÍA GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN URUGUAY



UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

Actualizada con los artículos 37 a 40 de la Ley N° 19.670, de 15 de octubre de 2018 y el decreto N° 64/020, de 17 de febrero de 2020.

## OBJETIVO

Esta guía orienta sobre el Derecho a la Protección de Datos Personales y los medios para facilitar su ejercicio, y espera constituirse en una herramienta de capacitación útil para todas las personas.

La protección de datos personales es un derecho humano regulado en diversos instrumentos internacionales. En nuestro país, la Ley N° 18.331, de 11 de agosto de 2008, reconoce la protección de datos personales como un derecho fundamental incluido en nuestra Constitución, crea la Unidad Reguladora y de Control de Datos Personales (en adelante URCDP) como el órgano que garantiza este derecho -con competencias necesarias para garantizar el cumplimiento de la normativa vigente-, e instituye un régimen basado en principios y derechos que se analizarán más adelante en este documento.

## ¿QUÉ SON LOS DATOS PERSONALES?

Para entender qué es la protección de datos personales es importante definir qué es un dato personal; según la Ley N° 18.331, es cualquier tipo de información que nos pueda identificar directamente o nos hace identificables. Por ejemplo, son datos personales nuestro nombre, dirección, teléfono, cédula de identidad, número de RUT, huella digital, número de socio, número de estudiante, una fotografía o incluso hasta el ADN.

Asimismo, cuando se habla de dato identificable, se refiere a un conjunto de datos que llevan a identificar a una persona sin necesidad de tener un nombre o cédula de identidad. Por ejemplo, si en una encuesta anónima, pero de universo acotado, se recaban datos de una determinada profesión, se analiza el contexto en el cual esa persona vive y el número de hijos que tiene, se puede, a través del análisis del conjunto de datos, identificar a la persona encuestada.

La Ley establece que dentro del universo de datos personales algunos son considerados como sensibles y por tanto tienen un régimen especial para su tratamiento. Estos datos son aquellos que revelen el origen racial y étnico, las preferencias políticas, las convicciones religiosas o morales, la afiliación sindical y las informaciones referentes a la salud o a la vida sexual. Se trata de una relación de género a especie, donde éstos son datos personales, pero la Ley les otorga una mayor protección porque su utilización puede generar efectos jurídicos negativos sobre las personas.

## ¿QUÉ ES EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES?

Se trata de un derecho humano, tal como lo menciona el artículo 1° de la Ley N° 18.331 y por ende se encuentra comprendido en el artículo 72 de la Constitución de la República.

El derecho a la protección de datos personales es reconocido en múltiples instrumentos internacionales, ente ellos, se puede citar al artículo 8° de la Carta de los Derechos Fundamentales de la Unión Europea y el Convenio N° 108, del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su protocolo adicional. Este Convenio del año 1981 -junto a su Protocolo Adicional de 2001- es el primer instrumento internacional en materia de protección de datos personales, que busca dotar de mayor eficacia su tutela.

El citado Convenio se incorporó a nuestro ordenamiento jurídico por la Ley N° 19.030, de 7 de noviembre de 2012, convirtiendo a Uruguay en el primer país no europeo en ratificarlo. En el mensaje enviado al Parlamento se indica que la adhesión a este tipo de instrumentos "…que incluyen principios básicos de la protección de datos, facilitará el intercambio de datos entre las Partes al promover mecanismos y plataformas de cooperación entre autoridades de protección de datos. Asimismo prevé la creación de autoridades que ejerzan sus funciones con completa independencia, promoviendo igualmente la implementación de un adecuado nivel de protección de datos (…)[1]".

**1.** El citado Convenio se incorporó a nuestro ordenamiento jurídico por la Ley N° 19.030, de 7 de noviembre de 2012. Consultar Convenio.

Uruguay ha formado parte además de los grupos organizados en el marco del Convenio N° 108, y participó puntualmente en la redacción del Protocolo de Modernización CETS N° 223 (conocido como "Convenio 108+").

Esta versión ya fue aprobada por el Parlamento Nacional por Ley N° 19.948, de 16 de abril de 2021, y se depositó el instrumento de ratificación correspondiente el 5 de agosto de 2021. [2] [3]


## ¿CUÁL ES LA IMPORTANCIA DE ESTE DERECHO?

La Ley reconoce el ejercicio de distintos derechos: de acceso, rectificación, supresión, entre otros, los cuales se constituyen en herramientas para el control del tratamiento de los datos, y establece además la acción de protección de datos personales (más conocida como habeas data) ante los órganos judiciales.

La Ley, y por ende la acción prevista, se aplica a los datos personales registrados en cualquier soporte que permite tratarlos y usarlos de diversos modos, tanto en el ámbito privado como público.

---

**2.** Consultar el contenido de la ley N° 19.948

**3.** Consultar fuente de la imagen.

# ¿QUÉ ES LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES?

## a. ¿Cuál es su conformación?

La Unidad Reguladora y de Control de Datos Personales es la autoridad establecida por ley para el contralor de todo tipo de tratamiento y en todos los ámbitos dentro del territorio nacional. Es un órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (Agesic), dotada de la más amplia autonomía técnica.

Está compuesta por tres miembros: el director ejecutivo de Agesic y dos miembros designados por el Poder Ejecutivo, que por sus antecedentes personales, profesionales y de conocimiento en la materia aseguren independencia de criterio, eficiencia, objetividad e imparcialidad en el desempeño de sus cargos.

Como características del Consejo Ejecutivo se pueden señalar las siguientes:

- Sus miembros duran 4 años en sus cargos.
- Pueden ser reelectos, a excepción del director ejecutivo de Agesic.
- No recibirán órdenes ni instrucciones en el plano técnico.

Además, tiene un órgano asesor que es el Consejo Consultivo, compuesto de la siguiente manera:

El Consejo Consultivo puede ser convocado para asesorar sobre cualquier aspecto de su competencia, así como tratar proyectos reglamentarios.

El decreto N° 414/009, de 31 de agosto de 2009, reglamentario de la Ley, regula el funcionamiento y las competencias de ambos Consejos. Su artículo 21 establece que la Presidencia de la URCDP será rotativa anualmente entre los miembros del Consejo Ejecutivo a excepción del director ejecutivo de Agesic. En ausencia temporal del presidente de la URCDP, la presidencia será ejercida en forma interina por el restante miembro nombrado por el Poder Ejecutivo[4].

### b. ¿Cuáles son las competencias de la URCDP?

Las competencias del órgano de control se encuentran reguladas en el artículo 34 de la Ley N° 18.331, a saber:

- Asistir y asesorar a las personas
- Dictar normas y reglamentaciones
- Realizar un censo de las bases de datos
- Controlar la observancia del régimen legal
- Solicitar información a entidades públicas y privadas
- Emitir opinión toda vez que sea requerido
- Asesorar el Poder Ejecutivo en proyectos de la ley relacionados con la mateia
- Informar a las personas sobre la existencia de bases de datos, finalidad e identidad de sus responsables

### c. ¿Qué potestades sancionatorias tiene la URCDP?

Las sanciones se aplican a responsables de tratamiento, encargados de tratamiento de datos personales y demás personas físicas o jurídicas alcanzadas por el régimen legal en caso de infracción a alguna de las normas de protección de datos personales, y se encuentran reguladas en el artículo 35 de la Ley N° 18.331.

