INTRODUCCIÓN A LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE PUEBLA

ITAIPUE

MARCO JURÍDICO GENERAL DE LA PROTECCIÓN DE DATOS PERSONALES

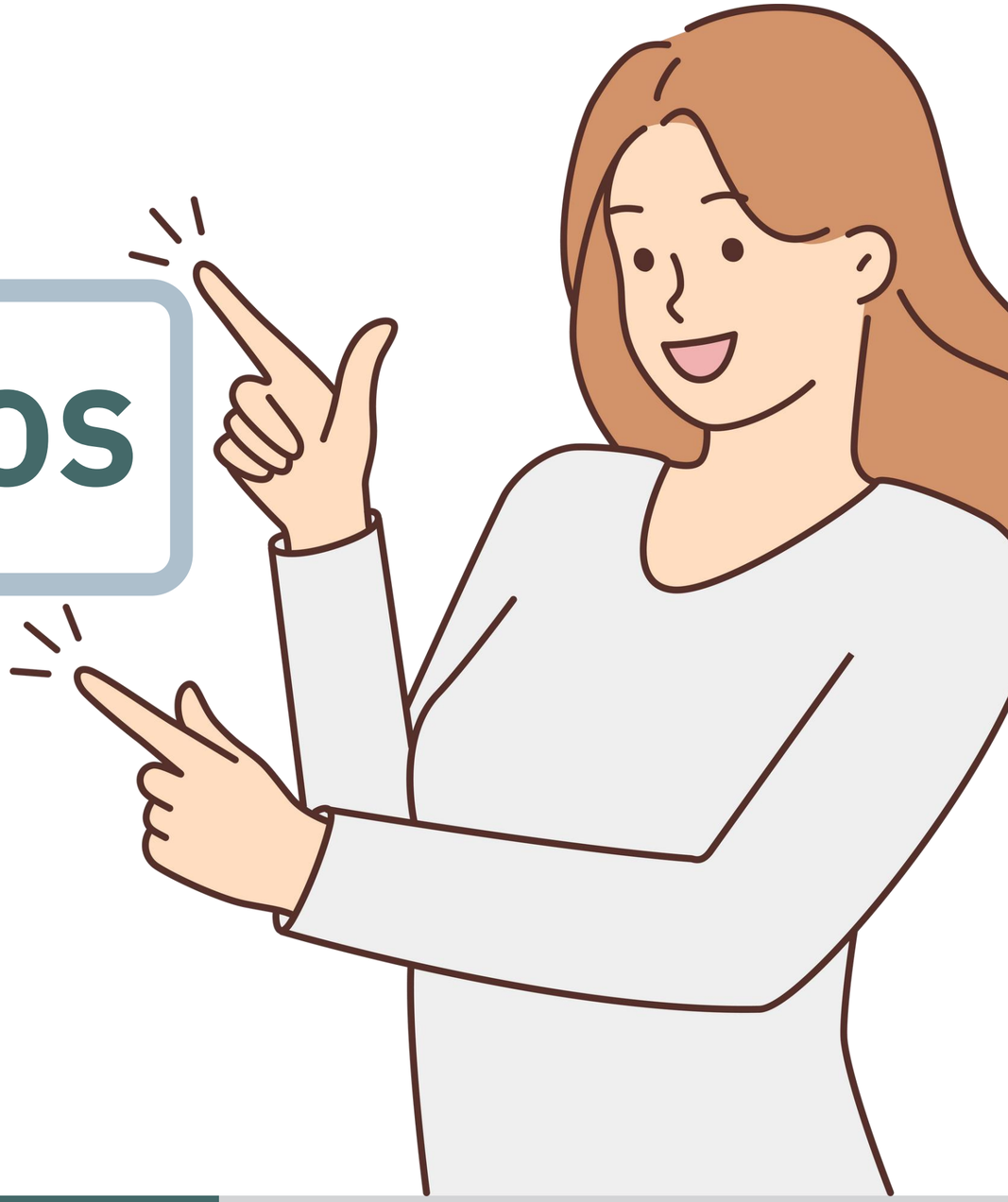
- Constitución Política de los Estados Unidos Mexicanos
- Constitución Política para el Estado Libre y Soberano de Puebla
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla
- Lineamientos Generales en Materia de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla

DERECHO HUMANO: PROTECCIÓN DE DATOS PERSONALES

- La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. (Art. 6, apartado A, fracción II).

- 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. (Art. 16, segundo párrafo)

