TRANSVERSAL

Incidencia estratégica en políticas públicas

Manual de Protección de Datos Personales

2024

En Transversal, nos distinguimos por el compromiso de la transformación de ideas en soluciones públicas mediante la generación de conocimiento útil. Adoptamos una perspectiva innovadora y orientada hacia el impacto social en la resolución de problemas públicos.

En consonancia con nuestros valores, hemos elaborado un Documento de Seguridad en cumplimiento con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Este Manual de Protecciòn de Datos refleja nuestro compromiso con la protección de los datos personales y el respeto a la privacidad de las personas. Reconocemos la importancia y obligatoriedad de implementar medidas de seguridad para proteger los datos personales en nuestra posesión, reflejando así nuestro compromiso con la integridad y confidencialidad de la información.

Entendemos la necesidad de contar con un Manual de Protecciòn de Datos que contenga los elementos requeridos por la legislación, garantizando así el cumplimiento de las disposiciones legales y la protección de los datos personales.Describimos los criterios y supuestos que motivaron la actualización del Documento de Seguridad en Transversal, asegurando su vigencia y adecuación a los cambios normativos y operativos.

En Transversal, estamos firmemente comprometidos con la protección de los datos personales y el desarrollo de soluciones públicas que generen un impacto positivo en la sociedad. Este Manual de Protecciòn de Datos refleja nuestro compromiso con la integridad, confidencialidad y disponibilidad de la información que manejamos.

ÍNDICE

ABREVIACIONES Y DENOMINACIONES

CPEUM o Constitución : Constitución Política de los Estados Unidos Mexicanos

GDPR: Reglamento General de Protección de Datos de la Unión Europea

IEPC: Instituto de Elecciones y Participación Ciudadana

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

LFPDPPP: Ley Federal de Protección de Datos Personales en Posesión de los Particulares

OSC : Organización u organizaciones de la sociedad civil

Reglamento : Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

ITEI: Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco

DIF: Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco (Sistema DIF Jalisco)

DOF: Diario Oficial de la Federación

Derechos ARCO: Derechos de acceso,rectificación, cancelación y oposición.

INTRODUCCIÓN

"En Transversal, convertimos ideas en soluciones públicas mediante la generación de conocimiento práctico. Somos una entidad comprometida con la resolución de problemas públicos a través de tres enfoques clave: Influencia en la esfera pública, fortalecimiento de habilidades, y promoción de políticas públicas."

En línea con nuestra misión, reconocemos la importancia crítica de proteger y salvaguardar los datos personales en todas nuestras actividades. Nos comprometemos a implementar medidas tecnológicas avanzadas para fortalecer la seguridad y confidencialidad de estos datos, garantizando así la integridad y privacidad de la información que manejamos.

"Transversal no solo es un método de análisis, sino una perspectiva de la realidad. Según la Real Academia de la Lengua Española, transversal significa que se extiende atravesando de un lado a otro; que cruza en dirección perpendicular con aquello de que se trata; que atañen a distintos ámbitos o disciplinas; que estudia la estructura un problema. Transversal es uno de los mantras de la Agenda 2030 del desarrollo sostenible que plantea la necesidad de abordar los retos del desarrollo de forma integral, holística, transversal."

En Transversal, adoptamos un enfoque integral para proteger los datos personales. Esto incluye la implementación de técnicas robustas de cifrado para garantizar que la información sensible esté protegida tanto en reposo como en tránsito. Además, establecemos sistemas de gestión de acceso y autenticación sólidos para controlar y verificar la identidad de quienes acceden a los datos.

De otra forma, aplicamos rigurosas políticas de anonimización y seudonimización para garantizar que los datos personales se utilicen de manera ética y responsable, minimizando el riesgo de identificación de individuos. Nos comprometemos a monitorear continuamente nuestros sistemas de seguridad, utilizando herramientas avanzadas de detección de intrusiones y análisis de registros para identificar y mitigar cualquier amenaza potencial.
En Transversal, estamos firmemente comprometidos con el desarrollo e implementación de iniciativas que generen un impacto duradero y significativo en la esfera pública.

