
Ley de Protección de Datos Personales

Fuente de Información

Biográficos

Familiares

Hijos

Infracciones

Origen Racial y Étnico

Nombre y DNI

Lugares Visitados

Condenas

Opinión Política

Domicilio

Biométricos

Estado Civil

Medidas de Seguridad

Laborales

Convicción Religiosa y Filosófica

Salarios

Pertenencia a Sindicatos

Bienes

Cumplimiento Obligaciones

Financieros

Salud

Genética

Académicos

Impuestos

Compras y Ventas

Sexualidad

Consumos

Tarjetas de Créditos

Deudas

Hobbies

De Localización

Proporcionamos DATOS

- Nos anotamos en atractivas promociones o sorteos
- Compramos en el supermercado
- Nos inscribimos en un gimnasio o curso
- Realizamos trámites públicos o privados
- Utilizamos tarjetas de crédito o débito y/o usamos nuestro teléfono celular

Proporcionamos DATOS

- Viajamos en transporte público
- Accedemos a nuestra cuenta de e-mail
- Bajamos archivos de la WEB
- Chateamos, intervenimos en foros de discusión, rede sociales

Datos sobre:

- Personalidad
- Actitud
- Comportamiento
- Economía
- Hábitos Sociales
- Hábitos de Consumo

Están en manos de terceros conocidos y desconocidos

¿Dónde están mis DATOS?

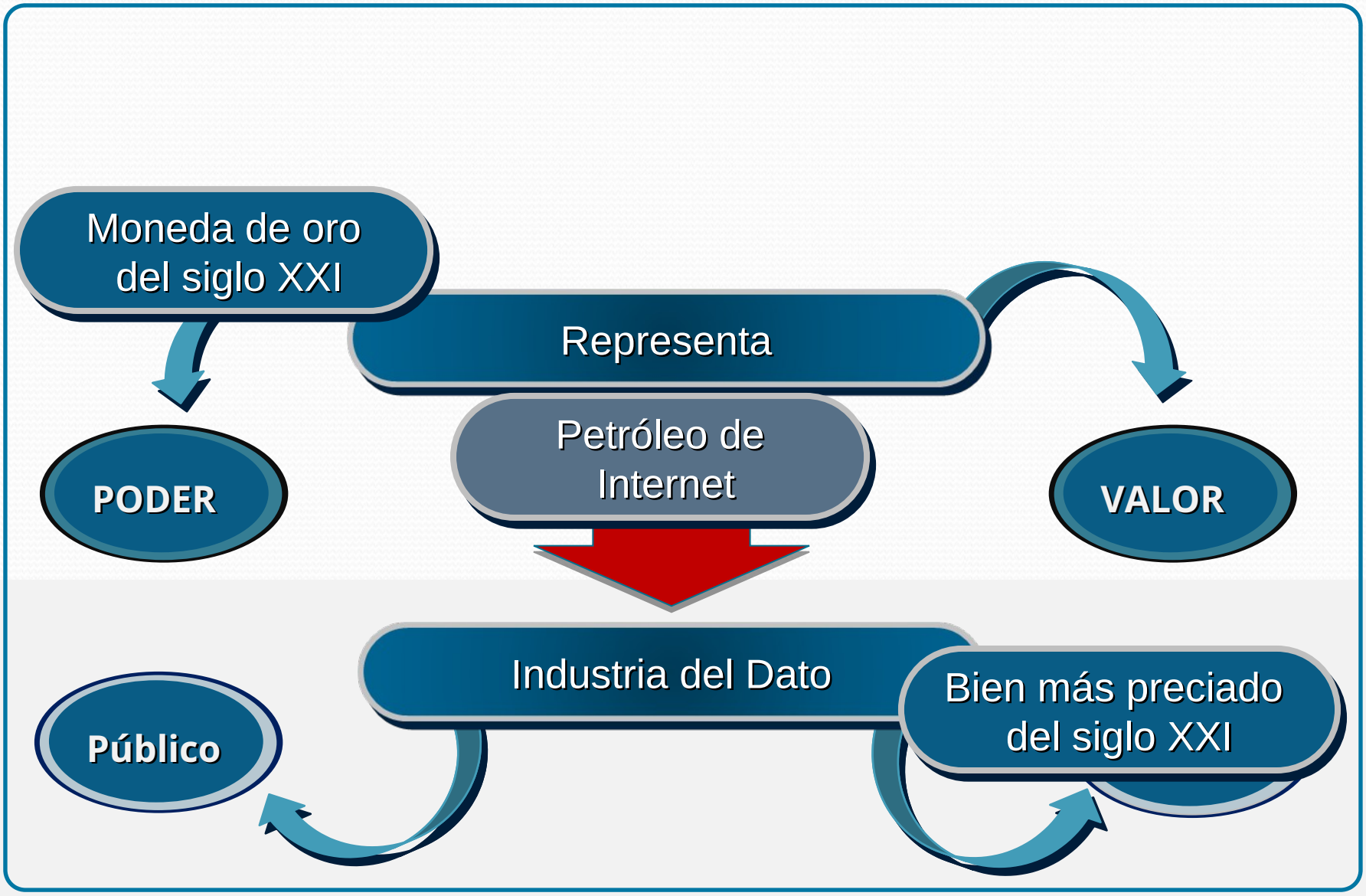
¿Cuál es el destino de los datos que proporcionamos en las múltiples transacciones cotidianas?