A los efectos de su aplicación, previamente se deben considerar algunos criterios

**4.** Por más información sobre el funcionamiento del órgano de control acceder al Decreto N° 414/009.

como ser la gravedad, la reiteración o la reincidencia.

La norma establece las siguientes sanciones de menor a mayor:

- Observación
- Apercibimiento
- Multa de hasta 500.000 unidades indexadas
- Suspensión de la base de datos por hasta 5 días
- Clausura de la base de datos

La clausura de la base de datos es la sanción más grave que puede imponer la Unidad, y requiere por ello del previo control judicial. El procedimiento dispuesto por las normas supone una presentación judicial por la URCDP con la documentación probatoria de la infracción, y un decreto judicial habilitando dicha clausura dentro de los 3 días de la solicitud. Si el juez no se pronuncia en ese plazo, la URCDP queda habilitada para disponerla por sí.

La resolución N° 105/015, de 23 de diciembre de 2015, del Consejo Ejecutivo de la URCDP dictada en el marco de las competencias definidas en el artículo 34 literal B de la Ley, determinó las infracciones pasibles de sanción y su categorización. Esta resolución cataloga las sanciones en muy leve, leve, grave o muy grave, las califica e indica que, para su determinación, se atenderá a la gravedad, reiteración o reincidencia de la infracción y a los antecedentes del infractor.

La citada resolución establece que, para la aplicación de la sanción, sin perjuicio de cualquier otra circunstancia que sea relevante para evaluar la posible infracción cometida, se considerarán los siguientes puntos:

- El tipo de datos personales objeto de tratamiento
- La adopción o no de medidas de seguridad.
- Los derechos personales vulnerados.
- El volumen de los tratamientos efectuados.
- Los beneficios obtenidos.
- Los daños y perjuicios causados a las personas interesadas y a terceros.

Esta resolución considera además como eximentes la fuerza mayor y el caso fortuito[5].

5. Resolución N° 105/015

De conformidad con el artículo 35 in fine de la Ley, las resoluciones firmes de la Unidad que determinen sanciones pecuniarias se constituyen en título ejecutivo a sus efectos, lo que habilita a la Unidad a iniciar los juicios ejecutivos y eventuales embargos ante el no pago de las multas correspondientes.

## ÁMBITO DE APLICACIÓN DE LA LEY

A los efectos de conocer a quiénes se aplica la normativa de protección de datos personales, corresponde distinguir tres grandes ámbitos de aplicación de la Ley:

### **a.** Ámbito objetivo:

La Ley es aplicable a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos tanto en ámbitos público o privado. Por tanto, se aplica a las bases de datos informatizadas, en papel o mixtas.

No obstante, existen bases de datos o tratamientos excluidas del ámbito de aplicación de la Ley, aunque, por tratarse de la protección de un derecho fundamental, sí se encuentran alcanzadas por los principios que ella establece.

De acuerdo con lo establecido en el artículo 3° inciso 2, no se aplican las disposiciones de la Ley a las siguientes bases de datos:

- Aquellas mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas, como por ejemplo las agendas personales.
- Las que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito, existiendo condiciones específicas para el ejercicio de los derechos.
- Las creadas y reguladas por leyes especiales, para las cuales se debe detallar la forma de tratamiento de la información personal.

### **b.** Ámbito subjetivo:

La Ley es de aplicación a todos los habitantes de la República, en virtud que el derecho a la protección de datos personales es un derecho humano considerado inherente a la persona.

Asimismo, y de conformidad con lo establecido en el artículo 2° de la Ley, ésta

se aplicará a las personas jurídicas en cuanto corresponda, lo que requiere de un análisis caso a caso.

### c. Ámbito territorial:

La Ley se aplica a todo tratamiento de datos personales que se realice en territorio uruguayo.

Para los responsables y encargados de tratamiento radicados en el exterior del país, se prevé su aplicación si las actividades de tratamiento están relacionadas con la oferta de bienes y servicios dirigidos a habitantes de la República, si las normas de derecho internacional público o un contrato así lo disponen, o si en el tratamiento se utilizan medios situados en el país. Esta ampliación del ámbito territorial fue establecida por el artículo 37 de la Ley N° 19.670, de 15 de octubre de 2018, y reglamentada por los artículos 1° y 2° del decreto Nº 64/020, de 17 de febrero de 2020, que precisan el alcance de los supuestos incluidos de las obligaciones de responsables y encargados[6].

En este sentido, existen ejemplos ilustrativos, aunque teniendo en cuenta que el análisis debe realizarse caso a caso: se puede mencionar el caso de un hotel o una empresa de reparto internacional que ofrece servicios a habitantes de Uruguay mediante promociones específicamente diseñadas para nuestro país, con la posibilidad de abonar en moneda local y en idioma español, y en ese sentido, encontrarse alcanzada por el ámbito territorial de la Ley en función de las presunciones establecidas en el propio decreto.

## Principales roles de la protección de datos personales.

A través de la Ley –y con el apoyo de la doctrina-, se pueden esbozar una serie de definiciones de los principales roles involucrados en el tratamiento de datos, lo que permite además entender el funcionamiento de la normativa. Dentro de ellas, se destacan las siguientes:

i. **Titular del dato personal:** toda persona física o jurídica.

ii. **Responsable del tratamiento:** persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento.

6. Acceder a los arts.1° y 2 Decreto 64/020

**iii. Encargado de tratamiento:** persona física o jurídica, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable de la base de datos o del tratamiento.

**iv. Tercero:** persona física o jurídica, pública o privada, distinta del titular del dato, del responsable de la base de datos o tratamiento, del encargado y de las personas autorizadas para tratarlos datos bajo la autoridad directa del responsable o del encargado del tratamiento.

**v. Delegado de protección de datos:** persona física o jurídica que tiene como funciones asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales, supervisar el cumplimiento de la normativa sobre dicha protección en su entidad, proponer todas las medidas que entienda pertinentes para adecuarse a ésta y a los estándares internacionales en la materia[7].

## ¿CUÁLES SON LOS PRINCIPIOS DE LA PROTECCIÓN DE DATOS PERSONALES?

El régimen normativo uruguayo se sustenta en un conjunto de principios, que determinan la forma, contenido y condiciones para el tratamiento de los datos, pero además operan como mandatos para responsables, encargados y titulares en la forma de cumplir las obligaciones impuestas, facilitar el ejercicio o ejercer efectivamente los derechos; y también como criterio orientador para la URCDP, con respecto a la forma de valorar los comportamientos en el cumplimiento de las disposiciones legales y reglamentarias.

Estos principios se encuentran detallados en el artículo 5°, y se especifican en los artículos 6° a 12 de la Ley, como se observa en el siguiente cuadro:

### a. Legalidad

De acuerdo con el principio de legalidad la formación de base de datos será lícita cuando se encuentra debidamente inscrita ante el órgano de control[8].

