TRATAMIENTO DE DATOS PERSONALES Y SENSIBLES PARA ORGANIZACIONES

GUÍA PRÁCTICA

</datagéner*

La presente guía tiene como objetivo compartir recomendaciones, lineamientos y buenas prácticas para la gestión y tratamiento de datos personales y sensibles por parte de organizaciones.

Equipo

Coordinación General
Mailén García

Redacción de contenidos
Facundo Benítez Piloni

Año: octubre 2025

DataGénero. Observatorio de datos con perspectiva de Género
datagenero.org | info@datagenero.org

CONTENIDOS

1. DATOS PERSONALES Y SENSIBLES

1.1 ¿Qué son los datos personales?

Cuando hablamos de datos personales nos referimos a la información que permite identificar a una persona, directa o indirectamente, por uno o varios elementos característicos de su identidad física, fisiológica, genética, biométrica, psíquica, económica, cultural, social o de cualquier otro tipo.
Datos como la dirección, datos de contacto, profesión, número de documento, fecha de nacimiento, el peso y altura de una persona, su salario, la huella dactilar y el IP de conexión son ejemplos de datos personales.

1.2 ¿Qué son los datos sensibles?

En determinadas situaciones, gestionar, administrar y relevar cierta información muy personal o de la esfera privada de las personas puede ser muy peligroso y conllevar varios riesgos. Si se conocen esos datos de una persona, se podrían usar para perjudicarla, afectar su intimidad, hacerle daño, discriminar o ponerla en desventaja. Por esto, se los considera como datos sensibles.
Los datos sensibles son aquellos permiten conocer aspectos de las personas como:

- su origen étnico;
- las creencias o convicciones religiosas, filosóficas y morales;
- su afiliación sindical u opiniones políticas;
- los datos relativos a la salud, discapacidad,
- los datos vinculados a la preferencia u orientación sexual, y
- sus datos genéticos o biométricos, entre otros.

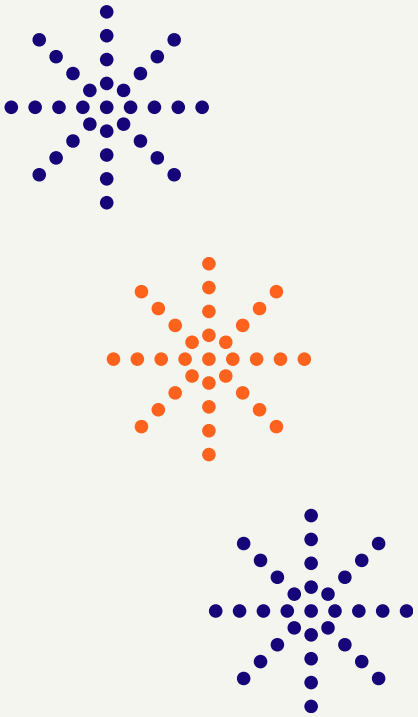
En Argentina, la Ley 25.326 regula la protección de datos personales. En su artículo 2 define a los datos personales como:

"Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables"

Por su parte, los datos sensibles son definidos como aquellos datos personales

"...que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual".

Los datos sensibles constituyen una categoría especial de datos personales que, si se divulgan o se utilizan de forma indebida, pueden poner en riesgo la **dignidad**, la **seguridad** o los **derechos** de una persona.
Mientras todos los datos personales deben ser protegidos, los datos sensibles requieren **mayores medidas de seguridad, precaución y protección**, debido a los posibles impactos negativos en caso de pérdida, filtración o mal uso.
Los datos personales **son importantes ya que identifican de manera única e irrepetible a las personas y forman parte de su identidad.**



2. EL MARCO NORMATIVO DE LA PROTECCIÓN DE DATOS PERSONALES

La protección de los datos personales es un derecho humano. En Argentina, existe un marco normativo específico que garantizan este derecho y regulan la protección y tratamiento de datos personales.

- El artículo 43 de la Constitución Nacional establece el derecho a conocer los datos propios que se guardan en registros públicos o privados. Si tienen alguna información falsa o discriminatoria, podemos exigir la supresión, rectificación, confidencialidad o actualización de esos datos.