¿Quiénes los utilizan y con qué fines?

¿Tenemos verdadera autodeterminación sobre ellos?

¿Qué CONTROL ejerce el ESTADO para protegernos?

DATOS


Moneda de oro del siglo XXI
Representa
PODER
Petróleo de Internet
VALOR
Industria del Dato
Público
Bien más preciado del siglo XXI

Industria del Dato

Público

Gobierno Electrónico

Servicios

Privado

Aglutinar Datos

Crear Bancos de Datos

Perfiles Virtuales

quien es una persona

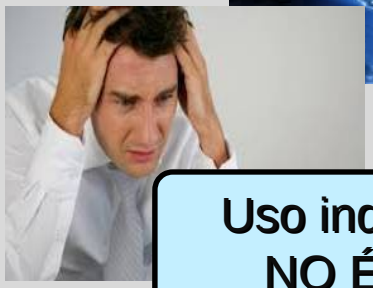
Factor para tomar decisiones

Afectan positiva o negativamente a las Personas

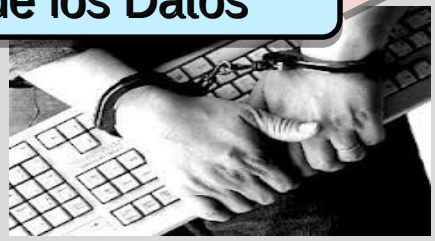
Tecnologia

Tecnología y el Tratamiento de Datos

NO AFECTAN



Uso indebido o NO ÉTICO de los Datos



Pone en RIESGO

DERECHOS de las PERSONAS

El camino hacia la PROTECCIÓN

Normas Sectoriales

- Censos Población y Vivienda
- Sector Financiero
- Sector Asistencial

- Constitución Nacional Art. 43 - Reforma 1994
- Ley Nacional de Protección de Datos Personales N° 25326 / 2000
- Decreto Reglamentario N° 1558 / 2001 y sus modificatorias
- Ley 26951/2014 - Registro Nacional "NO LLAME"
- Creación de la Dirección Nacional de Protección de Datos Personales

www.argentina.gob.ar/aaip/datospersonales

BASES DE DATOS PÚBLICAS SELLO ARGENTINO DE PRIVACIDAD

PDP

Reforma Constitución 1994

- **Incorporó Artículo 43**

Da a los ciudadanos la posibilidad de interponer la acción de amparo **Habeas Data** para que pueda **tomar conocimiento** de sus datos personales que consten en registros o bancos de datos públicos o privados, conocer la **finalidad** para las cuales los emplean y en caso de falsedad o discriminación poder **exigir** la supresión, rectificación, confidencialidad o actualización.

Ley 25.326 / 2000

Objeto

- **Protección Integral de los Datos Personales asentados en:**

- **Archivos**
- **Registros**
- **Bancos de Datos**
- **Otros medios técnicos de tratamiento de datos**

Públicos y Privados

Destinados a dar **INFORMES**

Personas Físicas e Ideales

Protección Integral: Para garantizar el **derecho al honor y a la intimidad de las personas**, así como también el acceso a la información que sobre las mismas se registre de conformidad a la constitución nacional art. 43.

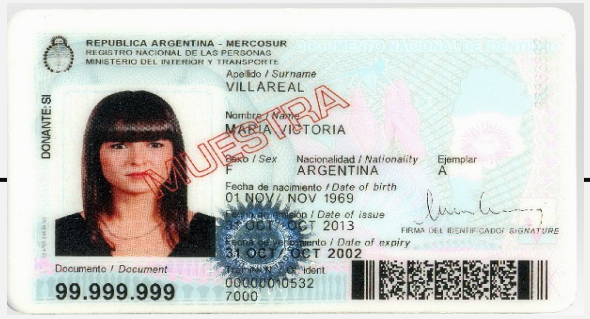
Datos Personales (DP)

¿Que son?

Información de cualquier tipo referida a Personas Físicas o de existencia Ideal determinadas o determinables

Nombres y Apellidos
DNI
Fecha Nacimiento
Domicilio

Identidad que pueda determinarse directa o indirectamente:
Perfil psicológico, físico, fisiológico, económico, cultural o social



Datos Personales Excluidos

- Datos Personales almacenados en archivos de uso interno, personal o doméstico

- **Bases de Datos de fuentes periodísticas**
- Archivos de datos recopilados con fines estadísticos, disociados de la entidad titular

Datos Sensibles (DS)

- **Datos Personales que revelan:**

- ➡ Origen racial y étnico
- ➡ Opiniones Políticas
- ➡ Convicciones Religiosas, Filosóficas o Morales
- ➡ Afiliación Sindical
- ➡ Información referente a la salud
- ➡ Información referente a la vida sexual

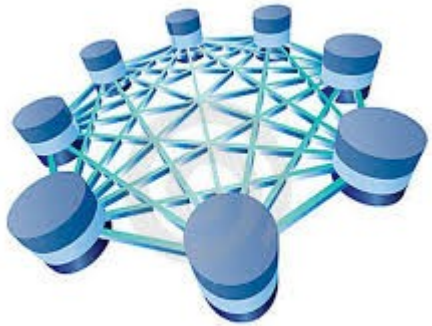
YO SÉ QUIÉN SOY

Archivo, Registro, Base o Banco de Datos

- Conjunto organizado de datos Personales que sean objeto de tratamiento o procesamiento, **ELECTRÓNICO o NO**, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

Responsable de Archivo, Registro, Base o Banco de Datos

- Persona Física o de existencia Ideal, Pública o Privada que es Titular de un archivo, registro, base o banco de datos.



