DESARROLLO URBANO
Secretaría de Infraestructura,
Desarrollo Urbano y Reordenación Territorial

# DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES

DE LA SECRETARÍA DE INFRAESTRUCTURA, DESARROLLO URBANO Y REORDENACIÓN TERRITORIAL DE BAJA CALIFORNIA.

Índice:

# I. INTRODUCCIÓN

El derecho a la protección de datos personales ha venido a replantear la importancia que tiene nuestra vida privada, íntima y el adecuado tratamiento de nuestra información personal que se proporciona para la prestación de un servicio, realizar un trámite o como parte de nuestro quehacer laboral.

En la Secretaría de Infraestructura, Desarrollo Urbano y Reordenación Territorial , la información es un activo que debe protegerse, con la finalidad de dar cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, dicho activo toma relevancia ya que existen riesgos inherentes de que sucedan vulneraciones a la privacidad y a la intimidad de los titulares de los datos personales que se tratan, por lo que es importante establecer un conjunto coherente de procesos y sistemas diseñados, administrados y mantenidos.

En esencia, en este documento de seguridad se visualizará, de manera general, la forma en la cual la Secretaría de Infraestructura, Desarrollo Urbano y Reordenación Territorial protege la información personal con que cuenta y el tratamiento de ésta conforme a su ámbito y competencia, así como las acciones a implementar para la mejora continua y la difusión del presente documento a las personas que laboran o prestan sus servicios en el recinto legislativo.

De esta manera, la gestión de la seguridad de la información de soportes físicos y electrónicos, como parte de un sistema de mejora continua más amplio, busca establecer, implementar, operar, monitorear y mejorar los procesos y sistemas relativos a la confidencialidad, integridad y disponibilidad de la información, aplicando un enfoque basado en sistemas de gestión de calidad, sistemas de seguridad informática y dando cumplimiento a los principios y deberes señalados en la normatividad aplicable, observando los riesgos que la organización afronta, con la metodología propuesta por el Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales, denominada “BAA” (Beneficio, Accesibilidad y Anonimidad), en la cual se detectan las amenazas y estar en la posibilidad de establecer las medidas de seguridad necesarias para disminuir al mínimo las posibles vulneraciones.

En ese sentido, el presente documento se elabora, principalmente, para dar certeza a las personas respecto de las medidas de seguridad implementadas, para el adecuado tratamiento de los datos y, a su vez, dar cumplimiento a lo establecido en la Ley de Protección de datos Personales en Posesión de Sujetos Obligados.

## II. NORMATIVIDAD APLICABLE

Con este documento de seguridad, se da cumplimiento a lo establecido de manera general, en los Artículos 35 de Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que dicen: “De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente”:

I. El inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación.

### I. **El inventario de datos personales y de los sistemas de tratamiento**:

La Secretaría de Infraestructura, Desarrollo Urbano y Reordenación Territorial, es responsable del manejo de diversos datos personales, por ello, debe establecer las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los mismos.

De acuerdo a la importancia que tienen para la seguridad individual, se destacan dos categorías de datos personales:

Datos sensibles: Son datos personales que informan sobre los aspectos más íntimos de las personas, y cuyo mal uso pueda provocar discriminaciones o ponerles en grave riesgo, por ejemplo, el origen racial o étnico; estado de salud (pasado, presente y futuro); información genética; creencias religiosas, filosóficas y morales; afiliación sindical; opiniones políticas y preferencia sexual.

Datos patrimoniales o financieros: Es la información sobre la capacidad económica de las personas físicas que hace referencia a los recursos que posee y a su capacidad para hacer frente a sus deudas, como pueden ser: dinero, bienes muebles e inmuebles; información fiscal; historial crediticio; ingresos y egresos; cuentas bancarias; seguros; afores; fianzas, número de tarjeta de crédito, número de seguridad, entre otros.

A continuación, se describen las categorías de datos personales con los que

cuenta la Secretaría de Infraestructura, Desarrollo Urbano y Reordenación Territorial:

Datos de identificación y contacto: nombre, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, domicilio, teléfono particular, teléfono celular, correo electrónico, firma autógrafa, edad, fotografía y referencias personales.

**II. Las funciones y obligaciones de las personas que traten datos personales:**

Las subsecretarías, direcciones y jefaturas encargadas de tratar datos personales de la Secretaría de Infraestructura, Desarrollo Urbano y Reordenación Territorial son las siguientes:

Subsecretaría de Reordenación Territorial y Desarrollo Urbano.
Dirección Inversión Sectorial, Programación Presupuestal y Administración de Obras.
Dirección de Administración y Transparencia.
Departamento de Planeación y Control Presupuestal.

