



Diplomado en Transparencia, Privacidad: Alcances y Límites del Estado

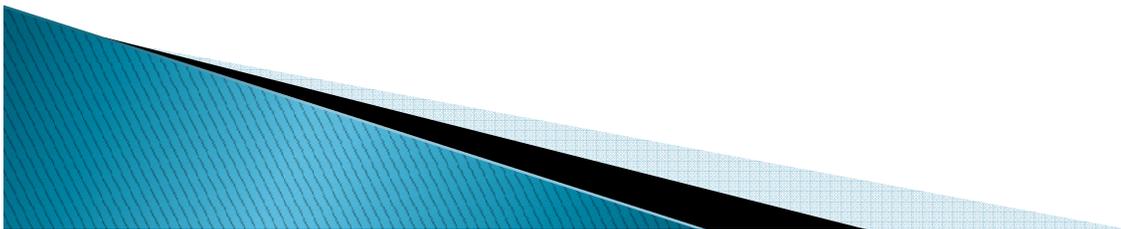
# Módulo 4

## Instrumentación de Procedimientos Entes Públicos

Guadalajara, Jalisco 21 de Octubre de 2011

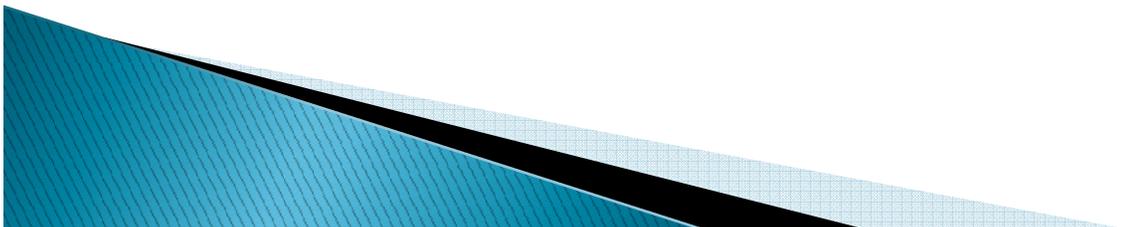
Lic. Alvaro Ruvalcaba Ascencio  
Secretario Ejecutivo

**¿Qué son los datos personales?**



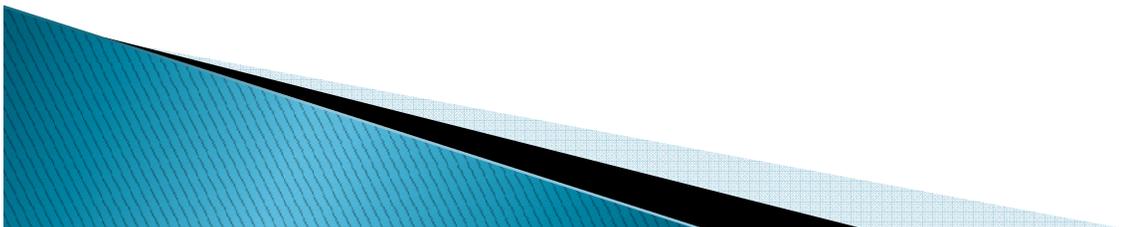
Los datos personales se refieren a toda aquella información relativa al individuo que lo identifica o lo hace identificable. Entre otras cosas, le dan identidad, lo describen, precisan su origen, edad, lugar de residencia, trayectoria académica, laboral o profesional.

Además de ello, los datos personales también describen aspectos más sensibles o delicados sobre tal individuo, como es el caso de su forma de pensar, estado de salud, sus características físicas, ideología o vida sexual, entre otros.



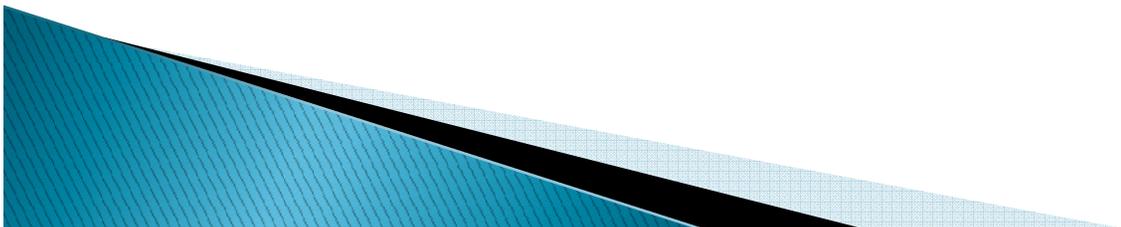
# Ejemplos de datos personales

- ▶ Origen Étnico o Racial
- ▶ Características Físicas, Morales o Emocionales
- ▶ Vida Afectiva y Familiar
- ▶ Domicilio
- ▶ Teléfono Particular
- ▶ Correo Electrónico Personal
- ▶ Patrimonio
- ▶ Ideología
- ▶ Creencias
- ▶ Convicciones Religiosas y Filosóficas
- ▶ Estado de Salud
- ▶ Preferencia Sexual
- ▶ Huella Digital
- ▶ ADN
- ▶ Número de Seguridad Social
- ▶ Opiniones Políticas

