GUÍA PARA LA

ELABORACIÓN DEL DOCUMENTO DE SEGURIDAD

DIRECCIÓN DE DATOS PERSONALES

Índice

1. Introducción
2. Marco normativo
3. Conceptos básicos y abreviaturas
4. Consideraciones previas
5. Estructura del documento de seguridad
   - 5.1. Datos generales del sistema
   - 5.2. Inventario de datos personales
   - 5.3. Funciones y obligaciones de las personas que intervienen en el tratamiento del sistema de datos personales
   - 5.4. Registro de incidencias
   - 5.5. Identificación y autentificación
   - 5.6. Control de acceso, gestión de soportes y copias de respaldo y recuperación
   - 5.7. Análisis de riesgo
   - 5.8. Análisis de brecha
   - 5.9. Responsable de seguridad
   - 5.10. Registro de acceso y telecomunicaciones
   - 5.11. Mecanismo de monitoreo y revisión de medidas de seguridad
   - 5.12. Plan de trabajo
   - 5.13. Plan de capacitación
6. Anexos

1. INTRODUCCIÓN

El Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, como organismo garante en materia de protección de datos personales en posesión de los sujetos obligados de la Ciudad de México, emite la presente guía con la finalidad de coadyuvar con el lícito, transparente y responsable tratamiento de datos personales que debe realizar cualquier autoridad, entidad, órgano y organismos pertenecientes a los poderes Ejecutivo, Legislativo y Judicial, organismos autónomos, partidos políticos, fideicomisos y fondos públicos de la capital de nuestro país.

Asimismo, de conformidad con las obligaciones establecidas en los artículos 26, 27, 28 y 29 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, así como del artículo 52 de los Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, la presente guía busca brindar elementos de carácter técnico para la elaboración del documento de seguridad, con el fin de mejorar las prácticas en el tratamiento y evitar el daño, pérdida, alteración, destrucción, uso, acceso o cualquier tipo de vulneración de los datos personales con los que cuentan los sujetos obligados; derivado de la información que poseen de las personas físicas a las cuales prestan, dan o reciben un servicio y de las personas que laboran en ellas, a fin de hacer eficiente sus procesos y ser expeditos en sus respuestas.

Para que el tratamiento de los datos personales sea lícito, transparente y responsable, se deberán adoptar las medidas de seguridad necesarias para la protección contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizados. Por lo que, las acciones relacionadas con dichas medidas deberán estar documentadas y contenidas en un documento de seguridad.

Por ello, la presente guía está diseñada de manera sencilla con el objetivo de dar a conocer el marco normativo y los conceptos básicos sobre la de protección de datos personales. Además, encontrará la estructura del documento de seguridad desglosada en apartados específicos, así como los anexos técnicos que le permitirán ahondar más al respecto.

2. MARCO NORMATIVO.

El **documento de seguridad** tiene su **fundamento legal** en el artículo 6°, párrafos segundo y cuarto, inciso A, fracciones I y II, de la Constitución Política de los Estados Unidos Mexicanos, que a la letra señalan:

> *"**Constitución Política de los Estados Unidos Mexicanos***
>
> ***Artículo 6o.***
>
> *(…)*
>
> *Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión.*
>
> *(…)*
>
> *Para efectos de lo dispuesto en el presente artículo se observará lo siguiente:*
>
> ***A.** Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:*
>
> ***I.** Los sujetos obligados deberán **documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones**, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información*
>
> ***II. La información que se refiere a la vida privada y los datos personales será protegida** en los términos y con las excepciones que fijen las leyes." (sic) **Énfasis añadido***

De igual manera, la Constitución Política de la Ciudad de México, en su artículo 7°, Ciudad Democrática, inciso D. Derecho a la información, numeral 3, así como el inciso E. Derecho a la Privacidad y a la Protección de los Datos Personales, numerales 1 y 2, establece:

> ***"Constitución Política de la Ciudad de México***
>
> ***Artículo 7***
>
> ***Ciudad democrática***
>
> *(…)*
>
> ***D.*** *Derecho a la información.*
>
> *(…)*
>
> ***3.*** *En la interpretación de este derecho prevalecerá el principio de máxima publicidad.* ***Los sujetos obligados deberán documentar los actos del ejercicio de sus funciones****. La información sólo podrá reservarse temporalmente por razones de interés público para los casos y en los términos que fijen la Constitución Política de los Estados Unidos Mexicanos y las leyes.*
>
> *(…)*
>
> ***E.*** *Derecho a la privacidad y a la protección de los datos personales,*
>
> ***1.*** *Toda persona tiene derecho a que se respete y* ***proteja*** *su privacidad individual y familiar, a la inviolabilidad del domicilio y de sus comunicaciones.*
>
> ***2. Se protegerá la información que se refiera a la privacidad y los datos personales****, en los términos y con las excepciones que establezcan la Constitución Política de los Estados Unidos Mexicanos y las leyes." (sic)* ***Énfasis añadido***

