C5 Jalisco®
Escudo Urbano

Políticas para la Gestión y Tratamiento de Datos Personales del Centro de Coordinación, Comando, Control, Comunicaciones y Computo del Estado de Jalisco “Escudo Urbano C5”.

Tabla de contenido

I. DISPOSICIONES GENERALES. 3

Objetivo. 4

Ámbito de aplicación. 4

Conceptos definiciones y abreviaturas. 4

II. CONTROLES PARA GARANTIZAR LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LOS DATOS PERSONALES. 12

Cumplimiento de principios, deberes y demás obligaciones. 12

1. Principios de licitud y lealtad 13
2. Principio del consentimiento 14
3. Principio de información 14
4. Principio de proporcionalidad 14
5. Principio de finalidad 15
6. Principio de calidad 16
7. Principio de responsabilidad 17

A. Deber de Confidencialidad 17

B. Deber de Seguridad 17

III. ROLES Y RESPONSABILIDADES DEL TRATAMIENTO DE DATOS PERSONALES. 22

¿Qué es un dato personal sensible? 22

¿Qué se entiende por tratamiento de datos personales? 22

IV. SANCIONES POR EL INCUMPLIMIENTO. 23

V. CICLO DE VIDA DE LOS DATOS PERSONALES. 25

VI. ATENCIÓN DE LOS DERECHOS ARCO. 25

VII. MARCO LEGAL. 27

Referencias. 27

Oficialía de Partes del C5 Jalisco, ubicado en la Fiscalía del Estado, segundo nivel,
(a un costado de la Dirección de Tramitación Masiva) con domicilio en la calle 14 No. 2550, colonia Industrial en Guadalajara, Jalisco

I. DISPOSICIONES GENERALES.

Las Políticas tienen por objeto establecer acciones generales y mecanismos para el cumplimiento de los principios, deberes, derechos y obligaciones en materia de datos personales, de conformidad con lo previsto en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios. Serán aplicables a cualquier tratamiento de datos personales que obren en posesión del Centro de Coordinación, Comando, Control, Comunicaciones y Computo, del Estado de Jalisco en lo sucesivo "Escudo Urbano C5", ya sea en soportes físicos, electrónicos o mixtos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

El tratamiento de datos personales deberá sujetarse a las facultades o atribuciones que la normatividad aplicable confiere al Escudo Urbano C5, y estar justificado por finalidades concretas, lícitas, explícitas y legítimas establecidas en los avisos de privacidad aplicables a este Organismo.

Previo a recabar datos personales, se deberá mostrar el Aviso de Privacidad Integral del sistema de tratamiento aplicable.

Los avisos de privacidad deben encontrarse visibles en todas las áreas administrativas de este Organismo, que recaben datos personales.

No deberán obtenerse y tratar datos personales, a través de medios engañosos o fraudulentos.

Cuando se recaben datos personales sensibles, de conformidad a lo establecido en el artículo 3, fracción X, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, deberá obtenerse el consentimiento expreso, con nombre y firma autógrafa de los titulares.

Cuando se recaben datos personales de menores deberá obtenerse el consentimiento expreso, con nombre y firma autógrafa de quienes ejerzan la patria potestad o tutela sobre éstos.

Se deberán adoptar las medidas necesarias para mantener exactos, completos, pertinentes, correctos y actualizados los datos personales que se reciban en ejercicio de las atribuciones y facultades del "Escudo Urbano C5".

Es obligación de todas las personas servidoras públicas del Escudo Urbano C5, que administren, actualicen o tengan acceso a bases de datos personales, conservar, manejar y mantener de manera estrictamente confidencial dicha información y no revelarla a terceros.

Los avisos de privacidad deberán ser elaborados en sus modalidades: integral, simplificado, y corto.

Los datos personales sólo pueden ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas a la persona titular en el aviso de privacidad y, en su caso, consentidas por ésta.

Se deben establecer y mantener medidas de seguridad técnicas, físicas y administrativas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Serán causas de sanción el incumplimiento a las obligaciones en materia de protección de datos personales, las establecidas en las disposiciones normativas aplicables.

Objetivo.

Contar con un instrumento que fortalezca los principios y deberes en materia de protección de datos personales en los procesos internos de gestión y tratamiento de datos personales dentro del Escudo Urbano C5; que facilite el actuar de los servidores públicos cumpliendo y velando en todo momento por la protección de los datos personales.

Ámbito de aplicación.

Las Políticas son de observancia general y obligatoria para el personal que labora en el Escudo Urbano C5, así como para terceros, que lleven a cabo el tratamiento de datos personales en posesión de este Organismo, o conozcan por alguna circunstancia de éstos en el cumplimiento de facultades, atribuciones, o competencias.

Conceptos definiciones y abreviaturas.

ITEI: Instituto de Transparencia Acceso a la Información y Protección de Datos personales del Estado de Jalisco

LGTAIP: Ley General de Transparencia y Acceso a la Información Pública

LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

LGA: Ley General de Archivos

LTAIPEJM: Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios

LPDPPSOEJM: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios

LAEJM: Ley de Archivos del Estado de Jalisco y sus Municipios

BAA: Beneficio, Accesibilidad y Anonimidad.

Anonimización: al tratamiento que permite evitar la identificación de la o el titular a través de sus datos personales

Archivo de concentración: el integrado por documentos transferidos desde las áreas o unidades productoras, cuyo uso y consulta es esporádica y que permanecen en él hasta su disposición documental.

Archivo histórico: el integrado por documentos de conservación permanente y de relevancia para la memoria del "Escudo Urbano C5", que concentra, organiza, conserva, resguarda, restaura y difunde los documentos de interés histórico.

Archivo de trámite: el integrado por documentos de archivo de uso cotidiano y necesario para el ejercicio de las atribuciones y funciones de los sujetos obligados.

Auditabilidad: característica que permite la revisión y análisis de eventos y análisis para su control posterior.

Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Autentificar: acción de comprobar que la persona es quien dice ser. Ello, mediante el cotejo de uno o más datos en dicha identificación oficial contra.