- La Ley N° 25.326 de Protección de los Datos Personales fue sancionada en el año 2000 y tiene como objetivo garantizar el derecho al honor, la intimidad y privacidad de las personas. Reconoce los derechos de información, acceso, rectificación y

- El Código Civil y Comercial, Ley No 26.994, contiene un capítulo dedicado a los derechos personalísimos o “derechos fundamentales” y sus artículos 52, 53 y 55 reconocen los derechos a la intimidad, la integridad, la imagen, la dignidad y la identidad de las personas.

3. TRATAMIENTO DE DATOS PERSONALES

En nuestro día a día como organizaciones, solemos trabajar con muchos datos personales y sensibles de personas para diferentes fines. En esta sección, aprenderemos los principales elementos sobre cómo manejar y tratar estos tipos de datos como organizaciones.

3.1 ¿Qué significa el tratamiento?

El tratamiento de datos personales se refiere a todas aquellas **acciones, tanto electrónicas o basadas en papel**, que se pueden hacer con los datos personales como:

- recolectar,
- conservar y almacenar,
- ordenar, analizar, relacionar, categorizar, procesar
- corregir, modificar, evaluar, destruir difundir o entregar a terceros.

En general, estos datos se encuentran almacenados en **archivos, registros, bases o banco de datos**. Indistintamente de sus características particulares, designan al conjunto organizado de datos que son objeto de tratamiento o procesamiento de datos.

3.2 ¿Quiénes participan en este tratamiento?

El tratamiento de los datos en general lo hace un responsable de la base de datos o del tratamiento. Esta figura se define como aquella **persona física o jurídica, pública o privada, propietaria de la base de datos** o que decida sobre la finalidad, contenido y uso del tratamiento.
Por su parte, se conoce como titular de datos personales a las personas físicas cuyos datos sean objeto de un tratamiento incluido dentro del ámbito de acción de la ley.

4. PRINCIPIOS DEL TRATAMIENTO

Ahora, recorremos algunos principios y elementos claves del tratamiento de datos personales.

4.1 Finalidad

En el tratamiento de los datos personales, el principio de finalidad tienen un rol central. Este principio establece que los datos personales sólo pueden ser tratados para fines específicos y legítimos, previamente informados al titular.
En otras palabras, los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación con el ámbito y finalidad para los que se hubieren obtenido.
Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.
Todo tratamiento de datos personales debe ser acorde a la finalidad y limitarse a los que sean necesarios para la que se los solicitó.

4.2 Licitud

Todo tratamiento de datos debe tener una base legal. Este principio establece que la recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contrata a las disposiciones legales.

En otras palabras, el tratamiento de datos personales debe ser lícito y respetar todos los principios que establece la ley y las reglamentaciones vigentes.

4.3 Minimización

El principio de minimización establece que solo se deben recopilar y procesar los datos personales que sean estrictamente necesarios para cumplir con un **propósito específico y legítimo**.
Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

4.4 Principio de seguridad y confidencialidad

Reconoce que responsable o usuario de la base de datos debe adoptar las medidas que resultaren 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, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

4.5 Consentimiento informado

El tratamiento de datos personales requiere el consentimiento libre, expreso e informado del titular de los datos. El consentimiento para el tratamiento de datos personales es la expresión del deseo o voluntad explícita del titular de los datos para autorizar el uso de los datos para un fin específico. Esa finalidad puede ser variada: por ejemplo, acceder a un servicio, postular a una beca, entre otros.

El consentimiento debe ser:

- Libre: sin ningún tipo de presión
- Expreso: solo para la finalidad que se informa previamente.
- Informado: se debe explicar, en lenguaje claro y accesible, para qué necesitan los datos y quienes tendrán acceso a ellos.

5. EJEMPLOS PRÁCTICOS

En este bloque, exploraremos diferentes situaciones o escenarios prácticos del día a día vinculados al tratamiento de datos personales y sensibles.