Por lo que respecta a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, en sus artículos 27 y 28, señala lo siguiente:

> *"**Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México***
>
> ***Artículo 27.*** *Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión denominado* ***Documento de Seguridad****.*

Artículo 28. *El responsable deberá* ***elaborar el documento de seguridad*** *que contendrá, al menos, lo siguiente:*

I*. El inventario de datos personales en los sistemas de datos;*
II. *Las funciones y obligaciones de las personas que intervengan en el tratamiento datos personales, usuarios y encargados, en el caso de que los hubiera;*
III. *Registro de incidencias;*
IV. *Identificación y autentificación;*
V. *Control de acceso; gestión de soportes y copias de respaldo y recuperación;*
VI. *El análisis de riesgos;*
VII. *El análisis de brecha;*
VIII. *Responsable de seguridad;*
IX. *Registro de acceso y telecomunicaciones;*
X. *Los mecanismos de monitoreo y revisión de las medidas de seguridad;*
XI. *El plan de trabajo; y*
XII. *El programa general de capacitación." (sic)* ***Énfasis añadido***

Por su parte, los Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, en sus artículos 51 y 52, establecen:

"Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México

Sistema de gestión
Artículo 51. El responsable deberá implementar un sistema de gestión de seguridad de los datos personales a que se refiere el artículo 27 de la Ley, *el cual permita planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales; tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad de la información.*

Documento de seguridad
Artículo. 52. El responsable elaborará, difundirá e implementará las normas internas de seguridad de la información mediante el documento de seguridad *que será de observancia obligatoria para todos los servidores públicos del sujeto obligado, así como para*

toda aquella persona que en su carácter de encargado, conforme al artículo 3, fracción XV de la Ley, tenga acceso a los sistemas de datos personales y/o al sitio donde se ubican los mismos, para ello, el responsable deberá tomar en cuenta lo dispuesto en la Ley y en los presentes Lineamientos.

El documento de seguridad deberá contener, como mínimo, lo siguiente:

***I.** El inventario de datos personales en los sistemas de datos;*
***II.** Las funciones y obligaciones de las personas que intervengan en el tratamiento de datos personales, usuarios y encargados, en el caso de que los hubiera;*
***III.** Registro de incidencias;*
***IV.** Identificación y autentificación;*
***V.** Control de acceso; gestión de soportes y copias de respaldo y recuperación;*
***VI.** El análisis de riesgos;*
***VII.** El análisis de brecha;*
***VIII.** Responsable de seguridad;*
***IX.** Registro de acceso y telecomunicaciones;*
***X.** Los mecanismos de monitoreo y revisión de las medidas de seguridad;*
***XI.** El plan de trabajo, y*
***XII.** El programa general de capacitación.*

El responsable deberá actualizar el documento de seguridad anualmente, o cuando se produzcan modificaciones relevantes en el tratamiento de los datos que impliquen un cambio en el nivel de riesgo; ante acciones de mejora continua derivadas del monitoreo del sistema de seguridad; ante una vulneración ocurrida; ante la implementación de acciones preventivas y correctivas derivadas de una vulneración de seguridad, o bien por recomendación del Instituto." (sic) ***Énfasis añadido***

3. CONCEPTOS BÁSICOS Y ABREVIATURAS

Para efectos de la presente guía se entenderá por:

Autentificación: Comprobación de la identidad de aquella persona autorizada para el tratamiento de datos personales.

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

Ciclo de vida: Tiempo que duración y conclusión del tratamiento de los datos personales, para después ser suprimidos, cancelados o destruidos por parte del responsable.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona física es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información como puede ser nombre, número de identificación, datos de localización, identificador en línea o uno o varios elementos de la identidad física, fisiológica, genética, psíquica, patrimonial, económica, cultural o social de la persona.

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 este. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, información biométrica, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

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

Finalidad: Los datos personales recabados y tratados tendrán fines determinados, explícitos y legítimos y no podrán ser tratados ulteriormente con fines distintos para los que fueron recabados. Los datos personales con fines de archivo, de interés público, investigación científica e histórica, o estadísticos no se considerarán incompatibles con la finalidad inicial.

GOCDMX: Gaceta Oficial de la Ciudad de México.

Incidencia: Cualquier anomalía que afecte o pudiera afectar la seguridad de los datos personales.

Instituto: Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.

Ley de Datos local: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

Lineamientos Generales: Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales y los sistemas de 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 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 consideran 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 de la organización.
d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad 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 los recursos involucrados en su tratamiento; de manera enunciativa más no limitativa, se consideran 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.
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, dentro o fuera del territorio mexicano.

