ANEXO III AGP-ITEI/025/2020

INSTITUTO DE TRANSPARENCIA, INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE JALISCO

GUÍA PARA ESTABLECER CONTROLES O MECANISMOS QUE TENGAN POR OBJETO QUE TODAS AQUELLAS PERSONAS QUE INTERVENGAN EN CUALQUIER FASE DEL TRATAMIENTO DE LOS DATOS PERSONALES GUARDEN CONFIDENCIALIDAD

Directorio

Cynthia Patricio Cantero Pacheco

Comisionada Presidenta

Salvador Romero Espinosa

Comisionado Ciudadano

Pedro Antonio Rosas Hernández

Comisionado Ciudadano

Miguel Ángel Hernández Velázquez

Secretario Ejecutivo

Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco
Avenida Vallarta 1312 colonia Americana C.P. 44160 Guadalajara, Jalisco, México.
Tel. (33) 3630 5745

Contenido

Contenido

Glosario[1][2]

Activo: es cualquier elemento que representa un valor para la organización cuando un activo es dañado o atacado se genera una pérdida directa o indirecta a la organización que se materializa en un impacto económico, operativo, funcional, legal, de reputación o inclusive un daño de carácter humano.

Los activos intangibles incluyen datos, información digital, aplicaciones, transacciones, planes, propiedad intelectual, conocimiento, imagen, reputación, principios, valores, entre otros.

Actualizaciones de las medidas de seguridad: La normatividad establece que los responsables deberán llevar a cabo la implementación de controles de seguridad que permitan la protección de datos personales permitiendo el cumplimiento previsto por la norma y a su vez están sujetos a una constante revisión y actualización práctica que puede implicar la adopción de controles más estrictos o robustos en caso de que se actualice un incidente de seguridad o un evento que pudiere representar un riesgo para la seguridad de los datos personales.

Anonimización: El término anonimización se refiere a la aplicación de determinadas técnicas o procedimientos tendientes a impedir la identificación o reidentificación de una persona física sin que para ello sea necesario el empleo de esfuerzos desproporcionados.

Áreas: Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales;

Autenticación: Es aquella característica de un documento que permite identificar y vincular a las personas que lo crearon y/o que han aceptado o expresado su consentimiento para obligarse en términos de su contenido, sin que estas puedan repudiar su consentimiento o voluntad.

Aviso de privacidad: 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 principales del tratamiento al que serán sometidos sus datos personales;

---

[1] F. de Marcos Isabel Davara. Primera edición (2019). *Diccionario de Protección de Datos Personales: Conceptos Fundamentales*. Ciudad de México. México. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

[2] Artículo 3 párrafo primero de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Bases de Datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionado a criterios determinados con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

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, hasta el plazo de prescripción legal o contractual correspondiente. Durante dicho período los datos personales no podrán ser objeto de tratamiento y concluido éste se deberá proceder a la supresión en la base de datos, archivo, registro, expediente o sistema de información que corresponda;

Cómputo en la nube: 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 digitales, en recursos compartidos dinámicamente;

Consentimiento: Manifestación de la voluntad libre, específica e informada del titular que autoriza el tratamiento de sus datos personales;

Consentimiento expreso: El consentimiento expreso puede manifestarse verbalmente, ya sea por escrito, por medios electrónicos, ópticos, por cualquier otra tecnología, o por signos inequívocos. Sin embargo, en el caso de datos personales sensibles, se exige la forma escrita, ya sea mediante firma autógrafa, firma electrónica o mecanismo de autenticación equivalente.

Consentimiento expreso y por escrito: El consentimiento expreso requiere ser claro, patente y especificado, lo que significa que requiere de una acción afirmativa por parte del titular. Es decir, si la voluntad del titular de los datos no es clara o específica, no se cumple con dicho requisito como base para la legitimación del tratamiento de los datos personales. Al añadir el elemento "escrito", lo que se incorpora es la obligación de que el consentimiento conste en cualquier documento.