CONCEPTOS BÁSICOS

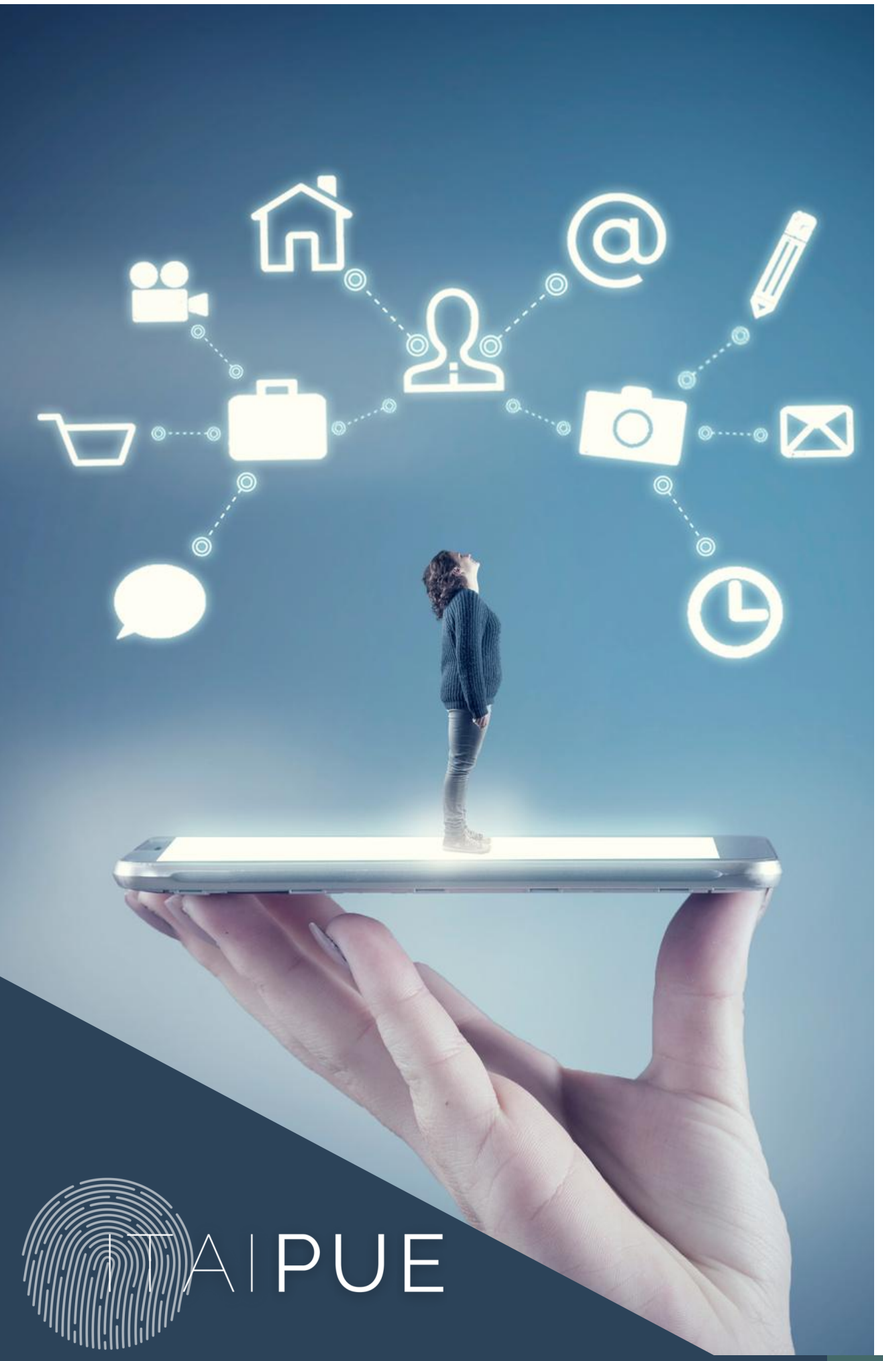


TAIPUE

¿QUÉ SON LOS DATOS PERSONALES?

Cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, gráfica, fotográfica, acústica o en cualquier otro formato.

Se considera que una persona es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información, siempre y cuando esto no requiera plazos, medios o actividades desproporcionadas.



¿QUÉ SON LOS DATOS PERSONALES SENSIBLES?

Aquéllos que se refieren a la esfera más íntima de su Titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. Se consideran sensibles, de manera enunciativa mas no limitativa, los Datos Personales que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente o futuro, creencias religiosas, filosóficas y morales, opiniones políticas, datos genéticos o datos biométricos.

POR REGLA GENERAL NO PODRÁN TRATARSE DATOS PERSONALES SENSIBLES, SALVO QUE:

- Los mismos sean estrictamente necesarios para el ejercicio y cumplimiento de las atribuciones y obligaciones expresamente previstas en las normas que regulan la actuación del Sujeto Obligado Responsable

- Se dé cumplimiento a un mandato legal

- Se cuente con el Consentimiento expreso y por escrito del Titular, o

- Sean necesarios por razones de seguridad pública, orden público, salud pública o salvaguarda de derechos de terceros

CATEGORÍAS DE DATOS PERSONALES

1. Datos identificativos: El nombre, alias, pseudónimo, domicilio, código postal, teléfono particular, sexo, estado civil, teléfono celular, firma, clave de Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Clave de Elector, Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, localidad y sección electoral, y análogos.

2. Datos de origen: Origen, etnia, raza, color de piel, color de ojos, color y tipo de cabello, estatura, complexión, y análogos.

3. Datos ideológicos: Ideologías, creencias, opinión política, afiliación política, opinión pública, afiliación sindical, religión, convicción filosófica y análogos.

4. Datos sobre la salud: El expediente clínico de cualquier atención médica, historial médico, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, estado físico o mental de la persona, así como la información sobre la vida sexual, y análogos.

5. Datos Laborales: Número de seguridad social, documentos de reclutamiento o selección, nombramientos, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio, y análogos.