RESDP: El Registro Electrónico de Sistemas de Datos Personales, es la aplicación informática desarrollada por el Instituto para la inscripción de los sistemas de datos personales en posesión de los entes públicos para su custodia y protección.

Responsable: Cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, Órganos Autónomos, Partidos Políticos, Fideicomisos y Fondos Públicos, que decida y determine finalidad, fines, medios, medidas de seguridad y demás cuestiones relacionadas con el tratamiento de datos personales.

Responsable de seguridad: Persona a la que el responsable del sistema de datos personales asigna formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

Responsable del sistema de datos personales: Persona servidora pública que decide sobre el tratamiento de los datos personales, su finalidad, la protección y las medidas de seguridad de los mismos.

Sistema de datos personales: Conjunto de organizado de archivos, registros, ficheros, bases o banco de datos personales en posesión de los sujetos obligados, cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

Los sistemas de datos personales se distinguen en:

- **Físicos**: Conjunto ordenado de datos de carácter personal que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos, estructurado conforme a criterios específicos relativos a personas físicas que permitan acceder sin esfuerzos desproporcionados a sus datos personales.

- **Automatizados**: Conjunto ordenado de datos de carácter personal que permita acceder a la información relativa a una persona física utilizando una herramienta tecnológica

Soporte físico: Son los medios de almacenamiento inteligibles a simple vista, es decir, 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, demás análogos.

Soporte electrónico: Son los medios de almacenamiento inteligibles solo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos, es decir, cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDs y DVDs), discos magneto-ópticos, discos magnéticos (flexibles y duros), tarjetas de memoria (USB y SD) y demás medios de almacenamiento masivo no volátil.

Titular: La persona física a quien corresponden los datos personales.

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

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas sobre datos personales o conjunto de datos personales, mediante procedimientos manuales o automatizados relacionadas con la obtención, uso, registro, organización, estructuración, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión o cualquier otra forma de habilitación de acceso, cotejo, interconexión, manejo, aprovechamiento, divulgación, transferencia, supresión, destrucción o disposición de datos personales.

Unidad de Transparencia: Instancia que auxilia, orienta, gestiona, establece, informa, propone, aplica, asesora, registra y realiza las gestiones necesarias para el manejo, mantenimiento, seguridad, y protección de los sistemas de datos personales en posesión del responsable.

Usuario: Persona autorizada por el responsable, y parte de la organización del sujeto obligado, que dé tratamiento y/o tenga acceso a los datos y/o a los sistemas 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, 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.

4. CONSIDERACIONES PREVIAS.

Para el desarrollo del documento de seguridad, resulta necesario conocer las acciones que deben contemplarse de manera previa a la elaboración del documento de seguridad:

ACCIÓN
1. Identificación de la atribución normativa que involucra el tratamiento de datos personales.
2. Elaboración y publicación en la GOCDMX, del acuerdo de creación del sistema de datos personales, del que se trate.
3. Inscripción del sistema de datos personales en el RESDP.
4. Notificar al Instituto sobre la publicación en la GOCDMX del acuerdo correspondiente.
5. Elaboración de los avisos de privacidad simplificado e integral, previo a la recabación de datos.
6. Elaboración del documento de seguridad de cada sistema de datos personales.

5. ESTRUCTURA DEL DOCUMENTO DE SEGURIDAD.

Como se observa, todas las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión denominado: **documento de seguridad**.

En ese sentido, se deben realizar las siguientes preguntas:

¿Qué es el documento de seguridad?
Es el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que se posean.

¿Quién genera el documento de seguridad?
La persona responsable del sistema de datos personales es quien deberá generar el documento de seguridad.

¿Cuál es el objeto y la finalidad de generar del documento de seguridad?
El objeto es garantizar que todo tratamiento de datos personales cuente con las medidas de seguridad para la protección de datos personales y las obligaciones previstas en la Ley de Datos local. Por su parte, la finalidad es que el sujeto obligado cumpla con el tratamiento lícito, seguro y responsable de los datos personales.

Ahora bien, en el artículo 28 de la Ley de Datos local; en relación con el artículo 52 de los Lineamientos Generales, se establecen los elementos mínimos que debe contener el documento de seguridad.