Reconocemos que la protección de los datos personales es fundamental para mantener la confianza en nuestras actividades y contribuir positivamente al bienestar de las comunidades que servimos. Por lo tanto, nos esforzamos por mantener los más altos estándares de seguridad y confidencialidad en todas nuestras operaciones, en línea con nuestra visión de promover un cambio positivo en nuestro entorno.

MARCO NORMATIVO

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD:

Reglamento general de protección de datos).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Boletín Oficial del Estado. Código vigente consolidado en materia de protección de datos personales.

Reglamento Interior del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Jalisco, fecha de publicación, 24 de octubre del 2023, fecha de aprobación, 18 de octubre del 2023, vigencia, 25 de octubre del 2023 y, última actualización fue el 18 de octubre del 2023.

LINEAMIENTOS Generales en Materia de Clasificación de la Información Pública que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. Fecha de publicación, 10 de junio del 2014, fecha de aprobación, 28 de mayo de 2014, vigencia, 11 de junio del 2014 y, última reforma, 05 de junio de 2015.

LINEAMIENTOS Generales en Materia de Publicación y Actualización de Información Fundamental que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. Fecha de publicación, 10 de junio del 2014, y última reforma, sin reformas.

Reglamento de Austeridad y Ahorro del Instituto de Transparencia e Información Pública de Jalisco. Fecha de publicación, 04 de agosto del 2015, fecha de aprobación, 08 de julio del 2015, vigencia, 05 de agosto del 2015 y última actualización, Sin reformas.

Reglamento Interior del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Jalisco. Fecha de publicación, 24 de octubre del 2023, fecha de aprobación, 18 de octubre del 2023, vigencia, 25 de octubre del 2023, última actualización: 18 de octubre del 2023

LOS DATOS PERSONALES

DEFINICIÓN DE DATOS PERSONALES

Las leyes de protección de datos personales en México definen que un dato personal es cualquier información que pueda ser utilizada para identificar de forma directa o indirecta a un individuo. Por ello, una persona es identificable cuando su identidad se determina directa o indirectamente a través de cualquier información.

La Ley Federal de Protecciòn de Datos Personales en Posesiòn de los Particulares **(LFPDPPP)** regula los datos personales en posesión de los particulares y regula el tratamiento legítimo, controlado e informado, para que garantice la privacidad y el derecho a la autodeterminación informativa de los individuos. Esta ley aplica para personas físicas o morales de carácter privado, donde presenten el tratamiento de datos personales. Por ello, las leyes tienen como objetivo la protección de datos personales en posesión de particulares, asegurando los siguientes elementos:

Establecer normativas para el manejo adecuado, supervisado y transparente de la información.

Los derechos fundamentales y prevenir posibles perjuicios a la privacidad y la intimidad.

Garantizar la privacidad y el derecho a la autodeterminación.

Prevenir cualquier discriminación.

Tipo de datos personales

Datos personales: Los datos personales son toda la información que nos dan identidad, nos describen y precisan, así como cualquier información concerniente a una persona física identificada o identificable. Entre los datos personales existen los siguientes:

Identidad: Nombre, domicilio, teléfono, correo electrónico, firma, contraseñas, RFC, fecha de nacimiento, edad, nacionalidad, estado civil, etc.

Trabajo: Institución o empresa donde trabajas, cargo, correo electrónico, teléfono, etc.

Educación: Institución educativa, calificaciones, certificados, etc.

Ideologìa: Religión, afiliación o preferencia política, sindical, participación en organizaciones civiles, etc.

Salud: Estado de salud, expediente clínico, historia y estudios clínicos, enfermedades, tratamientos, alergias, embarazos, condición psicológica,etc.

Datos financieros y patrimoniales: Cualquier información que hace referencia a los bienes monetarios, muebles y/o inmuebles, lo cual es información fiscal;historial crediticio; ingresos y egresos; cuentas bancarias; seguros; afores; fianzas, número de tarjeta de crédito, número de seguridad, entre otros.