Tratamiento de Datos

- **Operaciones y procedimientos sistemáticos, electrónicos o NO que permiten:**

Recolección
Conservación
Ordenación
Almacenamiento
Modificación
Relacionamiento
Evaluación
Bloqueo
Destrucción

y en general todo procesamiento de Datos Personales

Datos Informatizados *Datos personales sometidos a tratamiento o procesamiento electrónico o automatizado*

- **Así como también cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.**

Titular de los Datos

- Persona física o de existencia ideal con domicilio legal en el país, cuyos datos sean objeto del tratamiento que mencionamos

Usuarios de Datos

- Persona Pública o Privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o Base de Datos propios o a través de conexión con los mismos

Disociación de Datos

- Tratamiento de Datos Personales de manera que la información, obtenida no puede asociarse a persona determinada o determinable

Archivos de Datos - Licitud

Formar Archivos de datos Personales

Lícito solo sí

Se encuentran debidamente inscriptos

Organismo de Control

PDP

Agencia de Acceso a la Información Pública

Calidad de los Datos

- **Deben ser:**

Ciertos
Adecuados
Pertinentes y no excesivos

- **No utilizar medios desleales o fraudulentos**
- **No pueden utilizarse para otras finalidades distintas a las que motivaron su obtención**
- **Datos exactos y actualizados o deben suprimirse**
- **Almacenados de forma que permitan el derecho al acceso de su titular**
- **Destruirlos cuando dejan de ser necesarios o pertinentes**

Datos Sensibles (DS)

A. Ninguna persona puede ser obligada a proporcionarlos

B. Solo pueden ser recolectados por razones de interés general autorizadas por ley

C. También con finalidad estadística o científica cuando no se identifiquen sus titulares

D. Está prohibido formar archivos, bases o registros con datos sensibles

Datos Sensibles (DS)

Seguridad de los Datos

Responsable o Usuario de Archivo

- Debe: **Adoptar Medidas Técnicas y Organizativas**
- Garantizar: **Seguridad y Confidencialidad de los Datos Personales**
- Evitar: **Adulteración, Pérdida, Consulta o Tratamiento NO Autorizado**
- Detectar: **Desviaciones de Información**

- **Prohibido** reunir Datos Personales sin implementar medidas Técnicas de Integridad y Seguridad
- **Prohibido** transferir Datos Personales a países y organismos internacionales que no proporcionen niveles de protección adecuadas

Derechos de los Titulares de Datos

Derechos

- Derecho de Información
- Derecho de Acceso
- Derecho de Rectificación, Actualización o Supresión

Excepciones

- Protección de la Defensa de la Nación
- Orden y Seguridad Públicos
- Protección de Derechos e Intereses de Terceros

Registro de Archivos de Datos

Inscribirse en el Registro establecido por el Organismo de Control

- Nombre y Domicilio del Responsable
- Características y Finalidad del Archivo
- Forma de Recolección y Actualización de los Datos
- Destino de los Datos y a quienes pueden ser transmitidos
- Modo de Inter-relacionar la información registrada
- Medios para Garantizar la Seguridad de los Datos
- Tiempo de Conservación de los Datos
- Forma y Condiciones para el Acceso a los Datos
- Procedimientos para realizar Rectificación o Actualización

Recomendaciones

Utilizar Internet en forma segura

- No completar formularios al azar, concursos, premios u obsequios
- No entregue más información personal que la necesaria
- Proteja a sus hijos o familiares

Importante

- “La Educación sobre el uso responsable de los Datos Personales debe comenzar en la niñez”

Responsable de DB personales

- Son todas las personas humanas o jurídicas públicas o privadas (empresas, instituciones, organizaciones de la sociedad civil, etc.) que sean titulares de un archivo, registro, base o banco de datos.

- De acuerdo a la normativa vigente los responsables de bases de datos personales públicas y privadas destinadas a dar informes, deben inscribirlas en el Registro Nacional de Bases de Datos.

- Las bases de datos de uso exclusivamente personal están exceptuadas de la obligación de inscripción, por ejemplo: direcciones de amistades en computadoras personales, agendas personales, etc.

¿Qué es una base de datos personales destinada a dar informes?

- Es todo registro, archivo, base o banco de datos que permita obtener información sobre las personas, se transmitan o no a terceros.

- La Real Academia Española define a la palabra "informe" como:

  "Descripción oral o escrita de las características o circunstancias de un suceso o asunto".

- Así:

  "banco de datos destinado a dar informes" equivale a

  "banco de datos destinado a describir algo sobre las personas".

¿Qué es una base de datos personales destinada a dar informes?