Con base en esta normativo, se recomienda desarrollar el documento de seguridad con la siguiente estructura:

Documento de seguridad
Datos generales del sistema de datos personales
Inventario de datos personales
Funciones y obligaciones de las personas que intervienen en el tratamiento de los datos personales, usuarios y encargados
Registro de incidencias
Identificación y autenticación
Control de acceso, gestión de soportes, y copias de respaldo y recuperación
Análisis de riesgo
Análisis de brecha
Responsable de seguridad
Registro de acceso y telecomunicaciones
Mecanismos de monitoreo y revisión de las medidas de seguridad
Plan de trabajo
Programa general de capacitación

Asimismo, se deberá contar con los datos de identificación y validación de las personas que elaboran y aprueba el documento de seguridad que se desarrolle, indicando (se sugiere mantener como encabezado esta información):

Logo del sujeto obligado	**DOCUMENTO DE SEGURIDAD**	
	Nombre del sistema de datos personales	
	Fecha de elaboración del documento de seguridad	Fecha de la última actualización del documento de seguridad
	Elaboró el documento	Aprobó
	(Nombre y firma)	(Nombre y firma)

5.1. DATOS GENERALES DEL SISTEMA DE DATOS PERSONALES

Una de las particularidades que contempla la legislación en materia de datos personales a nivel local respecto al documento de seguridades es que se deben señalar los datos generales del sistema de datos personales. Es decir, se debe describir la formalización de la acción que involucra el tratamiento de datos personales, de la siguiente manera:

- ✓ **Nombre del sistema:** El nombre del sistema de datos personales, debe coincidir con el publicado en GOCDMX**,** mediante acuerdo de creación (en caso de que aplique) y/o con el inscrito en el RESDP.

- ✓ **Fecha de publicación en la GOCDMX del acuerdo de creación:** Se debe indicar la fecha de publicación en la GOCDMX del acuerdo de creación del sistema de datos personales (en caso de que aplique). (Se recomienda adjuntar como anexo copia de la publicación en la GOCDMX).

- ✓ **Fecha de inscripción en el RESDP:** Se debe indicar la fecha de inscripción del sistema de datos personales en el RESDP.

- ✓ **Folio de inscripción en el RESDP:** Se debe indicar el número de folio señalado en el acuse de inscripción del sistema de datos personales en el RESDP (se recomienda adjuntar como anexo el acuse).

- ✓ **Fecha de publicación en GOCDMX del acuerdo de modificación:** En caso de que aplique, se debe indicar la fecha de publicación en la GOCDMX del acuerdo de modificación del sistema de datos personales (se recomienda adjuntar como anexo copia de la publicación en la GOCDMX).

- ✓ **Fecha de última modificación en el RESDP:** Se debe indicar la fecha de última modificación del sistema de datos personales en el RESDP (se recomienda en todo momento, adjuntar como anexo los acuses de edición del sistema de datos personales).

- ✓ **Normatividad aplicable para el tratamiento:** Se debe indicar tanto la normativa general y especifica que faculta al responsable para realizar el tratamiento de datos personales.

    - o **General:** Las normas que son emitidas para ser cumplidas por todos los sujetos obligados en materia de protección de datos personales.
    - o **Específica:** Se refiere a la normatividad que da atribución directa a la persona responsable del sistema de datos personales para realizar la acción que involucra el tratamiento.

Ejemplo:

I. Constitución Política de los Estados Unidos Mexicanos, artículos 6, párrafo segundo, fracción II; 16, párrafo segundo (Diario Oficial de la Federación fecha de última reforma).

II. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México artículos…(GOCDMX fecha de última reforma).

III. Ley de Transparencia y Acceso a la Información Pública de la Ciudad de México artículos…(GOCDMX fecha de última reforma).
IV. Ley de Archivos de la Ciudad de México artículos...(GOCDMX fecha de última reforma).
V. Ley del Procedimiento Administrativo de la Ciudad de México artículos… (GOCDMX fecha de última reforma).
VI. Reglamento Interior…
VII. Lineamientos…
VIII. Manual…
IX. etc.…

5.2. INVENTARIO DE DATOS PERSONALES.

Para el desarrollo de este apartado, nos debemos preguntar:

¿En qué consiste el inventario de datos personales?
Consiste en identificar los tipos de datos personales que son tratados en el sistema de datos personales, enlistándolos y agrupándolos por categorías, indicando en su caso, si se tratan datos personales de carácter sensible. De igual forma, se debe plasmar la información básica de cada tratamiento de los datos personales contenidos en el sistema respectivo, la cual se relaciona de manera directa con el flujo de los datos personales.

Asimismo, para la elaboración de cada uno de sus elementos se deberá responder:

- **¿Cómo se realiza la obtención de los datos personales que se tratan en el sistema?**
- **¿Se realiza tratamiento de datos sensibles?**
- **¿Cuál es la finalidad del tratamiento que se realiza a los datos personales?**
- **¿Se realizan remisiones? En su caso, ¿quién es el encargado?**

- **¿Se realizan transferencias de datos personales? ¿con qué motivo y bajo qué fundamento se realizan?**

Conforme al "Catálogo de Disposición Documental" del sujeto obligado, así como de la información contenida en el RESDP ¿cuál es el ciclo de vida de los datos?