Consentimiento tácito: El consentimiento tácito es aquél que se obtiene del titular mientras éste, una vez informado sobre su alcance, no manifieste su oposición.

Control de seguridad: La expresión "control de seguridad" se emplea en la normatividad de datos personales para hacer referencia a las medidas de seguridad aplicables al tratamiento de los datos personales, relacionado con las propias medidas de seguridad establecidas para garantizar la seguridad y confidencialidad de los datos personales.

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 conlleve 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;

Deber de confidencialidad: La confidencialidad es la propiedad que posee un objeto, acción, pensamiento, idea, información o cualquier ente de no ser divulgado o expuesto a entidades no autorizadas. En el caso de la información, constituye una de las piedras angulares junto con la integridad y la disponibilidad de lo que es la seguridad de la información, características conocidas como la triada de la seguridad.

Por otro lado, el deber de confidencialidad es la obligación que tiene una entidad de resguardar la confidencialidad de lo que tiene bajo responsabilidad o custodia. En algunas profesiones como la medicina, el derecho, la psicología, el periodismo o la milicia, se considera un principio ético o de secreto profesional.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;

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;

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;

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;

Ética en la protección de datos personales: La ética en la protección de datos personales significa la responsabilidad que adquieren las empresas, dependencias, gobiernos y/o cualquiera otro ente que trate datos personales a grandes escalas de comprender y evaluar los tratamientos de datos personales que llevan a cabo con el propósito de identificar los impactos positivos y negativos tanto en el ámbito operacional, como en el de la protección de los derechos humanos de la persona cuyos datos personales están siendo sujetos a tratamiento.

Fuentes de acceso público: Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultados públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a esta Ley y demás disposiciones aplicables;

Información Confidencial: La información considerada como confidencial, al ser una excepción al principio de máxima publicidad, contemplado en el artículo 6, fracción I, de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) tiene como fin proteger no solo los datos personales, sino la vida privada y la intimidad de las personas. Por lo que nos encontramos ante dos derechos fundamentales previstos en los artículos 6 y 16 de la CPEUM, que deben ser equilibrados.

La definición de información confidencial en la legislación mexicana se encuentra en diversas disposiciones normativas y se define de la misma manera en los distintos ordenamientos. Los supuestos en los que las leyes consideran que la información es confidencial son los siguientes:

a) cuando contiene datos personales concernientes a una persona identificada o identificable,
b) los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil, y postal, cuya titularidad corresponda a particulares, sujetos de derechos internacional o sujetos obligados cuando no involucren el ejercicio de recursos públicos y
c) aquella que presenten los particulares a los sujetos obligados, siempre que tengan el derecho a ello, de conformidad con lo dispuesto por las leyes o los tratados internacionales.

Una característica importante de la información confidencial es que no está sujeta a ninguna temporalidad. Esto significa que siempre mantendrá su carácter confidencial y solo podrán tener acceso a ella los titulares de la misma, sus representantes y los servidores públicos facultados para ello.

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

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

Intimidad: El *Diccionario de la Real Academia Española* (DRAE) indica que por "intimidad" debe entenderse lo siguiente: "zona espiritual íntima y reservada de una persona o de un grupo, especialmente una familia".

El derecho a la intimidad es "un derecho subjetivo, de defensa de una parcela de nuestra vida que queremos mantener reservada, y de la que tenemos plena disposición". El derecho a la intimidad, entonces, "se asocia con la existencia de un ámbito privado que se encuentra reservado frente a la acción y conocimiento de los demás y tiene por objeto garantizar al individuo un ámbito reservado de su vida frente a la acción y conocimiento de terceros, ya sean simples particulares o bien los poderes del Estado".

Ley: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Jalisco y sus Municipios;

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

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

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

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 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; y

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 se valen 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.