CATEGORÍAS DE DATOS PERSONALES

6. Datos patrimoniales: Bienes muebles e inmuebles de su propiedad, información fiscal, historial crediticio, ingresos y egresos, número de cuenta bancaria y/o CLABE interbancaria de personas físicas y morales privadas, inversiones, seguros, fianzas, servicios contratados, referencias personales, beneficiarios, dependientes económicos, decisiones patrimoniales y análogos.

7. Datos sobre situación jurídica o legal: La información relativa a una persona que se encuentre o haya sido sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal, fiscal, administrativa o de cualquier otra rama del Derecho, y análogos.

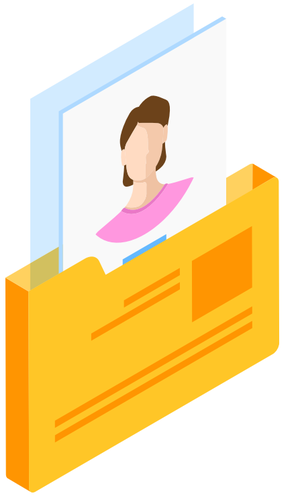
8. Datos académicos: Trayectoria educativa, avances de créditos, tipos de exámenes, promedio, calificaciones, títulos, cédula profesional, certificados, reconocimientos y análogos.

9. Datos de tránsito y movimientos migratorios: Información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria, cédula migratoria, visa, pasaporte. 10.Datos electrónicos: Firma electrónica, dirección de correo electrónico, código QR.

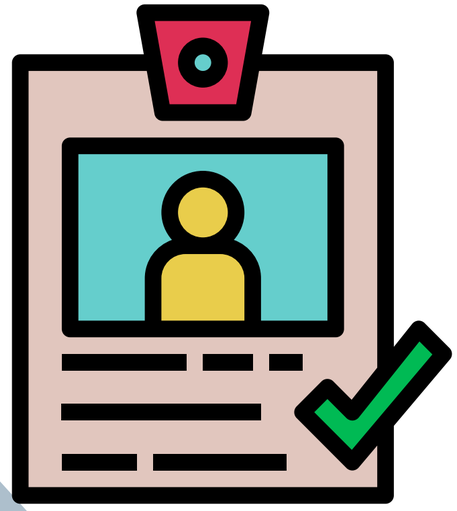
11.Datos biométricos: Huella dactilar, reconocimiento facial, reconocimiento de iris, reconocimiento de la geometría de la mano, reconocimiento vascular, reconocimiento de escritura, reconocimiento de voz, reconocimiento de escritura de teclado y análogos.

TITULAR

Persona física a quien hacen referencia o pertenecen los Datos Personales objeto del Tratamiento establecido en la Ley.



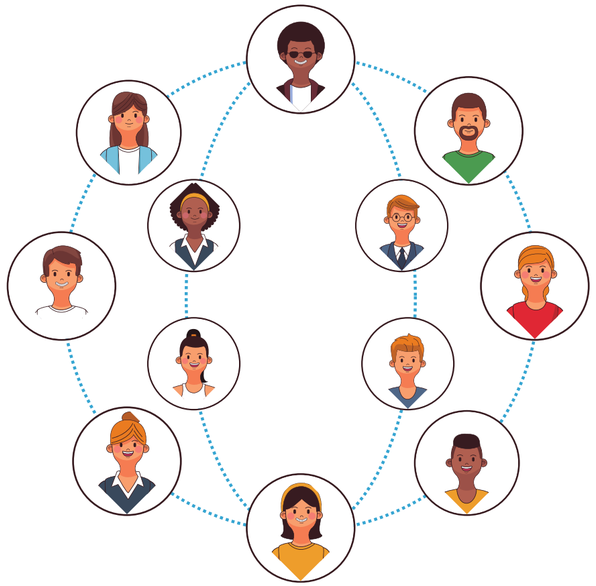
TRATAMIENTO DE DATOS PERSONALES



Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados aplicados a los Datos Personales, relacionadas, de manera enunciativa mas no limitativa, con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, Transferencia y en general cualquier uso o disposición de Datos Personales.

ENCARGADO

Prestador de servicios, que con el carácter de persona física o jurídica pública o privada, ajena a la organización del Responsable, trata Datos Personales a nombre y por cuenta de éste.



RESPONSABLE

Cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, fideicomisos y fondos públicos, a los Ayuntamientos y partidos políticos del Estado de Puebla, que decide y determina los fines, medios y demás cuestiones relacionadas con determinado Tratamiento de Datos Personales.

TRANSFERENCIA

Toda comunicación de Datos Personales dentro o fuera del territorio mexicano, realizada a persona distinta del Titular, del Responsable o del Encargado.