Cuando se accede a una base de datos que interrelaciona datos y produce una serie de informaciones acerca de una persona determinada, se configura la acción requerida por la norma:

"**brindar informe**"

Ejemplos prácticos

Hay numerosos casos de bases de datos en el ámbito empresario que dan información sobre una persona, y que exceden el uso exclusivamente personal, en virtud de las cesiones o transferencias de información que realizan.

- **Base de datos de CLIENTES**:

Con esta DB se llevan a cabo diversas cesiones de datos personales como:

la emisión de facturación,
se hacen retenciones y liquidaciones a AFIP, IIBB,
se puede informar morosidad.

Ejemplos prácticos

- Base de datos de **PROVEEDORES**:

Con esta DB se llevan a cabo diversas cesiones de datos personales como:

las retenciones de tributos,

emisión de recibos,

informaciones a las cámaras empresariales,

o sea, una serie de cesiones de información que exceden el uso personal de la base.

Ejemplos prácticos

- Base de datos de **PERSONAL**:

Con esta DB se llevan a cabo diversas cesiones de información cuando :

se liquidan cargas sociales a ANSES o a Cajas de Jubilaciones,
se informa sobre impuesto a las ganancias a AFIP,
se transfiere información al banco para depositar el sueldo,
información a la ART (implica cesión de datos sensibles),
información al sindicato si el empleado se encuentra afiliado (implica cesión de datos sensibles).

Obligaciones de los responsables de bases de datos personales

1. INSCRIPCION DE BASES DE DATOS PERSONALES:

Los archivos y bases de datos públicos y privados destinados a dar informes deben estar inscriptos en el Registro Nacional de Bases de Datos Personales. Incumplimiento acarrea sanciones.

Los archivos de uso exclusivo personal están exceptuados de la obligación de inscripción (Ej.: computadora personal con direcciones de amistades y agendas).

Obligaciones de los responsables de bases de datos personales

2 · INFORMACION AL TITULAR DEL DATO PERSONAL

Titular DEBE PRESTAR su Consentimiento

Debo ser informado sobre:

- **Finalidad para la que serán tratados y quienes pueden ser sus destinatarios.**
- **Existencia del banco de datos, electrónico o no y la identidad y domicilio del responsable.**
- **Caracter facultativo u obligatorio de las respuestas al cuestionario que se proponga.**
- **Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de estos.**
- **Posibilidad de ejercer los derechos de acceso, rectificación y supresión de los datos.**

Licitud sin consentimiento

Tratamiento de Datos Personales

Es Lícito SIN Necesidad de Consentimiento

- Datos Obtenidos por Fuentes de Acceso Público e Irrestricto
- **Recabados por el ejercicio de funciones propias de los Poderes del Estado o en virtud de una obligación legal**
- Listados limitados a: Nombre - DNI Identificación Tributaria o Previsional Ocupación – Fecha Nacimiento, Domicilio
- **Derivados de una relación contractual, científica o profesional del titular de los datos y resulten necesarios para su desarrollo o cumplimieneto**

Obligaciones de los responsables de bases de datos personales

3. SEGURIDAD DE LA INFORMACION:

Las bases de datos personales deben garantizar la seguridad y confidencialidad de los datos personales, para ello deben adoptarse determinadas medidas técnicas y organizativas.

Medidas de seguridad recomendadas

Obligaciones de los responsables de bases de datos personales

4. TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES:

- La Ley prohíbe la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados (proporciona un nivel adecuado de protección cuando dicha tutela se deriva directamente del ordenamiento jurídico vigente, o de sistemas de autorregulación).

- **Países con niveles de protección adecuada**

  Estados miembros de la Unión Europea y miembros del espacio económico europeo (EEE), Confederación Suiza, Guernsey, Jersey, Isla de Man, Islas Feroe, Canadá, Principado de Andorra, Nueva Zelanda, República Oriental del Uruguay y Estado de Israel sólo respecto de los datos que reciban un tratamiento automatizado.

Obligaciones de los responsables de bases de datos personales

4. TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES: EXCEPCIONES

La prohibición de transferencia internacional, a países u organismos que no proporcionen niveles de protección adecuado, **no rige en los siguientes casos**:

- Colaboración judicial internacional.
- Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica.
- Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable.
- Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte.
- Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.
- Cuando el titular de los datos hubiera consentido expresamente la cesión.
- Cuando existan cláusulas contractuales que brinden una protección similar a la de nuestra normativa.

Medidas de seguridad recomendadas para el tratamiento y conservación de los Datos Personales en medios informatizados

A. Recolección de datos

B. Control de acceso

C. Control de cambios

D. Respaldo y recuperación

E. Gestión de vulnerabilidades

F. Destrucción de la información

G. Incidentes de seguridad

H. Entornos de desarrollo

A - Recolección de datos

- A.1 **Integridad**
- A.1.1 Asegurar la completitud

  Verificar que los campos que componen el formulario de recolección de datos permitan el ingreso completo de los datos requeridos.
- A.1.2 Minimizar los errores de ingreso

  Indicar en forma clara y concreta el tipo de información a ingresar y el formato de la misma.
- A.1.3 Asegurar la integridad

  Verificar la exactitud del dato ingresado en caso de que el tipo de registro lo permita (ej. Fecha formato: DD/MM/AAAA)

A - Recolección de datos

- A.2 **Confidencialidad**

- A.2.1 Asegurar la confidencialidad durante el proceso de recolección.