Todo el proceso de inscripción de las bases de datos es mediante el sistema de registro en línea. A esos efectos, la Unidad tiene disponible en su sitio web el

7. Se pueden consultar más definiciones en el art. 4° de la Ley N° 18.331 y en el art. 4° del Decreto N° 414/009
8. El proceso de inscripción y las condiciones para ello se encuentran determinados en el decreto N° 664/008, de 22 de diciembre de 2008

Sistema de Registro que permite la solicitud de inscripción de registros de bases de datos en línea. Asimismo, se publican mensualmente los datos de los responsables que se encuentran inscriptos ante la Unidad[9].

Además, conforme con este principio, no se pueden formar base de datos que tengan finalidades violatorias de derechos humanos o que sean contrarias a la ley o a la moral pública.

### b. Veracidad

De acuerdo con el principio de veracidad, los datos personales que se recaben para ser objeto de tratamiento deben ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la que se obtuvieron. A estas características se agrega que los datos deben ser exactos y actualizarse cuando ello fuere necesario.

Este mismo principio agrega que los datos personales no pueden ser obtenidos por medios fraudulentos, desleales, abusivos, extorsivos o en forma contraria a las disposiciones de la normativa de protección de datos personales.

La norma agrega que cuando se constate la inexactitud de o falsedad de los datos, el responsable debe suprimirlos, sustituirlos o completarlos de acuerdo con cada situación.


Por ejemplo, si una persona cambia de estado civil y quiere actualizarlo en una base privada, debe acreditar el cambio en forma fehaciente y el responsable debe actualizar la información.

9. Acceder a información sobre el sistema de registro

Por último, se indica que deben ser eliminados aquellos datos que hayan caducado de acuerdo a las previsiones de la normativa de protección de datos personales.

### c. Finalidad

Respecto a este principio es importante resaltar que los datos personales objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

La norma aclara que los datos deben ser eliminados cuando hayan dejado de ser necesarios o pertinentes para los fines para los cuales fueron recolectados.

Por ejemplo, los datos personales recabados para un sorteo deben eliminarse una vez que se realiza éste.

Este mismo principio establece que se regularán los casos en los que, basados en valores históricos, estadísticos o científicos, conforme con la legislación específica, se pueden conservar datos personales aun cuando no exista tal necesidad o pertinencia.

El artículo 37 del decreto N° 414/009 regula el procedimiento para la autorización de conservación de datos en base a las finalidades indicadas, siempre a petición del responsable que pretenda obtener la declaración.

Es interesante destacar que, en la solicitud, el responsable deberá identificar el tratamiento de datos al que pretende aplicar a la excepción, establecer las causas que justificarían la declaración, presentar las medidas que se propone implantar para garantizar los derechos de los titulares de los datos y acompañar los documentos necesarios para justificar la solicitud.

Sobre este trámite se aclara que la Unidad puede previamente a adoptar una resolución, solicitar la opinión de instituciones u organismos, públicos o privados, que tengan competencia o mérito para ser consultados en relación al caso.

### d. Previo consentimiento informado

Otro principio de especial trascendencia para la protección de datos personales es el consentimiento. El responsable debe recabar en forma libre, previa e informada el consentimiento de los titulares de datos.

El consentimiento se puede recabar de distintas formas (dependiendo del tipo de dato): por grabaciones, formularios, aceptación en sitios web, entre otros.

Este principio indica los casos en los cuales no se considera necesario el previo consentimiento, y si bien el artículo los considera excepciones a éste, en los hechos funcionan como otras bases legitimantes del tratamiento, es así cuando:

- Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación. En este punto cabe señalar que la Ley define en forma taxativa las fuentes públicas de información en el artículo 9° bis.
- Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.
- Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma.
- Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.
- Se realice por personas físicas para su uso exclusivo personal, individual o doméstico.

**La información del Diario Oficial, los registros públicos, las publicaciones en medios de comunicación, entre otras, son fuentes públicas, pero internet no lo es.**

En cuanto al consentimiento, se deben tener presente los artículos 5° y 6° del decreto N°414/009, que establecen algunos requisitos especiales para su recolección. Es así que el primero de estos artículos indica que se debe informar a los titulares de los datos personales de la finalidad a la que se destinarán los datos y el tipo de actividad desarrollada por el responsable de la base de datos o tratamiento. En caso contrario se considera que el consentimiento es nulo.

Por su parte, el artículo 6° indica las formas existentes para recabarlo. Este deber se entiende cumplido cuando se permita al titular la elección entre dos opciones claramente identificadas que no encuentren pre marcadas a favor o en contra.

También es necesario indicar que el responsable de la base de datos debe recabar y guardar la prueba de la existencia del consentimiento o de la negativa a darlo, a

través de cualquier medio conforme a derecho, lo cual puede ser requerido por la URCDP en cualquier momento.

### e. Seguridad de los datos

De acuerdo con el principio de seguridad de los datos, el responsable o el usuario dela base de datos debe adoptar las medidas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado y detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

La norma establece que los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular. Por último, se indica que queda prohibido registrar datos personales en bases de datos que no reúnan condiciones técnicas de integridad y seguridad.

El artículo 38 de la Ley N° 19.670, incorpora el régimen de comunicación de vulneraciones de seguridad, y establece que cuando el responsable o encargado de una base de datos o de tratamiento, tome conocimiento de la ocurrencia de la vulneración de seguridad, debe informar inmediata y pormenorizadamente de ello y de las medidas que adopte, a los titulares de los datos y a la URCDP, la que coordinará el curso de acción que corresponda, con el Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay (CERTuy).

Se pueden establecer medidas físicas, como, por ejemplo, utilizar llaves de seguridad, alarmas, control de ingreso, y también medidas lógicas, como por ejemplo contraseñas, claves de seguridad.

El decreto N° 64/020 en sus artículos 3 y 4 reglamenta la comunicación mencionada, y establece que tanto el responsable como el encargado de tratamiento en su caso, deben adoptar las medidas técnicas y organizativas necesarias para conservar la integridad, confidencialidad y disponibilidad de la información, de forma de garantizar la seguridad de los datos personales. Además, especifica las circunstancias, contenido y plazo para las comunicaciones a los titulares de los datos afectados y a la URCDP.

### f. Reserva

Según este principio aquellas personas físicas o jurídicas que obtengan

legítimamente información proveniente de una base de datos que les brinde tratamiento están obligadas a utilizarlas en forma reservada y exclusivamente para el tratamiento habitual de su actividad. La norma indica que está prohibida toda difusión a terceros.

Además, esta norma establece que la infracción a este artículo hace incurrir en el delito de secreto profesional previsto en el artículo 302 del Código Penal.

Los funcionarios públicos tienen implícita la reserva en su relación funcional así como los dependientes en su relación laboral.

## g. Responsabilidad "proactiva"

El artículo 12 de la Ley N° 18.331 -modificado por el artículo 39 de la Ley N° 19.670- regula el principio de responsabilidad, modificando la redacción original de esta norma y estableciendo un nuevo parámetro en la materia.