Datos sensibles: Es aquel dato personal que puede afectar la intimidad del titular, ya que deben ser tratados y almacenados de una forma eficaz, cumpliendo ciertos requisitos de privacidad. Algunos datos sensibles son:

- Opiniones políticas.
- Origen racial o etnico.
- Creencias religiosas o filosóficas.
- Afiliación sindical.
- Los datos genéticos.
- Datos biométricos.
- Datos relativos a la salud.

La importancia de los datos sensibles en una organización es importante, ya que son datos confidenciales asociados a los trabajadores, por lo que la confianza del usuario tendrá reacciones sólidas y duraderas a lo largo del tiempo. Además, se deben proteger los datos personales, para que se cumplan las leyes y regulaciones, para garantizar la seguridad y la privacidad de cada individuo.

La tecnología desempeña un papel fundamental en la prevención de fuga de datos, al proporcionar herramientas y soluciones que ayuden a proteger los datos.

FORTALECIENDO LA SEGURIDAD DE DATOS PERSONALES

MEDIDAS TECNOLÓGICAS PARA LA PROTECCIÓN Y CONFIDENCIALIDAD

El cifrado de datos nos ayuda con el fortalecimiento de la seguridad de nuestros datos, ya que implica convertir la información legible en un formato ilegible utilizando algoritmos y claves de cifrado.

Esto se hace para proteger la confidencialidad de la información, asegurando que solo las personas autorizadas puedan acceder a los datos. Cuando se transmite o almacena información sensible, como contraseñas, información financiera o de salud, el cifrado se utiliza para protegerla de accesos no autorizados.

Por otro lado, el control de acceso se refiere al proceso de regular y gestionar quién tiene acceso a los recursos, sistemas y datos dentro de una organización.

Esto implica autenticar la identidad de los usuarios, autorizar qué recursos pueden utilizar y qué acciones pueden realizar, y monitorear y auditar las actividades de acceso para garantizar la seguridad y el cumplimiento normativo.

La protección de dispositivos implica implementar medidas de seguridad para proteger los dispositivos informáticos, como computadoras, teléfonos inteligentes, tabletas y dispositivos IoT, contra amenazas y ataques cibernéticos.

Esto incluye el uso de firewalls, antivirus, actualizaciones de seguridad, cifrado de datos, políticas de acceso seguro y prácticas de seguridad física para proteger la integridad y la confidencialidad de la información.

La auditoría de seguridad es un proceso de evaluación sistemática de los controles de seguridad de una organización para garantizar su eficacia y cumplimiento normativo.

Esto implica revisar y evaluar las políticas y procedimientos de seguridad, realizar pruebas de vulnerabilidad y explotación, analizar registros y registros de auditoría, y documentar hallazgos y recomendaciones para mejorar la postura de seguridad de la organización.

SUJETOS EN LA LFPDPPP Y OTRAS DEFINICIONES

1

El Titular: Este actor es la persona física a quien corresponden los datos personales. El titular de los datos personales es el dueño de los mismos. Es aquel individuo que es responsable de controlar y decidir cómo se utilizan los datos personales. Por ejemplo, si una persona quiere comprar en Amazon, el titular de los datos sería el cliente que va proporcionar datos de identidad. tal como nombre, dirección, información de pago, etc

El Responsable: Es una persona física o moral de carácter privado que decide sobre el tratamiento de datos personales, así como tal, Microsoft Corporation, es un proveedor de software y servicios en la nube en donde recopila datos personales a través de productos como Windows, Office 365, Linkedin & Azure, para crear servicios de productividad, confiabilidad y almacenamiento de datos.

2

3

El Encargado: El Reglamento General de Protección de Datos (RFPD) en la Unión Europea y la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) en México, considera que el encargado es una persona física o moral, pública o privada, ajena a la organización del responsable, siguiendo instrucciones y lineamientos establecidos por el eset último y en el acuerdo legal respecto a responsabilidades y obligaciones.

El tratamiento: El "tratamiento" de datos personales se refiere a un proceso dinámico que abarca la obtención, uso, divulgación y almacenamiento de información de carácter personal. Este proceso puede tomar diversas formas, como el acceso a la información, su manipulación, su aprovechamiento para distintos fines, su transferencia entre sistemas o su eliminación cuando ya no es necesaria.

