TEEMICH
TRIBUNAL ELECTORAL DEL ESTADO
MICHOACÁN

SERVICIO PÚBLICO CON PERSPECTIVA DE PROTECCIÓN DE DATOS PERSONALES. PRINCIPIOS Y DEBERES.

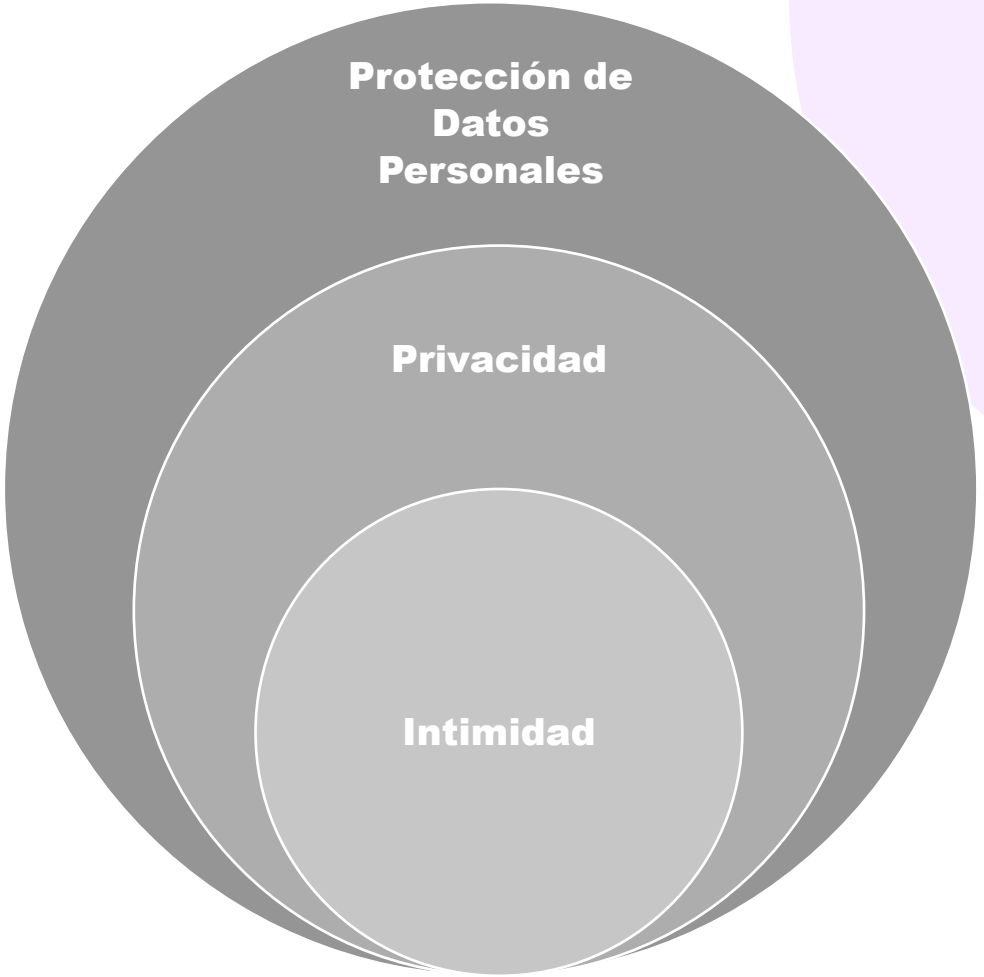
Morelia, Michoacán, 25 de febrero de 2025

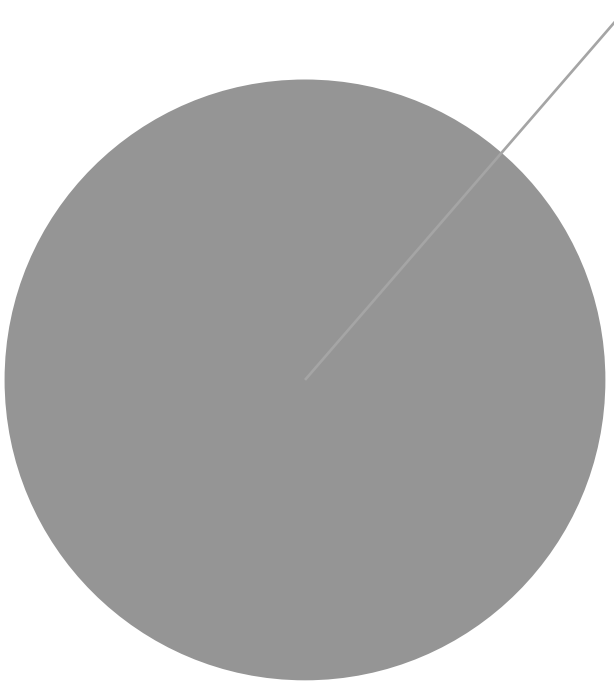
imaip
Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales


CADA MINUTO
01:00
DEL DÍA
PRESENTED BY
DOMO
LOS USUARIOS DE AIRBNB HACEN 747 RESERVAS
LOS CONSUMIDORES GASTAN EN AMAZON €416K
LOS USUARIOS DE X PUBLICAN 360K "TWEETS"
6.3M DE BÚSQUEDAS EN GOOGLE
LOS USUARIOS DE WHATSAPP MANDAN 41,6M DE MENSAJES
LOS USUARIOS DE LINKEDIN ENVÍAN 6.060 CURRICULUMS
LOS ESPECTADORES CONSUMEN EL EQUIVALENTE A 43 AÑOS DE CONTENIDO
3.720 USUARIOS DESCARGAN INSTAGRAM THREADS
LOS CIBER DELICUENTES LANZAN 30 ATAQUES DDOS
LOS USUARIOS DE CHATGPT GENERAN 6.944 SOLICITUDES
LOS USUARIOS DE INSTAGRAM COMPARTEN 694K REELS VÍA DM
LOS USUARIOS DE FACEBOOK DAN "ME GUSTA" A 4M DE POSTS
LOS COMENSALES DE DOORDASH HACEN PEDIDOS POR VALOR DE €111K
LOS FANS ESCUCHAN LAS CANCIONES DE TAYLOR SWIFT 69,4K VECES
LOS USUARIOS DE VENMO ENVÍAN €424K EN PAGOS
LOS USUARIOS PASAN 25,1M DE HORAS ONLINE
CADA PERSONA PRODUCE 102 MB DE DATOS
SE COMERCIAN €3.6M EN BONOS DEL TESORO
241M EMAILS SON ENVIADOS
EN TWITCH SE VISUALIZAN 48K HORAS DE CONTENIDO


Sujetos obligados y particulares
Política de Estado
Inteligencia Artificial
Transferencias y remisiones de datos personales
Privacidad e intimidad
Datos Personales y Datos Personales Sensibles
Era digital
Interés superior de la niñez
Derechos político-electorales
Datos personales de personas adultas mayores
Sistemas de videovigilancia
Derechos ARCOP (Acceso, Rectificación, Cancelación, Oposición, Portabilidad
Evaluación de impacto en la protección de datos personales
Principios y deberes
Autodeterminación informativa
Ley de protección de datos personales en posesión de sujetos obligados del Estado.
Auditorías voluntarias
Aviso de privacidad simplificado. Aviso de privacidad integral
Documento de seguridad
Comité de transparencia
Deber de confidencialidad
Unidad de transparencia
Tratamiento de datos personales
Procedimientos de impugnación. Recurso de revisión; de inconformidad; de verificación.
Delitos contra la intimidad
Oficial de protección de datos personales
Sanciones por tratamiento indebido de datos personales
Tratamiento indebido de datos personales
Medidas de apremio
Criterios de interpretación del INAI

PROTECCIÓN DE DATOS PERSONALES. CONCEPTOS Y DEFINICIONES BÁSICAS

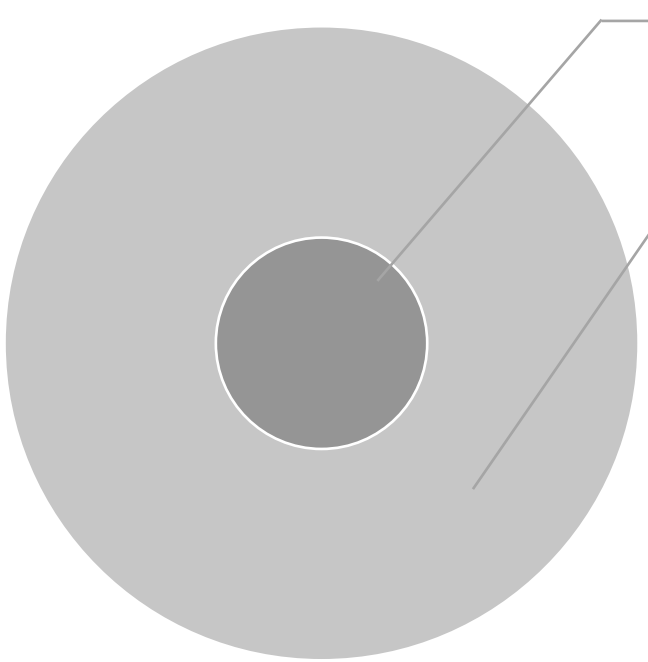




Intimidad.

Lo «íntimo» podría pensarse como el ámbito tanto de los pensamientos de cada cual, de la formación de decisiones («lo aún no expresado y que probablemente nunca lo será»), como de aquellas acciones cuya realización no requiere la intervención de terceros y tampoco los afecta.

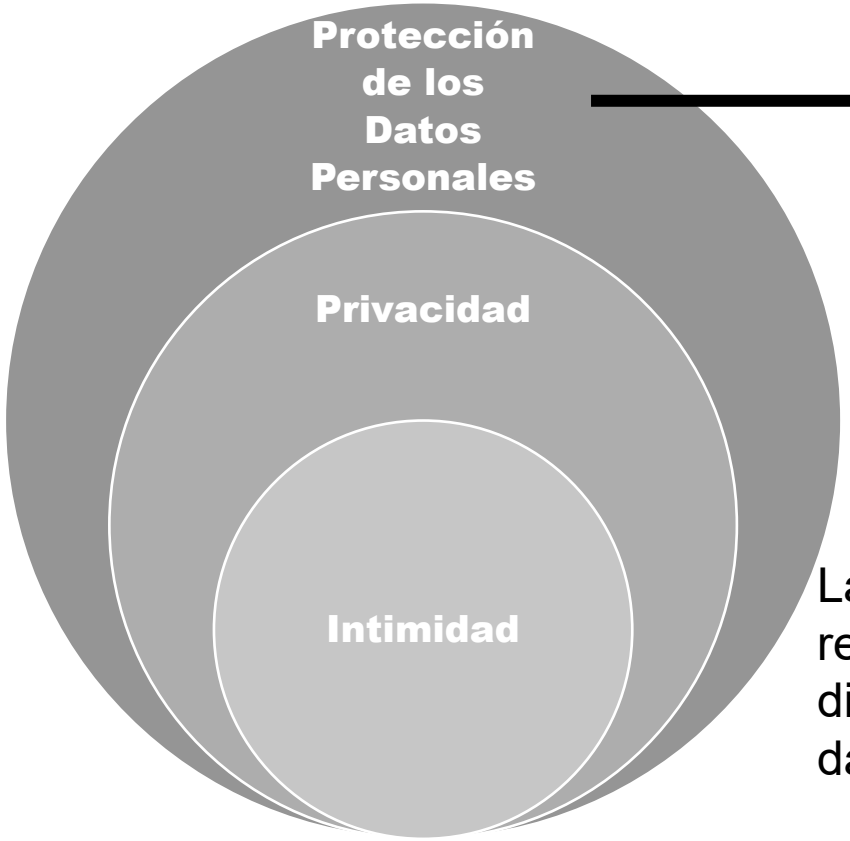
Dentro de este ámbito pueden pensarse aquellas acciones auto centradas en el individuo. **La intimidad es la parte más personal o lo reconocido como lo más recóndito del ser, es aquello que queda fuera de cualquier injerencia, sólo le pertenece a la persona, no se exterioriza, es su esfera espiritual y/o moral.**



Es el ámbito de nuestra vida **que como individuos dejamos fuera del escrutinio público.** Es parte de nuestra autodeterminación informativa, y es importante su protección, ya que en todo momento se puede ver afectado por un tercero o por el gobierno.

DERECHO A LA PRIVACIDAD

Es una prerrogativa que todo individuo tiene a separar aspectos de su vida privada del escrutinio público. Tiene dos componentes, el primero de ellos, es el que tiene el individuo de aislarse; lo cual permite poner una barrera y limitar el acceso de miramientos ajenos no consentidos. El segundo componente, es aquel referido al control que se tiene de la información propia. La privacidad vista como un derecho que se debe respetar, para garantizar la libertad y tener el control sobre quienes conocen y hasta donde conocen sobre la información de cada individuo.



El derecho a la privacidad es la base de la protección de los datos de carácter personal, ya que al proteger éstos se protege la privacidad de los individuos.

La autodeterminación informativa es el reconocimiento al individuo de la facultad de disposición y decisión respecto a sus propios datos personales.

Este derecho, reconoce al sujeto la facultad de decidir cuándo y cómo está dispuesto a permitir que se difunda su información personal o a difundirla él mismo. La protección de datos personales es una prerrogativa que tiene el titular de los datos para proteger cualquier información concerniente a su persona.

¿CUÁNTO VALEN NUESTROS DATOS PERSONALES?

¿CUÁL ES EL ACTIVO MÁS IMPORTANTE PARA EL FUNCIONAMIENTO DE LOS SUJETOS OBLIGADOS?

TEEMICH
TRIBUNAL ELECTORAL DEL ESTADO
MICHOACÁN

EXISTE UN TRÁNSITO GLOBAL DE DATOS PERSONALES PERO, ¿Y EL TRÁFICO DE DATOS PERSONALES?

YAHOO!

AdultFriendFinder

myspace.com

ebay

PlayStation Network

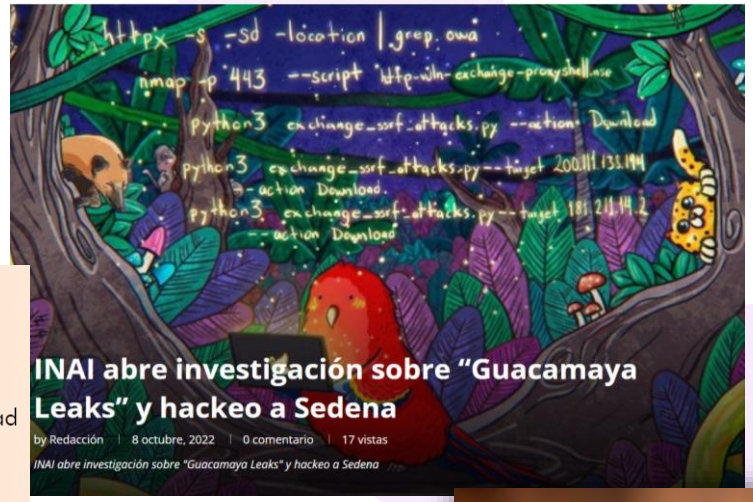
Dropbox

LA TENTACIÓN DE LOS DATOS PERSONALES

FUNCIÓN PÚBLICA
SECRETARÍA DE LA FUNCIÓN PÚBLICA

inai

La **Secretaría de la Función Pública** incumplió con la ley general de protección de datos personales y vulneró información privada contenida en la **declaración patrimonial de 830,000 servidores públicos**. Particularmente, la secretaría falló en sus deberes de confidencialidad y seguridad y en cinco de los ocho principios enunciados en la ley: los de consentimiento, responsabilidad, información, licitud y lealtad, determinó esta tarde el instituto garante de la protección de datos personales en México, el **Inai**.



TRIBUNAL ELECTORAL
del Poder Judicial de la Federación

Asuntos | Jurisprudencia | JEd | Comunicación | Escuela Judicial Electoral | Transparencia y protección de

Confirma TEPJF multa en contra de MC por publicación del listado nominal de electores en internet

20/septiembre/2018 / Sala Superior 306/2018

Ciudad de México

La Sala Superior ratificó la sanción impuesta a Movimiento Ciudadano por un monto de 34 millones 158 mil 411 pesos

Movimiento Ciudadano utilizó el padrón para fines distinto a los legales, pues lo reprodujo y almacenó por un tiempo adicional al permitido por la ley y su posterior exposición en un sitio de internet

PODER JUDICIAL ESTADO DE NUEVO LEÓN
CONSEJO DE LA JUDICATURA

Monterrey, N.L. a 15 de Enero de 2023

COMUNICADO

El Consejo de la Judicatura del Poder Judicial del Estado de Nuevo León informa que, este fin de semana, nuestras plataformas de ciberseguridad detectaron un intento de hakeo mediante un virus, por lo que se activó de manera preventiva el Protocolo de Seguridad de Informática que contempla las siguientes acciones:

Se bajaron todos nuestros sistemas internos y externos de informática, incluyendo el Tribunal Virtual, para aislar el virus y proteger nuestros equipos e información.

Se inició con el proceso de vacunación de los más de 70 Terabytes de información almacenada en nuestros servidores y de los mas de 3,500 equipos de cómputo.

Es importante resaltar que no hay hackeo de información y que la misma se encuentra en perfecto estado, que no ha sido extraída, eliminada o consultada por fuentes externas de manera indebida.

Nuestros Sistemas de Informática son de lo más avanzado y actuaron oportunamente ante la emergencia, contrarrestando y evitándo cualquier vulneración a nuestros equipos, programas, información y servidores. Se espera que todos los sistemas estén en servicio en las próximas 72 horas, por lo que las actividades jurisdiccionales continuarán de manera ordinaria, pero los términos judiciales estarán suspendidos durante este plazo.