El artículo en su versión original indicaba que el responsable era "responsable" de las infracciones a la normativa de protección de datos personales que pudieran suceder, con carácter general. En este caso la Unidad perseguía el cumplimiento de la normativa y exhortaba de diversas formas a responsables a los efectos de su cumplimiento.

Este principio fue objeto de la modificación señalada evolucionando el concepto hacia el de una responsabilidad "proactiva". Así, existe una nueva orientación en la materia que lleva a responsables y encargados de tratamiento a ir más allá del sólo cumplimiento de la Ley, y adoptar medidas en forma autónoma que demuestren dicho cumplimiento.

Sobre este punto cabe mencionar que en la nota de interés publicada en la revista de la Unidad sobre la modificación de este principio se expresó que:

"Esta formulación se visualizó como insuficiente, como ya se mencionó, a la luz de la evolución en las estrategias y medios para el tratamiento de los datos. Resultaba necesario virar hacia un régimen que impusiera un conjunto mayor de obligaciones en cabeza no sólo de responsables sino además de encargados, de modo de asegurar que todo tratamiento de datos incluyera, desde su concepción, los principios y normas en la materia".

Se agrega que "Se hace una explícita referencia a la responsabilidad proactiva, dentro de la que se incluyen la privacidad por diseño, privacidad por defecto, evaluación de impacto, entre otras, con el objetivo de garantizar un tratamiento adecuado de los datos personales, y demostrar su efectiva implementación.

Estas medidas deberán documentarse a efectos de demostrar, cuando sea requerido por la URCDP, el cumplimiento efectivo de las normas en la materia. Obligación que no corresponde sólo a los responsables, sino además, en determinados casos, a los encargados[10]".

La fuente de inspiración es la normatividad europea, donde también se la conoce como "accountability", e incluye entre otras medidas la implementación del principio de transparencia del responsable hacia el sujeto de los datos en relación al conjunto de tratamientos realizados, contar con un delegado de protección de datos personales, listar las actividades de tratamiento, realizar una evaluación de impacto a la privacidad y notificar las brechas de seguridad.

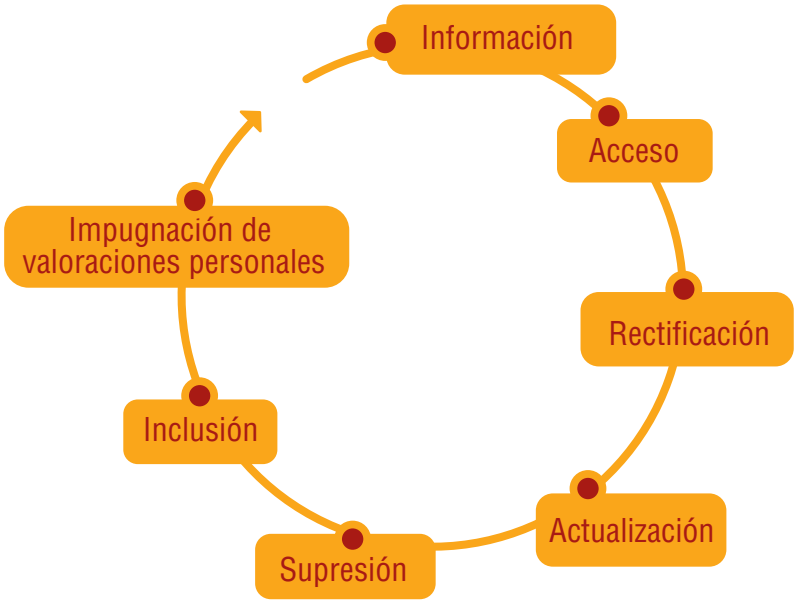
Los responsables y encargados deben adoptar medidas que aseguren y demuestren el cumplimiento de la normativa de protección de datos personales

En Uruguay el decreto N° 64/020 avanza en el tema y regula, entre otros, los casos en los cuales se debe realizar una evaluación de impacto en forma obligatoria (art. 6°), el concepto de privacidad por diseño (artículo 8°) y por defecto (artículo 9°). La Unidad podrá complementar estos aspectos, como en los hechos realizó a través de la inclusión de los datos biométricos en el elenco de tratamientos que requerían una evaluación de impacto previa (Resolución N° 30/020, de 12 de mayo de 2020). Todo ello se desarrollará más adelante en la presente guía.

Como se verá, en materia de evaluaciones de impacto, la Unidad en conjunto con su homónimo de Argentina publicaron una guía que tiene como objetivo explicar cuáles son los pasos y contenidos que hay que tener en cuenta para su realización.

**10.** Consultar la 4° Edición de la Revista de Protección de Datos Personales.

## ¿CUÁLES SON LOS DERECHOS DE LA PROTECCIÓN DE DATOS PERSONALES?




Como se indicó, la protección de datos personales supone además de un tratamiento en base a principios y el cumplimiento de obligaciones por responsables y encargados, el efectivo ejercicio de derechos por parte los titulares de los datos. Estos derechos se encuentran explicitados en los artículos 13 a 16 de la Ley.

El **derecho de acceso** es el que tiene toda persona que, previamente, acredite su identidad, de acceder a toda la información sobre sí mismo con la que cuente el responsable de tratamiento.

El **derecho de actualización** es el que tiene el titular a que se modifiquen los datos que resulten inexactos a la fecha de ejercicio del derecho.

El **derecho de rectificación** es el que tiene el titular a que se modifiquen los datos que resulten ser inexactos o incompletos.

El **derecho de inclusión** es el que tiene el titular a ser incorporado con la información correspondiente en una base de datos cuando acredite un interés fundado.

El titular del dato personal puede solicitar ser incluido en una base de datos si por ejemplo le trae aparejado un beneficio.

El **derecho de supresión** es el que tiene el titular a que se eliminen los datos cuya utilización por terceros resulte ilegítima, o que resulten ser inadecuados o excesivos. La supresión no procederá cuando los datos personales deban ser conservados en virtud de razones históricas, estadísticas o científicas y de acuerdo con la legislación aplicable o, en su caso, en las relaciones contractuales entre el responsable y el titular, que justificaren el tratamiento de los datos. El responsable deberá documentar ante el titular haber cumplido con lo solicitado indicando las cesiones o transferencias de los datos suprimidos e identificando al cesionario.

El titular del dato personal puede solicitar en cualquier momento que le supriman sus datos de una base de datos cuando ya no sea necesario su tratamiento, o si fue cargado por error, o sin su consentimiento.

El **derecho a la impugnación de las valoraciones personales** implica que las personas tienen derecho a no verse sometidas a una decisión basada en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, entre otros, con efectos jurídicos que les afecte de manera significativa. La persona afectada podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos personales que ofrezca una definición de sus características o personalidad. En este caso, la persona tendrá derecho a obtener información del responsable de la base de datos tanto sobre los criterios de valoración como sobre el programa utilizado en el tratamiento que sirvió para adoptar la decisión manifestada en el acto.