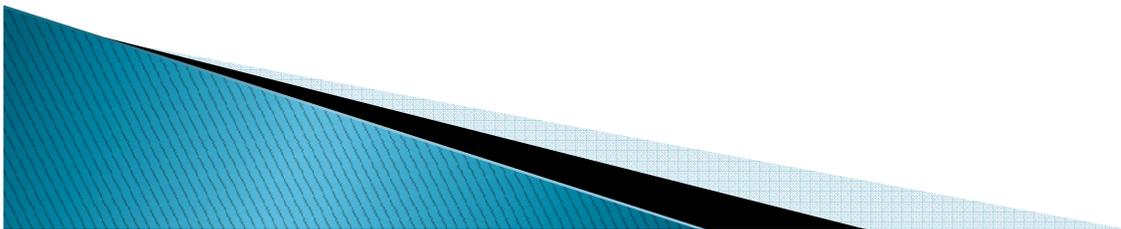


Los **DATOS PERSONALES** son intransferibles, indelegables e irrenunciables

**\* No se pueden vender, ni regalar, únicamente se pueden transmitir o ceder para que sean utilizados en la realización de algún trámite o servicio.**

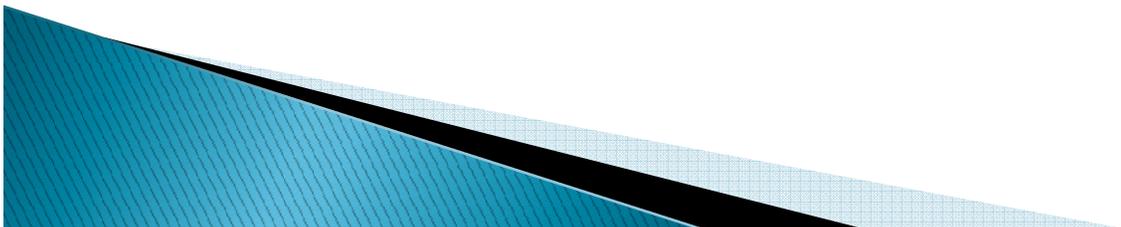


**¿Para que sirven los datos personales?**



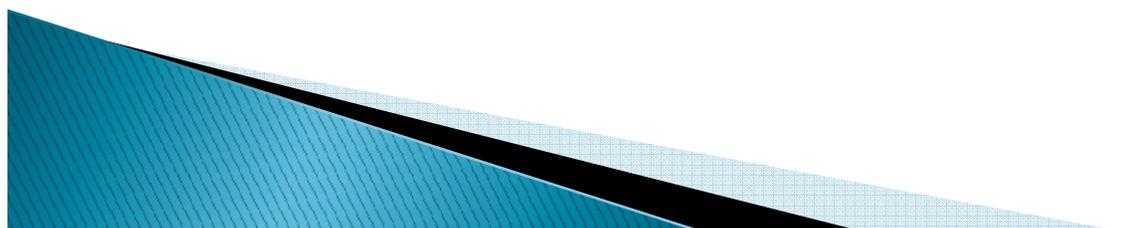
Los datos personales son necesarios para que un individuo pueda interactuar con otros o con una o más organizaciones sin que sea confundido con el resto de la colectividad y para que pueda cumplir con lo que disponen las leyes. Asimismo, hacen posible la oferta y obtención de bienes y servicios.

Sin embargo, el uso extensivo de las tecnologías de la información y las telecomunicaciones ha permitido que en muchas ocasiones, los datos personales sean tratados para fines distintos para los que originalmente fueron recabados, rebasando los límites de la esfera de privacidad de la persona, y lesionando en ocasiones otros derechos y libertades.