Agradecemos la comprensión de todos nuestros usuarios.

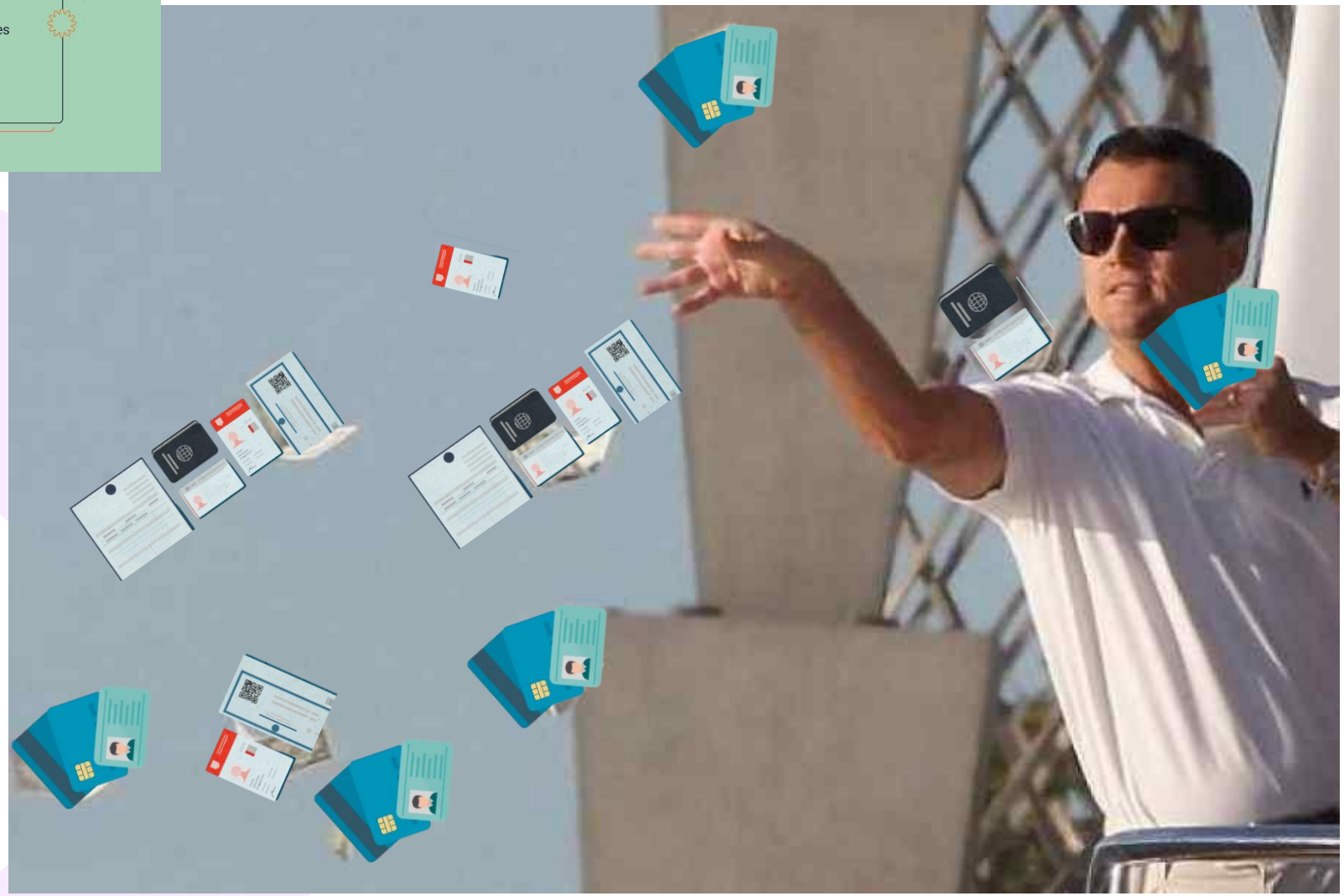
¿Qué sucedió en Ticketmaster?

El 13 de julio, **Ticketmaster** envió correos electrónicos a sus clientes para notificarles sobre un "**incidente**" en el cual su información personal pudo haber estado involucrada ya que "un tercero no autorizado" entró a una base de datos.

> **"Lamentamos notificarle acerca de un incidente en el que su información personal pudo haber estado involucrada. Para nosotros la protección de la información y el aviso a nuestros clientes de cualquier situación de riesgo son sumamente importantes,"**

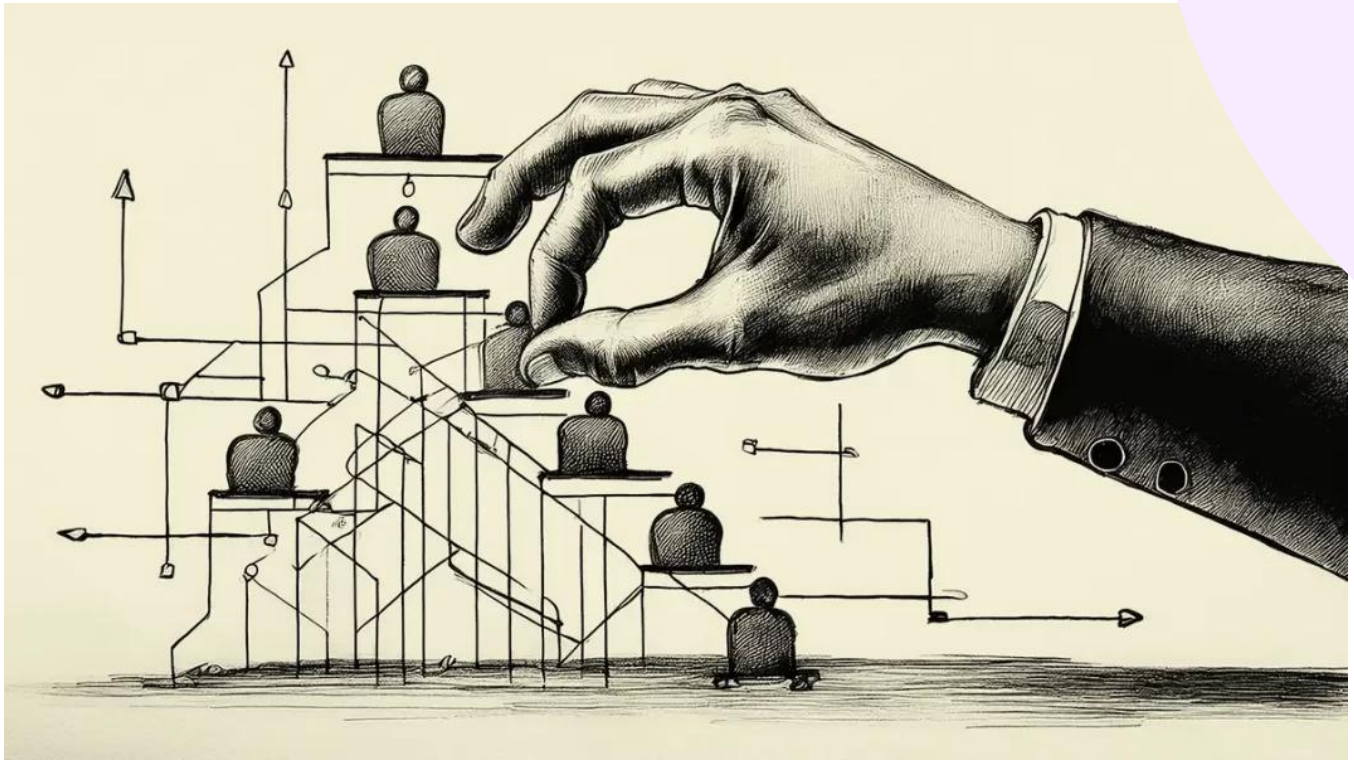
se lee en el correo electrónico.

¿SOMOS RESPONSABLES EN EL MANEJO DE NUESTROS DATOS PERSONALES?

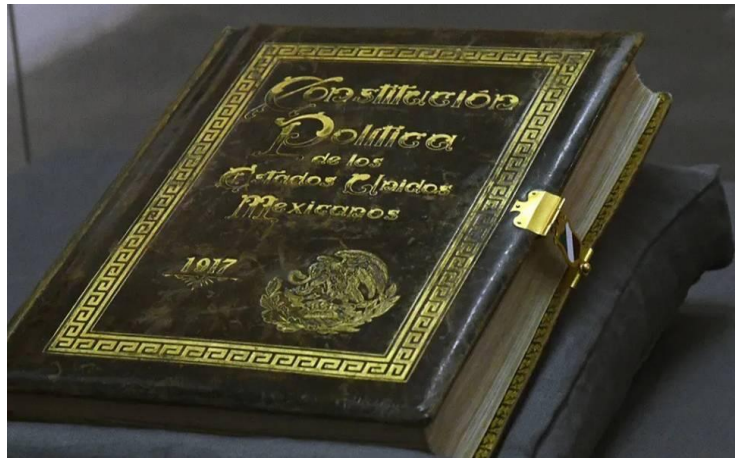


Es muy importante cuidar nuestros datos personales por razones de seguridad y porque es nuestro derecho; nuestros datos deben ser protegidos contra el mal uso como **robo de identidad, transmisiones indebidas o accesos no autorizados.**

ALGUNAS CONSIDERACIONES DE LA REFORMA CONSTITUCIONAL EN MATERIA DEL NUEVO MODELO DE TRANSPARENCIA Y PROTECCIÓN DE DATOS PERSONALES.



EL DAI Y LA PDP COMO DERECHOS HUMANOS PERMANECEN



CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS

Constitución publicada en el Diario Oficial de la Federación el 5 de febrero de 1917

TEXTO VIGENTE
Última reforma publicada DOF 06-06-2023

El C. Primer Jefe del Ejército Constitucionalista, Encargado del Poder Ejecutivo de la Nación, con esta fecha se ha servido dirigirme el siguiente decreto:

VENUSTIANO CARRANZA, Primer Jefe del Ejército Constitucionalista, Encargado del Poder Ejecutivo de los Estados Unidos Mexicanos, hago saber:

Que el Congreso Constituyente reunido en esta ciudad el 1o. de diciembre de 1916, en virtud del decreto de convocatoria de 19 de septiembre del mismo año, expedido por la Primera Jefatura, de conformidad con lo prevenido en el artículo 4o. de las modificaciones que el 14 del citado mes se hicieron al decreto de 12 de diciembre de 1914, dado en la H. Veracruz, adicionando el Plan de Guadalupe, de 26 de marzo de 1913, ha tenido a bien expedir la siguiente:

CONSTITUCION POLITICA DE LOS ESTADOS UNIDOS MEXICANOS QUE REFORMA LA DE 5 DE FEBRERO DE 1857

Título Primero

Capítulo I
De los Derechos Humanos y sus Garantías
Denominación del Capítulo reformada DOF 10-06-2011

Artículo 6o. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.
Párrafo reformado DOF 13-11-2007, 11-06-2013

Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión.
Párrafo adicionado DOF 11-06-2013

El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios.
Párrafo adicionado DOF 11-06-2013

Para efectos de lo dispuesto en el presente artículo se observará lo siguiente:
Párrafo adicionado DOF 11-06-2013

A. Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:
Párrafo reformado (para quedar como apartado A) DOF 11-06-2013. Reformado DOF 29-01-2016

Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo.
Párrafo reformado DOF 15-09-2017

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.
Párrafo adicionado DOF 01-06-2009

No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que preceda denuncia o querella de un hecho que la ley señale como delito, sancionado con pena privativa de libertad y obren datos que establezcan que se ha cometido ese hecho y que exista la probabilidad de que el indiciado lo cometió o participó en su comisión.
Párrafo reformado DOF 01-06-2009. Fe de erratas DOF 25-06-2009

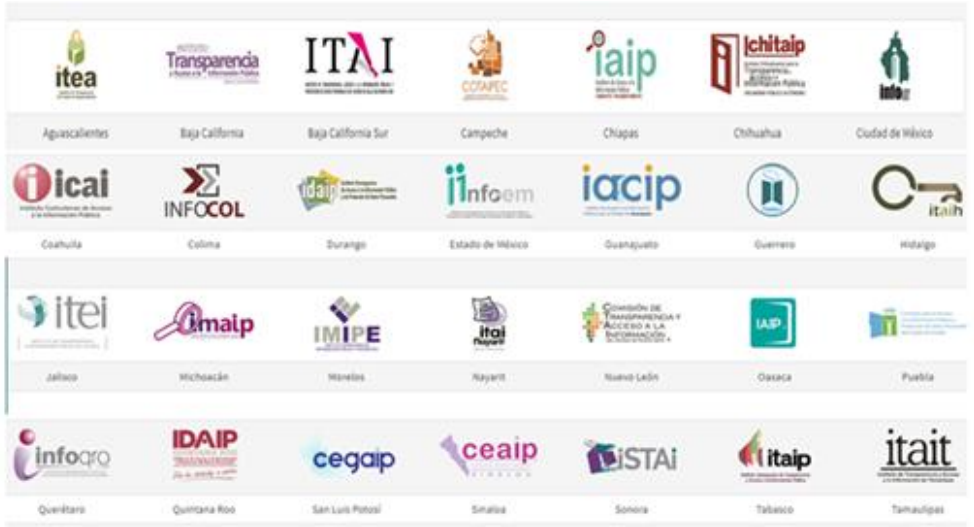
La autoridad que ejecute una orden judicial de aprehensión, deberá poner al inculpado a disposición del juez, sin dilación alguna y bajo su más estricta responsabilidad. La contravención a lo anterior será sancionada por la ley penal.

¿CUÁLES SON LAS CARACTERÍSTICAS DE LOS DERECHOS HUMANOS?

INALIENABLES

IGUALES Y NO DISCRIMINATORIOS

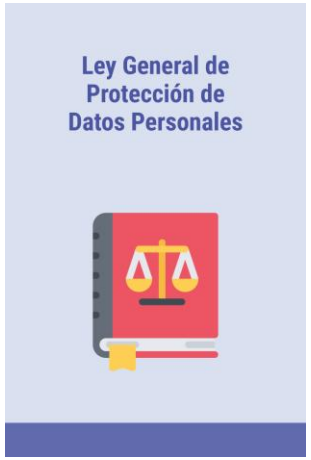
INCLUYEN TANTO DERECHOS COMO OBLIGACIONES



Órgano Interno de Control

SE CAMBIA DE SEDE, PERO SE MANTIENEN LAS MISMAS REGLAS PARA EL CUMPLIMIENTO DE AMBOS DERECHOS HUMANOS.

DENTRO DEL PAQUETE DE REFORMAS A LAS LEYES SECUNDARIAS, NO SE DEROGA LA LEGISLACIÓN EN MATERIA DE ACCESO A LA INFORMACIÓN PÚBLICA Y DE PROTECCIÓN DE DATOS PERSONALES.



Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo

imaip

PERIÓDICO OFICIAL
DEL GOBIERNO CONSTITUCIONAL DEL ESTADO DE MICHOACÁN DE OCAMPO
Fundado en 1867

Las leyes y demás disposiciones son de observancia obligatoria por el solo hecho de publicarse en este periódico. Registrado como artículo de 2a. clase el 28 de noviembre de 1921.

Director: Lic. José Juárez Valdovinos

Tabachín # 107, Col. Nva. Jacarandas, C.P. 58099 DÉCIMA SECCIÓN Tels. y Fax: 3-12-32-28, 3-17-06-84

TOMO CLXVIII | Morelia, Mich., Lunes 13 de Noviembre de 2017 | NUM. 58

CONTENIDO

PODER EJECUTIVO DEL ESTADO

SILVANO AUREOLES CONEJO, Gobernador del Estado Libre y Soberano de Michoacán de Ocampo, a todos sus habitantes hace saber:

El H. Congreso del Estado, se ha servido dirigirme el siguiente:

DECRETO

EL CONGRESO DE MICHOACÁN DE OCAMPO DECRETA:

NÚMERO 398

ÚNICO. Se expide la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, para quedar como sigue:

LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE MICHOACÁN DE OCAMPO

TÍTULO PRIMERO
DISPOSICIONES GENERALES

CAPÍTULO I
DEL OBJETO DE LA LEY

Artículo 1. La presente Ley es de orden público y de observancia general en el Estado de Michoacán de Ocampo, y es reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, así como del artículo 8° de la Constitución Política del Estado Libre y Soberano de Michoacán de Ocampo en materia de protección de datos personales en posesión de sujetos obligados.

Todas las disposiciones de esta Ley son de aplicación y observancia directa para los sujetos obligados pertenecientes al orden estatal.

El Instituto ejercerá las atribuciones y facultades que le otorga esta Ley, independientemente de las otorgadas en las demás disposiciones aplicables.

Tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.

Responsable de la Publicación
Secretaría de Gobierno

DIRECTORIO

Gobernador Constitucional del Estado de Michoacán de Ocampo
Ing. Silvano Aureoles Conejo

Secretario de Gobierno
Lic. Adrián López Solís

Director del Periódico Oficial
Lic. José Juárez Valdovinos

Aparece ordinariamente de lunes a viernes.