(i) los datos en alguna otra identificación, documento, certificado digital (como el de la firma electrónica) o dispositivo que tenga la persona,
(ii) los datos que sepa o tenga memorizados (su firma autógrafa o su contraseña, por ejemplo) o
(iii) una o más características que coincidan con lo que es dicha persona (fotografía o huella dactilar, por ejemplo).

Autorizar: se considera como el acceso que se le permite a la persona que se ha identificado y autenticado apropiadamente. Esto depende del o de los permisos que le conceda el responsable de autorizar los accesos.

Aviso de privacidad: al documento físico, electrónico o en cualquier formato generado por el responsable que es puesto a disposición del Titular con el objeto de informarle los propósitos del tratamiento al que serán sometidos sus datos personales.

Baja documental: la eliminación de aquella documentación cuya vigencia haya prescrito en sus valores administrativos, legales, fiscales o contables, y en su caso, plazos de conservación, siempre y cuando no posea valores históricos de acuerdo con esta Ley y las disposiciones legales aplicables.

Bloqueo: la identificación y conservación de los datos personales, una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, el ejercicio de derechos ARCO y Portabilidad, hasta el plazo de prescripción legal contractual correspondiente, con relación al catálogo de disposición documental y finalizando una vez realizado el proceso de disposición documental final ya sea para baja o transferencia secundaria. Durante dicho período los datos personales no podrán ser objeto de tratamiento diferente al de estar

almacenados o acceso previa solicitud de la unidad productora, por lo que concluido éste se deberá proceder a la supresión en la base de datos, archivo, registro, expediente o sistema de información que corresponda.

Catálogo de disposición documental: el registro general y sistemático que identifica los valores documentales, la vigencia documental, los plazos de conservación y la disposición documental.

Ciclo vital del documento: las etapas por las que atraviesan los documentos de archivo desde su producción o recepción hasta su baja documental o transferencia a un archivo histórico.

Clasificación de información pública: acto por el cual se determina que la información que posee el "Escudo Urbano C5" es reservada o confidencial de conformidad con la normatividad en materia de transparencia y acceso a la información.

Clasificación archivística: proceso de identificación y agrupación de expedientes homogéneos con base en la estructura funcional del "Escudo Urbano C5".

Comité: el Comité de Transparencia del "Escudo Urbano C5".

Cómputo en la nube: al modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

Conservación de archivos: el conjunto de procedimientos y medidas destinados a asegurar la prevención de alteraciones físicas de los documentos en papel y la conservación de los documentos a largo plazo.

Confiabilidad de la Información: expresa la garantía de que la información generada es adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad: propiedad de prevenir la divulgación de información a personas o sistemas no autorizados, y que garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma, es decir, asegurar que la misma no sea divulgada o accedida a personas o procesos no autorizados.

Control de acceso: medida de seguridad que permite el acceso únicamente a quien está autorizado para ello y una vez que se ha cumplido con el procedimiento de identificación y autentificación.

Conservación de archivos: el conjunto de procedimientos y medidas destinados a asegurar la prevención de alteraciones físicas de los documentos en papel y la conservación de los documentos a largo plazo.

Cuadro general de clasificación archivística: el instrumento técnico que refleja la estructura de un archivo con base en las series documentales generadas por las atribuciones y funciones de cada sujeto obligado.

Datos abiertos: los datos digitales en formatos abiertos de carácter público que son accesibles en línea y pueden ser usados, reutilizados y redistribuidos por cualquier interesado.

Datos personales: cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Datos personales sensibles: aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleva un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

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.

Disponibilidad: característica, cualidad o condición de la información de encontrarse presente de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones, garantizando el acceso a la información y a los recursos relacionados con la misma, cada vez que requieran, garantizando su localización expedita.

Disposición documental: la selección sistemática de los expedientes de los archivos de trámite o concentración cuya vigencia documental o uso ha prescrito, con el fin de realizar transferencias ordenadas o bajas documentales.

Documento de archivo: aquel que registra un hecho, acto administrativo, jurídico, fiscal o contable producido, recibido y utilizado en el ejercicio de las facultades, competencias o funciones de los sujetos obligados, con independencia de su soporte documental.

Documento de seguridad: 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.

Documentos: los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades o la actividad de del "Escudo Urbano C5" y sus servidores públicos, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico.

Documentos históricos: los que se preservan permanentemente porque poseen valores evidénciales, testimoniales e informativos relevantes para la sociedad, y que por ello forman parte íntegra de la memoria colectiva del Estado y son fundamentales para el conocimiento de la historia local, regional e incluso nacional.

Encargado: persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales a nombre y por cuenta del responsable.

Escudo Urbano C5: el Centro de Coordinación, Comando, Control, Comunicaciones y Cómputo del Estado de Jalisco.

Expediente: la unidad documental compuesta por documentos de archivo, ordenados y relacionados por un mismo asunto, actividad o trámite de los sujetos obligados con independencia de su soporte documental.

Ficha técnica de valoración documental: el instrumento que permite identificar, analizar y establecer el contexto y valoración de la serie documental.

Gestión documental: tratamiento integral de la documentación a lo largo de su ciclo vital, a través de la ejecución de procesos de producción, organización, acceso, consulta, valoración documental y conservación.

Identificar: consiste aportar las pruebas necesarias para corroborar que una persona es quien dice ser, lo cual puede realizarse, por ejemplo, con una identificación que tenga validez oficial y en un ambiente electrónico con el nombre de usuario que se introduce al momento de ingresar al sistema (logín).

Información pública: es toda información que generen, posean o administren los sujetos obligados, como consecuencia del ejercicio de sus facultades o atribuciones, o el cumplimiento de sus obligaciones, sin importar su origen, utilización o el medio en el que se contenga o almacene; la cual está contenida en documentos, fotografías, grabaciones, soporte magnético, digital, sonoro, visual, electrónico, informático, holográfico o en cualquier otro elemento técnico existente o que surja con posterioridad.