Caso 1: Registro en talleres comunitarios

Una organización desarrolla talleres de inserción laboral para mujeres en situación de vulnerabilidad. Para inscribirse, se pide llenar un formulario Google con nombre completo, teléfono, dirección, nivel educativo, cantidad de hijos y estado civil.

Errores comunes

- Solicitar más datos de los necesarios (por ejemplo, cantidad de hijos, estado civil situación familiar), cuando solo se necesita nombre y teléfono de contacto para poder acercar la propuesta formativa. Este punto es un caso de incumplimiento del principio de **minimización**.
- No se explica para qué se usarán los datos ni cuánto tiempo se conservarán, lo que incumple **finalidad** y **consentimiento**.

Buenas prácticas

- Recoger solo lo esencial (nombre y teléfono).
- Explicar por escrito en el formulario para qué se usa la información (por ejemplo, organizar el taller y mantener comunicación).
- Definir un plazo de conservación (ej. destruir formularios a los 6 meses de finalizado el taller).

Caso 2: Comunicación por WhatsApp con personas beneficiarias

Para agilizar la comunicación, la organización tiene un grupo de WhatsApp con mujeres de la comunidad para avisos sobre actividades culturales. En el grupo, hay beneficiarias de diversas actividades culturales. En la organización de cada evento, se publican listas con nombres, documentos y teléfonos de todas las participantes en el grupo.

Errores comunes

- Exposición de números personales a todo el grupo sin consentimiento, lo que afecta confidencialidad.
- Uso de datos de contacto para fines distintos (ej. otras participantes podrían contactar de manera indebida).
- Falta de matriz de accesos para saber quien puede acceder y quienes no a una base de personas inscriptas.

Buenas prácticas

- Crear listas de difusión en vez de grupos (así las participantes no ven los números de las demás).
- Informar al inicio que se usará WhatsApp solo para avisos relacionados con las actividades.
- Pedir consentimiento claro para agregar a alguien al grupo o lista.

Caso 3: Testimonios en campañas de sensibilización

Una organización publica en redes sociales historias de mujeres víctimas de violencia de género que participan en sus programas, incluyendo nombres y fotos, sin pedir autorización explícita.

Riesgos y errores comunes

- Difusión pública de datos personales y sensibles sin consentimiento ni licitud.
- Riesgo de revictimización o estigmatización, incumplimiento del principio de seguridad y licitud.
- Uso de la información para un fin distinto al original: falla a la finalidad.

Buenas prácticas

- Pedir consentimiento informado y por escrito antes de usar fotos, videos, nombres o testimonios de personas.
- Anonimizar (por ejemplo, cambiar nombre, cambiar voz, no mostrar rostro).
- Explicar claramente dónde se publicará la información (redes sociales, boletines, informes a donantes).
- Solicitar consentimiento escrito, específico para uso en redes o informes.

Caso 4: Bases de datos de beneficiarias para informes

Una organización que se dedica a generar talleres y espacios de reinserción laboral para mujeres y diversidades que fueron privadas de la libertad se postula a un fondo de una Fundación de una importante empresa para recibir fondos y equipamiento para emprendimientos textiles. La organización lleva un Excel con datos de beneficiarias (nombres, teléfonos, direcciones, situación socioeconómica) y lo comparte por correo electrónico completo a la fundación financiadora ya que le solicita datos estadísticos para su rendición de cuentas.

Riesgos y errores comunes

- Compartir información a nivel nominal y con datos personales y sensibles de personas de forma innecesaria con terceros: vulnera la minimización.
- Ausencia de medidas técnicas y de seguridad (envío de archivo sin protección como cifrados o contraseña): falla al principio de seguridad.
- Falta de transparencia con las beneficiarias sobre con quién se comparten sus datos: vulnera consentimiento y finalidad.
- Falta de matriz de accesos para saber quien puede acceder y quienes no a una base de personas inscriptas.

Buenas prácticas

- Compartir solo datos estadísticos o agregados (ej. número de participantes, rangos de edad, sin nombres ni contactos).
- Anonimizar, aplicando un identificador (ID) ficticio.
- Si es necesario compartir datos identificables, proteger el archivo con contraseña y limitar los accesos.
- Informar a las participantes de manera clara que ciertos datos podrían ser utilizados en informes, y con qué nivel de anonimización.