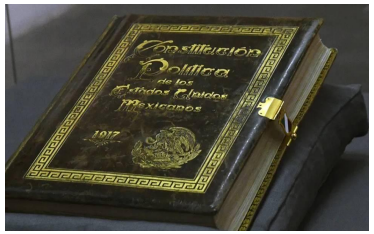
Tiraje: 150 ejemplares
Esta sección consta de 24 páginas

Precio por ejemplar:
$ 26.00 del día
$ 34.00 atrasado

Para consulta en Internet:
www.michoacan.gob.mx/noticias/p-oficial
www.congresomich.gob.mx

Correo electrónico
periodicooficial@michoacan.gob.mx

A MANERA DE CONCLUSIÓN PRELIMINAR:



EL DERECHO DE ACCESO A LA INFORMACIÓN Y EL DE PROTECCIÓN DE DATOS PERSONALES, RESPECTIVAMENTE, CONTINUAN EN LA CONSTITUCIÓN.

POR LO QUE, ESTARÁN SUJETOS A UN ESQUEMA DE CUMPLIMIENTO POR PARTE DE LOS SUJETOS OBLIGADOS.

PLATAFORMA NACIONAL DE TRANSPARENCIA

CONTINUA LA PLATAFORMA NACIONAL DE TRANSPARENCIA.

SE MANTIENE EL ACTUAL CUMPLIMIENTO DE OBLIGACIONES DE TRANSPARENCIA.

SE MANTIENE EL ACTUAL CUMPLIMIENTO DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS.

NUESTRAS HERRAMIENTAS

MARCO LEGAL PDP MÉXICO

Los datos personales y su protección

PRIVADO

- Ley Federal de Protección de Datos Personales en Posesión de los Particulares
- RLFPDPPP
- Lineamientos Aviso de Privacidad
- Lineamientos hiperenlaces e hipervínculos AP
- Criterios Generales instrumentación medidas compensatorias
- Parámetros de Autorregulación
- Reglas de Operación REA
- Guía de Esquemas de Autorregulación en Materia de Protección de Datos Personales
- Recomendaciones en materia de seguridad de datos personales
- Guía implementación SGDP
- Metodología de Análisis de Riesgo BAA
- Guía para cumplir con principios y deberes
- Guía para el borrado seguro de DP
- Manual para MiPyMEs
- Tabla de Equivalencia Funcional
- Recomendaciones designación responsable al interior
- Guía para Instrumentar Medidas Compensatorias
- El ABC del aviso de privacidad

PÚBLICO

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- Leyes estatales en materia de protección de datos personales
- Parámetros de **Mejores Prácticas** en Materia de Protección de Datos Personales del Sector Público
- Lineamientos Generales de Protección de Datos Personales para el Sector Público
- Lineamientos modalidades y procedimientos para la **portabilidad** de datos personales
- Disposiciones administrativas de carácter general para la elaboración, **presentación y valoración de evaluaciones de impacto en la protección de datos personales**.
- Criterios generales para la instrumentación de **medidas compensatorias en el sector público** del orden federal, estatal y municipal.
- Programa de Protección de Datos Personales
- Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- El ABC del aviso de privacidad (Sector Público)
- Guía para la elaboración del aviso de privacidad en el área de recursos humanos (Sector Público)

Guía para el tratamiento de datos biométricos

Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales

Recomendaciones para el manejo de incidentes de seguridad de datos personales

https://home.inai.org.mx/?page_id=3418

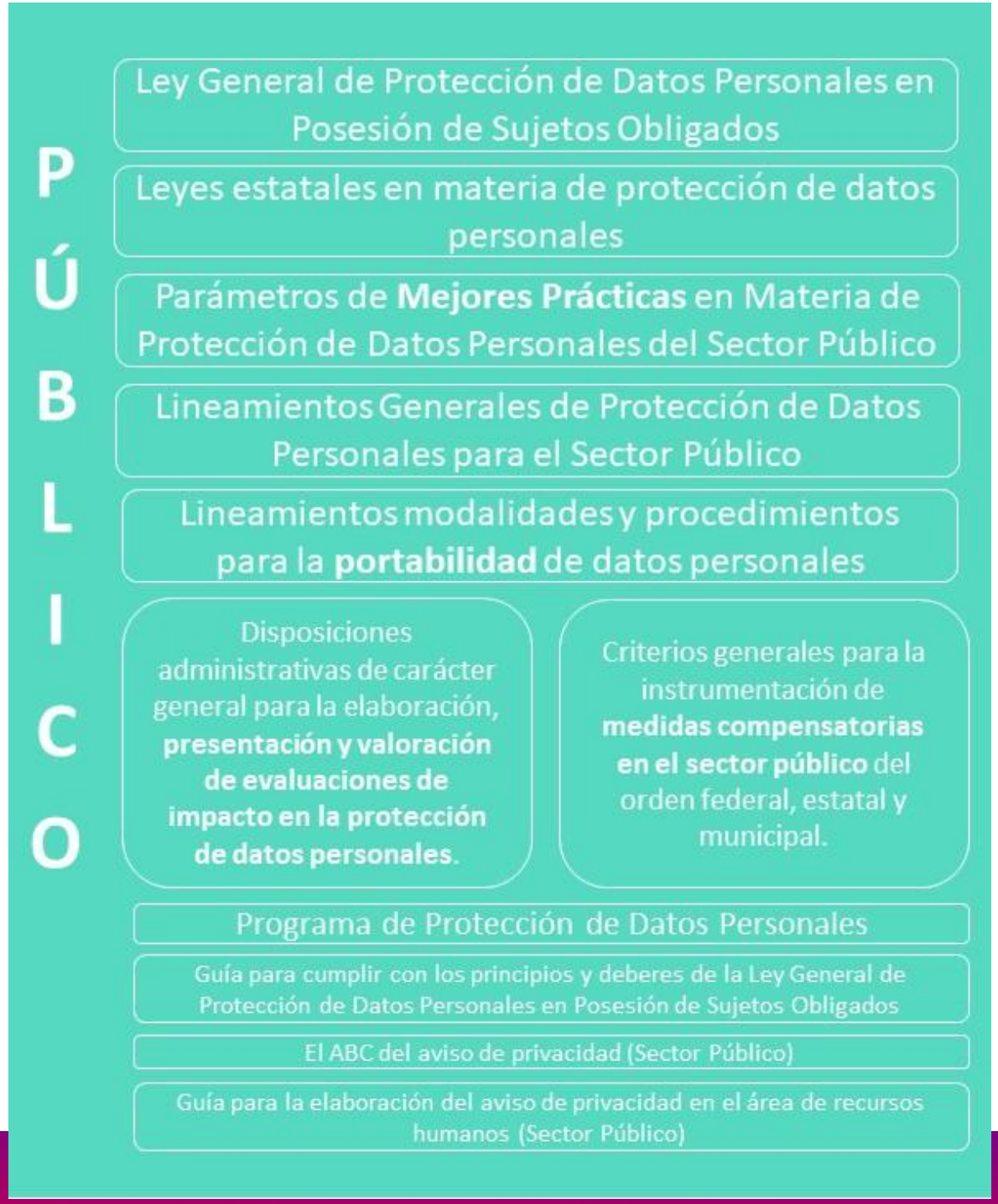
CLICK

PÚBLICO

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- Leyes estatales en materia de protección de datos personales
- Parámetros de **Mejores Prácticas** en Materia de Protección de Datos Personales del Sector Público
- Lineamientos Generales de Protección de Datos Personales para el Sector Público
- Lineamientos modalidades y procedimientos para la **portabilidad** de datos personales
- Disposiciones administrativas de carácter general para la elaboración, **presentación y valoración de evaluaciones de impacto en la protección de datos personales**.
- Criterios generales para la instrumentación de **medidas compensatorias en el sector público** del orden federal, estatal y municipal.
- Programa de Protección de Datos Personales
- Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- El ABC del aviso de privacidad (Sector Público)
- Guía para la elaboración del aviso de privacidad en el área de recursos humanos (Sector Público)

PRIVADO

- Ley Federal de Protección de Datos Personales en Posesión de los Particulares
- RLFPDPPP
- Lineamientos Aviso de Privacidad
- Lineamientos hiperenlaces e hipervínculos AP
- Criterios Generales instrumentación medidas compensatorias
- Parámetros de Autorregulación
- Reglas de Operación REA
- Guía de Esquemas de Autorregulación en Materia de Protección de Datos Personales
- Recomendaciones en materia de seguridad de datos personales
- Guía implementación SGDP
- Metodología de Análisis de Riesgo BAA
- Guía para cumplir con principios y deberes
- Guía para el borrado seguro de DP
- Manual para MiPyMEs
- Tabla de Equivalencia Funcional
- Recomendaciones designación responsable al interior
- Guía para Instrumentar Medidas Compensatorias
- El ABC del aviso de privacidad



https://home.inai.org.mx/?page_id=3418

CLICK

OBJETO DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO

I. Establecer las bases y condiciones que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, mediante procedimientos sencillos y expeditos;

II. Garantizar la observancia de los principios de protección de datos personales previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia;

III. Proteger los datos personales en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos del Estado y los municipios, con la finalidad de regular su debido tratamiento;

IV. Garantizar que toda persona pueda ejercer el derecho a la protección de los datos personales;

V. Promover, fomentar y difundir una cultura de protección de datos personales; y,

VI. Establecer los mecanismos para garantizar el cumplimiento y la efectiva aplicación de las medidas de apremio que correspondan para aquellas conductas que contravengan las disposiciones previstas en esta Ley.

EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

Le confiere al individuo la facultad de participar en el tratamiento que otros hacen de sus datos personales.

Protege el manejo justo de su información personal al garantizarle el acceso, rectificación y cancelación de sus datos personales, así como al permitirle manifestar su oposición al tratamiento de los mismos (derechos ARCO).

Diferencias entre:

El derecho de acceso a la información pública

- Le permite al individuo acceder a la información que obra en los archivos de los poderes públicos siempre que dicha información no se encuentre clasificada como **reservada o confidencial.**
- No limita el ejercicio del derecho de protección de datos personales salvo en casos excepcionales. (causas de interés público)

El derecho a la protección de datos personales

- Le confiere al individuo la facultad de acceder a los datos personales que sobre su persona obran en poder de los poderes públicos, así como rectificarlos, cancelarlos y oponerse a que sean tratados.
- Limita el ejercicio del derecho de acceso a la información pública salvo casos excepcionales. (causas de interés público)

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán.

¿Cuáles son las definiciones y las figuras fundamentales que nos permiten entender la Ley de Protección de Datos Personales?

Datos personales

Cualquier información concerniente a una persona física identificada (que sabemos quién es) o identificable (que fácilmente podemos determinar quién es); esto es, cuando su identidad se determina a través de cualquier información.

*Se entiende que una **persona física es identificable** cuando su identidad pueda determinarse directa o indirectamente.*

Ejemplo de datos personales son: nuestro nombre, la fecha de nacimiento, el domicilio donde residimos, nuestra dirección de correo electrónico, el número telefónico de casa, nuestras preferencias de entretenimiento, por citar algunos.

"Cualquier información concerniente a una persona física identificada o identificable"

Pueden estar expresados en:

forma numérica

forma alfabética

forma fotográfica

forma gráfica

acústica o de cualquier otro tipo

¿Cómo se clasifican los datos personales?

A continuación se exponen los grupos más comunes en los que se dividen los datos personales, con sus respectivos ejemplos; mismos que son enunciativos, más no limitativos:

Grupo de dato personal	Ejemplos de datos personales
De identificación: Información concerniente a su titular, porque permite diferenciarla de otras, en una colectividad.	• Nombres • Apodos o pseudónimos • CURP • RFC • Sonido de la voz • Firma • Cartilla militar • Lugar y fecha de nacimiento • Número de seguridad social • Circunstancia de modo, tiempo y lugar[4]
De contacto: Información concerniente a su titular, porque permite mantener o entrar en contacto con su titular.	• Domicilio • Correo electrónico • Teléfono • Celular • Dirección IP
Datos académicos: Información concerniente a su titular, porque es relativa a la formación académica que recibió, denotando así el nivel educativo de los titulares.	• Título y cédula profesional • Calificaciones • Número de matrícula • Tipos de escuelas

Grupo de dato personal	Ejemplos de datos personales
Datos laborales: Información concerniente a su titular, porque es relativa a datos de su profesión o empleo.	• Cargos • Puestos • Periodos
Datos de carácter patrimonial o financieros: Se considera que dichos datos están asociados al patrimonio de una persona física o moral, entendiendo éste como el conjunto de bienes, derechos y obligaciones correspondientes a una persona (física o moral) y que constituyen una universalidad jurídica.	• Información bancaria • Número de cuenta • Cuenta CLABE • Datos de inscripción en registro público • Marca, modelo, número de motor y serie, placas de circulación
Datos personales jurisdiccionales o administrativos: Información relativa sobre una persona (física o moral) que sostiene un proceso seguido en forma de juicio, ante cualquier órgano jurisdiccional o administrativo.	• Números de expedientes judiciales o administrativos • Multas • Claves de acceso a Tribunal Virtual • Posiciones de una persona identificada frente al estado
Datos sobre características físicas: Información concerniente a su titular, porque es relativa a la fisonomía, anatomía, rasgos o particularidades específicas de los titulares.	• Color de piel, iris o cabello • Estatura • Peso • Cicatrices visibles • Tatuajes

Información periférica:

También deben tomarse en cuenta los datos que se denominan periféricos, y que se obtienen de la valoración que se realice al efectuar cruces de datos o de información, pues a través de ellos, se puede llegar a identificar a una persona determinada. Como ejemplos de información periférica, se mencionan de manera enunciativa, la siguiente:

Este tipo de datos, generalmente deben ser testados de las versiones públicas, a fin de evitar la identificación indirecta del individuo, o bien, la segregación de otra información vinculada con la persona, a través de criterios de búsqueda o descarte de información, mediante el uso de la tecnología, o el uso de fuentes de acceso público, tales como el Registro Civil, el Instituto de la Propiedad y del Comercio y el Boletín Judicial, o bien, el uso de bases de datos sistematizadas.

Documentos aportados como prueba, como información confidencial relativa a datos personales.

Como información confidencial, también existen documentos que pueden estar agregados en las constancias de los expedientes judiciales y que su número, folio o registro, puedan ser considerados como datos personales sujetos a clasificación y que deban ser testados de las versiones públicas, de conformidad con los criterios referidos con antelación. A continuación, algunos ejemplos de ellos, que se señalan de manera enunciativa, más no limitativa:

Documento	Asociación a dato personal
Facturas u órdenes de compras	Especialmente los números con los que se identifican, si se integra de letras que identifican a las partes o que puedan ser rastreables a través de los portales de la página del Servicio de Administración Tributaria (SAT).
Póliza de seguro, entre otras	Por medio de su número, identifica a la compañía aseguradora y al beneficiario, su identificación, el tipo de seguro, su vigencia, la designación de beneficiarios e información sobre su patrimonio; la cobertura, prima asegurada, deducible, enfermedades cubiertas, preferencias deportivas o coberturas de riesgo, entre otros datos

Algunos de estos documentos pueden ser considerados como públicos, porque pueden ser consultados por cualquier persona a través de una fuente de acceso público, como lo es el Registro Civil y el Instituto Registral y Catastral, sin embargo, al ser aportadas como pruebas por las partes dentro de un proceso judicial, para hacer valer sus acciones y/o excepciones, **adquieren un carácter confidencial, porque pueden identificar a las partes afectas a los procedimientos.**

Datos personales sensibles

Un **dato personal** adquiere la categoría de **sensible** cuando afecta la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

En particular la Ley, de manera enunciativa más no limitativa, considera como **datos personales sensibles**, aquellos que puedan revelar aspectos de la persona, como:

- Origen étnico o racial
- Estado de salud presente y futuro
- Información genética
- Creencias religiosas, filosóficas y morales
- Opiniones políticas
- Preferencia sexual

Grupo de dato personal	Ejemplos de datos personales
Biométricos: Son características físicas que pueden ser utilizadas para identificar digitalmente a una persona.	• Imagen de iris • Huella dactilar
Datos ideológicos: Información sobre las posturas ideológicas, religiosas, filosóficas o morales de una persona.	• Afinidad social • Afinidad religiosa
Datos sobre opiniones políticas: Opinión de una persona en relación con un hecho político o sobre su postura política, en general.	• Afinidad por partido político específico • Afinidad sobre gobernantes

https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/GuiaDatosBiometricos_Web_Links.pdf

Grupo de dato personal	Ejemplos de datos personales
Datos sobre afiliación sindical: Pertenencia de una persona a un sindicato y la información que de ello derive.	• Afinidad sindical
Datos de salud: Información concerniente a un particular, relacionada con la valoración, preservación, cuidado, mejoramiento y recuperación de su estado de salud físico o mental, presente, pasado o futuro, así como su información genética.	• Valoración, estudios, resultados de estado de salud, pasado presente o futuro • Lesiones • Enfermedades • Discapacidades • Facturas sobre salud de la persona

¿Qué son los datos biométricos?

Son las propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles.

Por ejemplo:
la huella dactilar, el rostro, el iris, la retina, la geometría de la mano.

El INE solicita a la ciudadanía sólo dos datos biométricos: el rostro y las 10 huellas dactilares.
Esta información se encuentra resguardada junto con todos los datos que integran el Padrón Electoral.

EL INE PROTEGE TUS DATOS PERSONALES

CENTRAL ELECTORAL · INE · CONTAMOS TODAS TODOS · #Elecciones2020

LA CDMX USA BANCO DE ADN PARA RESOLVER DELITOS

TIPOS DE BIOMETRÍA EN SEGURIDAD

La biometría tiene múltiples ventajas:

- Mejora la precisión en el proceso de identificación.
- No hay contacto físico, por lo que es más higiénico.
- Existe compatibilidad con otros métodos biométricos.