Remisión: toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, con independencia de que se realice dentro o fuera del territorio mexicano;

Responsable: Los sujetos obligados señalados en el artículo 1, párrafo 5, de la presente Ley que determinarán los fines, medios y alcance y demás cuestiones relacionadas con un tratamiento 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;

Titular: Persona física a quien pertenecen los datos personales;

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

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.

Vulneración de datos personales: es la materialización de las amenazas pudiendo estar enfocadas a la pérdida o destrucción no autorizada de los datos personales en posesión de las personas físicas o morales que realizan el tratamiento de los datos, el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, así como el daño, alteración o modificación no autorizada.

Introducción

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, establece en su artículo 44 el deber de la confidencialidad, señalando expresamente lo siguiente:

"***Artículo 44.*** *Deberes — Deber de confidencialidad.*
1. El responsable deberá establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo; sin menoscabo de lo establecido en las disposiciones aplicables en materia de acceso a la información pública".

Por lo tanto, esta guía tiene como objetivo acompañar a los sujetos obligados en la creación y establecimiento de los controles y mecanismos que garantizarán que todo individuo que trate datos personales guarde la confidencialidad de los mismos.

Dentro del tratamiento de los datos personales, es importante que los responsables guarden control del acceso a los datos personales en su posesión así como de su divulgación, atendiendo a las medidas de seguridad correspondientes.

Finalmente, todas las personas que intervengan en el tratamiento de datos personales deben de cumplir con los principios de licitud, lealtad, responsabilidad, consentimiento, información, finalidad, calidad y proporcionalidad.

Identificación de activos y de personas que intervienen en el tratamiento

Antes de diseñar y establecer los controles y mecanismos para garantizar la confidencialidad de los datos personales tratados, es importante que dentro de los responsables se identifiquen el inventario de los datos personales que se tienen y se clasifiquen, destacando los datos personales sensibles.

Los datos personales sensibles son aquellos que de divulgarse, podrían poner en peligro a los titulares o provocarles alguna discriminación. Algunos ejemplos de datos sensibles son:

- Estado de salud.
- Preferencia sexual.
- Religión.
- Patrimonio.
- Afiliación política.
- Origen étnico.

Todo tratamiento de datos personales sensibles debe estar debidamente fundamentado, es decir, los datos que recabemos deben de tener un respaldo jurídico. Además en cumplimiento al principio de finalidad y proporcionalidad se deben recabar solamente los datos personales mínimos necesarios para lograr el propósito para el cual fueron recabados.

En ese sentido, el tratamiento de estos datos requiere un consentimiento expreso y por escrito del titular, salvo en los siguientes casos de excepción[3]:

- Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos por la Ley.

- Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;

- Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;

- Cuando los datos personales sean necesarios en la atención de algún servicio sanitario de prevención o diagnóstico;