4

5

Transacciones: se refieren a la comunicación de información personal a terceros que no son responsables ni encargados del tratamiento de dichos datos. Este proceso puede involucrar transferencias tanto a nivel nacional como internacional. En la mayoría de los casos, estas transferencias requieren el consentimiento explícito del titular de los datos, a menos que se apliquen excepciones específicas establecidas en las leyes pertinentes.

PRINCIPIOS DE LA PROTECCIÓN DE DATOS PERSONALES

El derecho a la protección de los datos personales en nuestro país se sistematiza a través de ocho principios y dos deberes, los cuales se traducen en tareas que se asignan obligatoriamente a los responsables del tratamiento, y en derechos de los titulares.

Tanto la LFPDPPP como la LGPDPPSO contemplan que los responsables del tratamiento de datos personales deberán observar los siguientes principios::

- Licitud
- Consentimiento
- Información
- Información
- Calidad
- Finalidad
- Lealtad
- Proporcionalidad
- Responsabilidad

Licitud: El principio de Licitud es aquel procesamiento de datos que debe basarse en una base legal válida, como el consentimiento del titular de los datos, el cumplimiento de una obligación legal, la ejecución de un contrato, el interés legítimo del responsable del tratamiento, entre otros.

Las obligaciones ligadas al principio de licitud están estrechamente relacionadas con garantizar que el tratamiento de datos personales se realice de acuerdo con la ley y los principios establecidos en la normativa de protección de datos,.

Consentimiento: El consentimiento implica que los titulares de los datos deben dar su consentimiento libre, específico e informado para el tratamiento de sus datos personales.

Información: Este principio establece que los titulares de los datos deben recibir información clara y completa sobre el tratamiento de sus datos personales.

Calidad: Este principio establece que los datos personales deben ser precisos, completos y actualizados según sea necesario para los fines para los que se recopilan y utilizan.

Los responsables del tratamiento deben tomar medidas razonables para garantizar la exactitud de los datos y corregir cualquier información inexacta o incompleta.

Finalidad: Este principio establece que los datos personales deben recopilarse para fines específicos y legítimos, y no deben utilizarse de manera incompatible con esos fines.

Los responsables del tratamiento deben definir claramente los propósitos para los cuales se recopilan los datos y no pueden utilizarlos para otros fines sin el consentimiento del titular.

Lealtad: La lealtad implica que el tratamiento de datos debe llevarse a cabo de manera honesta y transparente. Los responsables del tratamiento deben actuar de buena fe y no engañar a los titulares de los datos.

Proporcionalidad: La proporcionalidad implica que el tratamiento de datos debe ser adecuado, relevante y limitado a lo necesario para los fines para los que se recopilan. En relación al principio de proporcionalidad, existen ciertas obligaciones que los responsables del tratamiento de datos personales deben cumplir:

Relevancia y necesidad: Los datos personales deben ser tratados únicamente si son necesarios, adecuados y relevantes para las finalidades específicas para las cuales se obtuvieron.

Minimización de datos: Se debe tratar el menor número posible de datos personales en función de las finalidades que justifican su procesamiento.

Periodo de tratamiento limitado: Es fundamental limitar al mínimo posible el tiempo durante el cual se conservan los datos personales, especialmente cuando se trata de datos sensibles.

Responsabilidad: La responsabilidad implica que los responsables del tratamiento son responsables de cumplir con todas las disposiciones de protección de datos y deben poder demostrar su cumplimiento.

PRINCIPIOS DE LA PROTECCIÓN DE DATOS PERSONALES
DERECHOS Y DEBERES

Derecho de acceso: El derecho de acceso en protección de datos otorga al titular el derecho a conocer:

- Identidad del responsable del tratamiento, encargado o sus representantes.
- Tipos de datos personales que se van a tratar y la finalidad de ese tratamiento.
- Destinatarios o clases de destinatarios a los que se comunicaron o serán comunicados los datos personales.
- Plazo previsto durante el cual se conservarán los datos personales.