El afectado tendrá derecho a obtener información del responsable de la base de datos tanto sobre los criterios de valoración como sobre el programa utilizado en el tratamiento que sirvió para adoptar la decisión manifestada en el acto, como por ejemplo en el caso de un concurso de méritos.

Estos derechos se pueden ejercer de forma gratuita (cada 6 meses) y ante el responsable, quien tendrá un plazo de respuesta de 5 días hábiles a contar de la solicitud, por los medios que se hayan indicado. En caso de falta de respuesta se habilita la acción de Habeas Data.

## LA COMUNICACIÓN DE DATOS

En nuestro país, se permite la comunicación de datos personales. El literal B del art. 4 de la Ley la define como toda revelación de datos realizada a una persona distinta del titular. Por su parte, el art. 17 de la misma norma, regula los requisitos necesarios para realizar la comunicación de datos, los cuales son:

- la existencia de interés legítimo del emisor y destinatario, y
- el previo consentimiento informado del titular o en el marco de las excepciones.

Estas excepciones son:

**A)** cuando así lo disponga una ley de interés general.

**B)** en los supuestos del artículo 9° de la Ley.

**C)** se trate de datos personales relativos a la salud y sea necesaria su comunicación por razones sanitarias, de emergencia o para la realización de estudios epidemiológicos, preservando la identidad de titulares de datos mediante mecanismos de disociación adecuados cuando ello sea pertinente.

**D)** se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de datos no sean identificables.

Es importante remarcar que el destinatario y el emisor son responsables solidaria y conjuntamente por el cumplimiento de la normativa de protección de datos.

Son ejemplos de comunicación de datos la publicación de todo tipo de listados y los intercambios de información entre organismos públicos basados en normas que así lo indiquen, entre otros. En estos casos es necesario analizar el cumplimiento de

los requisitos y su adecuación a los requisitos legales. Asimismo, al momento de inscribir las bases de datos, se hace un control de la existencia de la comunicación de datos[11].

## REGÍMENES ESPECIALES DE TRATAMIENTO DE DATOS

### Datos sensibles

Datos sensibles todos aquellos datos personales que revelen el origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o la vida sexual de las personas.

La Ley N° 18.331 indica que para el tratamiento de este tipo de datos se requiere el consentimiento expreso y escrito de los titulares de datos. Además, se prevé que solamente las instituciones que traten este tipo de datos pueden generar bases de datos con ese contenido.

### Datos de salud

Dentro del elenco de datos sensibles se encuentran los datos de salud, los que merecen una referencia particular. Se consideran datos de salud las informaciones concernientes a la salud pasada, presente y futura, física o mental, de una persona. Entre otros, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad o a su información genética .

Estos datos pueden recabarse por parte de los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud, los datos relativos a la salud física o mental de los pacientes que acudan a ellos o que hubieran estado bajo su atención profesional, respetando los principios del secreto profesional, la normativa específica y lo establecido en la Ley Nº 18.331.

### Datos relacionados con el ámbito laboral

En el ámbito laboral, el uso y tratamiento de los datos personales está limitado al contrato de trabajo y en mérito a éste es que se debe recabar la información necesaria para cumplir la función. Las normas en la materia deben complementarse con las normas laborales vinculadas a los sectores específicos de actividad y a las normas en materia de prevención de accidentes de trabajo, y de seguridad y salubridad laboral.

Corresponde señalar, además, que en lo que refiere a la documentación para la

**11.** Se puede consultar los dictámenes y resoluciones sobre este tema en el sitio web de la Unidad.

protección y control del trabajo establecida en la reglamentación respectiva, ésta se considera adecuada a los términos de la Ley N° 18.331, de conformidad con lo establecido en el artículo 84 de la Ley N° 19.355, de 19 de diciembre de 2015, en la redacción dada por el artículo 91 de la Ley N° 19.438, de 14 de octubre de 2016.

## Datos de telecomunicaciones

Las telecomunicaciones en todas sus variedades (por hilos, por aire, redes, telefonía, fax, mensajes de texto, televisión por cable y satelital, etc.) son merecedoras de especial atención, a los efectos de la protección de los datos personales.

Según la Ley, los operadores que exploten redes públicas y los que prestan servicios de comunicaciones electrónicas disponibles al público deben garantizar la protección de los datos personales conforme a la Ley.

En ese sentido, se prevé la adopción de medidas particulares para presentar la seguridad en la explotación de su red o en la prestación de su servicio, e incluso se determina la obligación de informar a los abonados la existencia de riesgos de violaciones de seguridad a la red pública de comunicaciones electrónicas y las medidas a adoptarse.

Lo antedicho, sin perjuicio de las notificaciones que correspondan en caso de efectivas vulneraciones en mérito a lo establecido en el artículo 38 de la Ley N° 18.331.

## Datos de Publicidad

En el ámbito de la publicidad, en la recopilación de domicilios, reparto de documentos, publicidad, prospección comercial, venta u otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los titulares u obtenidos con su consentimiento.

En estos casos, el titular podrá en cualquier momento solicitar el retiro o bloqueo de sus datos de los bancos de datos, así como ejercer el derecho de acceso sin cargo alguno.

## Datos de la actividad comercial o crediticia

El tratamiento de datos destinado a informar sobre la solvencia patrimonial o crediticia está autorizado, incluyendo aquellos relativos al cumplimiento o

incumplimiento de obligaciones de carácter comercial o crediticia, que permitan evaluar la concertación de negocios en general, la conducta comercial o la capacidad de pago del titular de los datos.

Los datos deben ser obtenidos de fuentes de acceso público, o procedentes de informaciones facilitadas por el acreedor o en los casos previstos en la Ley.

> Los datos personales relativos a obligaciones de carácter comercial de personas físicas sólo podrán estar registrados por un plazo de cinco años contados desde su incorporación.
>
> En caso que al vencimiento de dicho plazo la obligación permanezca incumplida, el acreedor podrá solicitar al responsable de la base de datos, por única vez, su nuevo registro por otros cinco años. Este nuevo registro deberá ser solicitado en el plazo de treinta días anteriores al vencimiento original.

Los responsables de las bases de datos se limitarán a realizar el tratamiento objetivo de la información registrada tal cual ésta le fuera suministrada, debiendo abstenerse de efectuar valoraciones subjetivas sobre ésta.

Cuando se haga efectiva la cancelación de cualquier obligación incumplida registrada en una base de datos, la persona acreedora deberá, en un plazo máximo de cinco días hábiles de acontecido el hecho, comunicarlo al responsable de la base de datos o tratamiento correspondiente. Una vez recibida la comunicación por el responsable de la base de datos o tratamiento, éste dispondrá de un plazo máximo de tres días hábiles para proceder a la actualización del dato, asentando su nueva situación.

> Las obligaciones canceladas o extinguidas por cualquier medio, permanecerán registradas, por un plazo máximo de cinco años, no renovable, a contar de la fecha de la cancelación o extinción, dejando expresa constancia de que están canceladas o extinguidas.