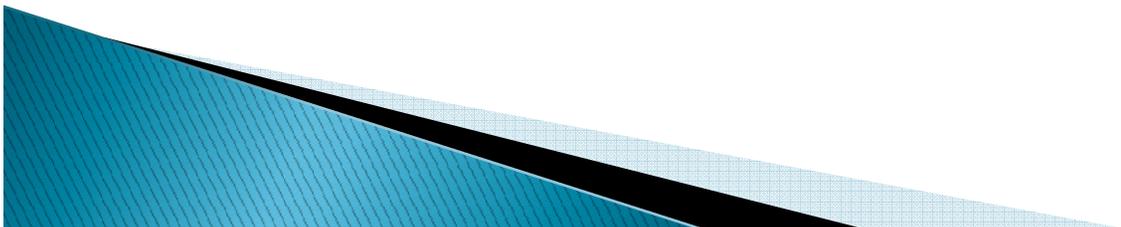


# Fundamento Legal

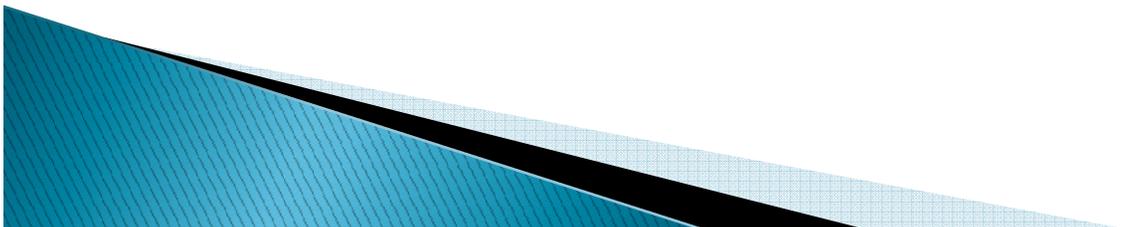
Ley	Artículos	Entrada en Vigor
Constitución Política de los Estados Unidos Mexicanos	<ul style="list-style-type: none"> <li>❑ Art. 6 fracción I y II</li> <li>❑ Art. 16 segundo párrafo</li> <li>❑ Art. 73 fracción XXIX-O</li> </ul>	<ul style="list-style-type: none"> <li>❑ 2007</li> <li>❑ 2008</li> <li>❑ 2008</li> </ul>
Constitución Política del Estado de Jalisco	❖ Art. 9 fracción V	❖ Ultima Reforma 2011
Ley de Transparencia e Información Pública de Jalisco	➤ Artículos 7 fracción II, 28 fracción I, 29, 30, 31, 32, 33, 34, 35.	➤ 2005
Ley Federal de Protección de Datos en Posesión de Particulares	Artículo 2 fracción V y VI	✓2010



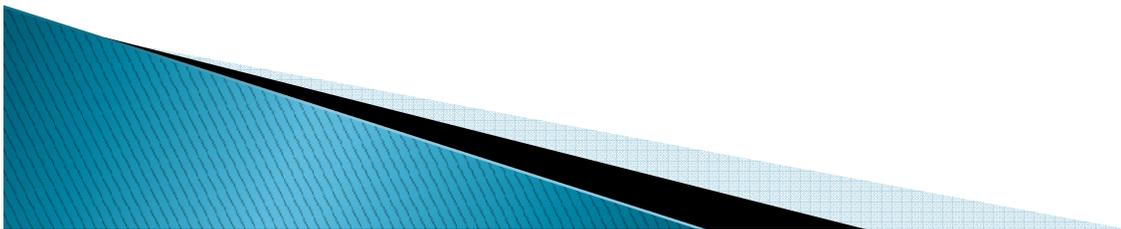
**¿ Por qué proteger los datos personales?**



A fin de equilibrar las fuerzas entre un individuo y aquellas organizaciones – públicas o privadas- que recaban o colectan datos sobre tal individuo, surge en Europa el concepto de la protección de datos personales. Un concepto similar surgió en América – el concepto de “privacidad” – aunque con alcances distintos.



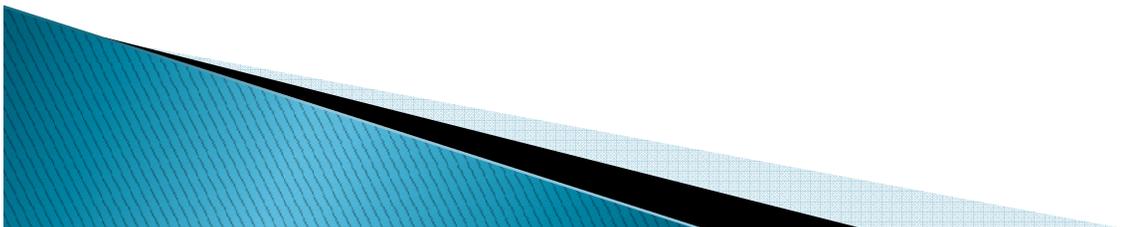
**¿Existe en México el derecho a la protección de datos personales?**



En México, desde el año 2000, se han promovido diversos proyectos legislativos en torno a la protección de datos personales en el Congreso de la Unión, sin que ninguno de ellos fructificara dada la ausencia de una disposición constitucional que les diera sustento. Si bien la reciente reforma constitucional en 2007 al artículo 6º establece en sus fracciones II y III que los datos personales y la información relativa a la vida privada será protegida, así como el derecho de acceder y corregir sus datos que obren en archivos públicos, el legislador quiso establecer límites al ejercicio del derecho de acceso a la información pública en los tres órdenes de gobierno (federal, estatal y municipal), pero no creó un derecho fundamental independiente.



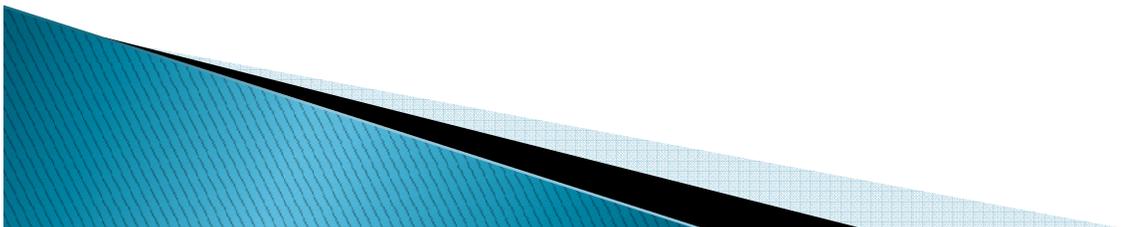
No es sino hasta la aprobación en 2008 de las reformas a los artículos 16 y 73 constitucionales que se introduce al más alto nivel de nuestra Constitución, el derecho de toda persona a la protección de su información. Lo anterior es relevante dado que los datos personales se encuentran en manos tanto de gobiernos como de particulares (empresas, organizaciones y profesionistas) y, porque con el uso indiscriminado de la tecnología, éstos pueden utilizarse para fines distintos de aquellos para los que fueron recabados, pudiendo causar afectaciones en las esferas de otros derechos de los titulares de dichos datos.