[3] Artículo 15 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

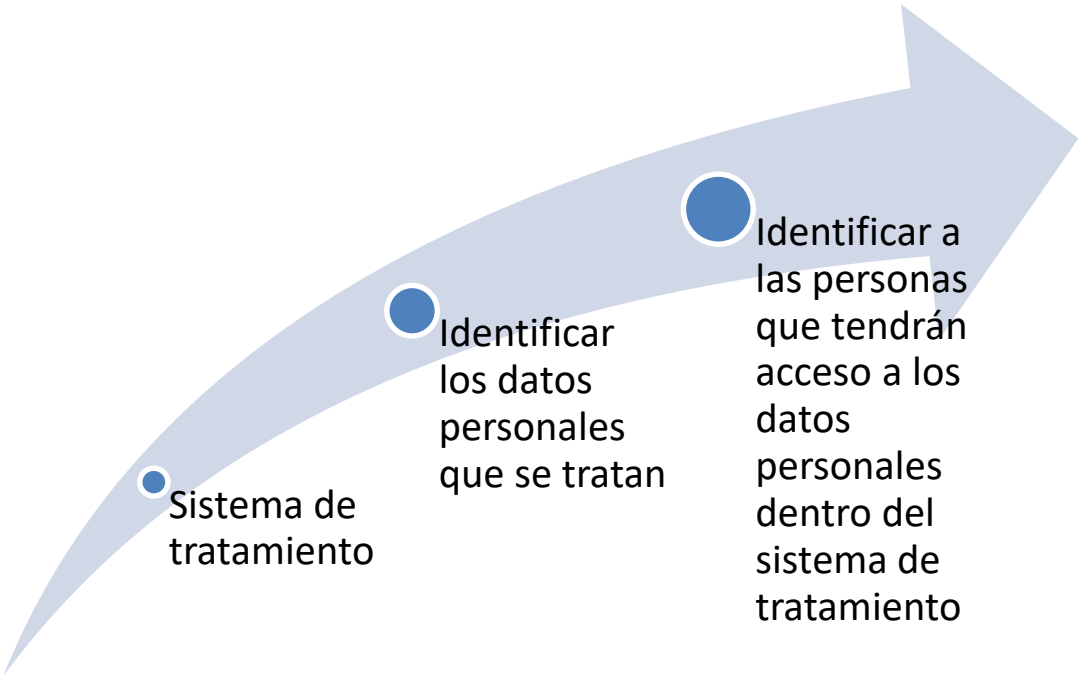
- Cuando los datos personales figuren en fuentes de acceso público;
- Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
- Cuando los datos personales se sometan a un procedimiento previo de disociación;
- Para el reconocimiento o defensa de derechos del titular ante autoridad competente;
- Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia; o
- Cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales.

Ahora bien, durante la realización del documento de seguridad, se identificaron a las personas que intervienen en el tratamiento de los datos personales recabados, es decir, aquellas personas que tienen acceso a los mismos. Lo anterior se encuentra descrito en el catálogo de sistemas de tratamiento que se encuentra en el documento de seguridad, por ejemplo:

Sistema de Tratamiento de Pagos a Empleados		
Administrador	Federico Alcalá Romero	
Cargo	Director de Recursos Humanos	
Funciones y Obligaciones	I. Administrar los recursos humanos a través de los procesos de reclutamiento, selección, control, evaluación del desempeño y remuneración. II. Coordinar y controlar el proceso de reclutamiento y selección de personal, conforme a los requerimientos de recursos humanos y con base en los perfiles de los puestos establecidos en la estructura organizacional del Instituto. III. Recabar, controlar y resguardar los expedientes laborales del personal del Instituto; tales como empleados y prestadores de servicios en general. IV. Vigilar la correcta elaboración, control y resguardo de los nombramientos relativos al personal seleccionado y contratado para la integración de la plantilla del Instituto. V. Supervisar y controlar el registro de asistencia del personal adscrito al Instituto, así como elaborar informe de incidencias de forma quincenal. VI. Coordinar y gestionar los trámites que se requieran de movimientos de personal.	
Personal que interviene en el tratamiento		
Nombre	Cargo	Funciones

Diego Gómez	Coordinador de recursos humanos	I. Recabar, controlar y resguardar los expedientes laborales del personal del Instituto; tales como empleados y prestadores de servicios en general. II. Vigilar la correcta elaboración, control y resguardo de los nombramientos relativos al personal seleccionado y contratado para la integración de la plantilla del Instituto.
Alejandra Torres	Técnico en recursos humanos	I. Supervisar y controlar el registro de asistencia del personal adscrito al Instituto, así como elaborar informe de incidencias de forma quincenal. II. Coordinar y gestionar los trámites que se requieran de movimientos de personal.
Georgina Valdivia	Servicio social	Ayudar en las funciones y obligaciones de la dirección de recursos humanos.

Al tener identificadas las personas que estarán involucradas en el tratamiento de los datos personales, basado en los perfiles de puestos, debemos entonces implementar los controles y mecanismos para que esas personas guarden la confidencialidad de los datos.