Información pública confidencial: que es la información pública protegida, intransferible e indelegable, relativa a los particulares, que por disposición legal queda prohibido su acceso, distribución, comercialización, publicación y difusión generales de forma permanente, con excepción de las autoridades competentes que, conforme a esta ley o la legislación estatal en materia de protección de datos personales en posesión de sujetos obligados, tengan acceso a ella, y de los particulares titulares de dicha información.

Información focalizada: que es la información de interés público sobre un tema específico, susceptible de ser cuantificada, analizada y comparada; en la que se apoyen los sujetos obligados en la toma de decisiones o criterios que permitan evaluar el impacto de las políticas públicas y que, asimismo, faciliten la sistematización de la información y la publicidad de sus aspectos más relevantes, de conformidad con los lineamientos del Instituto.

Información pública fundamental: que es la información pública de libre acceso que debe publicarse y difundirse de manera universal, permanente, actualizada y, en el caso de la información electrónica, a través de formatos abiertos y accesibles para el ciudadano, por ministerio de ley, sin que se requiera solicitud de parte interesada. Los sujetos obligados buscarán, en todo momento, que la información generada tenga un lenguaje sencillo para cualquier persona y se procurará, en la medida de lo posible y de acuerdo a la disponibilidad presupuestal, su accesibilidad y traducción a lenguas indígenas.

Información pública ordinaria: que es la información pública de libre acceso no considerada como fundamental. La información pública que obra en documentos históricos será considerada como información pública ordinaria.

Información proactiva: que es la información específica relativa a casos de especial interés público, en los términos de los lineamientos generales definidos para ello por el Sistema Nacional, diseñadas para incentivar a los sujetos obligados a publicar información adicional a la que se establece como mínimo la información fundamental.

Información pública reservada: que es la información pública protegida, relativa a la función pública, que por disposición legal temporalmente queda prohibido su manejo, distribución, publicación y difusión generales, con excepción de las autoridades competentes que, de conformidad con la ley, tengan acceso a ella.

Instituto: Instituto de Transparencia Acceso a la Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI).

Integridad: es garantizar la exactitud, totalidad y la confiabilidad de la información y los sistemas o métodos de procesamiento de manera que éstos no puedan ser modificados sin autorización, ya sea accidental o intencionadamente.

Ley: la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Ley General: la Ley General de Protección de Datos Personales en Posesión de Sujeto Obligados.

Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Medidas de seguridad: conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales.

Medidas de seguridad administrativas: políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación de información pública y borrado seguro de la información, así como la sensibilización, formación y capacitación del personal, en materia de protección de datos personales.

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. De manera enunciativa más no limitativa, se debe considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información.
b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información.
c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico, que pueda salir fuera de las instalaciones de la organización.

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

Medidas de seguridad técnicas: conjunto de acciones y mecanismos que salen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir que el acceso a las bases de datos o a la información, 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.

Plazo de conservación: periodo de guarda de la documentación en los archivos de trámite y concentración, que consiste en la combinación de la vigencia documental y, en su caso, el término precautorio y periodo de reserva que se establezcan de conformidad con la normatividad aplicable.

Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

Publicación: comunicación de información pública mediante la reproducción en medios electrónicos o impresos de información contenida en documentos, respecto de la información fundamental, focalizada, proactiva o de interés público señalada en la Ley o Ley General en materia de transparencia.

Recomendaciones: las opiniones, propuestas, sugerencias, comentarios, y otros actos que emite el Instituto.

Remisión: Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano;

Responsable: el "Escudo Urbano C5" y los sujetos obligados señalados en el artículo 1, párrafo 5, de la Ley que determinará.

Responsable Titular: el servidor público titular de la unidad administrativa, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales.

Responsable Enlace: Servidor público designado por el titular de la Unidad Administrativa que tiene a su cargo la responsabilidad de mantener actualizado el documento de seguridad.

Responsable Usuario: los servidores públicos del "Escudo Urbano C5" que están autorizados para tratar datos personales. Servidor público facultado por un instrumento jurídico o expresamente

autorizado por el Responsable que utiliza de manera cotidiana datos personales para el ejercicio de sus atribuciones, por lo que accede a los sistemas de datos personales.

Supresión: la baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el Responsable.

Servidores públicos: los mencionados en el párrafo primero del Artículo 108 Constitucional y todas aquellas personas que manejen o apliquen recursos públicos.

Sistema de datos personales: el conjunto ordenado de datos personales que estén en posesión de un Responsable.

Sistema de Información: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Soportes documentales: los medios en los cuales se contiene información además del papel, siendo estos materiales audiovisuales, fotográficos, fílmicos, digitales, electrónicos, sonoros, visuales, entre otros.

Soportes físicos: son los medios de almacenamiento identificables a simple vista, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados “a mano” o “a máquina”, fotografías, placas radiológicas, carpetas, expedientes, entre otros.

Sujetos obligados: cualquier autoridad, dependencia o entidad de los Poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, organismos públicos descentralizados, partidos políticos, fideicomisos y fondos públicos del Estado de Jalisco y de sus municipios; así como cualquier persona física, jurídica o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal.

Tecnología de la Información: se refiere al hardware y software operado por el Responsable o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Responsable, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Titular de los datos: persona física a quien se refieren los datos personales que sean objeto de tratamiento.

Transferencia: toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado;

Transferencia documental: el traslado controlado y sistemático de expedientes de consulta esporádica de un archivo de trámite a uno de concentración o transferencia primaria, y de expedientes que deben conservarse de manera permanente, del archivo de concentración al archivo histórico o transferencia secundaria.

Transmisión de datos personales. la entrega total o parcial de sistemas de datos personales a cualquier persona distinta del titular de los datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de computadoras o bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.

Transmisor: dependencia o entidad que posee los datos personales objeto de la transmisión.

Tratamiento: de manera enunciativa más no limitativa cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Unidades administrativas: las que, de acuerdo con la Ley Orgánica, y demás normatividad aplicable, tengan la información de conformidad con las facultades que les correspondan.