## ¿Qué logra la reforma al artículo 16?

El artículo 16 constitucional reconoce y da contenido al derecho a la protección de datos personales. En ese sentido, en la reforma se plasman los derechos con los que cuentan los titulares de los datos como lo son aquellos de acceso, rectificación, cancelación y oposición (denominados por su acrónimo como derechos ARCO).

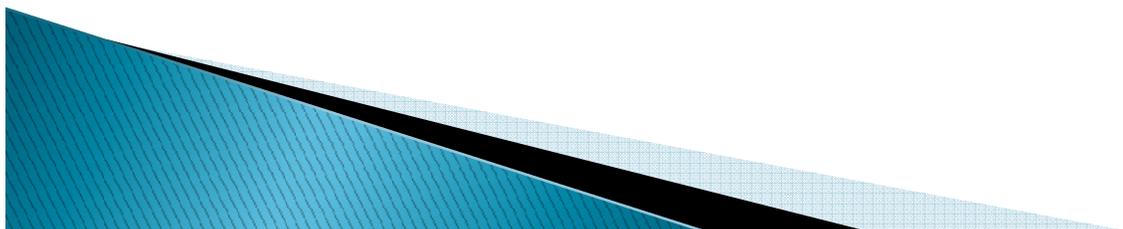
Por otra parte, se hace referencia a la existencia de principios a los que se debe sujetar todo tratamiento de datos personales, así como los supuestos en los que excepcionalmente dejarían de aplicarse dichos principios.



La reforma consistió en añadir un segundo párrafo que a la letra dice:

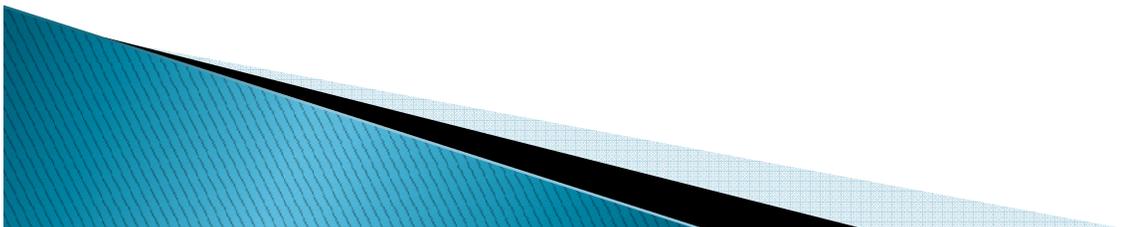
*“Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros”.*

El proyecto fue aprobado por el pleno del Senado en sesión del 4 de diciembre de 2008 y por el de la Cámara de Diputados el 11 de diciembre.



## ¿Qué aporta la reforma al artículo 73?

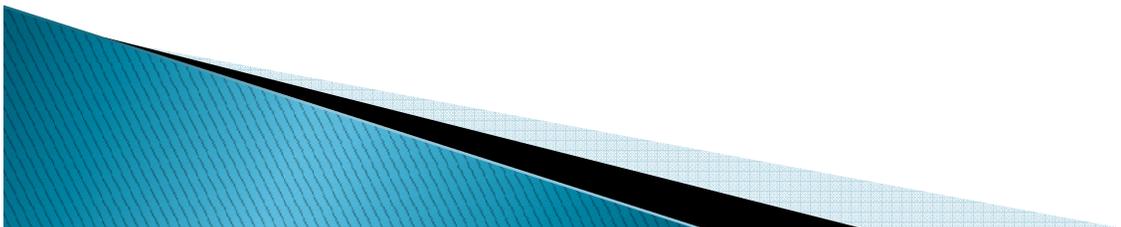
Por virtud de las leyes de transparencia y acceso a la información gubernamental, únicamente los sujetos obligados de las mismas en todo el país, están obligados a proteger la información personal que poseen en sus archivos. Sin embargo, dado que los particulares también tratan grandes cúmulos de información, resultaba indispensable dotar de facultades expresas al Congreso Federal para que regulara a escala nacional, la forma en que los particulares (bancos, hospitales, universidades, profesionistas, entre otros) pueden utilizar y transmitir la información relativa a las personas.