BIOMETRÍA FÍSICA

Los lectores, escáneres o sensores permiten registrar la información biométrica de la persona en una base de datos especifica y convertirla en un código digital que ayude a reconocer a la persona.

BIOMETRÍA DE COMPORTAMIENTO

Escanear las huellas dactilares

La huella digital se recoge con un escáner y nos ofrece un código para cada persona.

Escaneo por el iris

No existen 2 personas que tengan un patrón de ojo que coincida. Este método es de los más efectivos.

Reconocimiento facial

Puede localizar de forma automática la cara humana a través de la captura en vídeo o imagen.

Reconocimiento por voz

La voz es un rasgo que sirve para identificar a una persona.

Geometría de la mano

Los algoritmos de reconocimiento de firmas se basan en métodos matemáticos que usan el análisis de curvas.

Control por la retina

Usa un escáner que lee la retina con una luz infrarroja que penetra en los vasos sanguíneos de la pared posterior del ojo.

Grupo de dato personal	Ejemplos de datos personales
Datos sobre vida sexual: Información de una persona física, relacionada con su comportamiento, preferencias, prácticas o hábitos sexuales, entre otros.	• Hábitos, prácticas y vida sexuales
Datos sobre opiniones políticas: Opinión de una persona en relación con un hecho político o sobre su postura política, en general.	• Afinidad por partido político específico • Afinidad sobre gobernantes
Datos de origen étnico o racial: Información concerniente a una persona, relativa a su pertenencia a un pueblo, etnia o región que la distingue por sus condiciones e identidades sociales, culturales y económicas, así como por sus costumbres, tradiciones y creencias.	• Pueblos • Región • Etnia • Nacionalidad • Costumbres • Idioma

Los datos personales sensibles, deben testarse preferentemente de las sentencias públicas, especialmente si hacen identificables, directa o indirectamente, a los titulares, por el grado de discriminación que sobre las personas puede llegar a afectarles.

¿QUÉ NOS DICE LA LEY DE TRANSPARENCIA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES?

- Los sujetos obligados serán responsables de los datos personales en su posesión y, en relación con éstos, deberán:

I. Adoptar procedimientos adecuados para recibir y responder las solicitudes **ARCOP**;

II. Tratamiento de datos personales;

III. Poner a disposición de los individuos de los avisos de privacidad que correspondan;

IV. Que los datos personales sean exactos y actualizados;

V. Actuación de manera oficiosa en el tratamiento de los datos personales; y,

VI. Adoptar medidas que garanticen la seguridad de los datos personales.

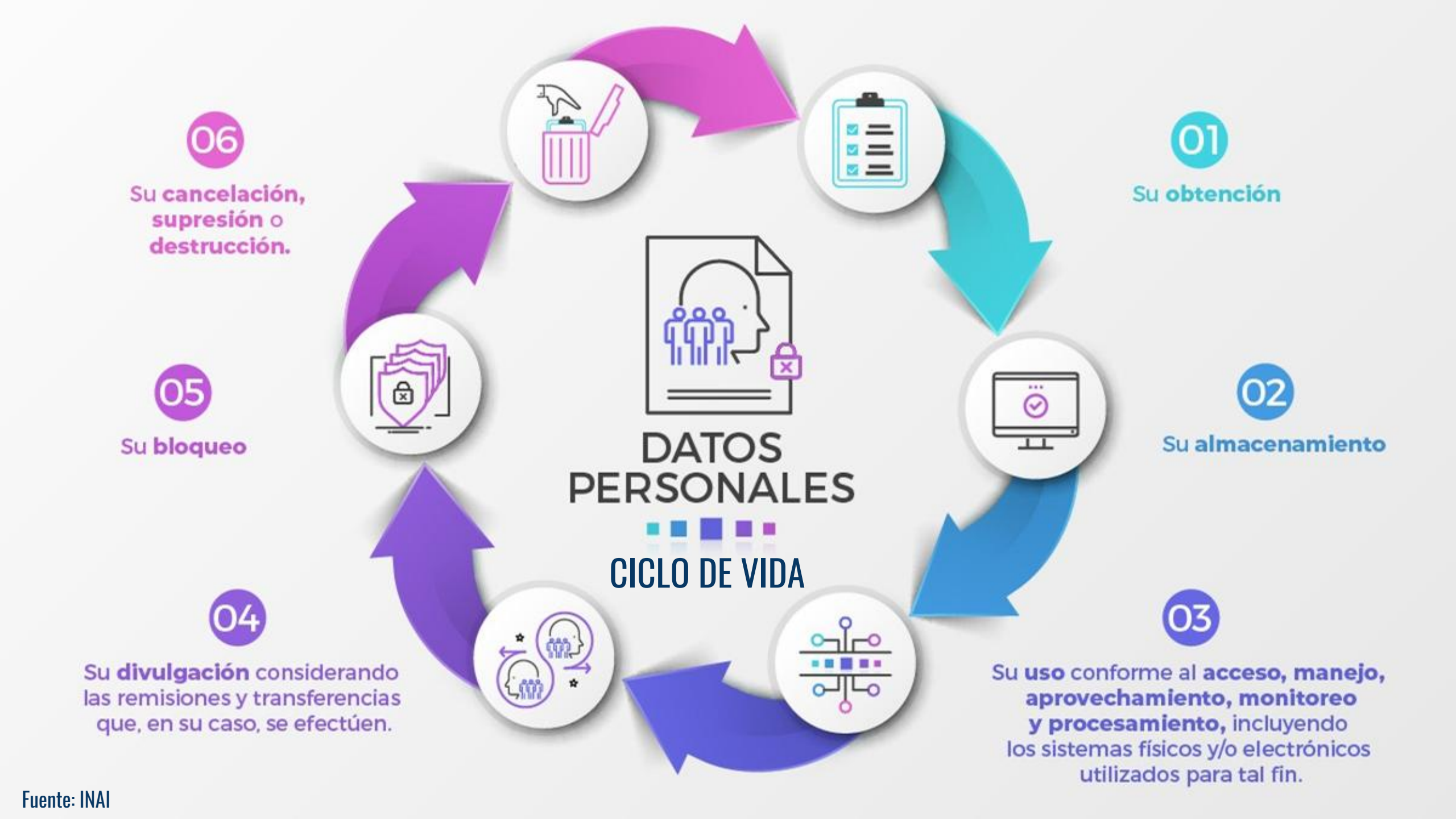
Los sujetos obligados <u>NO PODRÁN</u> difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autentificación similar, de los individuos a que haga referencia la información de acuerdo a la normatividad aplicable.

Figuras sustantivas que se desprenden de la Ley de PDPPP:

Tratamiento

Conjunto de operaciones realizadas con los datos personales para la consecución de ciertos fines que persigue el responsable; concretamente, **consiste en ejecutar distintas operaciones durante el ciclo de vida de los datos personales, desde el momento de su obtención, pasando por su explotación o aprovechamiento, hasta su supresión o eliminación.**

A manera de referencia enunciativa, no limitativa, un tratamiento de datos personales se distingue por efectuar cualquier operación o conjunto de operaciones mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas **a partir de la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.**


06
Su cancelación, supresión o destrucción.
01
Su obtención
05
Su bloqueo
02
Su almacenamiento
DATOS PERSONALES
CICLO DE VIDA
04
Su divulgación considerando las remisiones y transferencias que, en su caso, se efectúen.
03
Su uso conforme al acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin.

Fuente: INAI

Figuras sustantivas que se desprenden de la Ley de PDPPSO:

Titular

Persona física a quien corresponden los datos personales. Es decir, menores, adolescentes, adultos, adultos mayores, entre otros, a quienes se les brinda un servicio público y que a través del mismo es necesario la utilización de sus datos personales; es el caso de los beneficiarios de un programa social, o los ciudadanos mayores de 18 años que solicitan su credencial para votar, o los derechohabientes del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado.

Responsable

Cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, fideicomisos y fondos públicos del orden federal y partidos políticos que decide o establece determinado tratamiento de datos personales en el ejercicio de sus atribuciones y funciones.
Su poder de decisión implica establecer, por ejemplo:
•el tipo de datos que requieren
•los medios a utilizar en el tratamiento de datos personales
•las transferencias de datos personales que, en su caso, efectúe
•la forma o mecanismos para obtener, almacenar y suprimir los datos personales

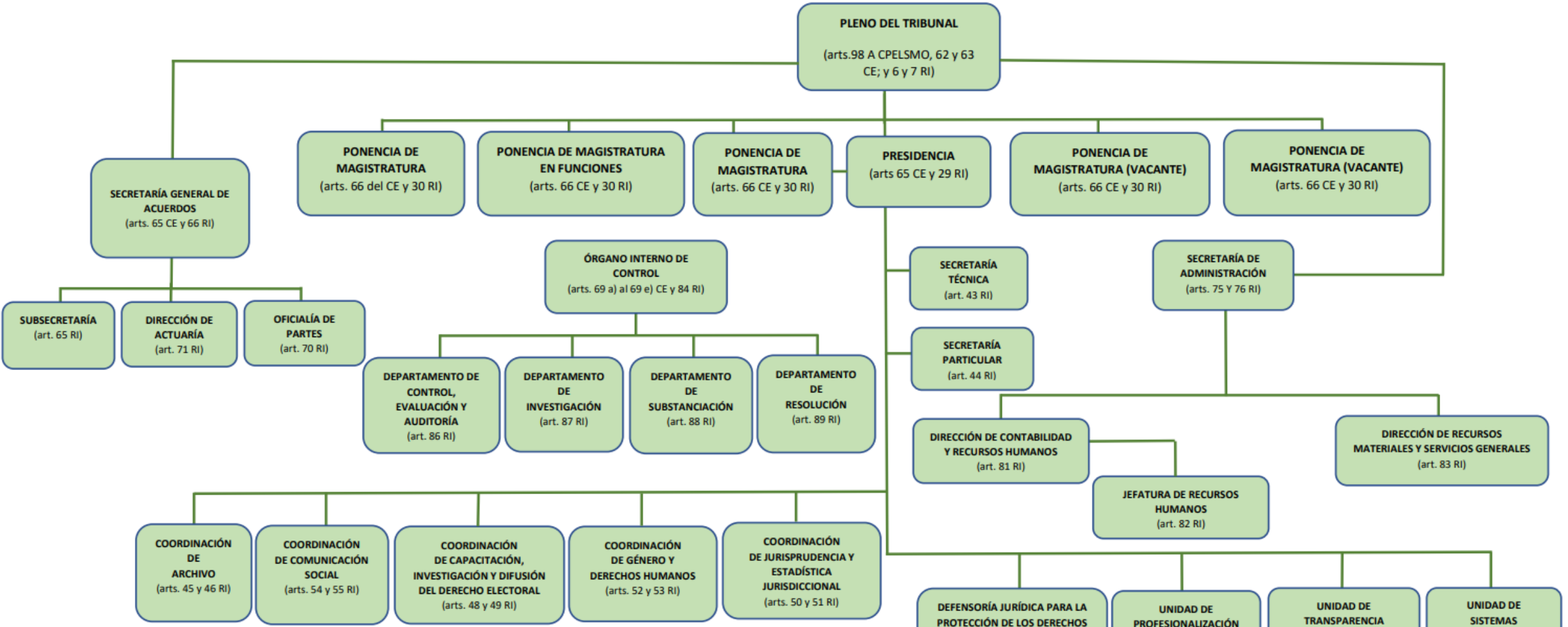
TEEMICH
TRIBUNAL ELECTORAL DEL ESTADO
MICHOACÁN

El Tribunal Electoral es el responsable del tratamiento de los datos personales que trata en el ejercicio de sus funciones y atribuciones, conforme a las finalidades establecidas, **las cuales deben ser informadas previamente en los avisos de privacidad a las personas titulares**.

Al interior del sujeto obligado, son (responsables) los órganos y personas servidoras públicas, así como toda persona o institución ajena al Instituto que esté vinculada con el tratamiento de datos personales que realice este.

TEEMICH
TRIBUNAL ELECTORAL DEL ESTADO
MICHOACÁN

ANEXO ÚNICO



CPELSMO: CONSTITUCIÓN POLÍTICA DEL ESTADO LIDBRE Y SOBERANO DE MICHOACÁN DE OCAMPO; **CE:** CÓDIGO ELECTORAL DE MICHOACÁN DE OCAMPO.
RI: REGLAMENTO INTERIOR DEL TRIBUNAL.
NOTA 1: LA ESTRUCTURA DE CADA MAGISTRATURA ELECTORAL FUE DESIGNADA POR SU TITULAR CONFORME AL ACUERDO DE PLENO TEEM-AD-04/2023.
NOTA 2: EL PRESENTE DOCUMENTO REPRESENTA UNICAMENTE PUESTOS A PARTIR DEL NIVEL DE JEFE DE DEPARTAMENTO O SU EQUIVALENTE CONFORME A LOS LINEAMIENTOS TÉCNICOS GENERALES PARA LA PUBLICACIÓN, HOMOLOGACIÓN Y ESTANDARIZACIÓN DE LA INFORMACION DE LAS OBLIGACIONES ESTABLECIDAS EN LA LEY DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA.
NOTA 3: LA MAGISTRATURA EN FUNCIONES SE SUSTENTA EN EL ACUERDO TEEM-AP-01/2025.

¿Qué es un SUJETO OBLIGADO?

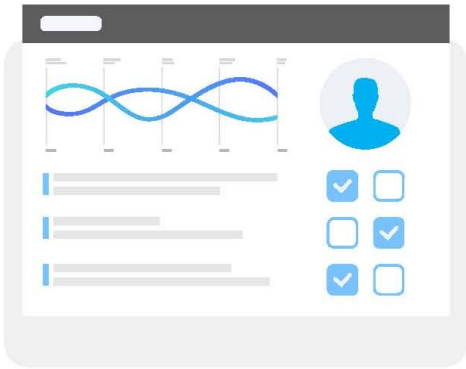
Son aquellos que deben **informar sobre sus acciones** y justificarlas.

Poderes:Ejecutivo, Legislativo y Judicial, Órganos Autónomos, Partidos Políticos, Fondos Públicos Estatales y Municipales, Administración Pública Municipal, Persona física, jurídico colectiva o Sindicato.

Obligaciones de un Sujeto Obligado

- Comité de Transparencia.
- Designar a los Titulares.
- Proporcionar capacitación continua.
- Constituir y mantener actualizados los sistemas de información.
- Promover la generación de documentos y su publicación en datos abiertos.
- Proteger y resguardar la Información.
- Informar al Instituto actividades en materia de transparencia.
- Atender oportunamente los requerimientos
- Fomentar el uso de tecnologías de la información.
- Cumplir las resoluciones emitidas por el Instituto.
- Difundir información de interés público.
- Asegurar la protección de los datos personales
- Informar de manera anual al Instituto las actividades realizadas.
- Procurar condiciones de accesibilidad para personas con discapacidad.
- Crear herramientas para consulta de información.
- Publicar información correspondiente a recursos públicos.
- Garantizar y respetar el derecho de acceso a la información pública.
- Proporcionar información a personas con discapacidad.
- Generar estadísticas de su información
- Documentar actividades.
- Orientar y asesorar el derecho de acceso a la información.

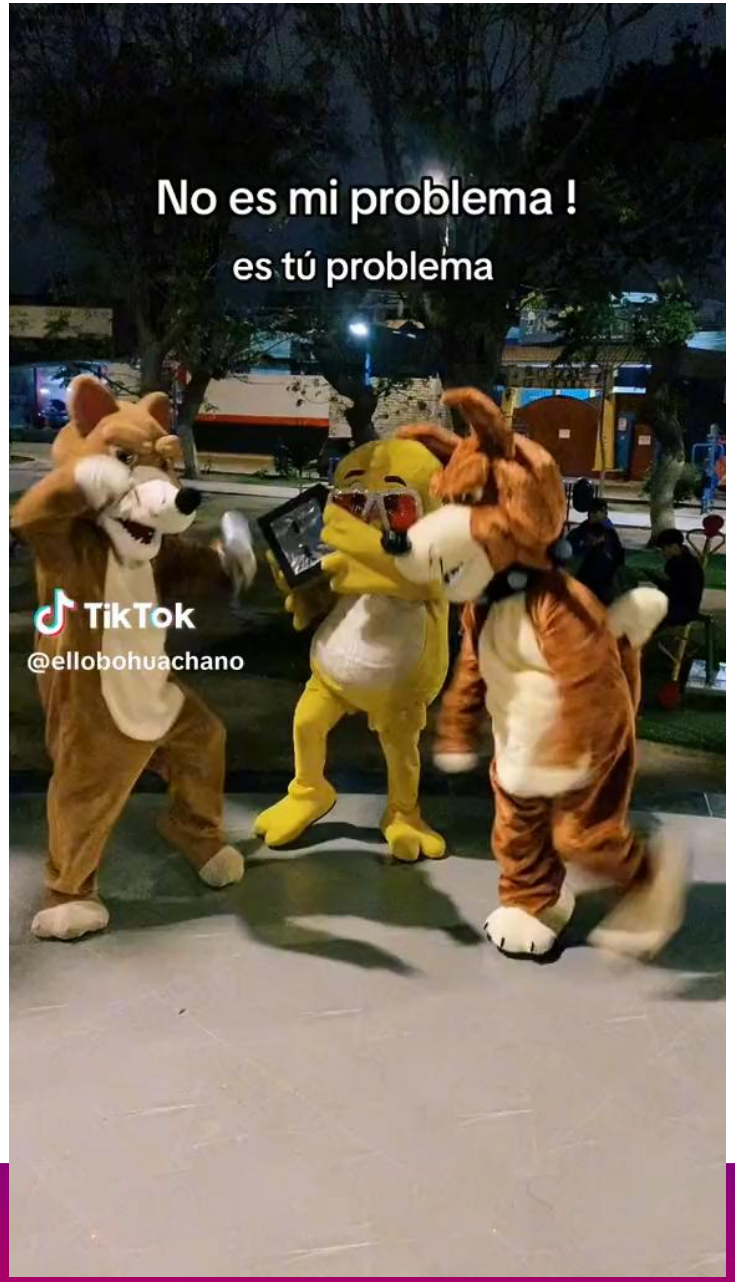
¿Qué es lo **primero que debo** hacer si soy SUJETO OBLIGADO?