Unidad de Transparencia: instancia que funge como vínculo entre el responsable y el titular, siendo la misma a la que se hace referencia en el artículo 31 de la Ley en materia de Transparencia para el Estado de Jalisco y en la Ley.

Valoración documental: análisis e identificación de los valores documentales, consistente en el estudio de la condición de los documentos que les confiere características específicas en los archivos de trámite, de concentración o de evidencia, testimoniales e informativos para los documentos históricos, con la finalidad de establecer criterios de destino final, así como para la disposición documental a través de los plazos de conservación.

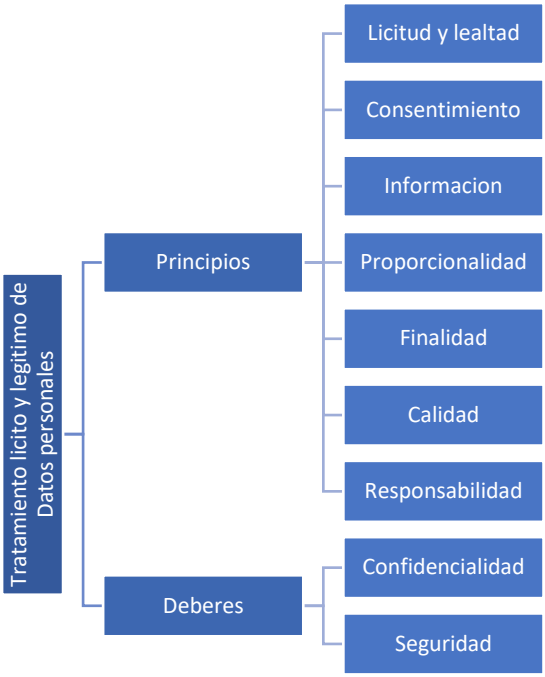
Versión pública: Documento en el que se elimine, suprime o borra la información clasificada como reservada o confidencial para permitir su acceso.

Vigencia documental: periodo durante el cual un documento de archivo mantiene sus valores administrativos, legales, fiscales o contables, de conformidad con las disposiciones legales aplicables en la materia

II. CONTROLES PARA GARANTIZAR LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LOS DATOS PERSONALES.

Cumplimiento de principios, deberes y demás obligaciones.

El tratamiento legítimo, controlado e informado de los datos personales en "Escudo Urbano C5"se basa en principios y deberes que los responsables deben observar en el tratamiento de los datos personales, que tiene que cumplir, así como hacer cumplir, en cada una de las fases del tratamiento.



1. Principios de licitud y lealtad

En "Escudo Urbano C5" los datos personales tienen que ser tratados por el responsable de manera lícita y leal, lo que supone que tiene que actuar con apego a las leyes en general y en lo particular a la normatividad sobre protección de datos personales.

En ese sentido, el responsable sólo podrá hacer con los datos personales aquello que esté legalmente permitido. De acuerdo con el principio de lealtad, la obtención de los datos personales no podrá hacerse a través de medios engañosos, ni fraudulentos, lo que implica que:

- No se recaben datos personales con dolo, mala fe o negligencia;
- No se vulnere la confianza del titular con relación a que sus datos personales serán tratados conforme a lo acordado; y
- Se informen todas las finalidades del tratamiento en el aviso de privacidad.

Obligaciones ligadas a los principios de licitud y lealtad: El responsable tiene las siguientes obligaciones en torno a los principios de licitud y lealtad:

1. Tratar siempre los datos personales con apego al cumplimiento de la legislación mexicana y el derecho internacional;

2. No hacer uso de medios engañosos o fraudulentos para la obtención de los datos personales, y

3. Respetar en todo momento la expectativa razonable de privacidad del titular. Una vez identificadas las obligaciones, en el siguiente apartado se darán recomendaciones para cumplir con las mismas.

2. Principio del consentimiento

Como regla general, el responsable deberá contar con el consentimiento del titular para el tratamiento de sus datos personales.
La solicitud del consentimiento deberá ir siempre ligada a las finalidades concretas del tratamiento que se informen en el aviso de privacidad, es decir, el consentimiento se deberá solicitar para tratar los datos personales para finalidades específicas, no en lo general.

3. Principio de información

Por virtud de este principio, los responsables se encuentran obligados a informar a los titulares de los datos personales, las características principales del tratamiento al que será sometida su información personal, lo que se materializa a través del aviso de privacidad.

En ese sentido, todo responsable que trate datos personales, sin importar la actividad que realice o si se trata de una persona física o moral, requiere elaborar y poner a disposición los avisos de privacidad que correspondan a los tratamientos que lleven a cabo.

Es importante tomar en cuenta que con independencia de que se requiera o no el consentimiento del titular para el tratamiento de sus datos personales, el responsable está obligado a poner a su disposición el aviso de privacidad.

4. Principio de proporcionalidad

El principio de proporcionalidad establece la obligación del responsable de tratar sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.

De igual forma, el responsable deberá realizar esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios para lograr la finalidad o finalidades para las cuales se obtuvieron, las cuales, como se señaló anteriormente, deben estar previstas en el aviso de privacidad.

Con relación al tratamiento de datos personales sensibles, además de lo anterior, el responsable debe realizar esfuerzos razonables para limitar el periodo de tratamiento al

Oficialía de Partes del C5 Jalisco, ubicado en la Fiscalía del Estado, segundo nivel,
(a un costado de la Dirección de Tramitación Masiva) con domicilio en la calle 14 No. 2550, colonia Industrial en Guadalajara, Jalisco

mínimo indispensable. Asimismo, de acuerdo con el artículo 9 de la LFPDPPP, no podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de estas para finalidades legítimas, concretas y acordes con las actividades del responsable. En ese sentido, sólo podrán crearse bases de datos personales sensibles cuando:

- Obedezca a un mandato legal;
- Se justifique para la seguridad nacional, el orden, la seguridad y la salud públicos, así como derechos de terceros, o
- El responsable lo requiere para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga.

5. Principio de finalidad

Los datos personales sólo pueden ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste. Se entiende por finalidad del tratamiento, el propósito, motivo o razón por el cual se tratan los datos personales.