Este derecho permite a los individuos participar en el tratamiento que otros hacen de sus datos personales. Además, protege el manejo justo de su información personal al garantizarles el acceso, rectificación, cancelación y oposición al tratamiento de los mismos (derechos ARCO).

Derecho de rectificación: El derecho de rectificación es fundamental para garantizar la exactitud y actualización de los datos personales. Los titulares pueden solicitar la corrección de información incorrecta, incompleta o desactualizada. Aquí hay algunos puntos clave sobre este derecho:

Inexactitudes: Si un dato personal es incorrecto o contiene errores, el titular tiene el derecho de solicitar su corrección. Por ejemplo, en el caso que mencionaste, si el domicilio registrado no es el correcto y afecta la entrega de documentación, se puede pedir la rectificación.

Completitud: Además de la corrección, el titular puede requerir que se completen datos personales que estén incompletos. Por ejemplo, si falta algún dato relevante en un expediente, se puede solicitar su inclusión.

Actualización: Si los datos personales están desactualizados (por ejemplo, cambio de dirección o número telefónico), el titular puede pedir que se actualicen.

Derecho de cancelación: El derecho de cancelación permite a los titulares solicitar al responsable que elimine o cancele sus datos personales de archivos, registros, expedientes, bases de datos o sistemas.

Esto implica detener el tratamiento de esos datos mediante un bloqueo y su posterior supresión. Sin embargo, hay algunas consideraciones importantes:

Limitaciones legales: No siempre es posible eliminar los datos personales. Puede haber cuestiones legales que impidan la cancelación, o los datos pueden ser necesarios para cumplir con responsabilidades derivadas del tratamiento.

Derecho de oposición: El derecho de oposición es fundamental en la protección de datos personales. Permite a los titulares solicitar al responsable que deje de utilizar sus datos personales o que cese su uso.

Ejemplo: Eres miembro de una red social y has estado recibiendo anuncios personalizados basados en tus intereses y comportamiento en línea. Sin embargo, decides que ya no deseas que la plataforma utilice tus datos para mostrarte publicidad específica. En este caso, puedes ejercer tu derecho de oposición. La red social deberá dejar de utilizar tus datos personales para fines publicitarios y ajustar la configuración de privacidad según tus preferencias.

Recuerda que es importante conocer tus derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) para proteger tus datos personales de manera efectiva.

Deber de Confidencialidad: Es un principio fundamental en la protección de datos personales. Se refiere a la obligación de mantener la privacidad y seguridad de la información confidencial que se maneja en una organización.

Deber de seguridad: El deber de seguridad es una responsabilidad fundamental cuando se trata de proteger los datos personales. Se refiere a la obligación de implementar y mantener medidas de seguridad de datos personales.

LAS OSC Y LOS DATOS PERSONALES

IMPORTANCIA DE LA PROTECCIÓN DE DATOS EN (OSC)

1 Elemento 1

Lasl OSC deben obtener el permiso explícito y consciente de las personas antes de recopilar, procesar o compartir sus datos personales.

2 Elemento 2

Las OSC deben implementar medidas de seguridad para proteger los datos que manejan. Esto incluye el uso de contraseñas seguras, cifrado de datos, acceso restringido y protección.

3 Elemento 3

Este principio se refiere a recopilar solo la información necesaria y relevante para el propósito específico. Las OSC deben evitar la recopilación excesiva de datos personales.

Derecho de cancelación: El derecho de cancelación permite a los titulares solicitar al responsable que elimine o cancele sus datos personales de archivos, registros, expedientes, bases de datos o sistemas.

Esto implica detener el tratamiento de esos datos mediante un bloqueo y su posterior supresión. Sin embargo, hay algunas consideraciones importantes:

Limitaciones legales: No siempre es posible eliminar los datos personales. Puede haber cuestiones legales que impidan la cancelación, o los datos pueden ser necesarios para cumplir con responsabilidades derivadas del tratamiento.