- Realizar un Nombramiento para el Titular de la Unidad de Transparencia.
- Se deberá realizar la Integración del Comité de Transparencia y su respectivo registro ante el Infoem.
- Saber cuáles son las Obligaciones comunes y específicas en materia de Transparencia.
- Saber que fracciones de la Ley local les aplican.
- Solicitar a OGI Infoem la cuenta de correo institucional.
- Identificar a los servidores públicos habilitados de cada unidad administrativa que atenderá las solicitudes.
- Dar atención y seguimiento de solicitudes de información.
- Identificar el tipo de información que existe (confidencial y reservada).

NUESTRAS ASIGNATURAS EN MATERIA DE PDP

ENTONCES ¿QUIÉN ES EL RESPONSABLE DE LAS ASIGNATURAS PARA LA PROTECCIÓN DE LOS DATOS PERSONALES DEL SO?



En palabras de Crompton y Trovato: **“La privacidad ya no puede ser sólo un problema de cumplimiento. El manejo de información personal tiene implicaciones financieras, legales, estratégicas y de riesgo”*,** por lo que la protección de datos personales es reconocida como una materia transversal. Esto implica que la organización debe:

- **Considerarla y aplicarla** en todas las áreas y procesos internos, así como en las actividades diarias, sin importar su tamaño o sector.

- **Integrarla** en todos los aspectos de las operaciones, desde la cultura organizacional y las políticas hasta los procedimientos y la capacitación del personal.

**M. Crompton y M. Trovato (2018). The New Governance of Data and Privacy: Moving beyond Compliance to Performance. Australian Institute of Company Directors. Edición de Kindle.*

La transversalidad de la protección de datos personales involucra una serie de aspectos clave a ser considerados, entre los que destacan:

1. Concientización y capacitación. Todo el personal de la organización debe estar consciente de la importancia de proteger los datos personales y procurar buenas prácticas en su manejo. Esto se logra a través de la concientización y la capacitación.

2. Implementación de políticas y procedimientos. Se deben establecer políticas y procedimientos claros en relación con la protección de datos personales. Estos instrumentos deben ser comunicados y entendidos por todas las personas que integran la organización, e implementados de manera consistente en todas las áreas.

3. Evaluación de riesgos. Se deben evaluar los riesgos en todos los procesos de negocio que traten datos personales, identificar medidas de mitigación y garantizar el cumplimiento de los principios de protección de datos, esto mediante la ejecución de evaluaciones de impacto en la materia para identificar y gestionar los riesgos y las vulnerabilidades potenciales.

Áreas

- Áreas: Las instancias que cuentan o puedan contar con la información. Tratándose del sector público, serán aquellas que estén previstas en el reglamento interior, estatuto orgánico respectivo o equivalente y tratándose de las personas físicas o morales que reciban y ejerzan recursos públicos o realicen actos de autoridad, serán aquellas que sean integrantes de la estructura de los sujetos obligados a la que se le confieren atribuciones específicas en materia de transparencia y acceso a la información.

Unidad de Transparencia

I. Recabar y difundir la información a que se refiere el Título Segundo, capítulos I y II de esta Ley y propiciar que las Áreas la actualicen periódicamente, conforme la normatividad aplicable;

II. **Recibir y dar trámite a las solicitudes de acceso a la información**;

III. Auxiliar a los particulares en la elaboración de solicitudes de acceso a la información y, en su caso, orientarlos sobre los sujetos obligados competentes conforme a la normatividad aplicable;

IV. Realizar los trámites internos necesarios para la atención de las solicitudes de acceso a la información;

V. Efectuar las notificaciones a los solicitantes;

VI. **Proponer al Comité de Transparencia los procedimientos internos que aseguren la mayor eficiencia en la gestión de las solicitudes de acceso a la información, conforme a la normatividad aplicable;**

VII. Proponer personal habilitado que sea necesario para recibir y dar trámite a las solicitudes de acceso a la información;

VIII. Llevar un registro de las solicitudes de acceso a la información, respuestas, resultados, costos de reproducción y envío;

IX. **Promover e implementar políticas de transparencia proactiva procurando su accesibilidad;**

X. Fomentar la transparencia y accesibilidad al interior del sujeto obligado;

XI. Hacer del conocimiento de la instancia competente la probable responsabilidad por el incumplimiento de las obligaciones previstas en la presente Ley y en las demás disposiciones aplicables; y,

XII. Las demás que se desprendan de la normatividad aplicable.

Los sujetos obligados promoverán acuerdos con instituciones públicas especializadas que pudieran auxiliarles a entregar las repuestas a solicitudes de información, en la lengua indígena, braille o cualquier formato accesible correspondiente, en forma más eficiente.

Comité de Transparencia

I. Instituir, coordinar y supervisar, en términos de las disposiciones aplicables, las acciones y los procedimientos para asegurar la mayor eficacia en la gestión de las solicitudes en materia de acceso a la información;

II. **Confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las Áreas de los sujetos obligados;**

III. **Ordenar, en su caso, a las Áreas competentes que generen la información que derivado de sus facultades, competencias y funciones deban tener en posesión o que previa acreditación de la imposibilidad de su generación, exponga, de forma fundada y motivada, las razones por las cuales, en el caso particular, no ejercieron dichas facultades, competencias o funciones;**

IV. Establecer políticas para facilitar la obtención de información y el ejercicio del derecho de acceso a la información;

V. **Promover la capacitación y actualización de los Servidores Públicos o integrantes adscritos a las Unidades de Transparencia;**

VI. **Establecer programas de capacitación en materia de transparencia, acceso a la información, accesibilidad y protección de datos personales, para todos los Servidores Públicos o integrantes del sujeto obligado;**

VII. Recabar y enviar al organismo garante, de conformidad con los lineamientos que estos expidan, los datos necesarios para la elaboración del informe anual;

VIII. **Solicitar y autorizar la ampliación del plazo de reserva de la información a que se refiere la presente Ley**; y,

IX. Las demás que se desprendan de la normatividad aplicable.

ÁREAS

- Áreas: Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales.
- Emiten el pronunciamiento relativo a la procedencia de los derechos ARCO, a la inexistencia y/o incompetencia.
- Mantienen estricto control sobre los datos personales que obren en sus archivos, teniendo prohibido difundir o realizar un uso no autorizado de los datos personales, incluso finalizado el tratamiento.
- **Fundamento: Artículo 3, fracción I de la LPDPPSOEM.**

UNIDAD DE TRANSPARENCIA

I. Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales;

II. Gestionar las solicitudes para el ejercicio de los derechos ARCO;

III. Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados;

IV. Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, con base en lo establecido en las disposiciones normativas aplicables;

V. Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;

VI. Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO; y,

VII. Asesorar a las áreas adscritas al responsable en materia de protección de datos personales.

Fundamento: Artículos 80 de la LPDPPSOEM

OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

Tiene las siguientes atribuciones:

I. Asesorar al Comité de Transparencia respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales;

II. Proponer al Comité de Transparencia políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley y los presentes Lineamientos;

III. Implementar políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley y los presentes Lineamientos, previa autorización del Comité de Transparencia;

IV. Asesorar permanentemente a las áreas adscritas al responsable en materia de protección de datos personales; y,

V. Las demás que determine el responsable y la normatividad que resulte aplicable.

Fundamento: Artículos 80 de los Lineamientos de la LPDPPSOEM

OTRAS FUNCIONES DEL OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

• Trabajar con los equipos de tecnologías de la información (TI) y seguridad para auditar los sistemas de TI existentes, e identificar dónde se almacenan los datos personales y cómo pueden verse comprometidos.

• Vigilar los programas de capacitación y trabajar con otros para garantizar que los trabajadores comprendan los pormenores del cumplimiento de la Ley General.

• Evaluar las prácticas de recopilación y gestión de datos de la organización, recomendar procedimientos de capacitación, cumplimiento y documentar el proceso.

• Recibir quejas de personas y autoridades, por lo que tienen interés en garantizar que todos hagan su parte.

• Informar y asesorar a la organización y a los servidores públicos que laboran en ellas, sobre el cumplimiento de sus obligaciones en el tratamiento de datos personales.

• Monitorear el cumplimiento, incluida la gestión de las actividades internas de protección de datos, aconsejar sobre las evaluaciones de impacto de la protección de datos, capacitar al personal y realizar auditorías internas.

• Ser el primer punto de contacto para las consultas individuales y de otras autoridades

COMITÉ DE TRANSPARENCIA

I. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;

II. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;

III. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO;

IV. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;

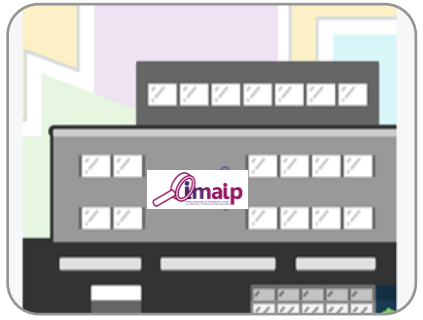
V. Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;

VI. Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto;

VII. Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales; y,

VIII. Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales; particularmente en casos relacionados con la declaración de inexistencia que realicen los responsables.

Fundamento: Artículo 79 de la LPDPPSOEM.

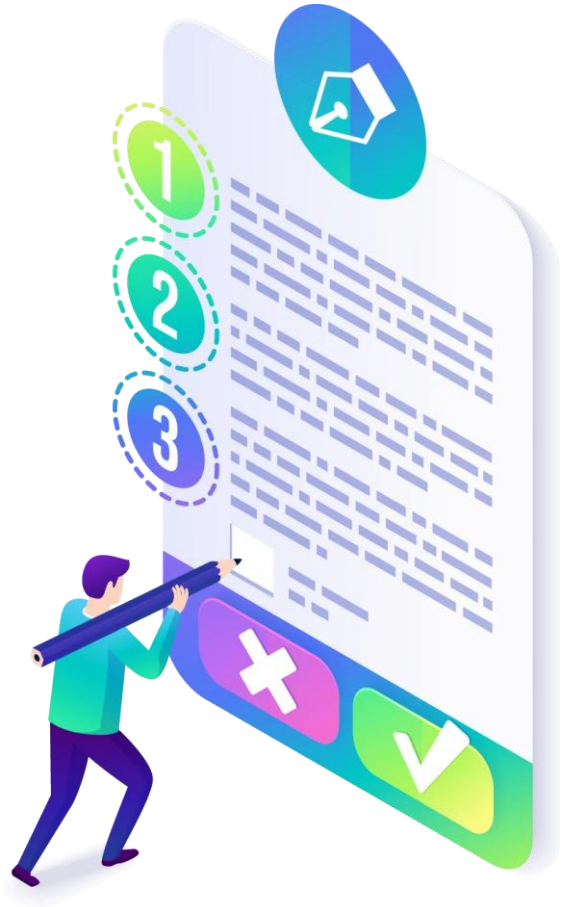


ORGANISMOS GARANTES

En materia de protección de datos personales existe un organismo garante para la federación con alcance nacional y 32 organismos estatales, correspondientes a cada una de las entidades federativas.

Manos
a la obra

ELABORACIÓN DE AVISOS DE PRIVACIDAD DE LOS DE DATOS PERSONALES RECABADOS EN LA INSTITUCIÓN EDUCATIVA.



Guía de Trámites y Servicios

Consulta los distintos Trámites y Servicios que ofrece el municipio de Morelia a través de sus Dependencias.
Selecciona el trámite de la lista y/o escribe por el nombre del trámite que buscas.

Buscar por nombre del trámite o Dependencia

Agricultura, ganadería y **pesca**
Agua
Alumbrado **público**
Aseo
Atención **animal**
Capacitaciones
Catastro
Construcción
Cultural
Deportes
Desarrollo **económico**
Desarrollo **rural**
Educación, ciencia y **tecnología**
Familia
Identidad
Jóvenes
Legalidad y **justicia**
Medio **ambiente**
Mercados
Movilidad
Niños
Obras **públicas**
Pagos e **impuestos**
Panteones
Parques y **jardines**
Personas con **discapacidad**
Policía **Morelia**
Programas **sociales**
Protección **civil**
Rastro
Servicios **públicos**
Social
Turismo
Área de la **Salud**
Desarrollo **urbano**

De conformidad con el artículo 102 del Reglamento de Mejora Regulatoria del Municipio de Morelia, la legalidad y el contenido de la información que se inscriba en el Catálogo serán de estricta responsabilidad de los Sujetos Obligados.

Consulta los distintos Trámites y Servicios que ofrece el municipio de Morelia a través de sus Dependencias.
Selecciona el trámite de la lista y/o escribe por el nombre del trámite que buscas.

Ver las categorías (Imágenes)

Buscar por categoría Todas

Buscar en la Dependencia (UPP) Todas

Buscar en la Dirección (UR) Seleccionar UPP

Buscar por nombre del Trámite o Servicio Buscar

Se encontraron 387

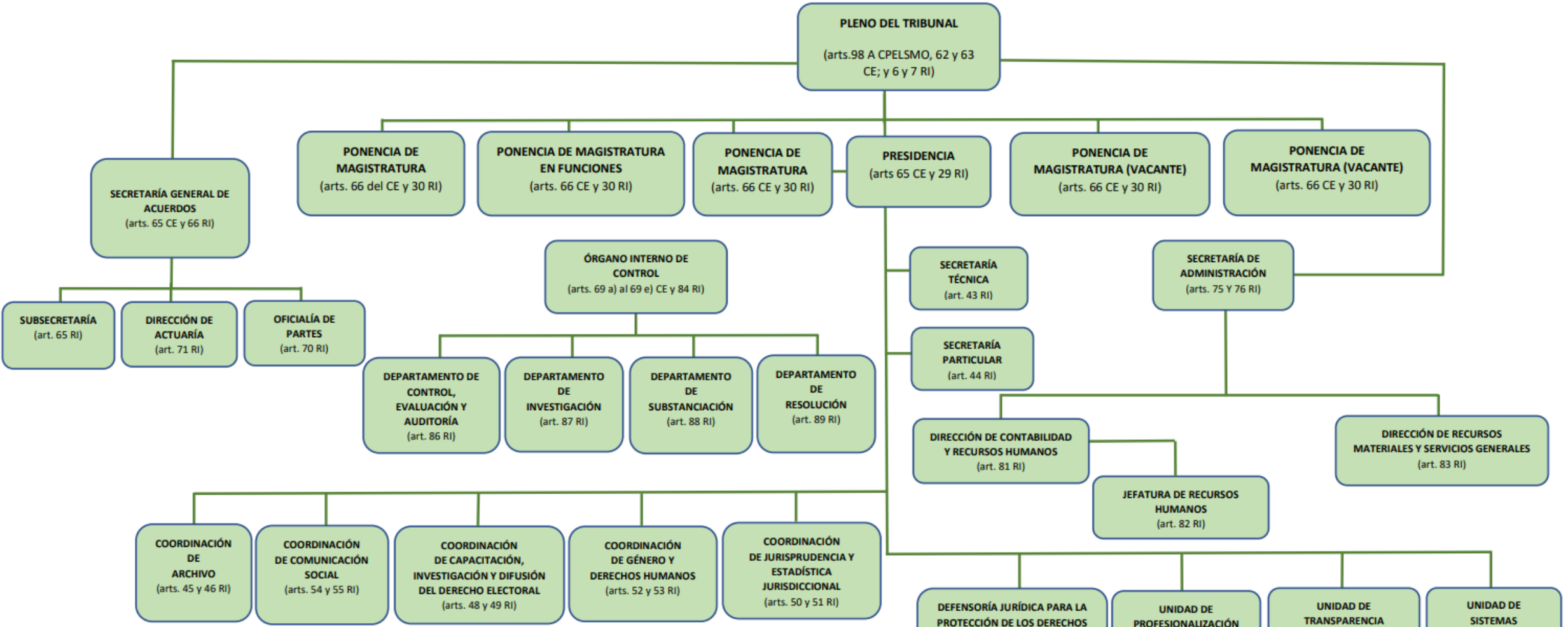
LISTADO DE TRÁMITES Y SERVICIOS
ACLARACIONES DE NOMENCLATURA
ACUERDO DE ASAMBLEA DE RECONOCIMIENTO DE AVECINDADO EN EL EJIDO O COMUNIDAD
ACUERDO DE ASAMBLEA PARA LA DELIMITACIÓN, DESTINO Y ASIGNACIÓN DE TIERRAS
ADOPCIÓN DE EJEMPLARES CANINOS Y FELINOS
APARATOS FUNCIONALES
APERTURA DE LISTA DE SUCESIÓN DE EJIDATARIO A COMUNERO
APOYO ALIMENTARIO
APOYO DE LENTES
APOYO DE MEDICAMENTOS
APOYO PARA EL MEJORAMIENTO DE LA VIVIENDA.
APOYOS CON VALES (MEDICAMENTOS, ESTUDIOS DE LABORATORIO)
APOYOS ECONÓMICOS
APOYOS SOCIALES CON MAQUINARÍA DE LA SECRETARÍA DE OBRAS PUBLICAS MUNICIPALES
APOYOS SOCIALES CON MATERIAL DE CONSTRUCCIÓN DE LA SECRETARIA DE OBRAS PUBLICAS MUNICIPALES
APOYOS VARIOS (LECHE, PAÑALES, MATERIAL DE CURACIÓN, MATERIAL QUIRÚRGICO)
APROBACION DE REGLAMENTOS DE CONDOMINIO
ARRENDAMIENTO DE ESPACIOS
ASESORÍA ESPECIALIZADA EN MATERIA DE PLANEACION (POR HORA O FRACCIÓN, NO INCLUYE VIÁTICOS)
ASESORÍA FINANCIERA (CRÉDITOS PARA MIPYMES)
ASESORÍA PARA DESARROLLO DE MARCA "MI MARCA"
ASESORIAS JURIDICAS
ATENCION A PROVEEDORES Y CONTRATISTAS DEL MUNICIPIO DE MORELIA
ATENCIÓN A REPORTES DE MALTRATO ANIMAL PERROS Y GATOS
ATENCIÓN A REPORTES DE PERROS AGRESORES
ATENCIÓN A VÍCTIMAS DEL DELITO
ATENCIÓN DE REPORTES CIUDADANOS POR ABANDONO DE RESIDUOS SÓLIDOS EN LA VÍA PÚBLICA
ATENCIÓN DENTAL
ATENCIÓN MÉDICA
ATENCIÓN MÉDICA (SALUD SEXUAL Y REPRODUCTIVA)