  Cifrar la comunicación cliente-servidor durante la recolección.

- A.2.2 Limitar el acceso a la recolección de los datos.

  - Limitar cache del formulario en el cliente únicamente al momento de carga de datos.

  - Limitar la carga de datos en el cliente a una sola sesión de usuario.

A - Recolección de datos

- A.2 **Confidencialidad**

- A.2.3 Limitar el acceso no autorizado durante la recopilación

  - Utilizar certificados digitales seguros y validados por entidades autorizadas (CA).

  - Para Datos Sensibles (DS), cifrar la comunicación durante el traslado desde el servidor de aplicación hacia la base de datos.

B – Control de acceso

- B.1 **Identificación de activos**
- B.1.1 Identificar los activos

  Elaborar un inventario de activos informáticos que almacenen o gestionen datos personales.
- B.1.2 Definir responsables y responsabilidades

  - Definir propietarios de activos informáticos que almacenen o gestionen datos personales.
  - Notificar a los propietarios de activos informáticos que almacenen o gestionen datos personales.
  - Especificar a los propietarios de activos informáticos autorizaciones de acceso (tipo de acceso y validez).

B – Control de acceso

- B.1 **Identificación de activos**

- B.1.3 Verificar la aplicación de controles

  - Elaborar un procedimiento de actualización periódica del inventario.
  - Elaborar un procedimiento de verificación de autorizaciones.
  - Elaborar un procedimiento para nuevos activos informáticos, definiendo responsable asignado y autorizaciones.

B – Control de acceso

- B.2 **Acceso a los datos**

- B.2.1 Gestionar los accesos a los sistemas

  - Elaborar un documento interno que defina los controles de acceso a cada sistema.
  - Definir e identificar aquellos usuarios que por su rol de superusuarios (administradores) puedan evadir los controles de acceso definidos para el propietario.
  - Controlar y monitorear a los superusuarios (registrando accesos y actividad).

B – Control de acceso

- B.2 **Acceso a los datos**

- B.2.2 Asignar los permisos

Disponer de una notificación concreta y formal de las responsabilidades asumidas por cada usuario que acceda internamente a los sistemas (notificación fehaciente).

B – Control de acceso

- B.2 **Acceso a los datos**

- B.2.3 Verificar la identificación y autorización

  - Disponer de un sistema que identifique inequívocamente a cada usuario.
  - Establecer una política de contraseñas seguras.
  - Disponer de un registro de acceso a los sistemas.
  - Disponer de un registro de uso de los sistemas.
  - Disponer de un procedimiento de Alta, Baja, Modificación de usuarios.
  - Limitar el acceso de los superusuarios a los datos personales o establecer un seguimiento de su actividad.
  - Asegurar la implementación de la política de contraseñas seguras en todos los sistemas.
  - Evitar el uso de usuarios genéricos.

B – Control de acceso

- B.2 **Acceso a los datos**
- B.2.4 Controlar el acceso físico al centro de datos

- Disponer de un control de acceso físico al centro de datos.
- Elaborar un procedimiento de control de acceso físico.
- Disponer de un registro de los accesos físicos (identificando día, hora, ingresantes y motivo).
- Asegurar el sistema de registro del control de acceso.

B – Control de acceso

- B.2 **Acceso a los datos**

- B.2.5 Monitorear la actividad

  - Definir un procedimiento de limpieza de cuentas inactivas con privilegios de acceso.

  - Para datos sensibles:

  - Limitar el acceso interno a los sistemas con un mismo usuario a una sola sesión concurrente.

  - Monitorear y controlar las cuentas de usuario que dispongan de privilegios especiales, identificarlas en forma diferencial.

  -Identificar y analizar intentos de autenticación fallidos.

C – Control de cambios

- C.1 **Control de cambios**
- C.1.1 Asegurar los cambios

- Verificar que los cambios a realizar en entornos productivos mantengan y aseguren la integridad de los datos.

-Asegurar durante los procesos de cambio las medidas de Recolección de datos (punto A) y Control de acceso (puntoB).

-Disponer de un registro de las verificaciones y/o pruebas realizadas para asegurar la integridad, disponibilidad y confidencialidad de los datos.

- Para datos sensibles:

- Definir un responsable de control de entornos productivos.

- Disponer de un procedimiento de control de cambios en entornos productivos.

D – RESPALDO Y RECUPERACIÓN

- D.1 **Copias de respaldo y proceso de recuperación**
- D.1.1 Asegurar un proceso formal de respaldo y recuperación

- Disponer de un procedimiento de resguardo de información donde se identifique:

qué tipo de información se resguardará

qué medio físico se utilizará

cantidad de copias de resguardo que se realizaran

periodicidad de las ejecuciones de copias de resguardo

descripción del proceso de la realización de resguardo

tiempo de almacenamiento de copias de resguardo

responsable de la realización de copias de resguardo

- Definir y verificar procedimiento de pruebas de recuperación.