Derecho de oposición: El derecho de oposición es fundamental en la protección de datos personales. Permite a los titulares solicitar al responsable que deje de utilizar sus datos personales o que cese su uso.

Ejemplo: Eres miembro de una red social y has estado recibiendo anuncios personalizados basados en tus intereses y comportamiento en línea. Sin embargo, decides que ya no deseas que la plataforma utilice tus datos para mostrarte publicidad específica.

Derecho de cancelación: El derecho de cancelación permite a los titulares solicitar al responsable que elimine o cancele sus datos personales de archivos, registros, expedientes, bases de datos o sistemas.

Esto implica detener el tratamiento de esos datos mediante un bloqueo y su posterior supresión. Sin embargo, hay algunas consideraciones importantes:

Limitaciones legales: No siempre es posible eliminar los datos personales. Puede haber cuestiones legales que impidan la cancelación, o los datos pueden ser necesarios para cumplir con responsabilidades derivadas del tratamiento.

Derecho de oposición: El derecho de oposición es fundamental en la protección de datos personales. Permite a los titulares solicitar al responsable que deje de utilizar sus datos personales o que cese su uso.

Ejemplo: Eres miembro de una red social y has estado recibiendo anuncios personalizados basados en tus intereses y comportamiento en línea. Sin embargo, decides que ya no deseas que la plataforma utilice tus datos para mostrarte publicidad específica.

EL AVISO DE PRIVACIDAD

EL AVISO DE PRIVACIDAD DEL INAI

El Aviso de Privacidad es un documento, físico, electrónico o en cualquier formato, que el responsable pone a disposición del titular para informarle sobre el tratamiento de sus datos personales.
Importancia:

Quién es responsable de tus datos.
Para qué se utilizan tus datos.
Qué tipo de datos se recopilan.
Tus derechos como titular de los datos.

Elementos Clave:

- **Responsable de tus datos:** El aviso debe indicar quién es la entidad o persona responsable de recopilar y procesar tus datos personales.

- **Finalidad del uso de datos:** El aviso debe explicar con claridad para qué se utilizarán tus datos. Por ejemplo, si es para proporcionar un servicio, para fines comerciales o para cumplir con obligaciones legales.

- **Tipo de datos recopilados:** Debe detallar qué información se recopila, asi como incluir datos personales como nombre, dirección, número de teléfono, correo electrónico, etc.

- **Derechos del titular de datos:** El aviso debe informarte sobre tus derechos. Estos pueden incluir el derecho a acceder a tus datos, corregirlos, eliminarlos o limitar su procesamiento.

El Generador de **Avisos de Privacidad del INAI** es un punto de partida ideal para crear tu propio aviso.

¿Por dónde empezar?

1. Selecciona el tipo de aviso que necesitas:

- **Sector Público:** Si eres una entidad pública, elige esta opción.

- **Sector Privado:** Si eres una empresa o persona física que trata datos personales, elige esta opción.

2. Responde las preguntas del formulario:

- **Información básica:** Nombre de tu organización, domicilio, etc.

- **Finalidades del tratamiento:** ¿Para qué vas a utilizar los datos personales?

- **Datos personales que se recaban:** ¿Qué tipo de datos personales vas a recopilar?

- **Derechos ARCO:** ¿Cómo pueden los titulares ejercer sus derechos?

- **Transferencias de datos:** ¿Vas a compartir los datos con terceros?

- **Mecanismos para ejercer derechos:** ¿Cómo pueden los titulares contactarte para ejercer sus derechos?

3. Descarga tu Aviso de Privacidad:

El sistema te proporcionará un aviso de privacidad personalizado en formato PDF.

- **Recuerda:** Completa el formulario con atención y veracidad.

- **Recursos adicionales:** Guía para elaborar el Aviso de Privacidad: https://home.inai.org.mx/

Consejos para crear un Aviso de Privacidad efectivo:

- Utiliza un lenguaje claro y sencillo.
- Evita el uso de tecnicismos legales.
- Organiza la información de forma lógica y ordenada.
- Destaca los puntos más importantes.
- Haz que sea fácil de leer y comprender

¡Con el apoyo del INAI y estos consejos, podrás crear un Aviso de Privacidad que proteja los datos personales de tus clientes y usuarios!