Caso 5 - Base de datos de niñas, niños y adolescentes accesible para toda la organización

Una organización se dedica al acompañamiento e inclusión educativa para niños, niñas y adolescentes en situación de extrema vulnerabilidad. Para el seguimiento, lleva una hoja de cálculo en Google Drive ya que todas las personas que trabajan tienen Gmail, están familiarizadas con el entorno y es muy útil para llevar el monitoreo de cada niño, niña o adolescente.

En los datos tienen información nominal como nombre completo, edad, escuela, domicilio, teléfono de la madre/padre/tutor, notas de salud (alergias) y observaciones sobre conducta. El enlace está “público con acceso” dentro del equipo y circula por WhatsApp interno; cualquier persona de la organización puede verlo y descargarlo.

Riesgos y errores comunes

- Acceso indiscriminado (“quien tenga el link entra”): vulnera confidencialidad y seguridad.
- Datos excesivos (domicilio y notas de salud para organizar tareas escolares): falla a la minimización.
- Finalidad difusa (la hoja se usa luego para enviar campañas o becas no informadas): incumple finalidad y licitud.
- Sin consentimiento del adulto responsable y del NNA cuando corresponde: afecta licitud/consentimiento.
- Copias locales en notebooks personales sin protección: riesgo de fuga (seguridad).

Buenas prácticas

- Acceso por “necesidad de saber”: limitar la hoja a quienes realmente la usan (docentes/tutores designados). Configurar permisos individuales y desactivar descarga/imprimir si la plataforma lo permite.
- Protección de rangos: separar columnas sensibles (salud/contactos) en una pestaña con permisos más restringidos. Esto se vincula a la clasificación de datos.
- Minimizar: pedir solo lo imprescindible para la actividad (ej. nombre y teléfono de contacto; evitar domicilio si no es necesario).
- Pseudonimizar: usar un ID interno y guardar la “llave” (ID↔identidad) en un archivo aparte, con acceso más limitado.
- Consentimiento informado del tutor (y del NNA según edad): desarrollar un breve formulario que explique finalidad, tiempo de conservación, quién accede y cómo revocar.
- Medidas de seguridad básicas: aplicar métodos de doble factor de autenticación, en cuentas, bloqueo de pantalla, almacenamiento cifrado en dispositivos.
- Retención: definir un plazo de borrado (ej. fin del ciclo lectivo + X meses).
- Registro de accesos y responsable: nombrar a una persona referente que revise permisos cada trimestre.

***No se necesitan grandes inversiones tecnológicas para cumplir con la protección de datos**. Muchas buenas prácticas son organizativas: pedir solo la información estrictamente necesaria, usar consentimientos claros, restringir accesos, anonimizar datos cuando sea posible y comunicar con transparencia a las personas para qué se usarán sus datos. Esto protege a la organización frente a riesgos legales y, sobre todo, fortalece la confianza de las comunidades y mujeres con las que trabaja.*

6. EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS (EIPD)

Una Evaluación de Impacto en la Protección de Datos (EIPD) 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**.

Esta evaluación resulta desde tiempo una buena práctica reconocida por normas y estándares internacionales 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. Para que este proceso resulte exitoso, es necesario involucrar a las personas que integran la organización, a consultores expertos e incluso a los sectores o grupos de titulares de datos que posiblemente puedan ser afectados.

Dado que muchas organizaciones trabajan y hacen tratamiento de datos personales de una alta sensibilidad y/o de personas en situación de espacial vulnerabilidad, la evaluación del impacto en la protección de datos se vuelve una práctica recomendada.

5.1 ¿Cómo hacer una evaluación?

El proceso de elaboración de la EIPD presupone distintas fases:

- ***Fase 1 - Determinación de participantes y documentación de los procesos de elaboración***

Esta fase se busca determinar los participantes de la evaluación y definir los procesos para la documentación de la EIPD.