Medidas de seguridad

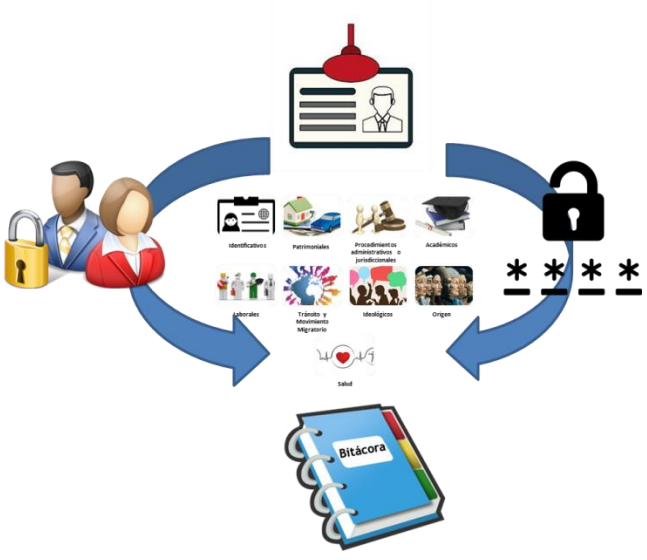
En la Ley, se obliga a los responsables a establecer medidas de seguridad de carácter físico, administrativo y técnico aplicables al tratamiento de los datos personales, establecidas para garantizar la seguridad y confidencialidad de los datos personales, por lo tanto, los responsables deben de mantener un control de las medidas de seguridad, es decir, que los responsables cada determinado tiempo hagan un análisis de los sistemas de tratamiento y sus medidas de seguridad, para que se determine la suficiencia de éstas y si es necesario llevar a cabo una actualización de las mismas, tendiendo siempre a la seguridad de un sistema de tratamiento de datos personales.

La revisión periódica de las medidas de seguridad implementadas constituyen un mecanismo para asegurar que se mantenga la confidencialidad de los datos personales, ya que se aumentan las barreras que rodean los datos y se disminuye el riesgo de alguna fuga de información.

Dentro de las medidas de seguridad administrativas recomendadas, se encuentra la identificación y autenticación de usuarios, es decir, garantizar que solo el personal que tiene las atribuciones necesarias acceda a las bases de datos, evitando así que personas no autorizadas tengan facilidad de acceso.

Algunas de las medidas de seguridad administrativa recomendadas son:

- Utilización de gafetes de identificación.
- Bitácoras de acceso a las instalaciones.
- Bitácoras de acceso a los datos personales.
- Usuarios y contraseñas en los equipos de cómputo.



En relación a las medidas de seguridad físicas, es importante que el personal que tiene bajo su resguardo datos personales, evite compartir o dar acceso a los datos personales a personas que no estén autorizadas,

Algunas las medidas de seguridad físicas recomendadas, relacionadas al personal que trata datos personales son:

- Que el personal no de acceso a los datos personales a individuos no autorizados.
- Restringir la entrada a los lugares donde se resguardan los datos.
- Llevar un control de quienes tienen los resguardos de archiveros, equipos de cómputo y llaves.
- Que el personal no preste las llaves ni entregue contraseñas.

Finalmente, el responsable debe asegurarse que los datos personales no se encuentren en lugares de fácil acceso, evitando que estén en zonas concurridas y sin ningún tipo de seguridad, garantizando que solo el personal autorizado descrito en el documento de seguridad sean quienes tengan acceso a las bases de datos.

Controles y mecanismos para garantizar la confidencialidad de los datos personales

De conformidad con los estándares internacionales por confidencialidad se entiende que el responsable debe establecer controles o mecanismos que tengan por objeto que todas aquellas personas que traten datos personales, en cualquier fase del tratamiento mantengan en secreto la información, así como evitar que la información sea revelada a personas no autorizadas y prevenir la divulgación no autorizada de la misma. Incluso la obligación de confidencialidad tiene que hacerse cumplir una vez que finalice la relación jurídica, a través de cláusulas de confidencialidad establecidas en los instrumentos jurídicos suscritos entre el responsable del tratamiento y quien tenga acceso a los datos personales[4].