¿EN QUÉ MOMENTO SE DEBE PONER A DISPOSICIÓN ?
EL AVISO DE PRIVACIDAD

El momento en que el responsable debe proporcionar el aviso de privacidad a los titulares varía según la manera en que se recopilen los datos personales. Si los datos se obtienen de forma personal, directa o indirecta del titular, se establece un momento específico para su entrega.

Obtención de forma personal: Sucede cuando el titular proporciona los datos personalmente al responsable o a una persona física designada por él, en presencia física de ambos.

Obtención de forma directa: Ocurre cuando el titular proporciona los datos mediante cualquier medio que permita su entrega directa al responsable, como medios electrónicos, ópticos, sonoros, visuales o cualquier otra tecnología disponible, como el correo postal, Internet o vía telefónica.

Obtención de forma indirecta: Se da cuando el responsable obtiene los datos sin que el titular los haya proporcionado de manera personal o directa.

A) Previo a la obtención de los datos personales	En el momento que se recolectan datos personales de manera directa o cara a cara con el titular de los mismos, el responsable está obligado a proporcionar al titular su aviso de privacidad antes de que este último le entregue su información personal.
B) Al primer contacto con el titular	Los datos personales se obtienen de manera indirecta, es decir, a través de fuentes como registros públicos, y el tratamiento de dichos datos implicará un contacto directo o personal con el titular, el responsable está obligado a proporcionar al titular su aviso de privacidad.
C) Previo al aprovechamiento de datos personales	Los datos personales se obtienen de manera indirecta y el tratamiento para el cual serán utilizados no requiere contacto personal o directo con el titular, el responsable debe poner a disposición del titular su aviso de privacidad antes de llevar a cabo cualquier actividad relacionada con el tratamiento de esos datos.

¿Se puede utilizar un único aviso de privacidad para distintas actividades?

Se puede usar un solo aviso de privacidad para diferentes actividades siempre y cuando los tratamientos de datos sean similares en términos de propósito, tipo de datos y transferencias. Sin embargo, no se recomienda si las actividades involucran información diferente.

¿Cuáles son las modalidades del aviso de privacidad?

Las modalidades del aviso de privacidad respecto a la ley, reglamento y lineamientos reconocen tres modalidades del aviso de privacidad:

- Integral
- Simplificado
- Corto

¿Por qué medios se puede difundir el aviso de privacidad?

Aviso de privacidad integral y simplificado

- Formato impreso
- Electrónico o digital
- Óptico o visual
- Sonoro
- Otra tecnología

Aviso de privacidad corto

- Espacios mínimos y limitados:
  - Cupón de una tarifa
  - Cajero automático
  - Mensaje SMS

MODALIDADES DEL AVISO DE PRIVACIDAD

El aviso de privacidad puede presentarse en tres modalidades: integral, simplificado y corto.

Modalidad	Casos en los que se utiliza
Aviso de privacidad integral	El aviso de privacidad integral se utiliza en casos donde los datos personales se recaban personalmente del titular, es decir, cuando el titular está presente físicamente ante el responsable. Este tipo de aviso proporciona una descripción detallada de todos los elementos necesarios para informar al titular sobre el tratamiento de sus datos personales, de acuerdo con la normativa de protección de datos aplicable.
Aviso de privacidad simplificado	El aviso de privacidad simplificado se utiliza cuando los datos personales se obtienen directamente del titular, a través de Internet o vía telefónica. Este tipo de aviso proporciona información esencial de manera clara y concisa, incluyendo la identidad y domicilio del responsable, las finalidades del tratamiento, los mecanismos para que el titular pueda expresar su negativa respecto al tratamiento de sus datos para finalidades secundarias o accesorias, y los mecanismos para que el titular pueda acceder al aviso de privacidad integral.
Aviso de privacidad corto	Este tipo de aviso proporciona información básica y esencial, incluyendo la identidad del responsable, el domicilio del responsable, las finalidades del tratamiento (sin necesidad de distinguir entre finalidades secundarias o accesorias), y los mecanismos para que el titular pueda acceder al aviso de privacidad integral para obtener más información si así lo desea.