En ese aspecto, el inventario de datos personales deberá incluir al menos los siguientes elementos:

- ✓ El catálogo de medios físicos y/o electrónicos a través de los cuales se obtienen los datos personales. La obtención de datos personales corresponde a la recolección directamente del titular, o bien, de manera indirecta a través de la transferencia de terceros, previo consentimiento del titular, por lo que se deben enlistar los medios, por los cuales se obtienen los datos personales. Ejemplo: formularios físicos o electrónicos, vía telefónica, entre otros.
- ✓ Las finalidades de cada tratamiento de datos personales. Se deben describir las finalidades por las cuales se realiza el tratamiento de datos personales, considerando que estas sean concretas, lícitas, explicitas y legítimas.
- ✓ El catálogo de los tipos de datos personales que se traten. En este catálogo se deben indicar si los datos personales son sensibles o no. Se deberá enlistar y catalogar la totalidad de datos personales que se recaban, considerando lo dispuesto en el artículo 62 de los Lineamientos Generales.
- ✓ El catálogo de formatos de almacenamiento, para este rubro, se deberá indicar la descripción general de la ubicación física y/o electrónica de los datos personales.
- ✓ La lista de personas servidoras públicas que tienen acceso a los datos personales del sistema. Es el listado de las personas del sujeto obligado involucradas en el tratamiento de los datos personales.
- ✓ En su caso, el nombre completo, denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable.

- ✓ En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican estas.
- ✓ El ciclo de vida de los datos personales y la clave archivística asignada al sistema.

Es de recalcar, que el inventario de datos personales deberá mantenerse actualizado.

Por lo antes descrito, se recomienda estructurar el apartado "inventario de datos personales" de la siguiente forma:

Obtención

Las personas sobre las que se pretenden obtener datos de carácter personal son… ***(Se debe describir el colectivo de personas de los cuales se obtienen los datos personales, de los que se dará tratamiento, es decir, ¿de quién se recaban los datos?, dicho rubro deberá corresponder a lo establecido en los acuerdos de creación o modificación del sistema de datos que corresponda, así como lo contenido en el RESDP, ejemplo: Beneficiarios del programa social X).***

Los datos personales se recaban de forma **(directa/indirecta)**, a través de **(enlistar y, en su caso, agregar como anexo, los medios por los cuales se recaba la información, ya sean físicos, electrónicos o en caso de considerar ambos este es mixto).**

- ✓ **Modo de tratamiento:** El procesamiento de los datos personales se llevará a cabo a través de procedimientos **(físicos, electrónicos o mixtos).**

- ✓ **Medio de actualización:** La actualización de los datos personales se llevará a cabo **(a petición del interesado, revisión periódica o mediante oficio).**

Finalidades del tratamiento

Finalidad y uso previsto: Se deberán describir las finalidades de cada tratamiento de datos personales **(deben coincidir con lo publicado en la GOCDMX, en caso de que aplique, así como lo contenido en el RESDP).**

De manera enunciativa, más no limitativa, las acciones o tratamiento que podemos realizar son:

- Uso
- Obtención
- Acceso
- Registro
- Organización
- Estructuración
- Adaptación
- Indexación
- Modificación
- Extracción
- Consulta
- Almacenamiento
- Conservación
- Elaboración
- Transferencia
- Difusión
- Posesión
- Aprovechamiento

Transferencias

La transferencia es toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

Se deben enlistar los terceros receptores, a los cuales se realiza la transferencia de datos personales. Así como, las finalidades que la justifican. Es decir, a quien se realiza la transferencia y las finalidades.

De igual forma, se deben indicar las transferencias que se realicen entre sujetos obligados, y que se encuentren de manera expresa en una ley o tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos **(Se**

recomienda anexar copia del instrumento jurídico, por el cual se formalizó la transferencia).

Ejemplo:

INSTANCIA	***FINALIDAD***
Comisión de Derechos Humanos de la Ciudad de México	*Para la atención de denuncias por probable violación a sus derechos humanos*
Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México	*Para la atención de Recursos de Revisión y Denuncias por Probable incumplimiento a la Ley de Datos local.*
Otros…	

Remisiones (responsable – encargados)

¿Qué es una remisión?

La remisión es toda comunicación de datos personales realizada exclusivamente entre responsable y encargado, dentro o fuera del territorio mexicano.

Se debe enlistar a la(s) persona(s) física(s) o jurídica(s), pública(s) o privada(s) **ajena(s) al responsable** y que tratan datos personales, a nombre y por cuenta del responsable; dicha información debe coincidir lo publicado en la GOCDMX en caso de que aplique, así como lo contenido en el RESDP.