Un control es definido, según el *Diccionario de la Real Academia Española*, como la regulación, manual o automática, sobre un sistema. Sobre esta acepción podemos entender que se trata de un mecanismo que puede ser físico o

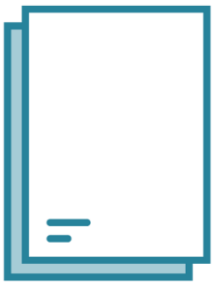
[4] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Ciudad de México. Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Recuperado de http://inicio.ifai.org.mx/DocumentosdeInteres/_GuiaPrincipiosDeberes.pdf

electrónico, tendiente a asegurar la seguridad de un sistema de tratamiento de datos personales.

Un mecanismo según la Real Academia de la Lengua Española es un medio práctico que se emplea en las artes[5], por lo tanto, esta obligación se traduce en que los responsables deben de implementar una forma práctica que permita garantizar la confidencialidad de los datos personales.

Por lo tanto, cualquier medio que se utilice que garantice que las personas que tratan datos personales guarden el secreto es válido. A continuación se señalan algunos ejemplos de los controles que pueden implementar los sujetos obligados.

Cartas compromiso



Las cartas compromiso podrán ser entregadas al personal que trata datos personales, en la misma deberá de señalarse lo siguiente:

- Nombre de la persona y puesto
- Lugar y fecha
- Señalamiento de que se tratarán datos personales con motivo de sus funciones
- La obligación de guardar la confidencialidad y el fundamento legal
- El compromiso de la persona para guardar confidencialidad
- Las consecuencias legales y administrativas que existirán en el caso de incumplimiento
- Firma autógrafa de la persona.

[5] https://dle.rae.es/mecanismo

Reglamento Interno

Los reglamentos internos de los responsables, deben de señalar la responsabilidad que tienen las personas que tratan datos personales de guardar la confidencialidad de los mismos. En dicho reglamento debe de establecerse lo siguiente:

- La obligación de todos los empleados del sujeto obligado de mantener el secreto profesional
- Ética y responsabilidad al tratar datos personales
- Las consecuencias legales y administrativas que existirán en el caso de incumplimiento
- La obligacion de cumplir con las políticas internas establecidas

Deberá existir un documento mediante el cual las personas que laboran en los sujetos obligados y que tratan datos personales tienen conocimiento del reglamento y que se comprometen a cumplirlo.

Políticas Internas

El responsable deberá elaborar políticas internas con el propósito de establecer acciones tendientes a mantener la confidencialidad de los datos personales que se tratan, algunas de los puntos importantes de las mismas son:

- Establecer la obligación de cumplir con lo establecido en las políticas.
- Acceder únicamente a los datos personales, que sean necesarios para el desarrollo de sus actividades laborales y/o contractuales, con el único propósito del cumplimiento de las mismas.
- No compartir el nombre de usuario y contraseña que se le asigne.
- Guardar confidencialidad de los datos personales a que tenga acceso.
- Cooperar con las acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información, así como a la identificación y clasificación de la información.
- Informar de forma inmediata a su superior jerárquico, cuando detecte que ha ocurrido una vulneración a datos personales.
- Asistir a los programas de capacitación para la protección de Datos Personales que lleve a cabo el responsable.
- Promover e implementar planes y programas de sensibilización en materia de protección de datos personales.
- Enlace entre las áreas involucradas en la protección de Datos Personales.
- Revisión y actualización periódica de los Avisos de Privacidad y las políticas internas.
- Atención y asesoría con el Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco.
- Atención de quejas y solicitudes de los titulares.
- Preparar y dar a conocer a los titulares, los informes de vulneraciones a sus datos personales.
- Vigilar el cumplimiento de las presentes políticas por parte de todos los integrantes de los sujetos obligados que estén involucrados en el tratamiento de Datos Personales.