¿Cuáles son las modalidades del aviso de privacidad?

Las modalidades del aviso de privacidad respecto a la ley, reglamento y lineamientos reconocen tres modalidades del aviso de privacidad:

- Integral
- Simplificado
- Corto

¿Cuáles son las modalidades del aviso de privacidad?

Las modalidades del aviso de privacidad respecto a la ley, reglamento y lineamientos reconocen tres modalidades del aviso de privacidad:

- Integral
- Simplificado
- Corto

AVISO IMPORTANTE:

El responsable debe proporcionar a los titulares un aviso de privacidad en sus modalidades simplificada o corta, pero también está obligado a tener un aviso de privacidad integral permanentemente disponible. Este aviso integral debe complementar las versiones simplificadas y debe ser accesible a través de medios convenientes para los titulares, privilegiando aquellos que sean de fácil acceso y con amplia cobertura, considerando el perfil de los titulares y los canales de comunicación disponibles

DEBERES DE LAS OSC COMO SUJETOS RESPONSABLES

Las Organizaciones de la Sociedad Civil (OSC) tienen una serie de deberes y responsabilidades como sujetos responsables dentro de la sociedad.

Confidencialidad:

La confidencialidad es crucial para proteger la información personal de los individuos, asegurando que no se divulgue sin su consentimiento. Las Organizaciones de la Sociedad Civil (OSC) y terceros responsables deben garantizar la estricta confidencialidad de los datos personales proporcionados por los individuos, incluso después de finalizar la relación entre la OSC y los titulares.

Medidas físicas:

Control de acceso físico a las instalaciones donde se almacenan los datos personales mediante cerraduras, tarjetas de acceso, cámaras de vigilancia, etc.

El almacenamiento seguro de documentos físicos en archivadores con llave o en salas con acceso restringido.

Protección contra incendios, inundaciones u otros desastres naturales que puedan dañar la infraestructura física que alberga los datos.

Medidas administrativas:

Políticas y procedimientos claros para el manejo de datos personales, que incluyan la identificación de responsables de la protección de datos y la asignación de roles y responsabilidades.

Capacitación regular del personal en cuanto a la importancia de la confidencialidad y la seguridad de la información, así como en los procedimientos establecidos para su protección.

Implementación de controles de acceso, como contraseñas robustas, autenticación de dos factores y políticas de acceso basadas en roles, para limitar el acceso solo a personal autorizado.

Medidas técnicas:

Uso de software antivirus y antispyware actualizado para proteger los sistemas contra amenazas cibernéticas.ar la disponibilidad y la integridad de la información.

Encriptación de datos tanto en reposo (almacenados) como en tránsito (transmitidos a través de redes) para evitar accesos no autorizados.

Implementación de firewalls y sistemas de detección de intrusiones para proteger la red y los sistemas informáticos contra accesos no autorizados.

Establecimiento de copias de seguridad regulares y sistemas de recuperación de datos para garantizar la disponibilidad y la integridad de la información en caso de incidentes.

Estas medidas deben ser parte de un enfoque integral de seguridad de la información, adaptado a las necesidades y características específicas de cada organización y en cumplimiento con las regulaciones y leyes de protección de datos aplicables.

MEDIDAS DE SEGURIDAD FÍSICA PUEDE SER:

Control de acceso físico: Limitar el acceso a las instalaciones donde se almacenan los datos personales mediante sistemas de cerraduras, tarjetas de acceso, códigos de acceso, o sistemas biométricos como escaneo de huellas dactilares o reconocimiento facial.

Vigilancia por cámaras: Instalación de sistemas de cámaras de seguridad para monitorear y registrar cualquier actividad sospechosa en áreas donde se manejan datos sensibles.

“Manual de Protección de Datos personales para Transversal ThinkTank se editó en la Ciudad de Guadalajara, Jalisco en marzo de 2024”