- ***Fase 2 - Análisis del marco normativo aplicable***

Busca analizar la normativa aplicable al tratamiento realizado para comprender su aplicación a las distintas etapas de dicho tratamiento.

- ***Fase 3 - Análisis preeliminar***

Esta fase se enfoca en realizar un análisis previo de varios factores que inciden en la necesidad de efectuar posteriormente una EIPD. Algunos de los factores se relacionan con el tratamiento de datos personales a gran

escala, la sensibilidad de los datos tratados, los titulares de datos en situación de espacial vulnerabilidad, uso de datos con el fin de elaborar perfiles, retención prolongada de los datos y mecanismo de almacenamiento, entre otros factores.

- ***Fase 4 - Contexto de tratamiento***

Se enfoca en analizar todas las instancias de tratamiento que se va a realizar desde la perspectiva de la protección de datos personales en todo el ciclo de vida de los datos.

1. Recolección: refiere a toda actividad de captura de datos de persona determinada o determinable para destinar a actividades de tratamiento. En lo que se refiere a la captura de datos, debemos:

  - determinar los tipos de datos recolectados con relación a la finalidad prevista
  - considerar la información provista a los titulares de los datos previo a su recolección
  - detallar las fuentes de datos obtenidos
  - especificar los mecanismos y personas involucradas en la recolección

2. Categorización: implica toda actividad de clasificación de la información, incorporándola en distintas categorías definidas.

También, refiere a la determinación de los potenciales vínculos o conexiones de los datos capturados con otros datos a efectos de tener asociaciones o inferencias al “cruzar” los datos.

3. Tratamiento: implica todo tipo de gestión sobre los datos, incluyendo su procesamiento, almacenamiento y aplicación.

4. Comunicación o cesión: refiere a toda revelación o envío de datos personales a personas distintas de titular.

5. Eliminación: el hecho de que se conserve la información no significa que ésta deba permanecer en poder del responsable o encargado de forma indefinida. Salvo excepciones, una vez cumplida la finalidad para la que se obtuvo la información, corresponde proceder a su supresión.

A continuación, proporcionamos algunas preguntas disparadoras para cada fase o etapa del ciclo de vida de los datos en relación especial a la gestión de datos personales y sensibles:

Recolección	• ¿Estoy recolectando estrictamente los datos que necesito en función de mi finalidad? • ¿Existen finalidades conexas y compatibles que requieran de otro tipo de datos? • ¿Estoy ofreciendo opciones al titular de datos para comunicar un tipo de datos personales y no otros? • ¿Se informó debidamente a los titulares de los alcances de la información que se recolectará? • ¿La información es clara y completa? ¿Obtengo la información directamente de los titulares? ¿Mis fuentes son fuentes públicas de acceso irrestricto? • ¿Por qué medios se realiza la recolección de datos? ¿Se realiza por algún mecanismo automatizado? • ¿Qué empleados de la organización o eventual personal tercerizado están involucrados en el proceso de recolección?
Categoriza-ción	• ¿Cuáles son los tipos o categorías de datos que estoy tratando? • ¿Estoy tratando datos sensibles o datos relativos a antecedentes penales o contravencionales? • ¿Poseo sistemas, programas o aplicaciones que relacionan múltiples datos en mi poder? • ¿La categorización de los datos es manual o procede por mecanismos automáticos? • ¿Quiénes intervienen en la categorización o tienen acceso a los datos ya categorizados?
Tratamiento	• ¿Implemento distintas medidas de seguridad para las diferentes categorías de datos? ¿El almacenamiento lo realizo en servidores locales o en la nube? ¿Almaceno varias copias de la información y, en ese caso, las tengo identificadas a efectos de correcciones y supresiones? • ¿Puse en práctica algún sistema de contraseñas o una política de acceso a la información de los miembros de mi organización? • ¿Cuento con un mecanismo sencillo y estudiado para habilitar el acceso a su información en caso de solicitudes de los titulares de los datos? • ¿Realizo operaciones de disociación de los datos? • ¿Quiénes intervienen en las operaciones de tratamiento? • ¿Cuál es la finalidad del tratamiento de datos previsto en el proyecto o en la actividad de la organización? • ¿Establezco vínculos entre los datos que cuento para obtener información adicional? • ¿Esa información generada también se vincula a los fines de mi organización? • ¿Cómo almaceno la información resultante?
Comunicación o cesión	• ¿Se realizan cesiones o transferencias internacionales? • ¿Existe una clara delimitación de las obligaciones de una y otra parte del contrato? • ¿Se define la finalidad para la cual se entregan los datos? • ¿Se han determinado los tipos de datos que se enviarán a efectos de no remitir más que los necesarios para cumplir con el contrato?
Eliminación	• ¿Cuáles son los motivos para mantener la información almacenada una vez agotada la finalidad del tratamiento? • ¿Existe alguna norma que me habilite a conservar esa infor mación? • En caso de que no corresponda la eliminación, ¿implementé procedimientos para bloquear o disociar los datos? • ¿Qué mecanismos debo emplear para eliminar la información? • ¿Contabilicé las copias y respaldos de seguridad que puedan existir para asegurar la eliminación completa?