## Datos biométricos

Si bien estos datos ya había sido reconocidos por el Consejo Ejecutivo de la Unidad como merecedores de una protección especial, la Ley N° 19.924, de 18 de diciembre de 2020 incorporó a la legislación nacional el concepto de datos biométricos, como datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona tales como datos dactiloscópicos, reconocimiento de imagen o voz (artículo 4° literal Ñ de la Ley N° 18.331).

Reiterando la opinión de la Unidad en la resolución N° 30/020, el nuevo artículo 18 bis de la Ley N° 18.331 incluyó a los datos biométricos en el capítulo destinado a datos especialmente protegidos e impuso la obligación de los responsables y encargados de realizar evaluaciones de impacto previas a su tratamiento

# TRANSFERENCIAS INTERNACIONALES

Nuestra Ley prohíbe la transferencia de datos personales de cualquier tipo a países u organismos internacionales que no proporcionen niveles de protección adecuados de acuerdo a los estándares del Derecho Internacional o Regional en la materia.

Existen ciertas excepciones cuando se trata de: cooperación judicial internacional, intercambio de datos de carácter médico, transferencias bancarias o bursátiles, acuerdos en el marco de tratados internacionales en los cuales el Uruguay sea parte, cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

También es posible realizar la transferencia internacional de datos cuando la parte interesada haya dado su consentimiento inequívocamente a la transferencia prevista; si es necesaria para la ejecución de un contrato entre la parte interesada y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición de la parte interesada; si es necesaria para la celebración o ejecución de un contrato celebrado o por celebrarse entre el responsable y un tercero, en interés de la persona interesada; si es necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial; si es necesaria para la salvaguardia del interés vital de la persona interesada; o si tiene lugar desde un registro que, en virtud de

disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para su consulta.

Sin perjuicio de lo anterior, la URCDP puede autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel adecuado de protección, cuando el responsable del tratamiento ofrezca garantías suficientes respecto a la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos.

Dichas garantías podrán derivar de cláusulas contractuales apropiadas. A estos efectos, el Consejo Ejecutivo emitió la resolución N° 41/021, de 8 de setiembre de 2021, en la que establece un contenido mínimo para dichas cláusulas. [12]

Corresponde indicar que, además, y en función de lo establecido por el artículo 6° del decreto N° 64/020, toda transferencia a un país u organización no adecuados deberá ser precedida de una evaluación de impacto en la protección de datos.

Ahora bien, las referidas previsiones son aplicables en el caso de países u organizaciones que no garantizan un nivel adecuado de protección, y en consecuencia la transferencia debe basarse en alguna de ellas, y en su caso obtener la autorización previa de la Unidad.

No obstante, es posible efectuar una transferencia de datos sin acreditar estos extremos (aunque sí cumpliendo con todos los restantes principios y obligaciones de la Ley), cuando ésta se realiza a un país u organización considerada adecuada. Por resolución N° 23/021, de 8 de junio de 2021, la URCDP ha considerado adecuados a los miembros de la Unión Europea y el Espacio Económico Europeo, Principado de Andorra, República Argentina, el sector privado de Canadá, Guernsey, Isla de Man, Islas Feroe, Estado de Israel, Japón, Jersey, Nueva Zelanda, Reino Unidode Gran Bretaña e Irlanda del Norte, y Confederación Suiza[13].

**12**. Resolución N° 41/021

**13.** Resolución N° 23/021

Es importante destacar que la Unidad puede ampliar o reducir el elenco de países u organizaciones mencionados en la resolución anterior, por lo que es de suma importancia realizar una revisión en forma previa a cualquier transferencia por parte de responsables y encargados.

## OTROS ASPECTOS A TENER EN CUENTA EN EL TRATAMIENTO DE DATOS

### a. Criterios de disociación[14]

En materia de disociación la Unidad ha publicado la Guía de disociación la cual cuenta con diversos criterios de no identificación de aquellos datos personales que se encuentran en la información que se deba publicar como dato abierto, como ser: seudonimización, disociación, anonimización entre otros.

Con estos criterios se pretende que toda persona que utilice estas técnicas incorpore los lineamientos dados en esta guía, para disminuir al mínimo la posibilidad de re-identificar al titular del dato que se maneje, teniendo en cuenta que esta es una actividad dinámica que varía por la constante aparición de nuevos mecanismos de re-identificación.

Si bien los criterios fueron generados con el objetivo de dar cumplimiento a las previsiones en materia de publicación de datos abiertos, su aplicación puede ser realizada por parte de cualquier responsable o encargado en el marco de cualquier operación de tratamiento de los datos.

### b. Tratamiento de datos de menores

El tratamiento de datos de menores ha sido una constante preocupación por parte de la Unidad. Con criterio general se debe señalar que es necesario recabar el consentimiento de sus padres o tutores antes del tratamiento de los datos de menores.

Los responsables deben cuidar la utilización de este tipo de datos personales,

**14.** Conforme lo dispuesto por el Decreto N° 54/017, de 20 de febrero de 2017,reglamentario del artículo 82 de la Ley N° 19.355, de 19 de diciembre de 2015, en el que se establece que las Entidades Públicas, sujetos obligados por la Ley N° 18.381,de 17 de octubre de 2008, deberán proceder a la publicación de la información contenida en los artículos 5° de la Ley y 38 y 40 del Decreto N° 232/010, 2 de agosto de 2010, en formato de dato abierto, la URCDP, por Resolución Nº 68/017, de 26 de abril de 2017, aprobó el documento Criterios de Disociación de Datos Personales. Acceder a la Guía Criterios de disociación de Datos Personales.

debiendo considerar la finalidad y las medidas de seguridad como elementos esenciales previo a su análisis.

Recientemente, el decreto N° 64/020 (art. 6°) incluye dentro de las hipótesis en las cuales debe realizarse previamente una evaluación de impacto, el tratamiento de datos de menores. Ello por las consecuencias que puede acarrear una utilización incorrecta de este tipo de datos personales.

La Unidad ha trabajado en forma constante, generando contenidos y promoviendo actividades para la concientización de este derecho en menores de edad, de forma tal que tengan conocimiento de su existencia desde temprana edad.

### **c.** Videovigilancia

Mediante la utilización de dispositivos de videovigilancia se pueden captar la imagen y la voz, los cuales son datos personales y por ende pasibles de protección según la normativa vigente.

La Unidad ha analizado esta temática desde sus comienzos, lo cual se refleja en el dictamen N° 10/010 de 16 de abril de 2010. En éste se expresa que la videovigilancia es "**toda grabación, captación, transmisión, conservación y almacenamiento de imágenes y en algunos casos de sonidos mediante la utilización de videocámaras u otro medio análogo**[15]".

En este dictamen se indica que la captación o grabación de imágenes constituye información personal, por lo que resulta de aplicación la normativa vigente sobre protección de datos personales. Por ende, corresponde tener en cuenta los diversos aspectos que puede comprender la videovigilancia, esto es, qué puede ser videovigilado, de qué forma, qué principios son aplicables y si se deben registrar los resultados, entre otros.

Es de destacar que la videovigilancia tiene como principales finalidades la protección de las personas físicas, del derecho de propiedad, la tutela del orden público, la detección y prevención de delitos, así como otros intereses legítimos.