La finalidad o finalidades del tratamiento de datos personales deberán ser determinadas, es decir, deberán especificar para qué objeto se tratarán los datos personales de manera clara, sin lugar a confusión y con objetividad.
En ese sentido, el responsable deberá evitar que las finalidades que describa en el aviso de privacidad sean inexactas, ambiguas o vagas,

¿Qué son las finalidades primarias y secundarias del tratamiento?

De acuerdo con el Reglamento de la LFPDPPP hay dos tipos de finalidades:

(i) aquéllas que dan origen y son necesarias para la relación jurídica entre el titular y el responsable, a las cuales identificamos como primarias, y

(ii) todas las demás que no cumplan con esta condición, a las que llamaremos secundarias o accesorias

En ese sentido, se hace indispensable que en el aviso de privacidad se identifique y distinga entre las finalidades primarias y secundarias del tratamiento. Asimismo, se deberá indicar el mecanismo habilitado para que el titular, si así lo desea, pueda manifestar su negativa al tratamiento de sus datos personales para todas o algunas de las finalidades secundarias.

Este mecanismo debe estar a disposición de los titulares previo a que su información personal sea tratada para dichos fines.

Ahora bien, como se explicó en el principio de consentimiento, cuando el aviso de privacidad no se haga del conocimiento del titular de manera personal o directa,

¿Se pueden tratar los datos personales para finalidades distintas a las previstas en el aviso de privacidad?

Es importante que el responsable tome en consideración que no se pueden llevar a cabo tratamientos para finalidades distintas que no resulten compatibles o análogas con aquéllas para las que se hubiese recabado de origen los datos personales y que hayan sido previstas en el aviso de privacidad, a menos que:

- Lo permita de forma explícita una ley o reglamento, o
- El responsable haya obtenido el consentimiento para el nuevo tratamiento.

6. Principio de calidad

El principio de calidad significa que, conforme a la finalidad o finalidades para las que se vayan a tratar los datos personales, éstos deben ser:

• Los datos personales son **exactos** cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles

• Los datos personales están **completos** cuando no falta ninguno de los que se requiera para las finalidades para las cuales se obtuvieron y son tratados, de forma tal que no se cause un daño o perjuicio al titular.

• Los datos personales son **pertinentes** cuando corresponden efectivamente al titular.

• Los datos están **actualizados** cuando están al día y corresponden a la situación real del titular.

• Los datos personales son **correctos** cuando cumplen con todas las características anteriores, es decir, son exactos, completos, pertinentes y actualizados.

7. Principio de responsabilidad

El principio de responsabilidad cierra el círculo con relación a los principios que regulan la protección de los datos personales.
A este principio se le conoce también como el principio de "rendición de cuentas", ya que establece la obligación de los responsables de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante titulares y la autoridad, que cumple con sus obligaciones en torno a la protección de los datos personales.
Bajo este principio, los responsables del tratamiento están obligados a velar por la protección de los datos personales aun y cuando los datos estén siendo tratados por encargados.
Asimismo, este principio supone que el responsable tome las medidas suficientes para que los términos establecidos en el aviso de privacidad sean respetados por aquéllos con los que mantenga una relación jurídica.

A. Deber de Confidencialidad

Este deber implica la obligación de guardar secreto respecto de los datos personales que son tratados. Este deber debe cumplirse para evitar causar un daño a su titular, de no ser así, un tercero no autorizado podría tener acceso a determinada información.
Es por ello que cuando se tratan datos personales, el responsable tiene que adoptar medidas para evitar que quienes tengan acceso a éstos divulguen dicha información. Incluso la obligación de confidencialidad tiene que hacerse cumplir una vez que finalice la relación contractual, laboral o de otra naturaleza, entre el responsable del tratamiento y quien tenga acceso a los datos personales para el desarrollo de las tareas o funciones que se le hubieran encomendado.
Además, el responsable tiene que garantizar también que el deber de confidencialidad se cumpla incluso una vez finalizada la relación con el titular de los datos personales
En definitiva, quienes traten datos personales, en cualquier fase del tratamiento, tienen que guardar secreto respecto de los datos que conozcan para el desarrollo de sus funciones.

B. Deber de Seguridad

Este deber se refiere a la obligación de establecer y mantener medidas de seguridad tanto técnicas, físicas y administrativas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.
Las medidas adoptadas no podrán ser menores a aquéllas que los responsables y encargados tengan para el manejo de su información. En ese sentido, el responsable deberá implementar las medidas de seguridad atendiendo lo que establece la LFPDPSO, su Reglamento y las disposiciones específicas que regulen el sector de la actividad que realice el responsable, siempre que éstas contemplen una protección mayor para el titular que las dispuestas en la LFPDPSO y su Reglamento.

¿Quién puede llevar a cabo las funciones de seguridad de los datos personales?

El responsable puede desarrollar y llevar a cabo las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.

¿Qué factores se deben tomar en cuenta para determinar las medidas de seguridad?

Las medidas de seguridad son el control o grupo de controles de seguridad destinados a la protección de los datos personales

En este sentido dentro de "Escudo Urbano C5" se lleva a cabo el siguiente

PLAN DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES

Propósito

El propósito de este plan de copia de seguridad de datos es garantizar que el Centro de Coordinación, Comando, Control, Comunicaciones y Cómputo del Estado de Jalisco pueda realizar copias de seguridad de datos, sistemas, bases de datos y otras tecnologías de misión crítica para que estén disponibles en caso de una interrupción que afecte la operatividad de este Organismo Público Descentralizado. Se espera que en todos los sistemas de tratamiento de datos personales implementen medidas de copia de seguridad de datos siempre que sea posible para minimizar las interrupciones operativas y recuperarse lo más rápido posible cuando ocurra un incidente.

Alcance

El alcance de este plan se limita a las actividades de copia de seguridad de datos y no es un documento diario de procedimientos de resolución de problemas.