Toda Transferencia de Datos Personales, sea ésta nacional o internacional, se encuentra sujeta al Consentimiento de su Titular, salvo las excepciones previstas en el artículo 94 de la Ley, y deberá ser informada al Titular en el Aviso de Privacidad, así como limitarse a las finalidades que las justifiquen

TRANSFERENCIAS QUE NO REQUIEREN CONSENTIMIENTO

Prevista en leyes o Tratados Internacionales suscritos y ratificados por México

Se realice entre Responsables, siempre y cuando se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el Tratamiento

Es legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia

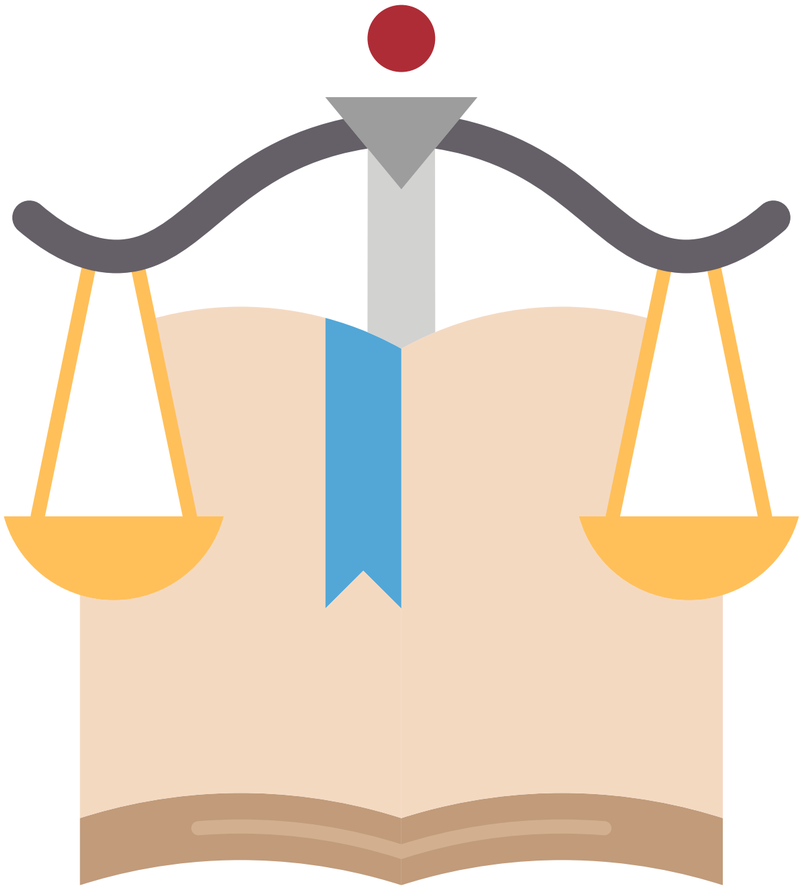
Es precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última

Es necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios

Sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el Responsable y el Titular

Es necesaria por virtud de un contrato celebrado o por celebrar en interés del Titular, por el Responsable y un tercero

LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE PUEBLA



ITAIPUE

ARTÍCULO 3. Son Sujetos Obligados y por lo tanto Responsables para efectos de la presente Ley:

I. El Poder Ejecutivo, sus Dependencias y Entidades;

II. El Poder Legislativo y cualquiera de sus Órganos;

III. El Poder Judicial y cualquiera de sus Órganos;

IV. Los Tribunales Administrativos, en su caso;

V. Los Ayuntamientos, sus Dependencias y Entidades;

VI. Los órganos constitucionalmente autónomos;

VII. Los Partidos Políticos, y

VIII. Fideicomisos y fondos públicos.

OBJETO

- Garantizar el derecho que tiene toda persona a la protección de sus Datos Personales.

- Es de orden público y observancia obligatoria en el Estado de Puebla

ITAIPUE

OBJETIVOS

- Garantizar que toda persona pueda ejercer el derecho a la protección de los Datos Personales
- Distribuir competencias entre el Instituto de Transparencia y los Responsables, en materia de protección de Datos Personales
- Establecer las bases mínimas y condiciones homogéneas 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
- 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 Ayuntamientos de Puebla, con la finalidad de regular su debido Tratamiento
- Garantizar la observancia de los principios de protección de Datos Personales Promover, fomentar y difundir una cultura de protección de Datos Personales
- Establecer los mecanismos para garantizar el cumplimiento y la efectiva aplicación de las medidas de apremio y establecer un catálogo de sanciones

APLICABILIDAD

Esta Ley será aplicable a cualquier Tratamiento de Datos Personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

ITAIPUE

OBLIGACIONES GENERALES PARA RESPONSABLES ESTABLECIDAS EN LA LEY

1. Principios que se deben observar en todo tratamiento de datos personales

2.Deberes para proteger los datos personales en cualquier fase de su tratamiento

3.Derechos de los Titulares de los datos personales y el procedimiento para su ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO)

ITA | PUE

PRINCIPIOS QUE SE DEBEN OBSERVAR EN TODO TRATAMIENTO DE DATOS PERSONALES

ITAIPUE

LICITUD

Llevar a cabo el tratamiento de datos personales conforme y en base a las facultades y atribuciones que la correspondiente normativa le confiera.

Obligaciones:

- Identificar el marco normativo (leyes, reglamentos, lineamientos, entre otros, con sus respectivos artículos) que faculta a la unidad administrativa a tratar los datos personales para cada una de las finalidades, y aquél que regula el tratamiento respectivo.

FINALIDAD

Efectuar el tratamiento de datos personales únicamente cuando se encuentre justificado por finalidades concretas (fines específicos y determinados, no genéricos), explícitas (se expresan y dan a conocer en el aviso de privacidad), lícitas y legítimas (atribuciones expresas), en relación con las atribuciones que la normativa aplicable le confiera.