Se encontraron 387

https://www.morelia.gob.mx/servicios-del-portal/tramites-y-servicios/guia-de-tramites/

TEEMICH
TRIBUNAL ELECTORAL DEL ESTADO
MICHOACÁN

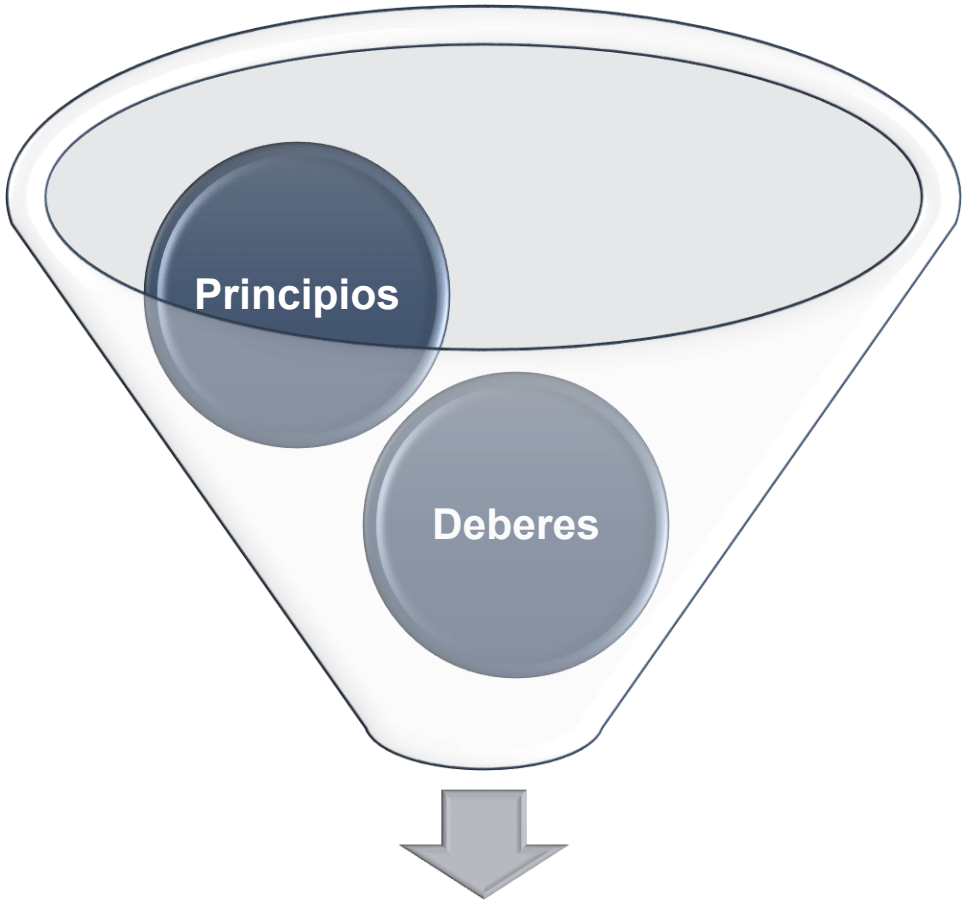
ANEXO ÚNICO



CPELSMO: CONSTITUCIÓN POLÍTICA DEL ESTADO LIDBRE Y SOBERANO DE MICHOACÁN DE OCAMPO; **CE:** CÓDIGO ELECTORAL DE MICHOACÁN DE OCAMPO.
RI: REGLAMENTO INTERIOR DEL TRIBUNAL.
NOTA 1: LA ESTRUCTURA DE CADA MAGISTRATURA ELECTORAL FUE DESIGNADA POR SU TITULAR CONFORME AL ACUERDO DE PLENO TEEM-AD-04/2023.
NOTA 2: EL PRESENTE DOCUMENTO REPRESENTA UNICAMENTE PUESTOS A PARTIR DEL NIVEL DE JEFE DE DEPARTAMENTO O SU EQUIVALENTE CONFORME A LOS LINEAMIENTOS TÉCNICOS GENERALES PARA LA PUBLICACIÓN, HOMOLOGACIÓN Y ESTANDARIZACIÓN DE LA INFORMACION DE LAS OBLIGACIONES ESTABLECIDAS EN LA LEY DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA.
NOTA 3: LA MAGISTRATURA EN FUNCIONES SE SUSTENTA EN EL ACUERDO TEEM-AP-01/2025.

La Ley General y Local establece las bases, principios y procedimientos para garantizar el derecho de toda persona a la protección de sus datos personales, en posesión de los sujetos obligados. Y regular el tratamiento legítimo, controlado e informado de los datos personales, para garantizar así la privacidad de las personas y la protección de su información personal.

Este tratamiento legítimo, controlado e informado de los datos personales **se basa en principios y deberes que los responsables deben observar en el tratamiento de los datos personales.** En concreto, los principios y deberes se convierten en obligaciones concretas para el responsable, que tiene que cumplir, así como hacer cumplir, en cada una de las fases del tratamiento.



Tratamiento lícito y legítimo de datos personales

En ese sentido, se debe considerar, al menos, lo siguiente:

- ¿De dónde se obtienen los datos personales? (A través del titular, transferencias, fuentes de acceso público, etcétera)
- Unidades administrativas de los sujetos obligados que recaban y/o tratan datos personales.
- En específico qué servidores públicos, empleados o personas recaban y/o tratan datos personales.
- Las finalidades del tratamiento (para qué se utilizan los datos personales)
- En su caso, con quién y para qué se comparten datos personales (encargados o terceros)
- En dónde y cómo se almacenan los datos personales (lugar físico, como archiveros; o electrónico, como computadoras, servidores, entre otros).
- ¿Qué procedimientos, mecanismos y tecnología utilizan en el tratamiento?
- ¿Cuánto tiempo se conservan los datos personales?

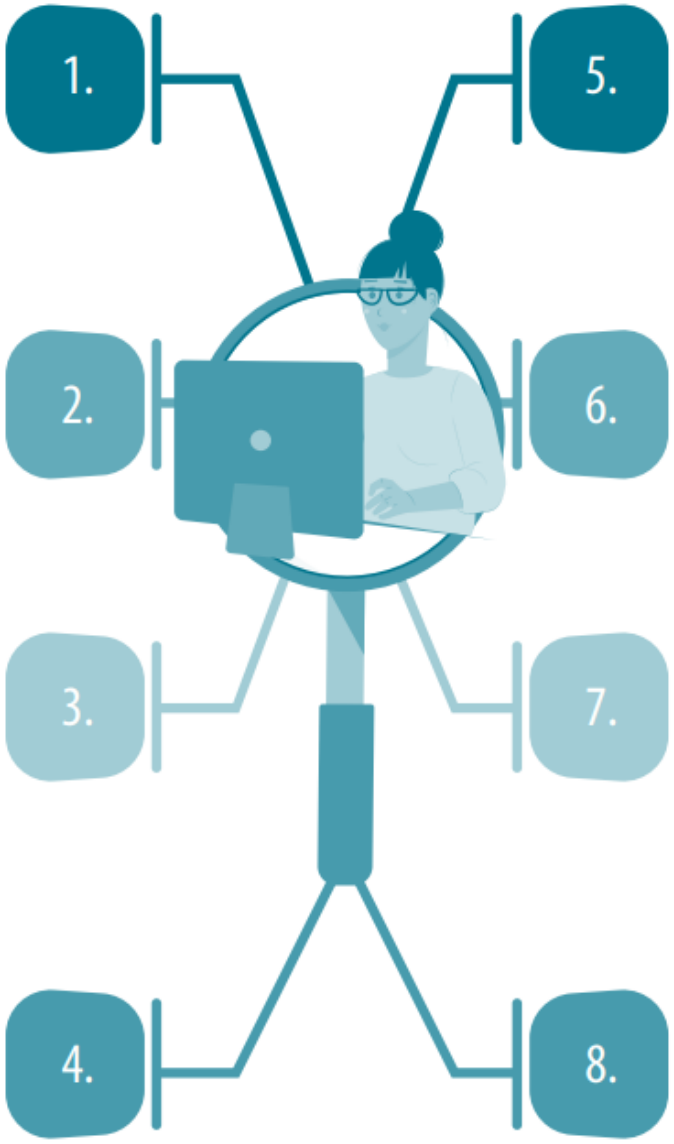
Los principios que rigen el tratamiento de los datos personales

Licitud
Tratar los datos de conformidad con las facultades y atribuciones, atendiendo a la normatividad.

Finalidad
Tratar los datos personales con un propósito concreto, lícito, explícito, legítimo y acorde con las atribuciones. Se debe limitar a lo establecido en el aviso de privacidad.

Lealtad
La obtención de los datos debe realizarse sin el uso de medios engañosos o fraudulentos.

Consentimiento
El titular debe otorgar su autorización para el tratamiento de sus datos de manera libre, específica e informada.



Calidad
Los datos deben ser exactos, completos y actualizados.

Proporcionalidad
Los datos tratados deben ser adecuados, relevantes y necesarios para cumplir con la finalidad.

Información
Informar al titular sobre el tratamiento de sus datos mediante el aviso de privacidad.

Responsabilidad
Establecer medidas para el cumplimiento de los principios y deberes; contar con evidencia del cumplimiento.

El plazo de conservación de los datos personales no debe exceder el tiempo estrictamente necesario para llevar a cabo las finalidades que justificaron el tratamiento, ni aquél que se requiera para cumplir con:

- Las disposiciones legales aplicables en la materia de que se trate;
- Los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información, y
- El periodo de bloqueo.

Entonces tenemos que:

Plazo de conservación= *Tiempo requerido para llevar a cabo las finalidades del tratamiento + plazos legales, administrativos, contables, fiscales, jurídicos e históricos aplicables + periodo de bloqueo*.

En algunos casos estos tres tiempos o plazos pueden coincidir.

7. PRINCIPIO DE INFORMACIÓN.

El Responsable está obligado a informar sobre la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a través del **aviso de privacidad,** a fin de que pueda tomar decisiones informadas al respecto.

¿Qué es un Aviso de Privacidad?

Documento que se debe poner a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

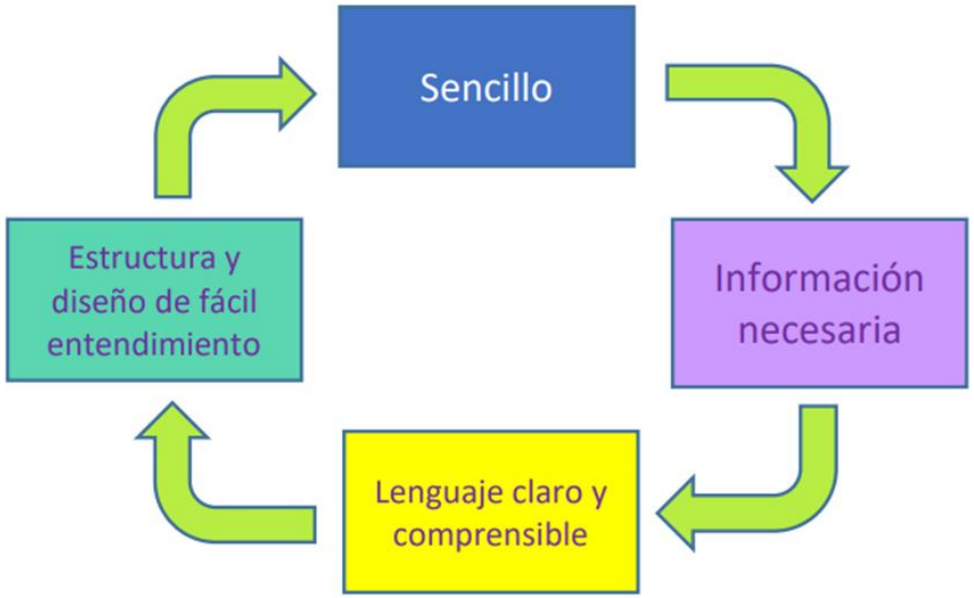
¿PARA QUÉ SIRVE EL AVISO DE PRIVACIDAD?

Para establecer y delimitar el alcance, términos y condiciones del manejo de los datos personales

El titular puede tomar decisiones referente a sus datos personales y mantener el control y disposición de su información

Fortalece el nivel de confianza del titular con relación a la protección de sus datos.

¿Qué características debe tener un aviso de privacidad?



¿Cuántos avisos de privacidad debo tener?

Los responsables **deben tener el número de avisos de privacidad que resulten necesarios de acuerdo con los tipos de tratamientos que realicen.**

Por ejemplo, se deberá elaborar un aviso de privacidad para el tratamiento relativo al personal del responsable y otro para las personas que acuden al sujeto obligado.

Lo anterior implica que en el aviso de privacidad se deberá:

- Abstener de usar frases inexactas, ambiguas o vagas;
- Tomar en cuenta el perfil de los titulares para su redacción;
- No incluir textos o formatos que induzcan al titular a elegir una opción en específico;
- No remitir al titular a textos y documentos que no estén disponibles; y
- No incluir casillas que estén marcadas previamente.

¿A través de qué medios puede difundirse o reproducirse el aviso de privacidad?

El aviso de privacidad podrá difundirse, ponerse a disposición o reproducir en formatos físicos y electrónicos, ópticos, sonoros, visuales o a través de cualquier otra tecnología que permita su eficaz comunicación.

En todo caso, el aviso de privacidad deberá estar ubicado en un lugar visible y que facilite su consulta. Esto último también tiene como finalidad acreditar ante el instituto el cumplimiento de su obligación.

Algunos ejemplos de medios para difundir el aviso de privacidad son los siguientes:

TIPO DE FORMATO	EJEMPLO
Físicos	Carteles o impresiones en papel
Electrónicos o digitales	En una página de Internet o pantallas Electrónicas
Ópticos o visuales	Videos o versión en caricatura
Sonoros	Grabación telefónica
Otro formato	Braille

¿El responsable está obligado a demostrar la puesta a disposición del aviso de privacidad?

Los responsables están obligados a comprobar o demostrar que han puesto a disposición del titular el aviso de privacidad y que el mismo cumple con los requisitos que al efecto establece la Ley, su Reglamento y los Lineamientos, a través de los medios que estime pertinentes, como, por ejemplo, fotografías, grabaciones telefónicas, fe de hechos o firmas de los titulares, entre otros.

Aviso de privacidad simplificado y Aviso de privacidad integral

AVISO DE PRIVACIDAD SIMPLIFICADO

- Denominación del responsable.
- Finalidades del tratamiento.
- En caso de transferencias que requieran consentimiento del titular, informar:
  - A quien se transfieren los datos personales y
  - Finalidades de la transferencia.
- Medios para que el titular manifieste su negativa al tratamiento y transferencia de sus datos personales.
  Estos medios deben estar disponibles previo al tratamiento o la transferencia de los datos personales.
- Sitio para consultar el aviso de privacidad integral.

AVISO DE PRIVACIDAD INTEGRAL

Debe contener la información del simplificado y al menos:

- Domicilio del responsable.
- Datos personales sometidos a tratamiento, identificando aquellos que sean sensibles.
- Fundamento legal del tratamiento.
- Finalidades del tratamiento, señalando aquellas que requieran el consentimiento del titular.
- Mecanismos, medios y procedimientos para ejercer los derechos ARCO.
- Domicilio de la Unidad de Transparencia.
- Medios para comunicar cambios en el aviso de privacidad.

El aviso de privacidad garantiza un respeto adecuado a la autonomía de los individuos respecto a sus datos personales.

La protección de datos personales y el interés superior de niñas, niños y adolescentes

Es un principio de la Convención sobre los Derechos del Niño (CDN), cuya aplicación busca la mayor satisfacción de todas y cada una de las necesidades de niñas, niños y adolescentes. Su aplicación exige adoptar un enfoque basado en derechos que permitan garantizar el respeto y la protección a su dignidad e integridad física, psicológica, moral y espiritual.

La protección de datos personales está vinculada al principio de interés superior de niñas, niños y adolescentes para garantizar, entre otros derechos, su seguridad, así como para regir la actuación del Estado respecto a la legislación y política pública que emita para proteger la informacón de las personas menores de edad.