Capacitación y sensibilización

Los responsables están obligados a establecer un programa anual de capacitación en el cual se sensibilice a todas las personas que traten datos personales con motivo de sus funciones sobre la protección de los datos personales, así como hacerlos conocedores de las obligaciones y responsabilidades que el tratamiento de datos conlleva.

Además, el responsable deberá a capacitar a todas las personas de nuevo ingreso sobre las responsabilidades, políticas y demás deberes establecidos, así como mantener actualizaciones en el tema.

Recomendaciones para mantener la confidencialidad de los datos personales entre responsables y encargados[6]

El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de éste[7].

Los tipos de encargado del tratamiento y las formas en que se regulará su relación pueden ser tan variados como los tipos de servicios que puedan suponer acceso a datos personales.

Así, podemos encontrar servicios cuyo objeto principal es el tratamiento de datos personales (por ejemplo, una empresa o entidad pública que ofrece un servicio

[6] Agencia Española de Protección de Datos (2018). España. *Directrices para la Elaboración de Contratos entre Responsables y Encargados del Tratamiento*. Recuperado de https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf

[7] Artículo 3.1 fracción XV de la Ley.

de alojamiento de información en sus servidores) y otros que tratan datos personales solo como consecuencia de la actividad que presta por cuenta del responsable del tratamiento (por ejemplo el gestor de un servicio público municipal).

El responsable del tratamiento no pierde esta consideración en ningún caso y, por tanto, continúa siendo responsable del correcto tratamiento de los datos personales y de la garantía de los derechos de las personas afectadas. El responsable tiene una obligación de especial diligencia en la elección y supervisión del encargado.

La regulación de la relación entre el responsable y el encargado del tratamiento debe establecerse a través de un contrato o de un acto jurídico similar que los vincule. El contrato o acto jurídico debe constar por escrito, inclusive en formato electrónico. En cualquier caso debe tratarse de un acto jurídico que establezca y defina la posición del encargado del tratamiento, siempre y cuando ese acto vincule jurídicamente al encargado del tratamiento.

Hay que establecer la forma en que el encargado del tratamiento garantizará que las personas autorizadas para tratar datos personales se han comprometido, de forma expresa, a respetar la confidencialidad o, en su caso, si están sujetas a una obligación de confidencialidad de naturaleza estatutaria.

El cumplimiento de esta obligación debe quedar documentado y a disposición del responsable. Por lo tanto, la utilización de cartas compromiso es una excelente forma de documentar este compromiso y hacerlo vinculante.

Responsabilidad administrativa, legal y penal ante la violación de la confidencialidad de los datos personales

En la Ley se establecen las responsabilidades que se pueden obtener del mal tratamiento de datos personales:

Artículo 151. *Infracciones— Responsabilidad Administrativa.*
1. Independientemente de la sanción que aplique el Instituto, éste deberá presentar ante las autoridades competentes denuncia en materia de responsabilidad administrativa de los servidores públicos para que, de ser procedente, se sancione al servidor público de conformidad con la Ley de Responsabilidades Políticas y Administrativas del Estado de Jalisco.

Artículo 152. *Infracciones— Procedencia de responsabilidades del orden civil o penal.*
1. Las responsabilidades que resulten de los procedimientos administrativos correspondientes, derivados de la violación a lo dispuesto por el artículo 177 de la presente Ley, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

2. Dichas responsabilidades se determinarán, en forma autónoma, a través de los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes, también se ejecutarán de manera independiente.

3. Para tales efectos, el Instituto podrá denunciar ante las autoridades competentes cualquier acto u omisión violatoria de la presente Ley y aportar las pruebas que consideren pertinentes, en los términos de las leyes aplicables.