Esta norma establece además la necesidad de contar con logos de videovigilancia, cuyo patrón fue aprobado por resolución de la Unidad N° 989/010, de 30 de julio de 2010[16] [17].

---

**15.** Consultar el Dictamen N°10/010
**16.** Consultar Resolución N°989/010
**17.** Descargar los logos

En lo que respecta a la instalación de cámaras en espacios laborales cerrados, la Unidad por resolución N° 79/014, de 12 de enero de 2014[18] , indicó que los sistemas deben ser analizados en el marco de los principios, considerando que ciertos lugares no pueden ser videovigilados como por ejemplo los vestuarios, comedores, cocinas y baños, así como tampoco deben alcanzar a ciertos lugares que no están dentro de la empresa.

Posteriormente, la Unidad emitió una serie de guías y recomendaciones en materia de videovigilancia por sectores de actividad, como la guía de drones, la guía para edificios y complejos habitacionales, la guía para el ámbito laboral, la guía para entidades públicas, y la guía para la utilización en vehículos, taxis y similares[19].

## ACTUALIZACIONES EN PROTECCIÓN DE DATOS PERSONALES

### a. Breve reseña

Como ya se ha mencionado, la Ley Nº 19.670, de 15 de octubre de 2018, en sus artículos 37 a 40, realiza actualizaciones a la normativa de protección de datos personales e incorpora nuevas tendencias internacionales en la materia. Su finalidad fue contemplar el avance de la tecnología y el nuevo contexto que esto apareja, y adoptar las mejores soluciones internacionales para dar respuesta adecuada a los titulares de los datos personales.

Es así entonces que se incorporan como elementos nuevos el concepto de extraterritorialidad, el de vulneraciones de seguridad, el de responsabilidad proactiva (que incluye la realización de evaluaciones de impacto, adopción de medidas de privacidad por diseño y por defecto), así como la creación de la figura del delegado de protección de datos para determinadas situaciones.

A dichos efectos, y para poder ampliar los conceptos que se incorporaron a la normativa de protección de datos, se reglamentaron los artículos indicados por decreto Nº 64/020, de 17 de febrero de 2020.

Parte de las modificaciones introducidas se mencionaron en los apartados anteriores, sin perjuicio de lo cual, debido a su trascendencia, se ampliará su desarrollo en los capítulos que siguen.

---

**18.** Consultar Resolución N°79/014
**19.** Acceder a Guías de Videovigilancia

### b. La adopción de nuevas medidas en el marco de la responsabilidad proactiva

En términos generales, la nueva normativa modifica el principio de responsabilidad haciéndolo evolucionar hacia el concepto de responsabilidad proactiva. En este sentido, nos remitimos a lo explicado con carácter general cuando desarrollamos este principio en la presente guía.

### c. Privacidad por diseño y Privacidad por defecto

La privacidad por diseño implica que desde el comienzo del tratamiento se adopten medidas que aseguren el cumplimiento de las normas de protección de datos personales.

El objetivo es que la protección de datos personales no sea una medida que se adopta con posterioridad, sino que se considera desde el inicio del tratamiento de datos personales.

En ese marco, responsables y encargados de tratamiento, en su caso, deberán incorporar en el diseño de las bases de datos, las operaciones de tratamiento, las aplicaciones y los sistemas informáticos, aquellas medidas dirigidas a dar cumplimiento a la normativa de protección de datos personales. A esos efectos, previo al tratamiento y durante todo su desarrollo, aplicarán medidas técnicas y organizativas apropiadas, tales como, por ejemplo:

**a)** Técnicas de disociación, seudonimización y minimización de datos.

**b)** Mecanismos para asegurar el ejercicio de los derechos de los titulares de los datos personales.

**c)** Documentación de los consentimientos o de otros fundamentos que legitimen el tratamiento.

**d)** Tiempo de conservación de los datos, considerando sus tipos y su tratamiento.

**e)** Adopción de planes de contingencia que incluyan medidas de seguridad de la información.

**f)** Análisis funcionales y modelos de arquitectura de los datos.

**g)** Otras medidas establecidas por la URCDP.

Asimismo, es importante tener en cuenta la privacidad por defecto. En este caso,

responsables y encargados del tratamiento (cuando corresponda) aplicarán las medidas técnicas y organizativas apropiadas a los efectos de garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

Es importante remarcar que esta obligación tiene relación directa con la cantidad de datos personales recogidos por el responsable, a la extensión de su tratamiento, a su plazo de conservación y a su comunicación cuando así corresponda.

### **d.** Las vulneraciones de seguridad.

Las nuevas disposiciones establecen que tanto el responsable y el encargado de tratamiento de datos deben adoptar las medidas técnicas y organizativas necesarias para conservar la integridad, confidencialidad y disponibilidad de la información, de forma de garantizar su seguridad.

A estos efectos, se considera importante valorar la adopción de estándares nacionales e internacionales en materia de seguridad de la información, tales como el Marco de Ciberseguridad elaborado por Agesic [20].

Constatada la existencia de incidentes de seguridad que ocasionen, entre otras, la divulgación, destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos, los responsables y encargados de tratamiento deberán iniciar los procedimientos previstos necesarios para minimizar el impacto de dichos incidentes dentro de las primeras 24 horas de constatados.

El responsable del tratamiento, una vez que constate la ocurrencia de alguna vulneración de seguridad que incida en la protección de datos, deberá comunicarlo a la Unidad Reguladora y de Control de Datos Personales en un plazo máximo de 72 horas de conocida la vulneración.

La comunicación a la Unidad Reguladora y de Control de Datos Personales deberá contener información relevante, tal como la fecha cierta o estimada de la ocurrencia de la vulneración, su naturaleza, los datos personales afectados, y los posibles impactos generados.

Se regula además que en caso que la vulneración hubiere sido conocida por el encargado del tratamiento, se la comunicará de inmediato al responsable del

**20.** Consultar el Marco de Ciberseguridad.

tratamiento. Por su parte, el responsable de tratamiento, una vez que constate la ocurrencia de alguna vulneración de seguridad que incida en la protección de datos, deberá comunicarla en un lenguaje claro y sencillo a los titulares de los datos que hayan sufrido una afectación significativa en sus derechos.

Solucionada la vulneración, el responsable deberá elaborar un informe pormenorizado de la vulneración de seguridad y las medidas adoptadas y comunicarlo a la URCDP.

Todo lo anterior podrá ser evaluado por el Consejo de la Unidad y solicitar información en caso de que entienda que no se cumplió con los pasos mencionados.

### **e.** Las evaluaciones de impacto en la protección de datos

La evaluación de impacto en la protección de datos es un proceso que las organizaciones deben efectuar para identificar y tratar los riesgos que puedan producir sus actividades habituales, sus nuevos proyectos o sus políticas corporativas cuando involucran el tratamiento de datos personales. Ello considerando que el tratamiento de datos personales puede provocar impactos en los derechos de las personas que deben ser de algún modo identificados, gestionados, minimizados o eliminados para cumplir con la normativa vigente[21].