LEALTAD

No se deberán obtener y tratar datos personales a través de medios engañosos o fraudulentos, esto es:

- Medie dolo, mala fe o negligencia en el Tratamiento de Datos Personales que lleve a cabo
- Realizar un Tratamiento de Datos Personales que dé lugar a una discriminación injusta o arbitraria contra el Titular
- Vulnerar la expectativa razonable de protección de Datos Personales.

Obligaciones:

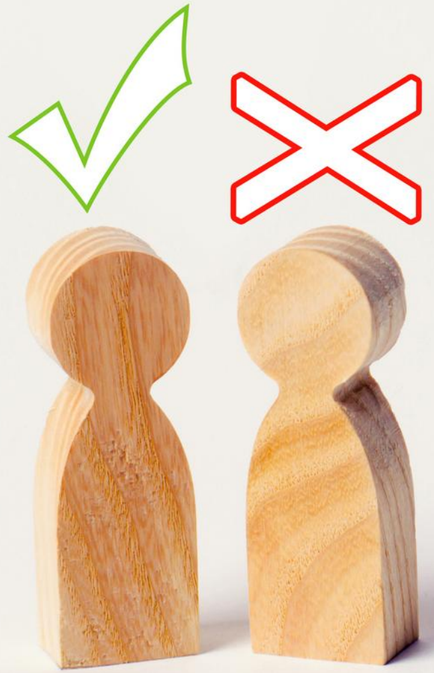
Privilegiar, en todo momento, la protección de los intereses del Titular y su expectativa razonable de protección de Datos Personales, entendida como la confianza que, respecto a que sus Datos Personales serán tratados conforme a lo señalado en el Aviso de Privacidad y en cumplimiento a las disposiciones previstas en la presente Ley.

CONSENTIMIENTO

Para el tratamiento de datos personales, el responsable deberá recabar la anuencia libre, específica e informada del titular. Lo anterior con la salvedad que la ley establece como excepciones.

El consentimiento deberá otorgarse de forma:

- Libre: sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular.
- Específica: referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento.
- Informada: que el titular tenga conocimiento del aviso de privacidad al tratamiento a que serán sometidos sus datos personales.



Tipos de consentimiento:

- **Expreso:** cuando la voluntad del Titular se manifieste de forma verbal, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología. (Datos Personales Sensibles)
- **Tácito:** cuando habiéndose puesto a disposición del Titular el Aviso de Privacidad, éste no manifieste su voluntad en sentido contrario.

Obligaciones:

- Obtener el Consentimiento del Titular para el Tratamiento de sus Datos Personales, de manera previa.
- Por regla general será válido el Consentimiento tácito, salvo que una ley exija que la voluntad del Titular se manifieste de manera expresa.
- Tratándose del Consentimiento expreso, demostrar de manera indubitable que el Titular otorgó su Consentimiento, ya sea a través de una declaración o una acción afirmativa clara.

EXCEPCIONES AL CONSENTIMIENTO

Art. 20 de la Ley

Existe una orden judicial, resolución o mandato fundado y motivado de autoridad competente

Una norma con rango de ley señale expresamente que no será necesario el Consentimiento, por razones de seguridad pública, salud pública, disposiciones de orden público o protección de derechos de terceros

Los Datos Personales figuren en fuentes de Acceso Público

Para el reconocimiento o defensa de derechos del Titular ante autoridad competente

Sean necesarios para la prevención, el diagnóstico médico, la prestación de servicios de asistencia sanitaria, el Tratamiento médico, o la gestión de servicios sanitarios

Se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el Titular y el Responsable

Existe una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes

CALIDAD

Adoptar medidas necesarias para mantener exactos, correctos y actualizados los datos personales que se encuentren en su posesión.

Se presume que se cumple con la calidad en los Datos Personales cuando éstos son proporcionados directamente por el Titular y hasta que éste no manifieste y acredite lo contrario.

PROPORCIONALIDAD

Exige que cualquier tratamiento de datos personales no vaya más allá de lo necesario para alcanzar sus objetivos.

Este deber se traduce en que los datos personales que se pretendan recabar del titular sean adecuados, relevantes, pertinentes y estrictamente necesarios para la finalidad que justifica su tratamiento.

INFORMACIÓN

Deber de comunicar al titular, a través de sendos avisos de privacidad, simplificado e integral, información suficiente acerca de la existencia, alcances, condiciones y características principales del tratamiento al que serán sometidos sus datos personales.

AVISOS DE PRIVACIDAD

El **aviso de privacidad simplificado** deberá contener la siguiente información:
1. La denominación del Responsable

2. Las finalidades del Tratamiento para las cuales se obtienen los Datos Personales, distinguiendo aquéllas que requieran el Consentimiento del Titular

3. Cuando se realicen Transferencias de Datos Personales que requieran Consentimiento, se deberá informar:

a) Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o jurídicas de carácter privado a las que se transfieren los Datos Personales, y
b) Las finalidades de estas Transferencias.