Se recomienda anexar copia del contrato o instrumento jurídico, según sea el caso, por el cual se formalizó la relación entre responsable y encargado.

Interrelación

Se debe señalar si el sistema de datos personales se interrelaciona con otro sistema del mismo sujeto obligado e indicar nombre del sistema y finalidad de la interrelación.

El catálogo de los tipos de datos personales

Se debe señalar el tipo de datos personales que contiene el sistema (datos personales, datos personales sensibles).

Además, se debe enlistar cada uno de los datos personales recabados, catalogándolos conforme a lo establecido en el el artículo 62 de los Lineamientos Generales.

Ejemplo:

En el sistema de datos personales (nombre del sistema del que se trata) se lleva a cabo el tratamiento de los siguientes datos:

> **Datos identificativos:** (nombre, teléfono particular, edad, etc.).
> **Datos electrónicos:** (correo electrónico no oficial, nombre de usuario, contraseñas, etc.).
> **Datos especialmente protegidos (sensibles):** (origen étnico o racial, ideología y opiniones políticas, etc.)

Se podrán indicar las demás categorías y tipos de datos que resulten aplicables.

Los datos personales del sistema se encuentran contenidos (señalar la serie documental, donde se encuentre identificado el sistema y anexar el Catálogo de Disposición Documental del sujeto obligado).

Ciclo de vida de los datos

Esta información debe coincidir con lo que señala el Catálogo de Disposición Documental del sujeto obligado. Así como también, con la información contenida en el RESDP. Se deberá indicar la temporalidad de resguardo de la información en cada uno de los medios siguientes:

- En medio automatizado.
- En archivo de trámite.
- En archivo de concentración.

Así como señalar si se contempla la transferencia de información al archivo histórico.

Nivel y medidas de seguridad

La determinación del nivel de seguridad está asociada en forma directa con la sensibilidad del dato personal, mientras más sensibles sean los datos tratados, mayor rigor se debe aplicar en la protección de estos.

Nivel de seguridad: Indicar el nivel de seguridad aplicable de acuerdo con el tipo de datos recabados:

- Básico.
- Medio.
- Alto.

Es pertinente mencionar que las medidas de seguridad asociadas a los niveles son acumulativas. Por ejemplo, en el nivel medio se incluyen, además de las medidas de seguridad que corresponden a este nivel, las adoptadas en el nivel básico.

En consecuencia, en el nivel alto se contendrán las correspondientes al nivel básico y al nivel medio, en adición a las propias del mismo.

De igual forma, se deben referir las medidas de seguridad adoptada (si son físicas y/o técnicas y/o administrativas).

Medidas de seguridad: Describir las medidas de seguridad adoptada, aplicable a cada caso conforme a lo establecido en la Ley de Datos local:

- Medidas de seguridad administrativas.
- Medidas de seguridad físicas.
- Medidas de seguridad técnicas.

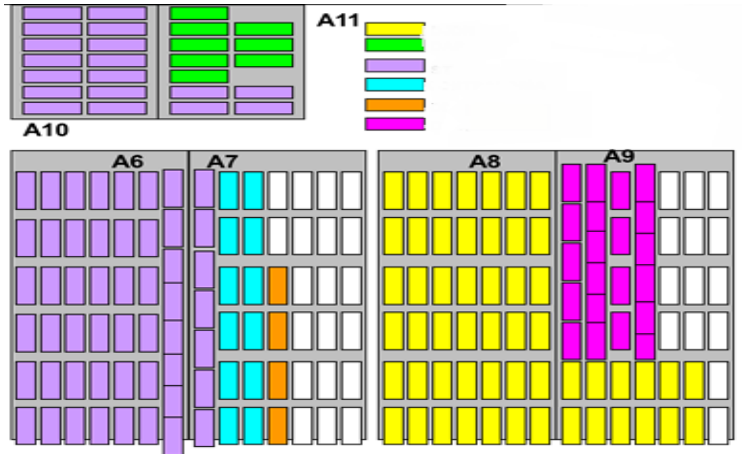
Catálogo de las formas de almacenamiento:

Se debe realizar la descripción general de la ubicación física y/o electrónica de los datos personales. Se puede hacer uso de mapas, planos etc., para señalar la ubicación específica donde se resguarda el sistema de datos personales.

Ejemplo:

Los expedientes del sistema de datos personales denominado (nombre del sistema), se encuentran resguardados en el inmueble localizado en (domicilio de ubicación).