El decreto N° 64/020 indica una serie de situaciones donde los responsables de tratamiento y eventualmente los encargados, deben realizarla en forma obligatoria:

- Utilizar datos sensibles como negocio principal
- Proyectarse un tratamiento permanente o estable de los datos especialmente protegidos
- Se realiza tratamiento con fines de perfilamiento
- Tratamiento de datos de grupos de personas en situación de escpecial vulnerabilidad.
- Tratamiento de grandes volúmenes de datos personales
- Transferirse datos personales a países no adecuados
- Otros que determina la URCDP

**21**. Definición contenida en la Guía de Evaluación de Impacto de esta Unidad y la AAIP. Acceder a la Guía.

El Consejo Ejecutivo de la Unidad, por resolución N° 30/020, de 12 de mayo de 2020 estableció la obligación de realizar una evaluación de impacto en forma previa al tratamiento de datos biométricos. Posteriormente, la ley N° 19.924, de 18 de diciembre de 2020 incorporó a la ley N° 18.331 el literal Ñ al artículo 4° y el artículo 18 bis, en los que se definen los datos biométricos y se impone legalmente la misma obligación.[22]

En general, a la hora de realizar una evaluación de impacto se recomienda determinar quiénes van a ser los participantes del proceso y la forma en que se va a documentar la evaluación. En segundo lugar, es necesario realizar un análisis del marco normativo aplicable. Ambas se consideran tareas previas e imprescindibles antes de la evaluación en sí misma[23].

En cuanto a las etapas subsiguientes, es necesario realizar en forma sucesiva un análisis preliminar, un contexto de tratamiento, un análisis de gestión de riesgos y culminar con un plan de tratamiento de riesgos, etapas que detallan en la Guía indicada, a cuya lectura y aplicación nos remitimos.

## **f.** Delegados de Protección de Datos Personales

Los Delegado de Protección de Datos Personales son un garante del cumplimiento de la normativa de la protección de datos en las organizaciones, sin sustituir las funciones que desarrolla la autoridad de control.

Dentro de la actualización del marco normativo nacional en materia de protección de datos personales, se crea la figura del Delegado de Protección de Datos Personales. La Ley establece determinados casos en los cuales resulta necesaria su designación, a saber:

- Entidades públicas o privadas, estatales o no, las privadas y las parcialmente de propiedad estatal
- Entidades privadas que traten datos sensibles como negocio principal.
- Entidades privadas que traten grandes volúmenes de datos personales. De acuerdo con la reglamentación posterior se entiende que gran volumen de datos es aquel que implique un tratamiento de datos de más de 35.000 personas.

La referencia a Entidades puede alcanzar a personas físicas o jurídicas que realicen el tratamiento de datos personales o terceros, en calidad de responsable o encargado de

**22.** Resolución N° 30/020

**23.** A los efectos de conocer más detalladamente cómo se debe realizar una evaluación de impacto se sugiere consultar la guía disponible aquí.

tratamiento.

El decreto reglamentario expresamente indica que además la Unidad, de oficio o ante una gestión expresa, puede expedirse en el sentido de indicar la pertinencia o no de su designación.

Sus funciones principales son [24]:

- Asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales.
- Supervisar el cumplimiento de la normativa sobre dicha protección en su entidad.
- Proponer todas las medidas que entienda pertinentes para adecuarse a la normativa y a los estándares internacionales en la materia.
- Actuar como nexo entre la entidad y la URCDP.

La norma además establece que debe poseer las condiciones necesarias para el correcto desempeño de sus funciones y actuar con autonomía técnica.

Además, existen otros aspectos que merecen ser analizados como por ejemplo la calidad y condiciones del delegado, su posición y su plazo de designación, cese o renuncia.

En ese marco, es importante indicar que el delegado puede desempeñar sus funciones a través de cualquier modalidad contractual sea en forma dependiente o no.

Conforme el decreto N° 64/020, los delegados deben contar con conocimiento en derecho, especializados en protección de datos personales debiendo acreditarse dicha calidad al momento de su comunicación a la URCDP. La Unidad ha clarificado el alcance de esta disposición a través de la resolución N° 32/020 del 19 de mayo de 2020, por la que se establece que se deberá tener en cuenta especialmente su calidad de profesional del área jurídica o poseer conocimientos en derecho, con énfasis en derechos humanos. Además, deberá contar con conocimientos sobre regulación en materia de protección de datos personales, lo que podrá acreditarse mediante cursos o actividades brindadas por la URCDP u otras entidades nacionales e internacionales. Se valorará especialmente la realización de cursos vinculados a responsabilidad proactiva y tratamiento de categorías especiales de datos. Se tendrá en cuenta,

24 Acceder al artículo 40 de la Ley N° 19.670

además, la experiencia previa en el ámbito de la protección de datos.[25]

La evaluación de sus conocimientos corresponde a responsables y encargados en función de los citados criterios, aclarándose por resolución de la URCDP N° 44/020 de 21 de julio de 2020 que el énfasis en derechos humanos es el necesario para contextualizar el derecho a la protección de datos en sus relaciones con otros derechos. [26]

El Delegado de Protección de Datos puede ser una persona jurídica. En estos casos, se debe informar a la URCDP quienes son sus integrantes y cuál es su órgano de administración, sin perjuicio de lo cual, es necesario identificar a sus representantes y a una persona física que se constituya en el nexo con la Unidad, de conformidad con la precitada resolución idéntica obligación existe para equipos de delegados, de conformidad con lo indicado por resolución de la URCDP N° 44/020.

A los efectos de desarrollar en tiempo y forma sus tareas, el delegado tiene que poder participar en forma adecuada en todas las cuestiones relativas a la protección de datos. Para ello debe poder tener acceso a las bases de datos y a las operaciones de tratamiento.

La persona designada como delegado debe guardar absoluta confidencialidad de las informaciones que tiene acceso por su calidad y no debe tener conflicto de intereses.

El delegado debe actuar con plena autonomía técnica y no debe recibir instrucciones en el desempeño de sus funciones.

Cabe indicar que cuando corresponde la designación de un delegado se cuenta con un plazo de 90 días a contar desde el inicio del tratamiento para comunicarlo a la Unidad. También se preveía un plazo para su designación para aquellas entidades que debían contar con esta figura desde la entrada en vigor del Decreto. La comunicación del delegado se realiza a través del Sistema de Registro de Base de Datos y Comunicaciones de Delegados disponible a través de la web de la URCDP.

Por otra parte, el decreto establece que un conjunto de entidades con cometidos o actividades afines pueden nombrar un único delegado de protección de datos, al igual que varias entidades públicas, siempre que pueda cumplir las funciones legalmente establecidas en relación a todas y cada una de ellas.

**25**. Consultar la Resolución 32/020

**26.** Consultar Resolución 44/020

## ¿CÓMO CONTACTARSE CON LA URCDP?

Los medios de contacto con la URCDP son:

- Sitio web: www.gub.uy/urcdp
- Mail de contacto: infourcdp@datospersonales.gub.uy
- Teléfono: 2901 0065, opción 3