4. Los mecanismos y medios disponibles para que el Titular, en su caso, pueda manifestar su negativa para el Tratamiento de sus Datos Personales para finalidades y Transferencias de los mismos que requieren su Consentimiento, y

5. El sitio donde se podrá consultar el Aviso de Privacidad integral.

Además de lo anterior, el aviso de privacidad integral deberá contener, la siguiente información:

1. El domicilio del Responsable

2. Los Datos Personales que serán sometidos a Tratamiento, identificando aquéllos que sean sensibles

3. El fundamento legal que faculta expresamente al Responsable para llevar a cabo: El Tratamiento de Datos Personales, y las Transferencias de Datos Personales

4. Los mecanismos, medios y procedimientos disponibles para ejercer los Derechos ARCO

5. El domicilio de la Unidad de Transparencia, y

6. Los medios a través de los cuales el Responsable comunicará a los Titulares los cambios al Aviso de Privacidad.

RESPONSABILIDAD

Impone al responsable la obligación de implementar mecanismos necesarios para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en las Leyes General y Estatal y en los Lineamientos Generales, así como el deber de rendir cuentas al titular con relación al tratamiento de los datos personales que estén en su posesión.

DEBERES PARA PROTEGER LOS DATOS PERSONALES EN CUALQUIER FASE DE SU TRATAMIENTO

ITAIPUE

DEBER DE CONFIDENCIALIDAD. Establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del Tratamiento de los Datos Personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el mismo.
Lo anterior, sin menoscabo de lo establecido en la Ley de Transparencia y demás disposiciones que resulten aplicables en la materia.

EJEMPLO:
Inclusión de cláusulas o contratos de confidencialidad para el personal laboral

DEBER DE SEGURIDAD: Establecer y mantener 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:**

- **Integridad:** salvaguardar la exactitud y completitud de la información, así como evitar la modificación no autorizada o accidental de la misma.

- **Disponibilidad:** es la propiedad de un dato para ser accesible y utilizable, prevenir interrupciones no autorizadas.

- **Confidencialidad:** es la propiedad de la información para no estar a disposición o ser revelada a personas no autorizadas.

MEDIDAS DE SEGURIDAD ADMNISTRATIVAS

Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de los Datos Personales a nivel organizacional, la identificación, clasificación y borrado seguro de los Datos Personales, así como la sensibilización y capacitación del personal en materia de protección de Datos Personales.

TA|PUE

EJEMPLOS

- Identificación y autentificación de persona autorizada para el tratamiento de datos personales
- Aprobación de normativa interna o políticas internas de tratamiento
- Implementación de contraseñas, claves y protocolos de seguridad
- Elaboración de bitácoras de registro y seguimiento de las actividades que se realizan con la base de datos personales
- Elaboración de procedimientos para dar aviso al personal custodio de los datos personales sobre la presencia y acceso de personas no autorizadas
- Emisión de reglas sobre la introducción de equipos de cómputo, accesorios y gadgets, o de conexión inalámbrica a áreas restringidas de tratamiento de datos personales
- Emisión de reglamentación interna que contemple infracciones y sanciones con relación al indebido tratamiento de datos personales
- Emisión de reglas para la baja documental en soportes físicos y electrónicos
- Emisión de medidas para la prevención y notificación de intrusiones e incidentes
- Elaboración de manuales de operaciones, instauración de protocolos para casos de emergencia, realización de pruebas y simulacros
- Procedimientos y canales para el ejercicio de derechos ARCO
- Procedimientos de disociación

Disociación: El procedimiento mediante el cual los Datos Personales no pueden asociarse al Titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

MEDIDAS DE SEGURIDAD FÍSICAS

Conjunto de acciones y mecanismos para proteger el entorno físico de los Datos Personales y de los recursos involucrados en su Tratamiento, para:

a) Prevenir el acceso no autorizado al perímetro de la organización del Responsable, sus instalaciones físicas, áreas críticas, recursos y Datos Personales;

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización del Responsable, recursos y Datos Personales;

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización del Responsable, y

d) Proveer a los equipos que contienen o almacenan Datos Personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

EJEMPLOS:

- Protección de instalaciones, equipos, soportes o bases de datos personales
- Utilización de candados, cerrojos, cerraduras, tarjetas de identificación, dispositivos electrónicos o cualquier otra tecnología que impida la libre apertura de puertas, gavetas, cajones, archiveros, etc.;
- Implementación de sistemas de vigilancia, alarmas, y de prevención y protección contra siniestros tales como incendios
- Señalamiento de áreas de acceso restringido
- Aparatos de identificación por medio de la voz, iris, huella, ADN, y demás datos biométricos
- Resguardo de datos personales a través de infraestructura que garantice condiciones adecuadas de humedad, polvo, iluminación solar y temperatura y evite el deterioro por plagas, consumo de alimentos, y otros factores presentes en el entorno

MEDIDAS DE SEGURIDAD TÉCNICAS

Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los Datos Personales y los recursos involucrados en su Tratamiento, para:

- a) Prevenir que el acceso a los Datos Personales, así como a los recursos, sea por usuarios identificados y autorizados;
- b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
- c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
- d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el Tratamiento de Datos Personales.