D – RESPALDO Y RECUPERACIÓN

- D.1 **Copias de respaldo y proceso de recuperación**
- D.1.1 Asegurar un proceso formal de respaldo y recuperación

- Disponer de un registro de pruebas de recuperación realizadas identificando:

Tipo de información recuperada

lugar y fecha donde se realizaron las pruebas de recuperación

resultado de las pruebas de recuperación

responsable de la realización de las pruebas de recuperación

personal interviniente en las pruebas de recuperación

notificación al responsable de datos

- Disponer de un inventario que identifique las copias de seguridad, su ubicación real y el medio físico en donde se encuentran.

D – RESPALDO Y RECUPERACIÓN

- D.1 **Copias de respaldo y proceso de recuperación**
- D.1.2 Asegurar control de acceso en los medios

- Aplicar las medidas de Control de acceso (B) a las copias de resguardo.
- Cifrar las copias de resguardo utilizando herramientas seguras.
- Asegurar los entornos de prueba de recuperación utilizando las mismas medidas de seguridad que un entorno productivo.
- Eliminar en forma segura la información recuperada durante las pruebas una vez verificada su exactitud.
- Para los datos sensibles:
- Disponer medidas de protección contra incendios o inundaciones en el sitio de almacenamiento de los medios físicos que contienen las copias de resguardo.
- Almacenar las copias de resguardo en una locación física diferente a la del sistema productivo.
- En caso de traslado de copias de resguardo, disponer de un procedimiento de registro y control del tránsito.
- Asegurar los entornos de prueba de recuperación utilizando las mismas medidas de seguridad que un entorno productivo.

E – GESTION DE VULNERABILIDADES

- E.1 **Gestión de vulnerabilidades**
- E.1.1 Prevenir incidentes de seguridad desde el diseño

- Considerar y analizar las posibles amenazas a la que estarán expuestos los sistemas informatizados.

- Disponer de un mapa conceptual que permita conocer el flujo de la información entre los distintos sistemas informatizados.

- Establecer un documento de seguridad que indique las medidas de seguridad adoptadas para los sistemas de información.

E – GESTION DE VULNERABILIDADES

- E.1 **Gestión de vulnerabilidades**
- E.1.2 Asegurar una protección adecuada

- Establecer controles de seguridad para las aplicaciones que procesen datos personales, entre ellas:

- Segmentación de roles y perfiles
- Autenticación segura
- Gestión de sesiones (cumpliendo apartado de Control de acceso (B))
- Gestión de mensajes de error en aplicaciones
- Implementar reglas y controles de seguridad en los servidores que estén conectados a una red externa y almacenen o gestionen datos personales, programando alertas ante posibles ataques.
- Segmentar en forma física o lógica la red de la entidad, separando las áreas públicas de las privadas.
- Separar los ambientes de Producción, QA, Prueba y Desarrollo.
- Implementar controles para la prevención de virus informáticos en los servidores que almacenen o gestionen datos personales.
- Implementar controles para la prevención de ataques en las estaciones de trabajo que gestionen datos personales.
- Implementar controles para la prevención de virus informáticos en las estaciones de trabajo que gestionen datos personales.
- Establecer y ejecutar un procedimiento de actualización periódica de software/hardware de todo el equipamiento.
- Definir a una persona responsable del cumplimiento de las medidas de seguridad.

E – GESTION DE VULNERABILIDADES

- E.1 **Gestión de vulnerabilidades**
- E.1.3 Detectar posibles incidentes de seguridad

- Disponer de un sistema de auditoria de incidentes implementando un sistema de registro que permita realizar un seguimiento ante eventos o acciones de un posible incidente (sistema de logs).
- Sincronizar todos los servidores/equipamiento con un servidor de horario público para asegurar una correcta trazabilidad en caso de realizar una auditoría.
- Implementar un proceso de denuncia que permita que los usuarios alerten eventos de seguridad.
- Disponer de un sistema de gestión de incidentes capaz de mostrar fecha de registro, documentación relevante, personas involucradas, activos afectados.
- Para datos snsibles
- Establecer controles de seguridad para las aplicaciones que procesen datos personales, entre ellas:
- Filtros de inyección de código en bases de datos
- Filtros de inyección de código en aplicaciones
- Implementar controles para la detección de intrusiones en la red.
- Implementar controles para la detección de intrusos y/o fuga de información en las estaciones de trabajo que tengan acceso al tratamiento de datos personales.

- E.1.4 Garantizar medidas eficaces y perdurables

- Implementar periódicamente procesos de auditoria interna para verificar el cumplimiento de lo mencionado con anterioridad, exportando informes y resguardándolos.
- Realizar auditorías externas a fin de evaluar la seguridad de los sistemas internos.

F – DESTRUCCIÓN DE LA INFORMACIÓN

- F.1 **Asegurar la destrucción de la información**
- F.1.1 Establecer modelo/formato de destrucción

  - Establecer un procedimiento de destrucción de datos en donde se identifique:
  tipo de información a destruir, medio que contiene la información, responsable de la destrucción, descripción del proceso y método de destrucción utilizado

- F.1.2 Establecer mecanismos seguros de eliminación

  - Implementar un proceso de destrucción físico o lógico de la información que asegure el borrado total de la información sin posibilidad de recuperación de la misma cumpliendo tres premisas: irreversibilidad, seguridad, confidencialidad.