- ***Fase 5 - Gestión de riesgos***

Esta fase se propone realizar un análisis de riesgo en cada una de las etapas del contexto de tratamiento definidas en la etapa anterior, para una adecuada gestión de dichos riesgos.
La gestión de riesgos es el proceso mediante el cual se identifica, analiza y valora la probabilidad e impacto de las ocurrencias de amenazas que, mediante la explotación de alguna vulnerabilidad, puedan materializar un riesgo para los derechos de las personas. El objetivo es establecer cuáles son las hipótesis de riesgo para, luego, en una etapa posterior, definir el plan de tratamiento necesario para minimizar aquellos riesgos que no se consideren aceptables.

- ***Fase 6 - Plan de tratamiento de riesgos***

El objetivo es realizar un adecuado plan de tratamiento de los riesgos determinados en la etapa anterior .En esta etapa, la organización debe planificar las acciones que llevará a cabo para mitigar o eliminar los riesgos que fueron identificados previamente.

Cuando una organización está evaluando soluciones, debe considerar, en qué medida el impacto en los derechos de las personas es proporcional a los fines del proyecto y cómo podría alcanzar los mismos objetivos a través de medios menos riesgosos para los derechos de las personas.

Hay muchas y muy diversas medidas que las organizaciones pueden tomar para reducir riesgos identificados en la EIPD.

- No recolectar o almacenar algún tipo de dato personal.
- No recolectar o almacenar datos sensibles.
- Monitorear o limitar la toma de decisiones automatizada cuando esta se funde en el tratamiento de datos personales.
- Otorgar al titular de datos la posibilidad de gestionar preferencias en la entrega de su información, permitiéndole entregar categorías de datos de manera discriminada.
- Implementar períodos razonables de conservación de los datos y mecanismos seguros para la destrucción de información.
- Implementar medidas adecuadas de seguridad de la información.
- Capacitar al personal en materia de protección de datos y concientizarlo respecto de los riesgos involucrados en las operaciones de tratamiento.
- Contratar un delegado de protección de datos que le dé seguimiento al proyecto o actividad bajo análisis.
- Establecer pactos de confidencialidad con el personal que desalienten la difusión no autorizada de información.
- Implementar técnicas de disociación de datos cuando sea posible.
- Producir códigos de procedimiento que enseñen cómo compartir información dentro de la organización.
- Diseñar sistemas que permitan el fácil acceso a la información por

parte de los titulares de datos, así como plataformas que hagan más sencillo atender y contestar a los requerimientos de rectificación y supresión.

- Establecer una política de privacidad que informe exhaustivamente a los titulares de datos cómo se utilizará su información y a quién deben y pueden contactar en caso de algún reclamo.

7. MATERIAL Y BIBLIOGRAFÍA CONSULTADA

- Ley 25.326 - Protección de Datos Personales. República Argentina. Enlace.
- Guía de Evaluación de Impacto en la Protección de Datos - Agencia de Acceso a la Información Pública. Enlace.