Insertar plano o mapa de ubicación del sistema de datos personales, ejemplo:



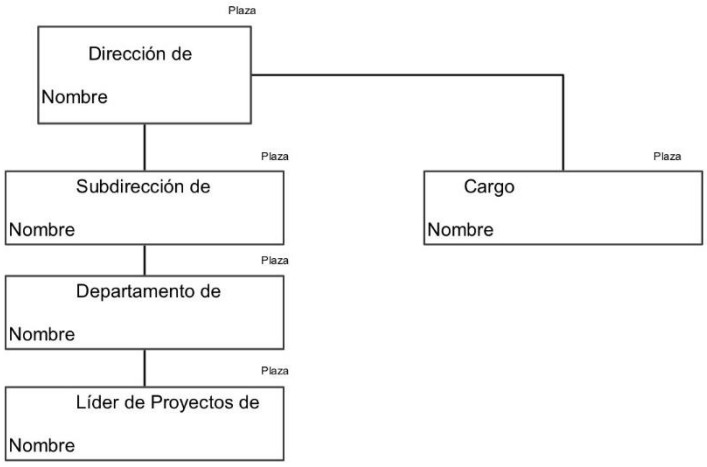
Lista de los servidores públicos que tienen acceso a los datos personales.

Se debe enlistar al personal dentro de la organización que esté involucrado en el tratamiento de datos personales, incluyendo el cargo de la persona y el área de adscripción.

Ejemplo:

Solo los siguientes servidores públicos que forman parte de la estructura orgánica de X dirección (ver diagrama de la estructura orgánica) podrán acceder a los contenidos del sistema, con el objeto de dar paso al desarrollo de las funciones y atribuciones que les han sido conferidas.

1. Nombre
   Director de…
2. Nombre
   Subdirector de…
3. Jefe de Departamento de…
4. Líder de proyectos/Enlace
5. Jefe de Departamento de…



5.3. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE INTERVIENEN EN EL TRATAMIENTO DEL SISTEMA DE DATOS PERSONALES.

En este apartado del documento de seguridad, nos debemos preguntar **¿Cuáles son las funciones y obligaciones del responsable, usuarios y encargados?** Por lo tanto, se deben indicar las funciones y obligaciones para garantizar la protección de los datos personales que deben cumplir las personas que intervienen en el tratamiento de datos personales del sistema correspondiente.

Se deben describir, las funciones y obligaciones que establecen la normativa en materia de protección de datos local, así como las relativas a la normativa interior o especifica del sujeto obligado.

Estas funciones y obligaciones deben también relacionarse con las de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso, esta designación supone una delegación de las facultades y atribuciones que le corresponden al responsable del sistema de datos personales de acuerdo con la normativa en materia de protección de datos local.

El responsable del sistema de datos personales deberá establecer y documentar los roles y las responsabilidades del personal involucrado en el tratamiento de datos personales, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización.

El responsable del sistema de datos personales deberá establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales en su organización conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento.

En ese aspecto, se deben considerar las siguientes figuras que intervienen en el tratamiento de los datos:

- Responsable del sistema de datos personales.
- Usuario.
- Encargado.

Asimismo, podremos observar algunas de las funciones y obligaciones que dichas figuras pueden tener, en el entendido de que las acciones aquí plasmadas son enunciativas más no limitativas:

Responsable del sistema de datos personales.- Elaborar políticas y programas, poner en práctica un programa de capacitación actualización sobre las obligaciones y deberes, revisar periódicamente las políticas y programas de seguridad de datos personales, determinar las modificaciones que se requieran, establecer un sistema de supervisión de vigilancia interna y externa, adoptar las medida de seguridad necesarias, elaborar los criterios específicos sobre el manejo, mantenimiento, seguridad y protección del sistema de datos personales, registrar ante el Instituto el sistema de datos personales, determinar las modificaciones o la supresión del sistema, coordinar y supervisar la adopción de medidas de seguridad a que se encuentran sometidos los datos personales del sistema de datos personales respectivo.

Usuario.- Deberá identificar, clasificar, borrar, prevenir el acceso no autorizado, a las instalaciones físicas, aéreas críticas, prevenir daños e interferencias a sus instalaciones, proteger los recursos móviles, portátiles, soportes físicos, electrónicos, dar mantenimiento al sistema, asegurar la disponibilidad e integridad, proteger el entorno digital, prevenir el acceso a las bases de datos, a la información, los recursos, generar esquemas de privilegios, revisar la configuración de seguridad, apoyar en la adquisición, operación, desarrollo, y mantenimiento del software y hardware, gestionar las comunicaciones, operaciones y medios de almacenamiento de la información en el tratamiento de datos personales.

Encargado.- Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable, abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable, implementar las medidas de seguridad conforme a la naturaleza de los datos, informar al responsable cuando ocurra una vulneración, guardar la confidencialidad, suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.