- F.1.3 Designar responsable de destrucción

  - Establecer una persona autorizada para la destrucción y documentar su autorización.

- F.1.4 Monitorear el proceso

  - Disponer de un inventario que identifique los medios destruidos.

F – DESTRUCCIÓN DE LA INFORMACIÓN

- F.1 **Asegurar la destrucción de la información**
- F.1.2 Descarte de medios magnéticos

- Para datos sensibles:

- Implementar un proceso de destrucción lógico de reescritura continua, de modo que los datos originales no puedan ser recuperados, pudiendo reutilizar el medio magnético.

- En caso de no poder realizar el proceso de destrucción lógica, implementar un proceso de destrucción física utilizando técnicas de desmagnetización, desintegración, incineración, pulverización, trituración o fundición.

G – INCIDENTES DE SEGURIDAD

- G.1 **Notificación ante incidentes de seguridad**
- G.1.1 Establecer responsabilidades y procedimientos

- Elaborar un procedimiento de gestión ante incidentes de seguridad.
- Establecer una persona responsable de la comunicación.

- G.1.2 Elaborar informe

- Elaborar un informe del incidente de seguridad que tenga de contenido mínimo:
- la naturaleza de la violación
- categoría de datos personales afectados
- Identificación de usuarios afectados
- medidas adoptadas por el responsable para mitigar el incidente
- medidas aplicadas para evitar futuros incidents.

- G.1.3 Enviar notificacion

- Enviar notificación de incidente anexando el informe a:
Av. Pte. Gral. Julio A. Roca 710 - CABA - C1067ABP - Correo electrónico: incidente.seguridad@aaip.gob.ar

H – ENTORNOS DE DESARROLLO

- H.1 **Seguridad en los entornos de desarrollo**
- H.1.1 Implementar política de desarrollo seguro

- Utilizar técnicas de enmascaramiento o disociación de la información en entornos de desarrollo, prueba y QA.

- En caso de no cumplir el punto H.1.1 y utilizar datos personales en entornos de desarrollo, prueba y QA, deberán considerarse y aplicar todas las medidas recomendadas anteriormente en los puntos A,B,C,D,E,F,G.

Medidas de seguridad recomendadas para el tratamiento y conservación de los Datos Personales en medios NO informatizados

A. Recolección de datos

B. Control de acceso

C. Conservación de la información

D. Destrucción de la información

E. Incidentes de seguridad

¿Que hacer en caso de violación de nuestros derechos?

Órgano de Control

Hacer cumplir la Ley y Disposiciones

Informar a los Titulares

Censar Archivos

Dictar Normas y Reglamentaciones

Solicitar

Información a Entidades Públicas y Privadas

Controlar Integridad y Seguridad existente sobre los Datos

Imponer Sanciones

ACCIONES de la Agencia de Acceso a la Información Pública

- INSPECCIONES - ***Objetivos***

  1. Tomar conocimiento de las actividades del responsable de la base de datos, los datos personales que administra, los medios y la forma en que lo hace.

  2. Verificar que el responsable de la base de datos adopte las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos personales.

  3. Evaluar el grado de cumplimiento a lo prescripto por la Ley.

  4. Realizar observaciones.

ACCIONES de la Agencia de Acceso a la Información Pública

- SANCIONES

  Se encuentra facultada para imponer las sanciones administrativas .

  A fin de dar **publicidad** sobre los infractores se pueden consultar:

  Los **Registros de infractores** donde constan:

  – La falta cometida, la sanción aplicada, el grado de acatamiento, los recursos planteados, la decisión final recaída, la reincidencia y todo otro elemento de juicio que sea de interés para la Agencia de Acceso a la Información Pública.

¿Por qué hay que registrar bases de datos de videovigilancia?

- Según lo establecido en la Disposición 10/2015, "... una imagen o registro fílmico constituyen, a los efectos de la Ley N° 25.326, un dato de carácter personal, en tanto que una persona pueda ser determinada o determinable...".

- Una imagen con formato digital permite su tratamiento a través de sistemas informáticos y conformar un sistema organizado de fácil consulta.

¿Por qué hay que registrar bases de datos de videovigilancia?

La base de datos de **videovigilancia** debe ser declarada (al igual que se declaran, por ejemplo, los empleados, clientes y proveedores). En ese momento, al presentar el formulario, debe presentarse también el "manual de tratamiento de datos personales" cuyos requisitos mínimos están indicados en el artículo 7° de la disposición 10/2015.

Manual de Videovigilancia

El manual de videovigilancia debe contener:

- Forma de la recolección.
- Referencia de los lugares, fechas y horarios en los que se prevé que operarán.
- Plazo de conservación de los datos.
- Mecanismos técnicos de seguridad y confidencialidad previstos.
- Medidas dispuestas para el cumplimiento de los derechos del titular del dato contemplados en los artículos 14, 15 y 16 de la Ley 25326.
- Los argumentos que justifiquen la toma de fotografías para el ingreso al predio, en caso de disponerse dicha medida de seguridad.
- A su vez, en el caso de actividades de videovigilancia se debe informar previamente al público:
- La existencia de cámaras de seguridad (sin que sea necesario precisar su ubicación puntual).
- Los fines para los que se captan las imágenes.
- Los datos de contacto del responsable de la base de datos, para que las personas puedan ejercer sus derechos como titulares de datos personales.