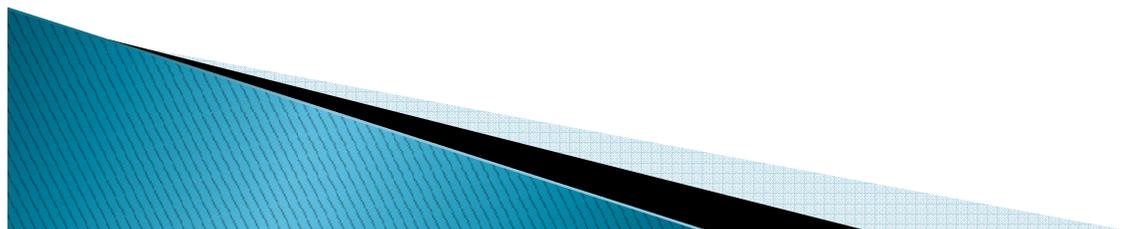
Por lo anterior, la reforma al artículo 73 consistió en añadir la fracción “O” que a la letra dice:

*“Artículo 73. El Congreso tiene facultad:*

*XXIX-O. Para legislar en materia de protección de datos personales en posesión de particulares”.*



# **Principios de Tratamiento Integración y Tutela de los Datos Personales en Posesión de Entes Públicos**



The diagram features two teal rounded rectangular boxes, one at the top containing the word 'Licitud' and one at the bottom containing 'Calidad'. A light blue circular arrow surrounds the boxes, pointing from 'Calidad' up to 'Licitud' on the left and from 'Licitud' down to 'Calidad' on the right, indicating a reciprocal relationship. In the bottom-left corner, there is a decorative graphic consisting of a blue textured triangle pointing right, a black triangle pointing left, and a light blue dotted triangle pointing right.

Licitud

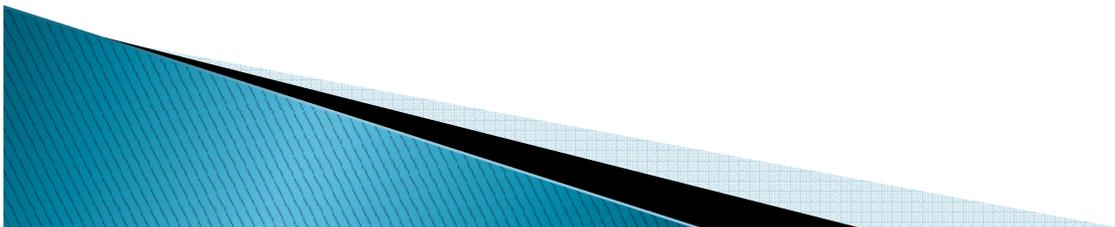
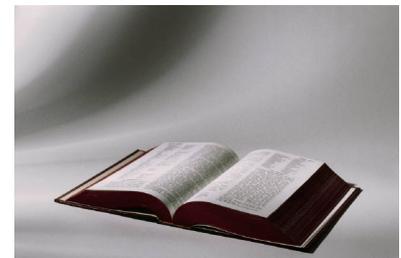
Calidad

# Licitud

Los datos se deben recabar a través de los medios legales y ser tratados exclusivamente para la finalidad que fueron obtenidos.

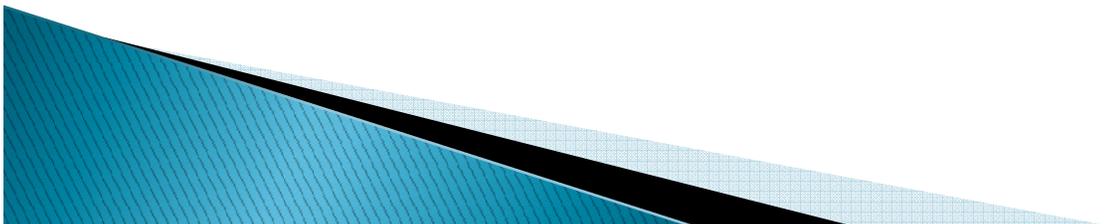
Hacer del conocimiento al titular lo siguiente:

- a) Responsable.
- b) Los fines.
- c) El fundamento.
- d) Las personas que pueden acceder a los datos.
- e) Los datos serán protegidos en términos de la ley y los lineamientos.
- f) La posibilidad del titular al acceso y rectificación de los datos personales.

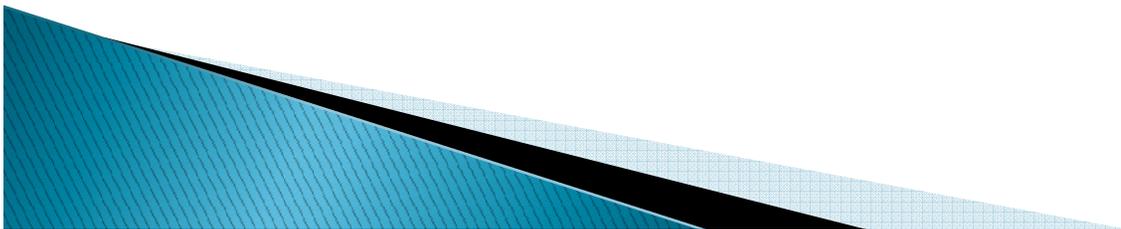


# Calidad

- El tratamiento de los datos personales debe ser: exacto, adecuado, pertinente y no excesivo.
- Almacenarse de forma que sean identificables y permitan el ejercicio de los derechos de acceso y corrección de los mismos.
- Los datos recabados para un fin particular, agotado éste serán devueltos a su titular levantando constancia.