La Declaración Universal de los Derechos Humanos, permitió el reconocimiento de derechos que protegen la libertad individual y la defensa de la persona frente al ámbito de actuación del poder público, a través del Estado. Dichos derechos incluyen los relativos al aislamiento, entendiéndose como el derecho el derecho al honor, a la vida, a la integridad y a la intimidad de la persona.

Marco jurídico de protección de los datos personales de niñas, niños y adolescentes

Convención sobre los Derechos del Niño (Artículos 3, 8 inciso e) y 16)

Constitución Política de los Estados Unidos Mexicanos (1, 4, 6, fracción II y 16 segundo párrafo)

Ley General de Protección de los Derechos de Niñas, Niños y Adolescentes (Artículos 76 y 77)

Ley General de Protección de Datos Personales en posesión de Sujetos Obligados (Artículos 7 y 107 fracción I, último párrafo)

Ley Federal de Telecomunicaciones y Radiodifusión (Artículos 222 y 223, fracción II)

¿QUÉ NOS DICE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO?

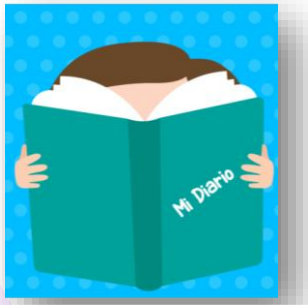
Art. 7. En el tratamiento de datos personales de menores de edad **se deberá privilegiar el interés superior de la niña, el niño y el adolescente**, en términos de las disposiciones legales aplicables.

Art. 16. En la obtención del **consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley,** se estará a lo dispuesto en las reglas de representación previstas en la legislación civil que resulte aplicable.

Art. 45. En el ejercicio de los **derechos ARCO de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad**, de conformidad con las leyes civiles, se estará a las reglas de representación dispuestas en la misma legislación.

Ley de los Derechos de Niñas, Niños y Adolescentes del Estado de Michoacán.

Niñas, niños y adolescentes tienen derecho a la **intimidad** en su vida privada y en la de su familia, domicilio o correspondencia y a la protección de sus datos personales.



Niñas, niños y adolescentes no podrán ser objeto de injerencias (sic) arbitraria o ilegales en su vida privada, su familia, su domicilio o su correspondencia; de divulgaciones o difusiones ilícitas de información o datos personales, incluyendo aquélla que tenga carácter informativo a la opinión pública o de noticia que permita identificarlos, que atente contra su honra, imagen o reputación.

Quienes ejerzan la patria potestad, tutela o guardia y custodia, deberán orientar, supervisar y, en su caso, restringir las conductas y hábitos de niñas, niños y adolescentes, siempre que atiendan al interés superior de la niñez.

Cualquier persona, autoridad o medio de comunicación local <u>que difunda entrevistas, imágenes, voz o datos</u> deberán atender lo establecido en la Ley General, cuidando en todo momento el desarrollo integral de niñas, niños y adolescentes.

En caso de incumplimiento se promoverán las acciones civiles, denuncias, querellas y procedimientos de conformidad con las leyes Civil, Penal y Administrativa del Estado de Michoacán y demás disposiciones jurídicas aplicables.

Consentimiento en datos personales sensibles.

En caso de que se requiera el consentimiento del titular para el tratamiento de datos personales sensibles por no actualizarse alguna de las causales de excepción previstas en el *artículo 10 de la Ley Federal*, el responsable está obligado a obtener dicho consentimiento de manera expresa y por escrito, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación.

Recomendaciones para proteger los datos personales de niñas, niños y adolescentes

Al tomar fotografías a menores de edad, se recomienda tomarlas de espaldas o de perfil. Si se hacen tomas de frente, deberán difuminarse los rostros para la publicación de las mismas.

Se recomiendan no publicar datos como: nombre, domicilio, edad, nombre de la escuela o cualquier otro dato que haga identificable al menor.

Evitar realizar registros de datos personales de los asistentes y/o participantes menores de edad en actividades llevadas a cabo al interior de la institución.

Se recomienda que si se trata de una premiación o entrega de reconocimientos, se deberá solicitar el consentimiento de los padres o tutores de los menores que resulten ganadores, el cual deberá ser acorde a las finalidades establecidas en el Aviso de Privacidad. Dicho consentimiento, deberán suscribirlo ambos padres, su tutor o el padre que por disposición de una autoridad ejerza la patria potestad para que el menor de edad pueda ser publicado en el material fotográfico, video, redes sociales y/o cualquier otro medio de comunicación o difusión.

Los medios de comunicación deberán asegurarse que las imágenes, voz o datos a difundir, no pongan en peligro, de forma individual o colectiva la vida, integridad, dignidad o vulnere el ejercicio de derechos de niñas, niños y adolescentes.

Cualquier medio de comunicación o institución que difunda entrevistas de niñas, niños y adolescentes, deberá recabar el consentimiento expreso y por escrito de los padres, tutores, o de quien ejerza la patria potestad de los menores; así como la opinión de la niña, niño o adolescente respectivamente.

En los eventos escolares, extra escolares o en aquel donde el motivo del mismo sean los menores de edad, el maestro de ceremonias deberá hacer lectura del Aviso de Privacidad sobre la toma de fotografías y videos a los menores; exhortando a los padres de familia a tomar las precauciones pertinentes para no fotografiar a otros menores sin el consentimiento de sus padres; así como de tener el cuidado de no publicar en sus redes sociales u otros medios electrónicos a los menores sin dicha autorización. Asimismo deberá hacer hincapié a los fotógrafos, periodistas o representantes de los medios de comunicación presentes, de no publicar imágenes o datos de los menores, sin el consentimiento de sus padres.

Manos
a la obra

ELABORACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES.

Deberes que señala la LPDPPSOEM

Deber de Seguridad: El responsable deberá de establecer y mantener las medidas de seguridad necesarias para la protección de los datos personales, **que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso acceso o tratamiento no autorizado o ilícito,** así como garantizar los principios y obligaciones de la ley.

Deber de Confidencialidad: Consiste en que la información no se pone a disposición, no se revela a individuos o entidades sin el consentimiento del titular del dato personal; siendo responsable el encargado o los usuarios autorizaos los únicos que pueden llevar a cabo el tratamiento de los datos personales.

Deber de Seguridad

Independientemente del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener **las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales,** que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Medidas de seguridad:

Conjunto de acciones, actividades, controles o mecanismos administrativos, técnico y físicos que permiten proteger los datos personales.

Medidas de seguridad administrativas

Se refieren al establecimiento de políticas y procedimientos para:

a) La gestión, soporte y revisión de la seguridad de la información a nivel organizacional;

b) La identificación, clasificación y borrado de la información.

Medidas de seguridad técnicas

Se refieren al establecimiento de políticas y procedimientos para:

- Asegurar que el acceso a las bases de datos sea por usuarios identificados y autorizados;
- Generar privilegios o perfiles de acceso a los datos personales en función de las atribuciones y funciones de cada usuario.
- Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- Revisar la configuración de seguridad del software y hardware;
- Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Medidas de seguridad físicas

Se refieren al establecimiento de políticas y procedimientos para:

- Prevenir el acceso no autorizado al perímetro de la organización, instalaciones físicas, áreas críticas, recursos e información;
- Prevenir daño o interferencia a instalaciones físicas, áreas críticas de la organización, recursos e información;
- Proteger recursos móviles, portátiles, soportes físicos o electrónicos que salgan de la organización;
- Proveer a equipos que almacenan datos personales de mantenimiento eficaz

Implementación de un sistema de gestión de seguridad de los datos personales

Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión. Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la Ley General y Local.

Documento de seguridad

De manera particular, el responsable deberá elaborar un documento de seguridad.

Documento de **SEGURIDAD** de **Datos Personales**

¿Qué es?

Es un instrumento que describe y da cuenta de las medidas de seguridad adoptadas por un responsable o sujeto obligado para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

¿Quién está obligado a tenerlo?

Los sujetos obligados, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

MARCO NORMATIVO

Los instrumentos normativos que rigen en la materia de protección de datos personales son los siguientes:

- Artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán
- Lineamientos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán

Guía de Apoyo para la elaboración del Documento de Seguridad. INAI.
https://home.inai.org.mx//wp-content/documentos/DocumentosSectorPublico/Guia-apoyo-DS.pdf

Artículos 35 de la LGPDPPSO y 31 de la LPDPPSOEMO

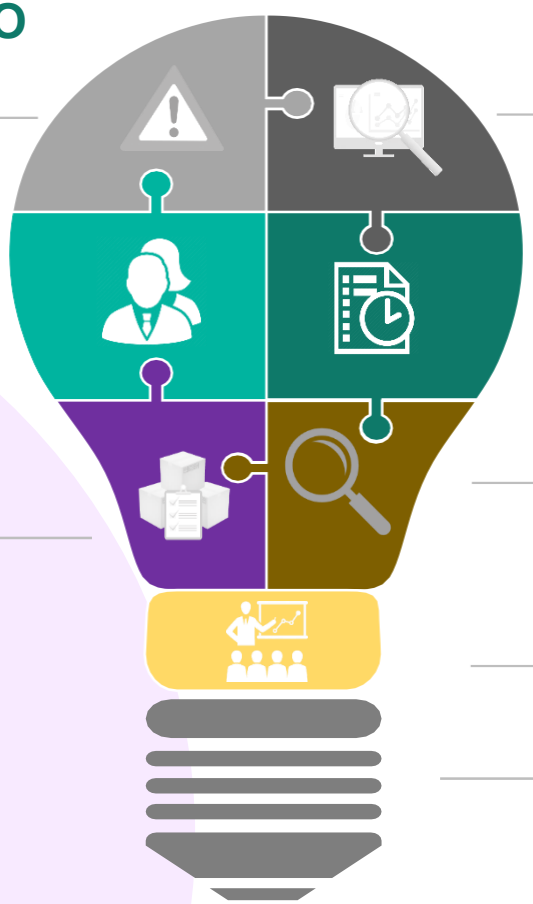
Artículos 3 fracc. XIV de la LGPDPPSO y 3 fracc. XIII de la LPDPPSOEMO

Documento de seguridad

Análisis de riesgos

Funciones y obligaciones

Inventario de datos personales



Análisis de brecha

Plan de trabajo

Mecanismos para monitoreo y revision medidas de seguridad

Programa general de capacitación

. Nombre y cargo del personal del Responsable o Encargado.

Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

Deber de confidencialidad

Es la obligación que tiene por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, **guarden confidencialidad** respecto a éstos, la cual debe subsistir aún después de finalizar sus relaciones con el sujeto obligado.

Manos
a la obra

GARANTIZAR EL EJERCICIO DE LOS DERECHOS DE LOS TITULARES.

Acceso

Es la prerrogativa que tiene la persona titular de solicitar el acceso a sus datos personales que están en las bases de datos, sistemas, archivos, registros o expedientes de cualquier instancia, así como de conocer información relacionada con el uso que se da a los datos personales.

Rectificación

Es la prerrogativa que tiene la o el titular de solicitar la corrección de sus datos personales, cuando éstos sean inexactos, incompletos o no se encuentren actualizados.

Cancelación

Es la prerrogativa que tiene la persona titular de solicitar que sus datos personales se eliminen de los archivos, registros, expedientes, sistemas, bases de datos de cualquier instancia.

Oposición

Es la prerrogativa que tiene la o el titular de solicitar que sus datos personales no se utilicen para ciertos fines, o de requerir que se concluya el uso de los mismos a fin de evitar un daño a su persona.

PORTABILIDAD DE DATOS PERSONALES

Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener una copia en un formato que le permita seguir utilizándolos.

Cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitirlos y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos.

El Sistema Nacional de Transparencia, establece en sus lineamientos los parámetros a considerar para determinar los supuestos en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales.

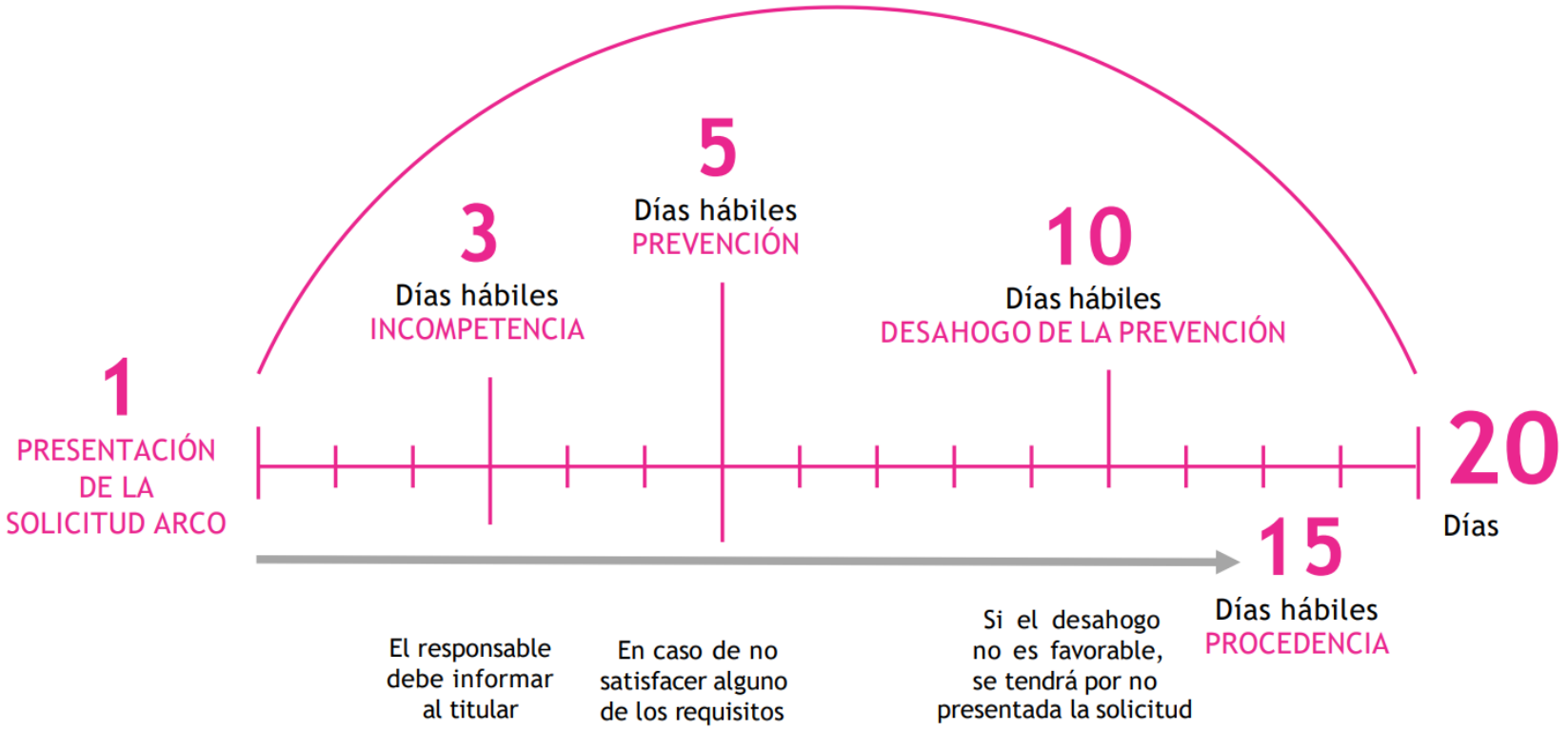
Canales para ejercer los derechos ARCO

Plataforma Nacional de Transparencia

https://www.youtube.com/watch?v=-F79Cf2aAbA

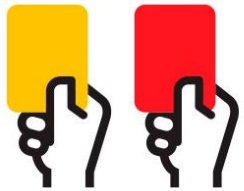
Unidades de Transparencia de los Sujetos Obligados: formatos.

RUTA CRÍTICA DEL EJERCICIO DE LOS DERECHOS ARCO



El plazo de 20 días puede ser ampliado por una sola vez hasta por diez días, siempre y cuando se justifique esta situación.

MEDIDAS DE APREMIO Y RESPONSABILIDADES.