EJEMPLOS:

- Encriptación y cifrado de los datos
- Copias de seguridad, resguardos o backups
- Almacenamiento en dos ubicaciones diferentes; atención de fallas de equipo electrónico y de cómputo
- Indicación de software autorizado
- Deshabilitación o cancelación de puertos de comunicación (USB, paralelo, serial, etc.),

•dispositivos de almacenamiento removible (unidades de disco flexible, quemadores de CD/DVD, etc.), dispositivos de conexión inalámbrica (Wi-Fi, Bluetooth, infrarrojo, etc,)

- Realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo;
- Brindar soporte técnico de equipos, sistemas, programas de software, etc.
- Instalación de firewalls, antivirus, watchdogs, mecanismos para evitar la pérdida y filtración de datos (data loss prevention);
- Segregación de funciones mediante perfiles de acceso
- Mecanismos de control de acceso
- Monitorización del uso de datos personales

ACTIVIDADES QUE DEBEN REALIZAR LOS RESPONSABLES PARA ESTABLECER Y MANTENER MEDIDAS DE SEGURIDAD

- Crear políticas internas para la gestión y Tratamiento de los Datos Personales, que tomen en cuenta el contexto en el que ocurren los Tratamientos y el ciclo de vida de los Datos Personales, es decir, su obtención, uso y posterior supresión;

- Definir las funciones y obligaciones del personal involucrado en el Tratamiento de Datos Personales;

- Elaborar un inventario de los Datos Personales y de los sistemas de Tratamiento;

- Realizar un análisis de riesgo de los Datos Personales, considerando las amenazas y vulnerabilidades existentes para los Datos Personales y los recursos involucrados en su Tratamiento, como pueden ser, de manera enunciativa mas no limitativa, hardware, software, personal del Responsable, entre otros;

- Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del Responsable;

- Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y Tratamiento de los Datos Personales;

- Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los Datos Personales, y

- Diseñar y aplicar diferentes niveles de capacitación de su personal, dependiendo de sus roles y responsabilidades respecto del Tratamiento de los Datos Personales.

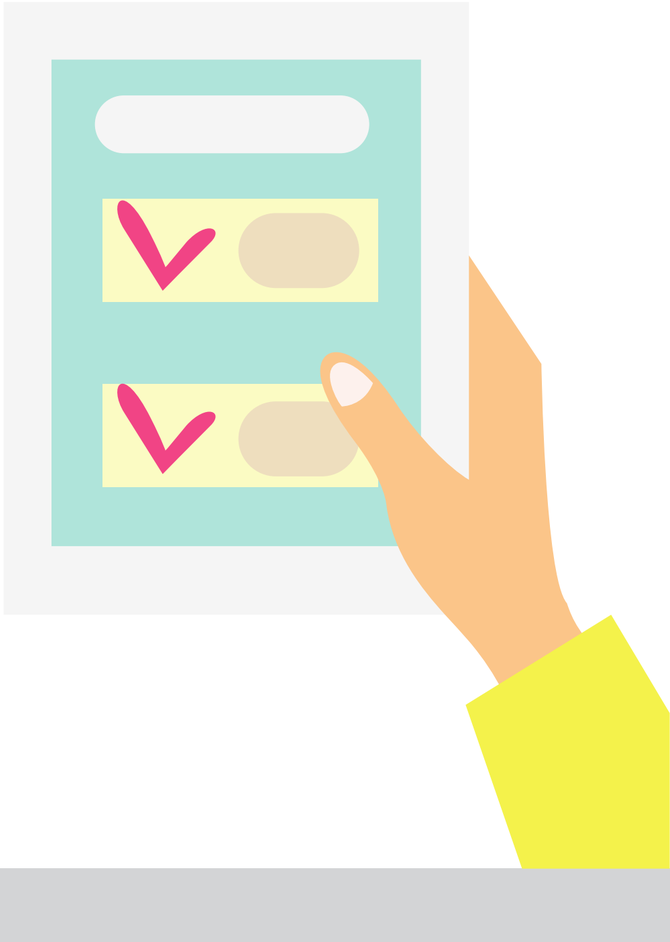
Estas acciones relacionadas con las medidas de seguridad para el Tratamiento de los Datos Personales deberán estar documentadas y contenidas en un **SISTEMA DE GESTIÓN.**

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 y las disposiciones que le resulten aplicables en la materia.

DOCUMENTO DE SEGURIDAD

De manera particular, el Responsable deberá elaborar un Documento de Seguridad que contenga, al menos, lo siguiente:

I. El inventario de Datos Personales y de los sistemas de Tratamiento;
II. Las funciones y obligaciones de las personas que traten Datos Personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad;
VII. El programa general de capacitación, y
VIII. Nombre y cargo del personal del Responsable o Encargado



DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES Y EL PROCEDIMIENTO PARA SU EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN (ARCO)

En todo momento el Titular o su representante podrán solicitar al Responsable el acceso, rectificación, cancelación u oposición al Tratamiento de los Datos Personales.

ACCESO: Derecho del Titular de acceder a sus Datos Personales que obren en posesión del Responsable, así como a conocer la información relacionada con las condiciones, generalidades y particularidades de su Tratamiento.

RECTIFICACIÓN: Derecho del Titular a solicitar al Responsable la rectificación o corrección de sus Datos Personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados.

CANCELACIÓN: Derecho del Titular a solicitar la cancelación de sus Datos Personales de los archivos, registros, expedientes y sistemas del Responsable, a fin de que los mismos ya no estén en su posesión.