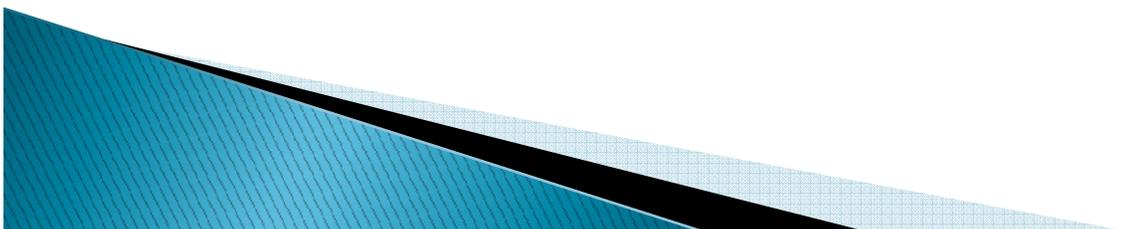


# Obligaciones de los entes Públicos o Sujetos Obligados

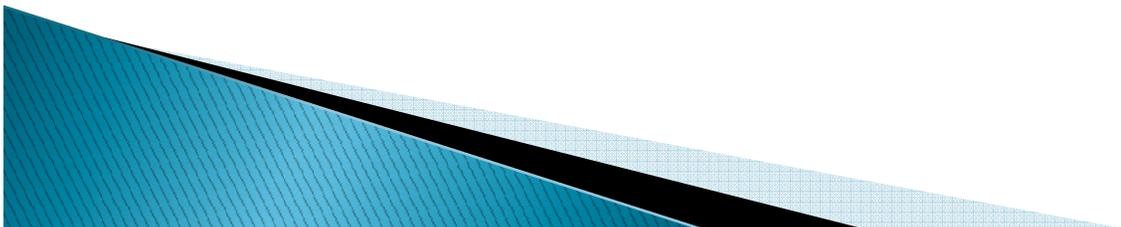


Es obligación de los sujetos obligados el informar a los titulares, que existe un Sistema de Datos Personales donde se almacenará su información, en que serán utilizados los datos solicitados, en caso de que sea necesario transmitirlos a quien serán transmitidos, si es opcional u obligatorio el solicitarle datos personales, y a la vez de su derecho de Acceso, Rectificación, Cancelación y Oposición de sus datos personales ( derechos ARCO).

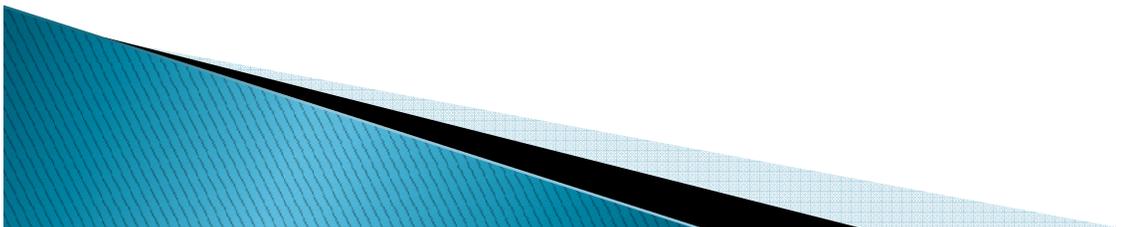
Así como también de la posibilidad de que sus datos personales sean difundidos y que para ello se requerirá invariablemente de su autorización precisa.



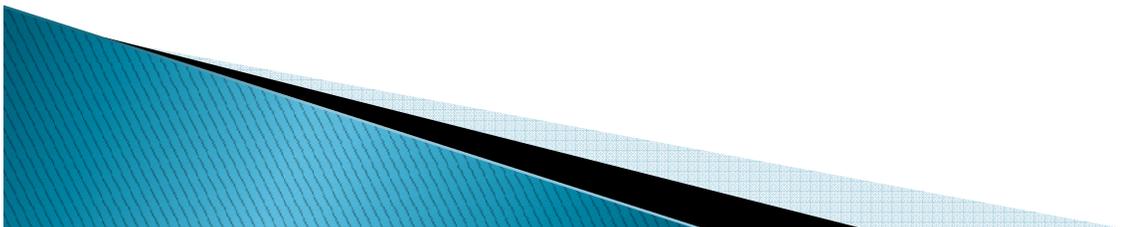
# Derechos que establece la Ley de Transparencia e Información Pública del Estado de Jalisco



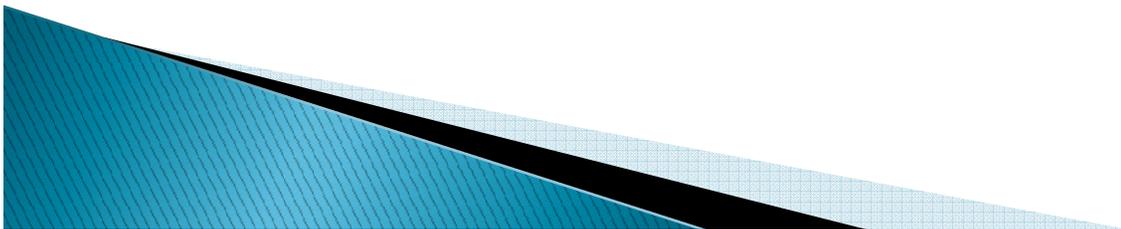
La Ley de Transparencia e Información Pública del Estado de Jalisco, establece cuatro derechos para garantizar la protección de los datos personales, del mismo modo establece que solamente será el particular el que decida sobre el uso y destino de los mismos.