Artículo 132. Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes:

…

III. **Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales,** que se encuentren bajo su custodia o a los cuales tenga acceso o conocimiento con motivo de su empleo, cargo o comisión;

IV. **Dar tratamiento**, de manera intencional, a los datos personales **en contravención** a los principios y deberes establecidos en la Ley;

V. **No contar con el aviso de privacidad**, o bien, omitir en el mismo alguno de los elementos a que se refiere la presente Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;

VII. **Incumplir el deber de confidencialidad** establecido en la presente Ley;

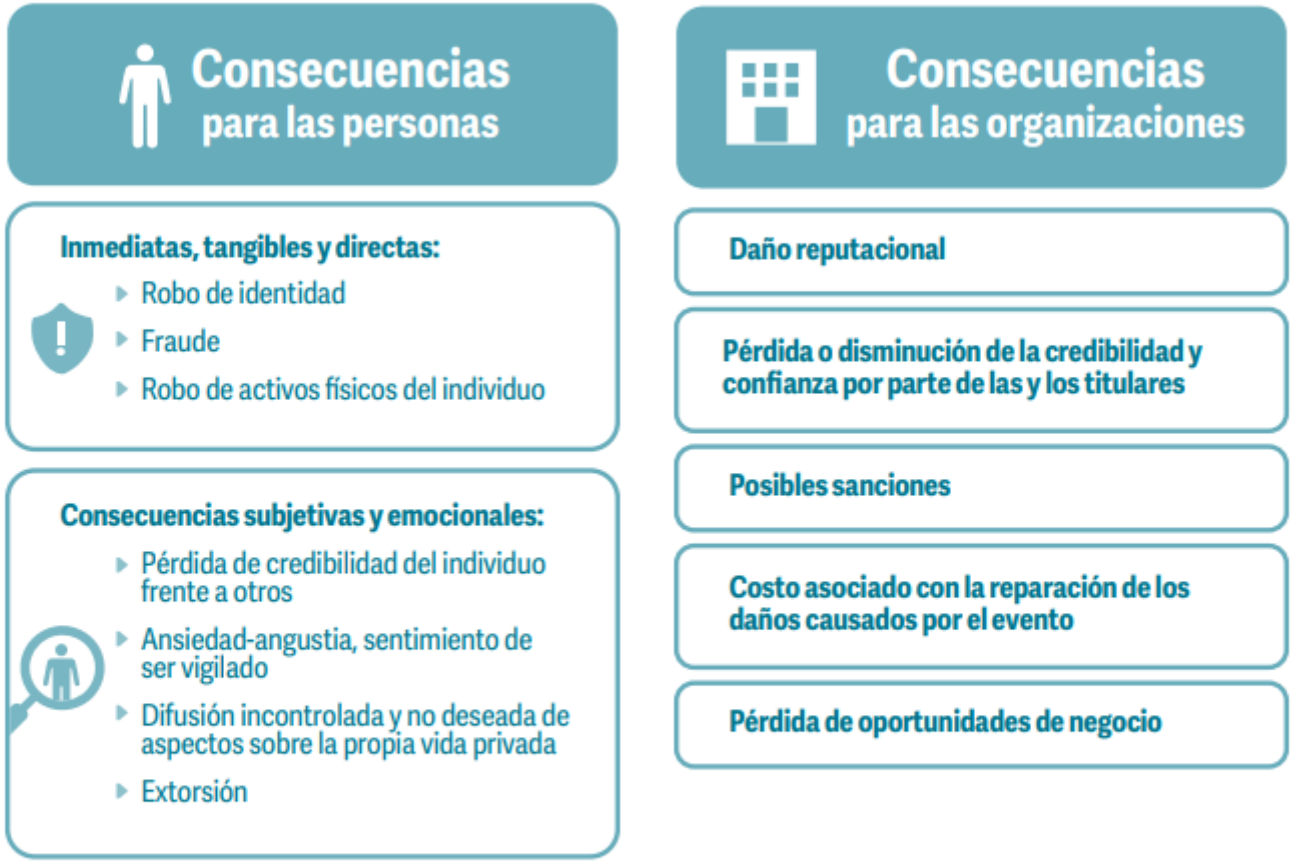
VIII. **No establecer** las medidas de seguridad en los términos establecidos en el Capítulo de los Deberes de la presente Ley;

IX. **Presentar vulneraciones** a los datos personales **por la falta de implementación** de medidas de seguridad contempladas en la presente Ley;

…

XIII. No acatar las resoluciones emitidas por el Instituto;

Ejemplos de consecuencias del incumplimiento



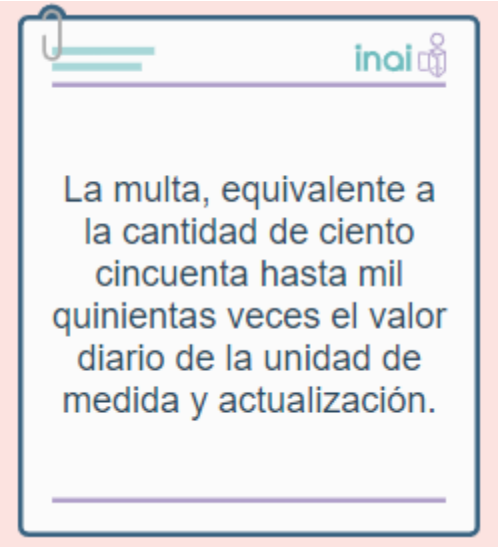
Fuente: Elaboración propia con base en S. Joyee y D. Le Métayer (2016). *Privacy Risk Analysis*. Morgan & Claypool Publishers. Edición de Kindle.

Régimen Sancionador. De las medidas de apremio

Las medidas de apremio son aplicables para asegurar el cumplimiento de las resoluciones y determinaciones tanto del INAI, como de los organismos garantes estatales, según corresponda. En caso de persistir incumplimiento, se fijan las medidas de apremio para asegurar su obediencia normativa.

Tipos de medidas de apremio

Las medidas de apremio aplicables para asegurar el cumplimiento de las resoluciones y determinaciones del Instituto son:



UMA 2025: $113.14
150 UMAS: $16,971.00
1500 UMAS: $169,710.00

El incumplimiento de los responsables se hará mediante la difusión en los portales de obligaciones de transparencia del Instituto y los organismos garantes estatales, según corresponda, considerados en las evaluaciones que estos realicen.

Acciones preventivas para la protección de datos personales.

RECOMENDACIONES PARA EL TRATAMIENTO DE DP

Antes de recabar cualquier dato personal debes dar a conocer, por medios electrónico o físicos, el Aviso de Privacidad que corresponda.

Sólo puedes solicitar o recabar los datos personales que sean indispensables para el ejercicio de tus funciones .

Al recabar el consentimiento del titular de los datos evita que medie error, mala fe, violencia o dolo.

Recuerda que la imagen de personas en fotografías o vídeos también son datos personales que deben ser tratados con apego al Aviso de privacidad respectivo.

La finalidad del tratamiento de datos personales que realices debes debe ser concreta, lícita, explícita y legítima.

En todo momento debes implementar y observar las medidas de seguridad establecidas para su protección.

Atiende en tiempo y forma las solicitudes de ejercicio de derechos ARCO respecto de los datos personales que se encuentran bajo tu resguardo.

Identifica los posibles vulneraciones que existan para el resguardo de los datos personales y comunícalos a tu superior jerárquico.

Cuando adviertas alguna modificación en el tratamiento de los datos personales, actualiza los inventarios de datos personales y los avisos de privacidad.

MEDIDAS DE SEGURIDAD FÍSICAS Y ADMINISTRATIVAS PARA LA PROTECCIÓN DE DATOS PERSONALES

- Garantizar que el acceso a los expedientes que contengan datos personales sea de acceso restringido.
- Realizar periódicamente el mantenimiento de los archiveros, cerraduras y candados.
- Considerar la digitalización y resguardo seguro de la información.
- Mantener un registro de los medios de acceso y resguardo existentes (Cantidad de equipos).
- Implementar el uso de bitácoras o registro de quiénes tienen acceso a los documentos digitales y físicos.
- Realizar revisiones periódicas de los medios de resguardo, para garantizar que se encuentren en óptimas condiciones.
- Promover la política de “escritorio limpio”, no dejando al alcance de cualquier persona documentos que contengan datos personales.
- No utilices como hojas de reciclaje, documentos que contengan datos personales.


Protección de Datos Personales |
No es seguro | imaip.org.mx/pdp/
imaip
INICIO
TRANSPARENCIA
PUBLICACIONES
SUJETOS OBLIGADOS
SOLICITUDES
MICROSITIOS
imaip
Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales
PROTECCIÓN DE DATOS PERSONALES
Inicio
¿Qué son los datos personales?
¿Cómo se clasifican los datos personales?
¿Qué son los datos personales sensibles?
¿Cómo se clasifican los datos personales sensibles?
¿Qué es la protección de los datos personales?
¿Cómo denunciar el tratamiento inadecuado de tus datos personales?
Derechos ARCOP
Ejercicio de los derechos ARCOP
¿Cómo realizo una solicitud de datos personales?
Procedimiento, plazos y
Los datos personales se clasifican en diversas categorías atendiendo a las características del dato que se trate:
Datos de identificación: Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, estado civil, firma, firma electrónica, cartilla militar, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), nombres de familiares, dependientes y/o beneficiarios.
Datos laborales: Pueden referirse a los contenidos en las solicitudes de empleo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, recomendaciones, capacitaciones, documentos de selección, reclutamiento, nombramiento, incidencias, hojas de servicio y otras generadas derivadas de nuestra relación laboral.
Datos patrimoniales: Se refiere a los bienes muebles e inmuebles, ingresos y egresos, cuentas bancarias, seguros, fianzas, afores, historial crediticio, información fiscal, servicios contratados y afines.
Datos sobre procedimientos administrativos y jurisdiccionales: Es aquella información relacionada íntimamente a nosotros, disponible en procedimientos administrativos o juicios en materia laboral, civil, penal, fiscal, mercantil o de cualquier otra rama del Derecho.
Datos académicos: Son los datos que permiten identificar nuestra trayectoria académica y formación profesional como son calificaciones, boletas, constancias, certificados, reconocimientos, títulos, cédulas profesionales.
Datos de tránsito y movimientos migratorios: Información necesaria para nuestro tránsito dentro y fuera de país.

Acciones del TEEMICH para la protección de datos personales.

Acciones del TEEMICH para la protección de datos personales.

TEEM
TRIBUNAL ELECTORAL DEL ESTADO DE MICHOACÁN

ACUERDO DEL PLENO DEL TRIBUNAL ELECTORAL DEL ESTADO DE MICHOACÁN, POR EL QUE SE EXPIDEN LOS LINEAMIENTOS PARA LA ELABORACIÓN Y PUBLICACIÓN DE VERSIONES PÚBLICAS DE LAS SENTENCIAS EMITIDAS POR ESTE ÓRGANO JURISDICCIONAL.

CONSIDERACIONES:

PRIMERO. En términos del artículo 6, apartado A, base I, de la Constitución Política de los Estados Unidos Mexicanos, lo establecido en los numerales 23, 70 y 74 de la Ley General de Transparencia y Acceso a la Información Pública, lo previsto en los dispositivos 1, 2 fracciones IV y VI, 31 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, lo dispuesto en el diverso 8, tercer párrafo, de la Constitución Política del Estado Libre y Soberano de Michoacán de Ocampo, 1, 4, 8, 11, 27, 33 fracción IV y último párrafo, 35 y 39, fracción IV, inciso i), de la Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo, el Tribunal Electoral del Estado, deberá poner a disposición del público, la información a que aluden los citados dispositivos legales.

SEGUNDO. Conforme a lo dispuesto en los artículos 98-A, de la Constitución Política del Estado Libre y Soberano de Michoacán de Ocampo; 60 y 64, fracción IV, del Código Electoral del Estado, el Tribunal Electoral del Estado, es el Órgano Autónomo y máxima autoridad jurisdiccional en materia electoral y el Pleno podrá expedir los acuerdos necesarios para el funcionamiento del mismo.

TERCERO. Para cumplir con las obligaciones en materia de transparencia, garantizando el pleno ejercicio de acceso a la información, el principio de máxima publicidad constitucionalmente establecido, y la protección de datos personales, que se encuentra reconocido como derecho humano, es necesario llevar a cabo un

TEEMICH
TRIBUNAL ELECTORAL DEL ESTADO
MICHOACÁN

TRIBUNAL ELECTORAL DEL ESTADO
AVISO DE SESIÓN PÚBLICA DE 23 DE ENERO DE 2025

Conforme con lo previsto en el artículo 98-A de la Constitución Política del Estado Libre y Soberano de Michoacán de Ocampo; los numerales 65, fracción II y 66 en sus fracciones I, II, III y IV del Código Electoral del Estado de Michoacán de Ocampo; 6, 7, fracción I, 8, fracción I, 9, 10, 11, fracciones I, II, III, IV, V y VI, 12, 13 y 14 del Reglamento Interior del Tribunal Electoral del Estado, así como 6 de los Lineamientos para el uso de tecnologías de la información y comunicación en las sesiones, reuniones, recepción de medios de impugnación, promociones y notificaciones electrónicas; se hace del conocimiento público que el Pleno del Tribunal Electoral del Estado realizará **Sesión Pública,** misma que se llevará a cabo de manera **virtual, el jueves 23 veintitrés de enero del presente año a las 15:30 quince treinta horas,** con la finalidad de desahogar el siguiente:

ORDEN DEL DÍA

PRIMERO. Análisis y, en su caso, aprobación del **Proyecto de sentencia** del Procedimiento Especial Sancionador **TEEM-PES-VPMG-218/2024,** denunciado por el Instituto Electoral de Michoacán, en contra de José Enrique Mora Cárdenas y otros. **Magistrada Ponente:** Yurisha Andrade Morales.

SEGUNDO. Análisis y, en su caso, aprobación del **Proyecto de sentencia** del procedimiento especial sancionador **TEEM-PES-VPMG-212/2024,** denunciado por DATO PROTEGIDO en contra de Eric René Padilla Andrés y otros. **Magistrada Ponente:** Yurisha Andrade Morales.

TERCERO. Análisis y, en su caso, aprobación del **Proyecto de sentencia** del Juicio para la Protección de los Derechos Político-Electorales del Ciudadano **TEEM-JDC-005/2025,** promovido por Servando Pérez Ayala, en contra de la Comisión Especial Electoral Municipal del Ayuntamiento de Morelia. **Magistrada Ponente:** Alma Rosa Bahena Villalobos.

CUARTO. Análisis y, en su caso, aprobación del **Proyecto de sentencia** del Juicio para la Protección de los Derechos Político-Electorales del Ciudadano **TEEM-JDC-275/2024,** promovido por Ana Guadalupe Posas Flores, en contra del Ayuntamiento de Morelia. **Magistrado Ponente:** Everardo Tovar Valdez.

Lo anterior, para los efectos legales procedentes.

ShQBicgU09jSbED2l4Z/nNlah31lg8
EoZRbCdsxlVrY=
alma.bahena@teemcorreo.org.mx
Dra. Alma Rosa Bahena Villalobos
Magistrada Presidenta del Tribunal Electoral del Estado

Este documento es una representación gráfica autorizada mediante firmas electrónicas certificadas, el cual tiene plena validez jurídica de conformidad con el numeral tercero y cuarto del ACUERDO DEL PLENO POR EL QUE SE IMPLEMENTA EL USO DE LA FIRMA ELECTRÓNICA EN LOS ACUERDOS, RESOLUCIONES Y SENTENCIAS QUE SE DICTEN CON MOTIVO DEL TRÁMITE, TURNO, SUSTANCIACIÓN Y RESOLUCIÓN DE LOS ASUNTOS JURISDICCIONALES, ASÍ COMO EN LOS ACUERDOS, LAS GESTIONES Y DETERMINACIONES DERIVADAS DEL ÁMBITO ADMINISTRATIVO DEL TRIBUNAL

Tratamientos de Datos Personales de mayor atención.

Violencia Política en razón de Género


Interés Superior de la Niñez


Comunidad LGBTIQ+


Personas con discapacidad


Personas migrantes/Comunidades y pueblos originarios


Listas nominales

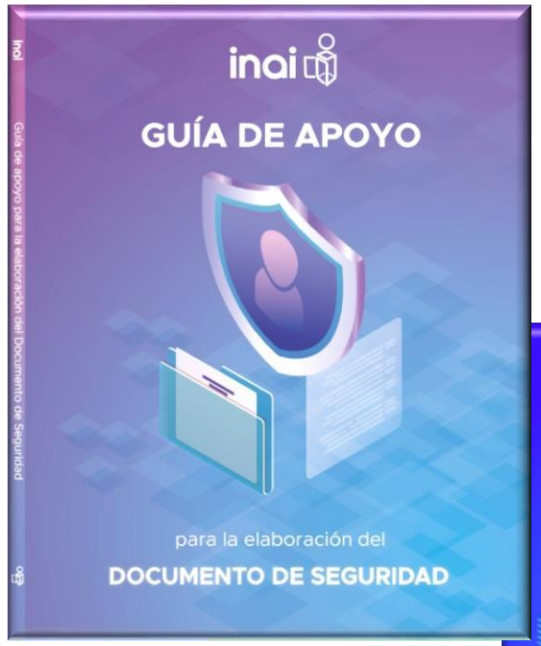

Debida afiliación

ALCANCES ADICIONALES DEL CUMPLIMIENTO DE LA PDP

GOBIERNO DIGITAL
MICHOACÁN
SFA

CAJA DE HERRAMIENTAS

Materiales de utilidad (https://home.inai.org.mx/?page_id=3420)



Reflexiones finales

Nuevo Paradigma…"Autodeterminación Informativa"	
Antes	**Hoy**
•El dato personal es de quien lo capta.	•El dato personal es propiedad del titular.
•El dato personal no tiene valor.	•El dato personal es un derecho fundamental.
•El dato personal es un bien libre.	•El dato personal es un bien protegido.
•No hay restricción en su uso.	•El uso esta sujeto a finalidad y consentimiento.
•El titular no tiene derecho.	•Derechos ARCO

CONSIDERACIÓN FINAL

Sé una buena persona servidora pública: protege los datos personales que recabas, de la misma manera que proteges los tuyos.

¡Gracias!

Dirección de Protección de Datos Personales y Políticas de Promoción de Derechos ARCOP

Mtra. Dulce Rubí Méndez Walle

CONTACTO

•(443) 312-3806 y 312-6632, ext. 105
•imaip@imaip.org.mx
•dmendez@imaip.org.mx
•http://imaip.org.mx/
•Av. Camelinas 571, Félix Ireta, 58070, Morelia, Michoacán.

Subdirección de Protección de Datos Personales

Lic. Víctor Alfonso Cruz Ricardo

CONTACTO

•(443) 312-3806 y 312-6632
•imaip@imaip.org.mx
•vcruz@imaip.org.mx
•http://imaip.org.mx/

Victor Alfonso Cruz Ricardo