Objetivos del plan

- Sirve como guía para los equipos de copia de seguridad de datos personales en sus sistemas de tratamientos.
- Referencias y puntos a la(s) ubicación(es) de datos personales, sistemas, aplicaciones y otros recursos de datos personales de misión crítica respaldados ordinarios y sensibles.
- Proporciona los procedimientos y recursos necesarios para realizar copias de seguridad de datos personales, sistemas y otros recursos.
- Identifica a los proveedores y servidores públicos que deben ser notificados en caso de una interrupción que pueda requerir la recuperación de datos respaldados y otros recursos.
- Minimiza las interrupciones operativas mediante la documentación, prueba y revisión de los procedimientos de copia de seguridad de datos personales.
- Identifica fuentes alternativas para las actividades de copia de seguridad de datos personales.
- Documenta el almacenamiento de datos personales, copias de seguridad y procedimientos de recuperación de registros vitales y otros datos relevantes.

Suposiciones

Oficialía de Partes del C5 Jalisco, ubicado en la Fiscalía del Estado, segundo nivel,
(a un costado de la Dirección de Tramitación Masiva) con domicilio en la calle 14 No. 2550, colonia Industrial en Guadalajara, Jalisco

- Los servidores públicos clave de respaldo de datos personales tendrán disponible la información después de un desastre (por ejemplo, el Director Sub Director).
- Este plan y los documentos relacionados se almacenan en un lugar seguro fuera del sitio y no solo sobrevivieron al desastre, sino que son accesibles inmediatamente después del desastre.
- el Centro de Coordinación, Comando, Control, Comunicaciones y Cómputo del Estado de Jalisco, tendrá planes de recuperación de desastres (DR) de tecnología que se alinean con este plan de respaldo de datos.

Bases de datos del sistema

- Se debe hacer una copia de las bases de datos personales crítica (sensibles) más recientes al menos dos veces al mes, o en función de la frecuencia de los cambios realizados.
- Las copias de seguridad deben almacenarse fuera del sitio.
- El administrador principal de datos es responsable de esta actividad.

Datos de misión crítica

- Se debe realizar una copia de seguridad de los datos personales y sus bases de datos de misión crítica actuales de acuerdo con los objetivos de punto de recuperación (RPO) establecidos, y se deben duplicar o replicar para proteger las ubicaciones de copia de seguridad dentro de los plazos de RPO.
- Las copias de seguridad deben almacenarse fuera del sitio en una o más ubicaciones seguras en la nube o en centros de datos u oficinas alternas, o una combinación de estos.
- El administrador principal de datos es responsable de esta actividad.

Datos no críticos

- Los datos personales y sus bases de datos actuales que no son de misión crítica deben respaldarse de acuerdo con los RPO establecidos, y se pueden duplicar o replicar para asegurar las ubicaciones de respaldo dentro de los plazos de RPO.
- Alternativamente, las copias de los datos personales y bases de datos actuales deben hacerse al menos dos veces por semana, o en función de las métricas de RPO o la frecuencia de los cambios realizados.
- Las copias de seguridad pueden almacenarse *"in situ"* en instalaciones de almacenamiento seguras o almacenarse fuera del sitio en una o más ubicaciones seguras en la nube o en centros de datos u oficinas alternativos de la empresa, o una combinación de estos.
- El equipo de administración de datos es responsable de esta actividad.

Los medios de copia de seguridad se almacenan en ubicaciones seguras, aisladas de los peligros ambientales y geográficamente separadas de la ubicación que alberga los componentes de la red.

Procedimientos de almacenamiento fuera del sitio

- Los discos, y otros medios adecuados se almacenan en instalaciones ambientalmente seguras.
- La rotación de discos se produce en una programación regular coordinada con el proveedor de almacenamiento de información.
- El acceso a las bases de datos de copia de seguridad y otros datos se prueba anualmente.

Realización de copias de seguridad de datos

Las copias de seguridad de datos deben programarse diariamente, semanalmente y mensualmente, dependiendo de la naturaleza de la copia de seguridad. Los administradores de datos deben utilizar la tecnología de copia de seguridad de datos aprobada para preparar, programar, ejecutar y verificar las copias de seguridad. Las copias de seguridad se pueden realizar en recursos de almacenamiento local (por ejemplo, disco) localmente o en ubicaciones seguras fuera del sitio (por ejemplo, proveedores de servicios de copia de seguridad de datos en la nube, proveedores de copia de seguridad como servicio) aprobadas por la Dirección de Área de Tecnologías de la Información y Comunicaciones.

Actividades de copia de seguridad de datos

En la siguiente tabla se enumeran las actividades de copia de seguridad de datos que deben realizarse de forma regular.

	Acción	Quién realiza
1.	Programa de revisión con gestión de Tecnologías de la Información; Asegure las aprobaciones según sea necesario	Líder de administración de respaldo de datos, Sub Director de Sistemas
2.	Identificar y categorizar los datos de los que se va a realizar una copia de seguridad	Administrador principal de copias de seguridad; Equipo de copia de seguridad
3.	Identificar y categorizar los sistemas de los que se va a realizar una copia de seguridad	Administrador principal de copias de seguridad; Equipo de copia de seguridad
4.	Identificar y categorizar otros recursos para realizar copias de seguridad	Administrador principal de copias de seguridad; Equipo de copia de seguridad
5.	Programar actividades de copia de seguridad, por ejemplo, fecha, hora, frecuencia, tipo de recurso para realizar copias de seguridad, destino de las copias de seguridad	Administrador principal de copias de seguridad; Equipo de copia de seguridad
6.	Programe sistemas y recursos de copia de seguridad de acuerdo con el cronograma y la política	Administrador principal de copias de seguridad; Equipo de copia de seguridad
7.	Programar actividades de backup y rotación en cinta	Administrador principal de copias de seguridad; Equipo de copia de seguridad
8.	Ejecutar copias de seguridad de datos, sistemas y otros recursos	Administrador principal de copias de seguridad; Equipo de copia de seguridad