OPOSICIÓN: El Titular podrá oponerse al Tratamiento de sus Datos Personales o exigir que se cese en el mismo, cuando:

I. Exista una causa legítima y su situación específica así lo requiera, lo cual implica que aun siendo lícito el Tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al Titular, o

II. Sus Datos Personales sean objeto de un Tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

ITAIPUE

FIGURAS EN LOS SUJETOS OBLIGADOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

COMITÉ DE TRANSPARENCIA

Coordinar, realizar y supervisar 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 Ley y en aquellas disposiciones que resulten aplicables en la materia, en coordinación con el oficial de protección de Datos Personales, en su caso;

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

Confirmar, modificar o revocar las determinaciones en las que se declare la **inexistencia** de los Datos Personales, o se declare **improcedente**, por cualquier causa, el ejercicio de alguno de los Derechos ARCO;

Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de esta Ley y demás ordenamientos que resulten aplicables en la materia;

Coordinar el **seguimiento y cumplimiento** de las resoluciones emitidas por el Instituto de Transparencia;

Establecer **programas de capacitación y actualización** para los servidores públicos en materia de protección de Datos Personales, y
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**.

UNIDAD DE TRANSPARENCIA

Auxiliar y orientar al Titular o, en su caso, a su representante legal que lo requiera con relación al ejercicio del derecho a la protección de Datos Personales;

Gestionar las solicitudes para el ejercicio de los Derechos ARCO;

Establecer **mecanismos para asegurar que los Datos Personales** sólo se entreguen a su Titular o su representante debidamente acreditados;

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;

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;

Aplicar **instrumentos de evaluación de calidad** sobre la gestión de las solicitudes para el ejercicio de los Derechos ARCO;

Asesorar a las Áreas adscritas al Responsable **en materia de protección de Datos Personales**, y

Dar **seguimiento y cumplimiento a las resoluciones emitidas** por el Instituto de Transparencia.

OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

- Aquellos Responsables que en el ejercicio de sus funciones sustantivas lleven a cabo Tratamientos de Datos Personales relevantes o intensivos, podrán designar a un oficial de protección de Datos Personales, el cual formará parte del Comité de Transparencia.

- La persona designada como oficial de protección de datos personales deberá:

- Contar con la jerarquía o posición dentro de la organización del Responsable que le permita implementar políticas transversales en esta materia.

- Será designado atendiendo a su experiencia y cualidades profesionales, en particular, a sus conocimientos en la materia y deberá contar con recursos suficientes para llevar a cabo su cometido.

ATRIBUCIONES

Asesorar al Comité de Transparencia respecto a los temas que sean sometidos a su consideración en materia de protección de Datos Personales;

Diseñar, ejecutar, supervisar y evaluar políticas, programas, acciones y actividades que correspondan para el cumplimiento de la presente Ley y disposiciones que resulten aplicables en la materia, en coordinación con el Comité de Transparencia;

Asesorar permanentemente a las Áreas adscritas al Responsable en materia de protección de Datos Personales.

RESPONSABILIDADES ADMINISTRATIVAS POR INCUMPLIMIENTO A LA LEY

ARTÍCULO 188. Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes:

I.Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los Derechos ARCO;

II.Incumplir los plazos de atención previstos en la Ley para responder las solicitudes para el ejercicio de los Derechos ARCO o para hacer efectivo el derecho de que se trate;

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 tengan 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 refieren los artículos 38 y 39 de la Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;

VI.Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales.

ITAIPUE

VII.Incumplir el deber de confidencialidad establecido en el artículo 59 de la Ley;
VIII.No establecer las medidas de seguridad en los términos que establecen los artículos 47, 48 y 50 de la Ley;

IX.Presentar vulneraciones a los Datos Personales por la falta de implementación de medidas de seguridad según los artículos 47, 48 y 50 de la Ley;

X.Llevar a cabo la Transferencia de Datos Personales, en contravención a lo previsto en la presente Ley;

XI.Obstruir los actos de verificación de la autoridad;

XII.Crear bases de Datos Personales en contravención a lo dispuesto por el artículo 9 de la Ley;

XIII.No acatar las resoluciones emitidas por el Instituto de Transparencia;

XIV.Aplicar medidas compensatorias en contravención de los criterios que tales fines establezca el Sistema Nacional;

XV.Declarar dolosamente la inexistencia de Datos Personales cuando éstos existan total o parcialmente en los archivos del Responsable;

XVI.No atender las medidas cautelares establecidas por el Instituto de Transparencia;

XVII.Tratar los Datos Personales de manera que afecte o impida el ejercicio de los derechos fundamentales previstos en la Constitución Política de los Estados Unidos Mexicanos;

XVIII.No cumplir con las disposiciones previstas en los artículos 85, 90 y 91 de la Ley;

XIX.Tratar Datos Personales en aquellos casos en que sea necesario presentar la evaluación de impacto a la protección de Datos Personales, de conformidad con lo previsto en la Ley y demás normativa aplicable, y

XX.Realizar actos para intimidar o inhibir a los Titulares en el ejercicio de los Derechos ARCO.

ITAIPUE

INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE PUEBLA

Av. 5 Ote 201 Centro Histórico Puebla, Pue. C.P. 72000 Tel. (222) 309 6060
Horario: Lunes a Viernes 8:00 a.m. a 4:00 p.m.