- Derecho a saber si se está procesando información que le concierne.
- Derecho a conseguir una comunicación inteligible de esa información sin demoras.
- Derecho a obtener la rectificaciones o supresiones que correspondan cuando la posesión de información confidencial sea ilícita injustificada o inexacta.
- Derecho a conocer los destinatarios cuando esta información sea transmitida.

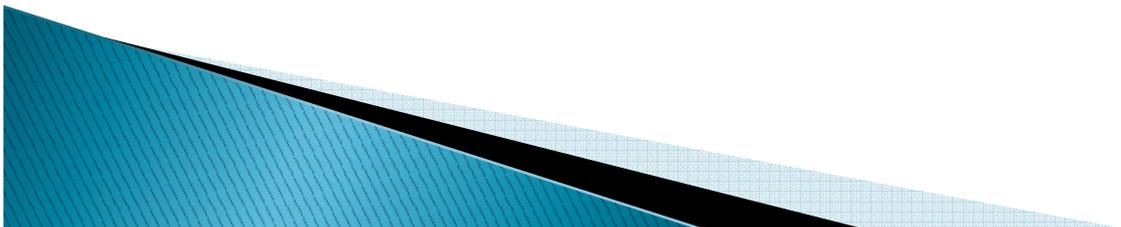


# Medidas de Seguridad



**Seguridad:** las medidas administrativas, físicas y técnicas que sirven para asegurar la protección de la información confidencial.

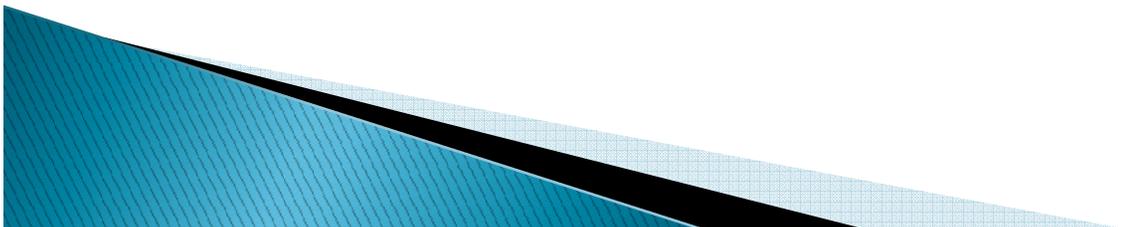
**Protección:** todo acto encaminado garantizar la no revelación de la información confidencial.



## •Medidas de seguridad:

- Dar a conocer los lineamientos y la normatividad al personal.
- Asignar un espacio físico seguro y adecuado para la operación de los sistemas de información confidencial.
- Llevar a cabo verificaciones periódicas de la aplicación de la medidas de seguridad.
- Controlar el acceso a las áreas donde se encuentra la información.

La información relativa a datos personales podrá ser proporcionada si se lleva acabo el procedimiento de **disociación**.



# Documento de Seguridad

- Expedido por el comité de clasificación.
- Contendrá las medidas de seguridad aplicables a los datos

personales, deberá ser actualizado periódicamente

1. Nombre, cargo y adscripción de los responsables.
2. Estructura y descripción de los sistemas.
3. Tipo de información confidencial.
4. Funciones y obligaciones del personal.
5. Medidas y criterios de seguridad como:
  - a) Procedimientos para operar los sistemas de datos personales.
  - b) Creación de copias y respaldo de los datos.
  - c) Notificación, gestión y respuesta ante los incidentes.
  - d) Registro de cambios en las medidas de seguridad.

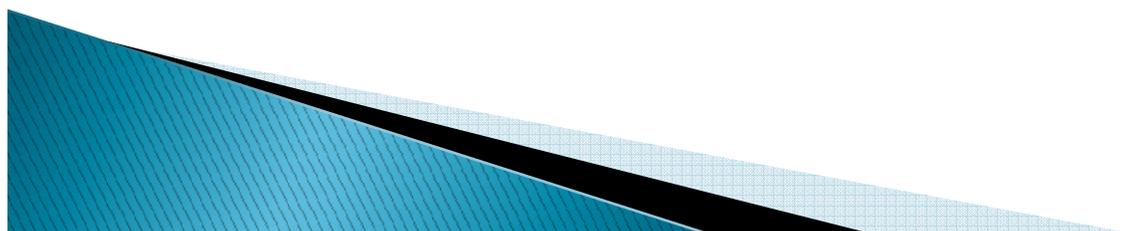


## Obligaciones del Comité

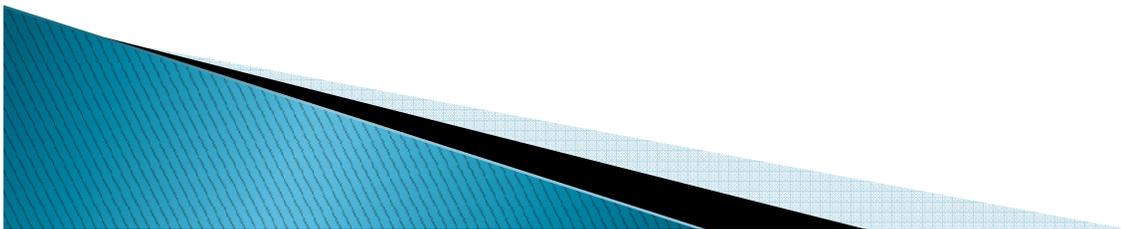
- Designar a los responsables de la información confidencial.
- Coordinar las acciones del manejo, mantenimiento y seguridad.
- Expedir el documento de seguridad y actualizarlo.