9.	Asegúrese de que los discos estén asegurados para la recogida y estén debidamente etiquetados; Verificar recogida	Administrador principal de copias de seguridad; Equipo de copia de seguridad
10.	Compruebe que se completaron las copias de seguridad y que todos los recursos de copia de seguridad no han cambiado	Administrador principal de copias de seguridad; Equipo de copia de seguridad
11.	Preparar y distribuir informes de copia de seguridad	Administrador principal de copias de seguridad; Equipo de copia de seguridad
12.	Programar y realizar pruebas de copias de seguridad de datos	Administrador principal de copias de seguridad; Equipo de copia de seguridad
13.	Programar y aplicar revisiones a los recursos de copia de seguridad	Administrador principal de copias de seguridad; Equipo de copia de seguridad
14.	Actualizar los sistemas y tecnologías de copia de seguridad según sea necesario	Administrador principal de copias de seguridad; Equipo de copia de seguridad

Recuperación de datos

Las políticas deben establecerse, documentarse y probarse por el Comité de Transparencia mediante el documento de seguridad de los sistemas de tratamiento de los datos personales, periódicamente para recuperar datos, bases de datos, sistemas, aplicaciones y otros activos de información si ocurre un evento disruptivo que requiera la recuperación de esos activos y recursos.

Revisión y mantenimiento del plan

Este plan de copia de seguridad de datos debe revisarse periódicamente y los procedimientos deben validarse (y actualizarse según sea necesario) para garantizar que las copias de seguridad se realicen según sea necesario y cuando sea necesario. Como parte de esta actividad, es aconsejable revisar la lista de personal del equipo de copia de seguridad de datos, proveedores de servicios de copia de seguridad de datos y proveedores de copia de seguridad de datos en la nube, y actualizar los datos de contacto según sea necesario.

La versión impresa de este plan de copia de seguridad de datos se almacenará en una ubicación común donde pueda ser vista por el personal de la Dirección de Área de Tecnologías de la Información y Comunicaciones, como los administradores de datos. Las versiones electrónicas estarán disponibles en la Sub Dirección de Soporte.

El plan de contingencia

El Plan de Contingencia se subdivide en:

- Plan de emergencia
- Pan de restauración (BACKUP)
- Plan de recuperación

Oficialía de Partes del C5 Jalisco, ubicado en la Fiscalía del Estado, segundo nivel,
(a un costado de la Dirección de Tramitación Masiva) con domicilio en la calle 14 No. 2550, colonia Industrial en Guadalajara, Jalisco

	Emergencia	Restauración	Recuperación
Objetivo	Limita el daño	Continuar procesos vitales	Recuperación proceso total
Actuación	Inmediata	A corto plazo	A mediano plazo
Contenido	Evacuación Valoración de daños Arranque de acciones	Alternativas para los procesos vitales	Estrategias para la recuperación de todos los recursos
Responsabilidad principal	Escudo Urbano C5	Usuarios	Dirección de Área de Tecnologías de la Información y Comunicaciones

III. ROLES Y RESPONSABILIDADES DEL TRATAMIENTO DE DATOS PERSONALES.

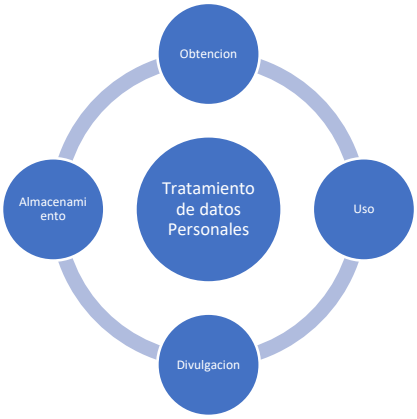
Un dato personal es cualquier información concerniente a una persona física identificada o identificable, como puede ser el nombre, los apellidos, la dirección postal, el número de teléfono, la dirección de correo electrónico, el número de pasaporte, una fotografía, la Clave Única de Registro de Población (CURP) o cualquier otra información que permita identificar o haga identificable al titular de los datos.
Los datos personales pueden estar expresados en forma numérica, alfabética, gráfica, fotográfica, acústica o en cualquier otra modalidad.
Se considera que una persona es identificable cuando su identidad puede determinarse mediante los datos personales de que se traten.
La información relativa a una persona moral no se considera como dato personal, quedando ésta excluida de la protección que otorga la normatividad sobre protección de datos personales a las personas físicas.
Es importante considerar que si los datos personales son objeto del procedimiento de disocian, de forma tal que no es posible asociarse a su titular, ni permitir su identificación, dejarán de ser considerados como tales y, por lo tanto, no será aplicable la normatividad sobre protección de datos personales.

¿Qué es un dato personal sensible?

Son datos personales que afectan la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen o conlleve un riesgo grave para éste

¿Qué se entiende por tratamiento de datos personales?

Tratar datos personales es un concepto amplio, ya que incluye:



IV. SANCIONES POR EL INCUMPLIMIENTO.

La siguiente tabla incluye las infracciones previstas en la Ley, el tipo de sanción aplicable en cada caso y la sanción correspondiente:

Infracción	Tipo de sanción	Sanción
No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en la Ley	No económica	Apercibimiento
Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales	Económica	Multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal6
Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable		
Dar tratamiento a los datos personales en contravención a los principios establecidos en la Ley		
Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de la Ley.		
Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares		
No cumplir con el apercibimiento a que se refiere la fracción I del artículo 64 de la Ley.		
Incumplir el deber de confidencialidad establecido en el artículo 21 de la Ley.		Multa de 200 a 320,000 días

Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto por el artículo 12 de la Ley		de salario mínimo vigente en el Distrito Federal
Transferir datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos		
Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable		
Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley		
Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible.		
Obstruir los actos de verificación de la autoridad.		
Recabar datos en forma engañosa y fraudulenta		
Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares.		
Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos de acceso, rectificación, cancelación y oposición establecidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos		
Crear bases de datos en contravención a lo dispuesto por el artículo 9, segundo párrafo de la Ley.		
Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la Ley	-	-
Cuando de manera reiterada persistan las infracciones anteriores.	Económica	Multa adicional de 100 a 320,000 días de salario mínimo vigente en el Distrito Federa
Infracciones cometidas en el tratamiento de datos sensibles.		en el Distrito Federal Infracciones cometidas en el tratamiento de datos sensibles. Los montos podrán incrementarse

		hasta por dos veces
El que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.	Penal	De tres meses a tres años de prisión.
Al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos		De seis meses a cinco años de prisión.
Las indicadas en los apartados anteriores.		Se duplican.