Las personas que desempeñan los puestos anteriormente mencionados, tienen como funciones y obligaciones las siguientes:

a) Garantizar la seguridad en el tratamiento de datos personales, esto con la finalidad de evitar algún riesgo, como la pérdida, robo, alteración o acceso no autorizado.
b) Garantizar la debida protección de los datos personales, conforme a la Ley y las demás disposiciones aplicables en la materia.
c) Implementar medidas de seguridad físicas, técnicas y administrativas convenientes para el tratamiento diario de los datos personales.
d) Garantizar la confidencialidad de los datos personales derivada de los procedimientos que tienen a su cargo.
e) Conocer y aplicar las acciones derivadas de este Documento de Seguridad.
f) Garantizar el cumplimiento de los derechos ARCO a los titulares de los datos personales.

## III. El análisis de riesgos:

Realizar un análisis de riesgos por cada tratamiento ayudará a identificar el nivel de medidas de seguridad que deben ser implementadas para la protección de los datos personales.

Una vez identificado el ideal de medidas de seguridad que deberían implementarse, se realiza un comparativo con aquellas que son implementadas por las áreas, obteniendo con ello un análisis de brecha, a través del cual se han construido los planes de trabajo, mecanismos de monitoreo y revisión de medidas de seguridad y programas de capacitación, elementos que conforman el Documento de Seguridad de la Secretaría de Infraestructura, Desarrollo Urbano y Reordenación Territorial.

De acuerdo al Estudio de riesgos realizado por la Unidad de Transparencia de la Secretaría de Infraestructura, Desarrollo Urbano y Reordenación Territorial en donde se analizaron las direcciones de la Secretaría de Infraestructura, Desarrollo Urbano y Reordenación Territorial que dan tratamiento a datos personales, se consideran como vulneraciones comunes las siguientes:

a) Robo, extravío o copia no autorizada.

b) Destrucción no autorizada

c) Daños por situaciones fortuitas.

## IV. El análisis de brecha:

El análisis de brecha, en materia de datos personales, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en sus artículos 33 y 35, hacen referencia a las medidas de seguridad que los responsables deben implementar para la protección de datos personales en donde señala que es necesario, entre otras actividades, llevar a cabo un análisis de brecha el cual debe ser incluido en el Documento de Seguridad, en conformidad con el artículo 34

Además, los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en el artículo 61, establecen que, para la realización del análisis de brecha, los responsables deben considerar las medidas de seguridad existentes y efectivas, las faltantes y la existencia de nuevas

medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

A través de la ejecución de un análisis de brecha aplicado a las medidas de seguridad que poseen datos personales durante su ciclo de vida, es posible obtener un diagnóstico de las prácticas de seguridad de la información con base en estándares nacionales y contar con mecanismos efectivos para su protección.

En este contexto, la Unidad de Transparencia realizó un Análisis de Brecha en la Seguridad Aplicada a los Datos Personales y se concluyó que, actualmente se tiene un nivel de medidas de seguridad óptimo en relación con los datos personales a los que se les da tratamiento en las distintas áreas de la Secretaría de Infraestructura, Desarrollo Urbano y Reordenación Territorial en relación con el ciclo de vida en el flujo de los datos personales, el cual está compuesto por las siguientes fases:

Etapa 1. Creación / colecta / captura.

Etapa 2. Procesamiento.

a) Mantenimiento de datos.
b) Almacenamiento.
c) Síntesis de datos / transformación.
d) Uso de la información.

Etapa 3. Transferencia / publicación / revelación.

Etapa 4. Archivado / retención.

Etapa 5. Destino final.

## V. El plan de trabajo:

El plan de trabajo para la protección de los datos personales que la Secretaría de Infraestructura, Desarrollo Urbano y Reordenación Territorial será: cumplir con los principios y deberes de la Ley General y la Ley, proyecto que se llevará a cabo a través del Comité de Transparencia y Acceso a la Información Pública, el cual se denomina “Certificación a Sujetos Obligados en materia de Datos Personales”, que a continuación se enlistan:

1. Canalizar a cada unidad administrativa que trate datos personales, la encuesta sobre el estado actual del cumplimiento de las obligaciones en materia de datos personales para que sea contestada y así poder conocer las áreas de oportunidad con las cuales se trabajará.

2. Capacitar al personal de la Secretaría de Infraestructura, Desarrollo Urbano y Reordenación Territorial en materia de datos personales.
3. Implementar medidas de seguridad físicas, administrativas y técnicas para la debida protección de los datos personales.
4. Conformar el documento de seguridad como lo requiere la Ley.
5. Llevar a cabo visitas de seguimiento y de verificación, esto con el objetivo de corroborar el cumplimiento de las obligaciones que marca la Ley.
6. Conformar la carpeta de evidencia del cumplimiento de las obligaciones según marca la Ley para que ésta sea revisada y aprobada por Comité de Transparencia y Acceso a la Información Pública.
7. De ser aprobada la carpeta de evidencia, la Secretaría de Infraestructura, Desarrollo Urbano y Reordenación Territorial tendrá por cumplidas las obligaciones de la Ley.

## VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad:

En ese sentido existen tres tipos de medidas de seguridad en el tratamiento de las bases de datos personales los cuales se definen a continuación:

*a) Administrativos*: Medidas de seguridad basadas en la cultura del personal, conocidas como medidas de seguridad administrativas. Se encuentran enfocadas en roles y responsabilidades de personas o entidades involucradas en el tratamiento de datos personales.

La Ley define estas medidas como:

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.
Sensibilización y capacitación del personal, en materia de Protección de Datos Personales.

Dentro de las medidas administrativas podríamos encontrar los siguientes ejemplos:

Concientización del personal en seguridad de la información y Protección de Datos Personales.
Políticas de escritorio limpio.
Bloqueo de pantalla del equipo.
Sanciones.

*b) Técnicos*: Medidas de seguridad en el entorno de trabajo digital, conocidas como medidas de seguridad técnicas. La Ley considera las acciones y mecanismos tecnológicos relacionados con software y hardware para proteger el entorno digital de datos personales y de los recursos involucrados en su tratamiento.

Para ello recomienda considerar al menos lo siguiente:

Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea identificados y autorizados.

Generar un esquema de privilegios para que el usuario realice las actividades que requiere con motivo de sus funciones.

Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento de software y hardware.

Gestionar de las comunicaciones, operaciones y medios de almacenamiento de los recursos informático en el tratamiento de datos personales.

Dentro de las medidas técnicas podríamos encontrar los siguientes ejemplos:

Bloqueo de equipo por inactividad.
Respaldos.
Roles de usuario.
Control de acceso.
Desbloqueo de pantalla con contraseña.

c*) Físicos*: Medidas de seguridad en el entorno de trabajo físico, conocidas como medidas de seguridad físicas. La Ley de Datos considera la protección del entorno físico de datos personales y de los recursos involucrados en su tratamiento y recomienda considerar lo siguiente

Prevenir acceso no autorizado al perímetro, instalaciones físicas, áreas críticas, recursos e información.

Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas, recursos e información. La identificación, clasificación y borrado seguro de la información.

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

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

En el caso del mantenimiento eficaz, busca asegurar en los equipos, la disponibilidad y la confidencialidad de datos personales, es decir, que siempre se pueda acceder a ellos y que sólo sean modificados por aquellos que han sido autorizados.

Dentro de las medidas físicas podríamos encontrar los siguientes ejemplos:

Candados
Circuitos Cerrados de Televisión (CCTV);
Bitácoras de entrada y salida de personal y visitantes.

## VII. El programa general de capacitación:

El programa de capacitación es una de las medidas de seguridad administrativa del tipo preventivo, efectiva y eficiente, en razón de que, permite que el tratamiento de datos personales se haga de una manera correcta y se evite el mal uso, sustracción, divulgación.

Ocultamiento, alteración, mutilación, destrucción total o parcial y de manera indebida de datos personales, que pongan en peligro la confidencialidad, integridad y disponibilidad de la información.

El objetivo principal del programa de capacitación es capacitar y concientizar a las y los servidores públicos de la Secretaría de Infraestructura, Desarrollo Urbano y Reordenación Territorial, en materia de protección de datos personales para el mejor desempeño de sus atribuciones, la especialización de sus funciones, el óptimo cumplimiento de los objetivos institucionales y promoción de la profesionalización en el servicio público.

Es de destacar que la capacitación en términos de protección de la información, permite a las personas identificar el tipo de información que manejan y el nivel de sensibilidad de la misma, además de conocer las mejores prácticas de tratamiento de la información desde el punto de vista de seguridad. Los planes de capacitación deben diseñarse e instrumentarse de acuerdo con el perfil y las responsabilidades de las personas a lo largo del ciclo de vida de los datos personales.

Resulta indispensable la obtención de técnica y perfeccionamiento de buenas prácticas en el tratamiento de los datos personales para el debido cumplimiento de las atribuciones de todo servidor público dentro de la Secretaría de Infraestructura, Desarrollo Urbano y Reordenación Territorial.

La parte de capacitación se considera una acción sumamente importante dentro del proceso de mejora continua.

Del mismo modo se busca garantizar la protección del tratamiento de los datos personales obtenidos como sujeto obligado, optimizar recursos, maximizar beneficios, establecer directrices para el correcto uso de la información en términos de su seguridad y generar esquemas de capacitación diferenciales e integrales que atiendan los siguientes rubros:

Desarrollar los niveles de competencias laborales a través del perfeccionamiento de conocimientos, habilidades, actitudes y valores.

Elevar los niveles de apropiación del conocimiento en materia de protección de datos personales.

Establecer herramientas para realizar un efectivo tratamiento de datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO).

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

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

Una vez aceptado el programa de capacitación, la Unidad de Transparencia enviará a las Direcciones de la Secretaría de Infraestructura, Desarrollo Urbano y Reordenación Territorial a través de sus enlaces de capacitación, los cursos disponibles en materia de protección de datos personales.