Ahora bien, en los Lineamientos que Regulan las Atribuciones de las Áreas Encargadas de Calificar la Gravedad de la Falta de Observancia de las Determinaciones del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, así como la Notificación y Ejecución de las Medidas de Apremio Señaladas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, establecen lo siguiente:

DÉCIMO PRIMERO. Criterios para la determinación de medidas de apremio. *De conformidad con lo previsto en el artículo 141 de la Ley, para calificar las medidas de apremio el Instituto deberá considerar:*

I. La gravedad de la falta del responsable considerando:

a) El daño causado: el perjuicio, menoscabo o agravio a los principios generales o bases constitucionales reconocidos en el artículo 16, segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos, así como la afectación a los principios, objetivos y obligaciones previstas en la Ley y los Lineamientos para el Debido Tratamiento de los Datos Personales que Deberán Observar los Sujetos Obligados del Estado de Jalisco y sus Municipios;

b) Los indicios de intencionalidad: los elementos subjetivos que permiten individualizar el grado de responsabilidad, entendidos como el aspecto volitivo en la realización de la conducta antijurídica. Para determinar lo anterior, deberá considerarse si existió contumacia total para dar cumplimiento a las disposiciones en la materia o, en su caso, se acreditó estar en vías de cumplimiento a las mismas;

c) La duración del incumplimiento: el periodo que persistió el incumplimiento, y

d) La afectación al ejercicio de las atribuciones del Instituto: el obstáculo que representa el incumplimiento al ejercicio de las atribuciones de éste conferidas en el artículo 9, de la Constitución Política del Estado de Jalisco así como en la Ley y los presentes Lineamientos.

II. La condición económica del infractor: las áreas encargadas de calificar la gravedad de las faltas podrán requerir al infractor y a las autoridades competentes la información y documentación necesaria para determinar la condición económica del infractor. Sin perjuicio de lo anterior, deberán utilizarse los elementos que se tengan a disposición o las evidencias que obren en registros públicos, páginas de Internet oficiales, medios de información o cualesquier otra que permita cuantificar la multa.

III. La reincidencia: al que se le hubiere impuesto una medida de apremio y se le imponga otra por la misma causa. La reincidencia deberá ser considerada como agravante, por lo que siempre deberán consultarse los antecedentes del infractor.

La Ley General de Responsabilidades Administrativas establece lo siguiente:

Artículo 56. *Para efectos del artículo anterior, se considera información privilegiada la que obtenga el servidor público con motivo de sus funciones y que no sea del dominio público.*
La restricción prevista en el artículo anterior será aplicable inclusive cuando el servidor público se haya retirado del empleo, cargo o comisión, hasta por un plazo de un año.

Documentos consultados

Normatividad consultada

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.
- Ley General de Responsabilidades Administrativas.
- Código Civil del Estado de Jalisco.

- Lineamientos que Regulan las Atribuciones de las Áreas Encargadas de Calificar la Gravedad de la Falta de Observancia de las Determinaciones del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, así como la Notificación y Ejecución de las Medidas de Apremio Señaladas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Referencias

- F. de Marcos Isabel Davara. Primera edición (2019). *Diccionario de Protección de Datos Personales: Conceptos Fundamentales*. Ciudad de México. México. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Ciudad de México. Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Recuperado de http://inicio.ifai.org.mx/DocumentosdeInteres/_GuiaPrincipiosDeberes.pdf

- Agencia Española de Protección de Datos (2018). España. *Directrices para la Elaboración de Contratos entre Responsables y Encargados del Tratamiento*. Recuperado de https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf

Cynthia Patricia Cantero Pacheco
Presidenta del Pleno

Salvador Romero Espinosa
Comisionado Ciudadano

Pedro Antonio Rosas Hernández
Comisionado Ciudadano

Miguel Ángel Hernández Velázquez
Secretario Ejecutivo

La presente hoja de firmas, forma parte integral de Guía para establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase de tratamiento de los datos personales guarden confidencialidad, aprobada en la Vigésima Primera Sesión ordinaria del Pleno del Instituto, celebrada en fecha 17 diecisiete de Septiembre del año del 2020 dos mil veinte. -