V. CICLO DE VIDA DE LOS DATOS PERSONALES.

VI. ATENCIÓN DE LOS DERECHOS ARCO.

Usted tiene derecho a lo siguiente:

Acceder: conocer qué datos personales tenemos de usted, para qué los utilizamos y las condiciones del uso que les damos;

Rectificar: solicitar la corrección de su información personal en caso de que esté desactualizada, sea inexacta o incompleta;

Cancelar: que la eliminemos de nuestros registros o bases de datos cuando considere que la misma no está siendo utilizada adecuadamente;

Oponerse: al uso de sus datos personales para fines específicos.

Portabilidad: Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.

A los derechos citados se les conocen como derechos **ARCO y portabilidad**.

Para el ejercicio de cualquiera de los derechos **ARCO**, usted deberá presentar solicitud en las oficinas de la Unidad de Transparencia de Este Organismo Descentralizado, en la Plataforma Nacional de Transparencia a través el sistema de solicitudes de acceso a la Información (SISAI 2.0), misma que será respondida por el medio señalado por el solicitante o bien puede presentarla de manera electrónica al correo: transparencia@c5jalisco.gob.mx.

Los requisitos para presentar su solicitud de derechos **ARCO** son los siguientes:

I. De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud;
II. Nombre del solicitante titular de la información y del representante, en su caso;
III. Domicilio o cualquier otro medio para recibir notificaciones;
IV. Los documentos con los que acredite su identidad y, en su caso, la personalidad e identidad de su representante;
V. La descripción del derecho **ARCO** que se pretende ejercer, o bien, lo que solicita el titular;
VI. Descripción clara y precisa de los datos sobre los que se busca ejercer alguno de los derechos **ARCO**, salvo que se trate del derecho de acceso; y
VII. Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.

A continuación, se describe el procedimiento de atención:

Paso	Tiempo
Requerimiento de información adicional en caso de que la solicitud no sea clara.	5 días, hábiles
Respuesta a la solicitud en caso de existencia de trámite.	3 días hábiles
Respuesta a la solicitud en caso de que el sujeto obligado no sea competente	3 días hábiles
Reconducción de la solicitud en caso de ser un derecho diferente	3 días hábiles
Respuesta a la solicitud	10 días hábiles
Respuesta a la solicitud en caso de ampliación	15 días hábiles
Plazo para hacer efectivo el derecho o en caso de que resulte procedente	5 días hábiles

En caso de haber presentado una solicitud de acceso a datos personales, se le dará acceso a través del medio de reproducción señalado por el solicitante, el cual puede ser: consulta directa, copia certificada, dispositivo de almacenamiento, disco compacto, copia simple u otro medio.

En caso de que el titular se encuentre inconforme con la respuesta emitida por esta Institución, podrá interponer recurso de revisión ante nuestra Unidad de Transparencia, dentro del plazo de quince días contados a partir del día siguiente a la fecha de notificación de la resolución de la solicitud.

El derecho a la Portabilidad de sus datos personales no es posible, al no ser técnicamente viable por no tratarse en medios automatizados, en formato estructurado, de uso común, de lectura mecánica e interoperable.

VII. MARCO LEGAL.

El uso, recolección y tratamiento de datos personales por parte del ITEI, se fundamenta en las siguientes normativas:

La Constitución Política de los Estados Unidos Mexicanos; Ley Orgánica del Organismo Público Descentralizado denominado Centro de Coordinación, Comando, Control, Comunicaciones y Cómputo del Estado de Jalisco; Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; la Norma Técnica para la Estandarización de los Servicios de Llamadas de Emergencia a través del Número Único Armonizado 9-1-1 (nueve, uno, uno); la Ley de Compras Gubernamentales, Enajenaciones y Contrataciones de Servicios del Estado de Jalisco y sus Municipios; la Ley de Adquisiciones y Enajenaciones del Estado de Jalisco; el Reglamento de la Ley de Compras Gubernamentales, Enajenaciones y Contrataciones de Servicios del estado de Jalisco y sus Municipios; la Ley Federal del Trabajo; Ley Federal de los Trabajadores al Servicio del Estado; la Norma Oficial Mexicana Nom-035-STPS2018, Factores de Riesgo Psicosocial en el Trabajo-Identificación, Análisis y Prevención; la Ley de Archivos del Estado de Jalisco y sus Municipios; la Ley para los Servidores Públicos del Estado de Jalisco y sus Municipios; las Políticas Administrativas para Entidades Públicas Paraestatales del Estado de Jalisco; la Ley General del Sistema Nacional de Seguridad Pública; la Ley del Sistema de Seguridad Pública para el Estado de Jalisco; la Ley General de Responsabilidades Administrativas; la Ley de Responsabilidades Políticas y Administrativas del Estado de Jalisco; la Ley de Movilidad y Transporte del Estado de Jalisco; la Norma Técnica para estandarizar las características técnicas y de interoperabilidad de los Sistemas de Videovigilancia.

Referencias.

INAI. (2016, junio). Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Disponible en: file:///Z:/C12.14%20políticas%20de%20privacidad/Politicas%20de%20privacidad%20Julio%202023/Guia_obligaciones_lfpdppp_junio2016.pdf

INAI. (2022, Junio). Recomendaciones para la elaboración de Políticas internas de Gestion y tratamiento de datos personales Disponible en: file:///Z:/C12.14%20políticas%20de%20privacidad/Politicas%20de%20privacidad%20Julio%202023/RecomendacionesPol_ticasPDP.pdf

INAI. (2018, Enero) Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados , Disponible en: file:///Z:/C12.14%20políticas%20de%20privacidad/Politicas%20de%20privacidad%20Julio%202023/_GuiaPrincipiosDeberes.pdf