ISOLOGO “Responsable Registrado”

Los responsables de bases de datos personales que tengan trámite aprobado de inscripción en el Registro Nacional de Bases de Datos podrán hacer uso del los isologotipos aprobados por la Resolución 12/2018, de acuerdo al caso correspondiente (bases de datos públicas o privadas).

Para ello, deberán solicitar la autorización a la Dirección Nacional de Datos Personales de la Agencia de Acceso a la Información Pública.

Ley 26.951 – Registro Nacional “NO LLAME”

OBJETO

Proteger a los titulares o usuarios autorizados de los servicios de telefonía, en cualquiera de sus modalidades, de los abusos del procedimiento de **contacto, publicidad, oferta, venta y regalo de bienes o servicios no solicitados**.

Ley 26.951 – Registro Nacional “NO LLAME”

EFECTOS

Quienes publiciten, oferten, vendan o regalen bienes o servicios utilizando como medio de contacto los servicios de telefonía en cualquiera de sus modalidades **son considerados usuarios y/o responsables** de archivos, registros y bancos de datos de acuerdo a lo dispuesto en la ley 25.326 (Protección de datos personales).

Ley 26.951 – Registro Nacional “NO LLAME”

Servicios de telefonía

Telefonía básica, telefonía móvil, servicios de radiocomunicaciones móvil celular, de comunicaciones móviles y de voz IP, así como cualquier otro tipo de servicio similar que la tecnología permita brindar en el futuro.

Inscripción – Gratuidad

Inscripción en el Registro Nacional “No llame”.

Trámite hecho por el titular y es gratuito.

Ley 26.951 – Registro Nacional “NO LLAME”

Excepciones

a) Las campañas de bien público.

b) Llamadas de emergencia para garantizar la salud y seguridad de la población.

c) Las campañas electorales

d) Las de quienes tienen una relación contractual.

e) Las de quienes se hayan permitido e inscripto.

Autoridad de Aplicación

Agencia de acceso a la Información Pública (AAIP).

NORMATIVA

- Leyes
- Decretos
- Resoluciones
  - Casos particulares
  - Casos Generales
- Disposiciones
  - Por año
  - Por tema
- Criterios interpretativos
  - Dictámenes
  - Notas e informes
- Normativa y jurisprudencia internacional
  - Corpus luris
  - Estandares de protección de datos para países iberoamericanos
- Anteproyecto de nueva Ley de Protección de Datos Personales

Regulación General de Protección de Información (GDPR)

- Nueva ley de seguridad de información de la UE.
- Entró en vigencia el 25 de MAYO de 2018 en la UE.
- Dá a las personas más control sobre sus datos personales y obliga a las empresas a asegurarse de que la forma en que recopilan, procesan y almacenan información es **SEGURA**.
- Idea central: “PRIVACIDAD POR DEFECTO”.

Regulación General de Protección de Información (GDPR)

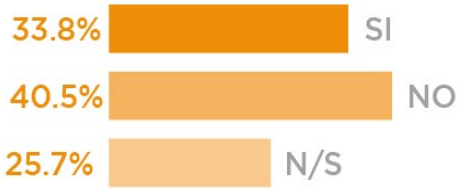
AFECTADOS

Organizaciones que retengan o usen información de personas pertenecientes a la Unión Europea, independientemente en dónde estén ubicadas.

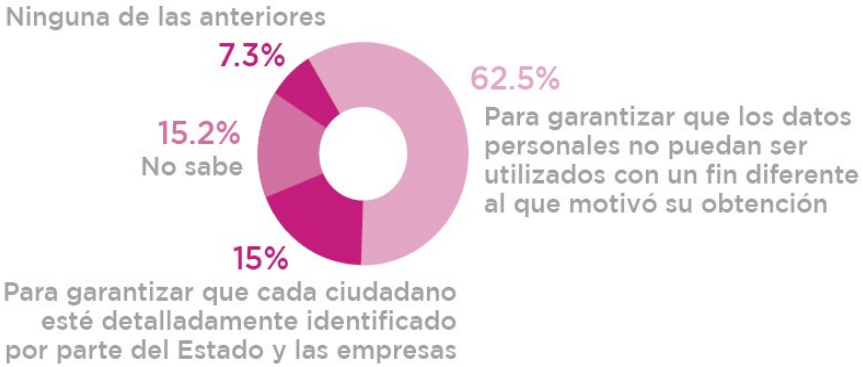
Encuesta **DATOS** | Junio 2019

Total país | 4400 casos | Población mayor de 16 años

1 ¿Conoce el derecho de protección de los datos personales?

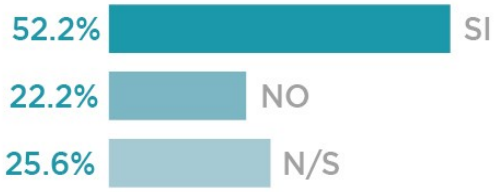


2 ¿Para qué sirve el derecho de protección de los datos personales?



3 ¿Qué tan importante es el derecho de protección de los datos personales?

4 ¿Conoce el sitio web de la Agencia y cómo realizar denuncias?



Preguntas