## Obligaciones del Responsable

- Adoptar las medidas de seguridad que dicte el comité.
- Llevar un registro de las personas que tengan acceso a la información
- Llevar registro de la información que deberá actualizarse.

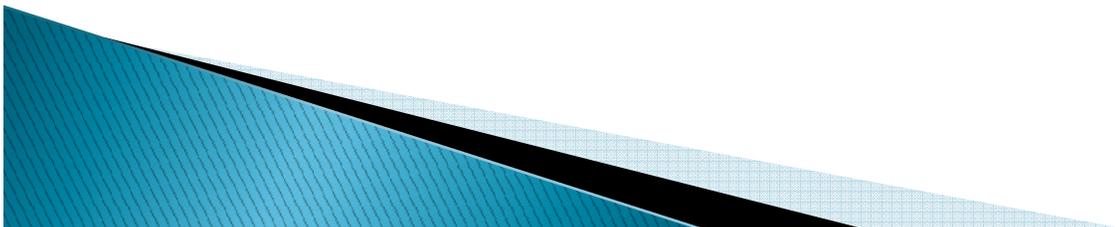


# Niveles de Seguridad



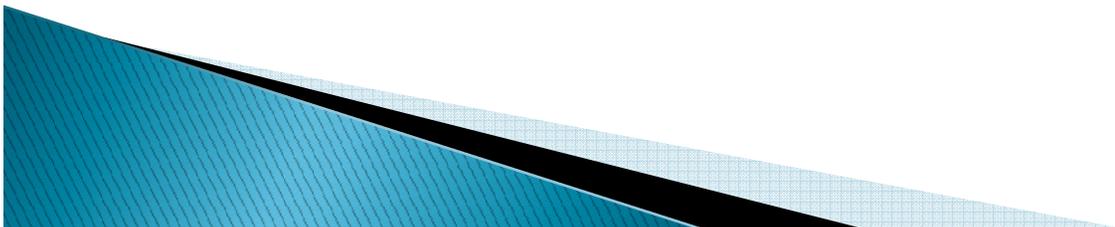
## Niveles de seguridad:

- I. Básico.- Se entenderá como tal, el relativo a las medidas generales de seguridad cuya aplicación es obligatoria para todos los sistemas de datos personales. Dichas medidas corresponden a los siguientes aspectos:
  - a) Documento de seguridad;
  - b) Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales;
  - c) Registro de incidencias;
  - d) Identificación y autenticación;
  - e) Control de acceso;
  - f) Gestión de soportes, y
  - g) Copias de respaldo y recuperación.



II. Medio.- Se refiere a la adopción de medidas de seguridad cuya aplicación corresponde a aquellos sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como a los sistemas que contengan datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo. Este nivel de seguridad, de manera adicional a las medidas calificadas como básicas, considera los siguientes aspectos:

- a) Responsable de seguridad;
- b) Auditoria;
- c) Control de acceso físico; y
- d) Pruebas con datos reales.

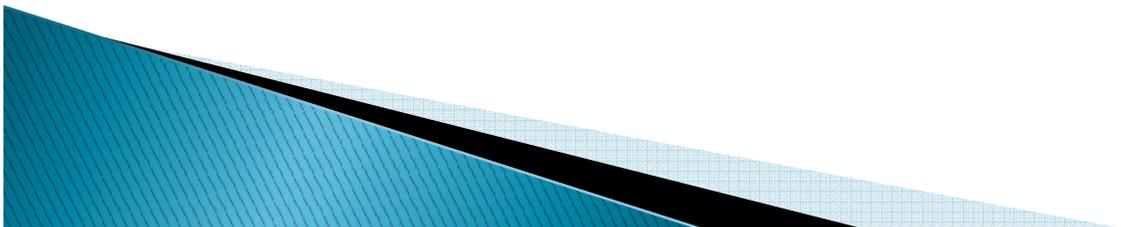


III. Alto.- Corresponde a las medidas de seguridad aplicables a sistemas de datos concernientes a la ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad, prevención, investigación y persecución de delitos. Los sistemas de datos a los que corresponde adoptar el nivel de seguridad alto, además de incorporar las medidas de nivel básico y medio, deberán completar las que se detallan a continuación:

- a) Distribución de soportes;
- b) Registro de acceso; y
- c) Telecomunicaciones.



*“Las medidas de seguridad constituyen mínimos exigibles, por lo que el ente público adoptará las medidas adicionales que estime necesarias para brindar mayores garantías en la protección y resguardo de los sistemas de datos personales. Por la naturaleza de la información, las medidas de seguridad que se adopten serán consideradas confidenciales.”*





**Muchas gracias, por  
su atención !!!**

Lic. Alvaro Ruvalcaba Ascencio  
Secretario Ejecutivo