Se recomienda estructurar el presente apartado de la siguiente manera:

Funciones y obligaciones de las personas que intervienen en el tratamiento de los datos personales

Responsable:

- Nombre
- Cargo
- Funciones: con relación al tratamiento de los datos personales en el manejo del sistema.
- Obligaciones: en cuanto al tratamiento de los datos personales en el sistema.

Usuarios:

- Nombre
- Cargo
- Nombre
- Cargo

Y así sucesivamente, dependiendo de cuantos usuarios intervengan en el sistema de datos del que se trate.

- Funciones: con relación al tratamiento de los datos personales en el manejo del sistema (se deben indicar las funciones que le competen de acuerdo con las atribuciones del responsable del sistema de datos personales).
- Obligaciones: en cuanto al tratamiento de los datos personales en el sistema (se deben indicar las obligaciones que le competen de acuerdo con las atribuciones del responsable del sistema de datos personales).

De igual forma, se recomienda realizar la formalización mediante oficio, signado por el responsable del sistema de datos personales, a través del cual se designe a las personas que son usuarias, para que conozcan sus funciones y obligaciones y, en su caso, deslindar responsabilidades ante las vulneraciones de seguridad, que pudieran presentarse y afecten los datos personales del sistema; dichos oficios deberán anexarse al documento de seguridad.

Encargado (s):

- Nombre
- Cargo
- Funciones: además de lo que establecen los artículos 55 y 56 de la Ley de Datos local, se deben de indicar las funciones que le competen de acuerdo con las atribuciones del sujeto obligado, así como las que se establezcan en el instrumento jurídico mediante el cual se formalizó la relación entre el encargado y el responsable.
- Obligaciones: además de lo que establecen los artículos 55 y 56 de la Ley de Datos local, se deben de indicar las obligaciones que le competen de acuerdo con las atribuciones del sujeto obligado, así como las que se establezcan en el instrumento jurídico mediante el cual se formalizó la relación entre el encargado y el responsable.

Establecer las obligaciones generales no incluidas en las categorías señaladas al principio de este apartado

Se deben establecer las políticas generales de seguridad que aplican a todo el personal o a personas ajenas a la unidad administrativa que detenta el sistema de datos personales.

Ejemplo:

- Guardar la debida secrecía sobre los datos personales que conozcan en el desarrollo de sus funciones, evitando su difusión y/o transmisión.
- Informar al responsable del sistema de datos personales o al responsable de seguridad sobre cualquier incidencia que tenga conocimiento.
- No dejar información visible cuando abandone su puesto, ya sea que se ausente de manera temporal o si hay alguna persona ajena a la unidad administrativa a la que esté adscrito.
- Conservar el buen estado físico de los soportes documentales a que tengan acceso, por motivo del ejercicio de sus funciones.
- Reportar alguna vulneración de los datos personales.

5.4. REGISTRO DE INCIDENCIAS

En el presente punto, es conveniente preguntarnos:

¿Qué es una incidencia?

Una incidencia de seguridad puede ser cualquier incumplimiento de las disposiciones establecidas en el documento de seguridad, y/o cualquier anomalía que afecte o pueda afectar la seguridad de los datos de carácter personal en el sistema.

Estas pueden ser generadas por la acción u omisión de las personas que tienen acceso al sistema o a causa de desastres naturales y/o tecnológicos, así como por la comisión de delitos dolosos o culposos.

La Organización de las Naciones Unidas[1] señala que los desastres se clasifican en:

1. Naturales.
2. Tecnológicos.

DESASTRES NATURALES[2].

Son los desastres producidos por la fuerza de la naturaleza. Algunos tipos de desastres son:

1. **Desastres generados por procesos dinámicos internos de la tierra.**
   - Sismos: Son los movimientos de la corteza terrestre que generan deformaciones intensas en las rocas del interior de la tierra, acumulando energía que súbitamente es liberada en forma de ondas que sacuden la superficie terrestre.
   - Tsunamis: Movimiento de la corteza terrestre en el fondo del océano, formando y propagando olas de gran altura.
   - Erupciones Volcánicas: Es el paso del material, cenizas y gases del interior de la tierra a la superficie.

2. **Desastres generados por procesos dinámicos externos de la tierra.**
   - Deslizamiento de tierras: Que ocurren como resultado de cambios súbitos o graduales de la composición, estructura, hidrología o vegetación de un terreno en declive o pendiente.
   - Derrumbes: Es la caída de una franja de terreno que pierde su estabilidad o la destrucción de una estructura construida por el hombre.
   - Aludes: Masa de nieve que se desplaza pendiente abajo.

[1] Estrategia Internacional para la Reducción de Desastres, *Terminología sobre reducción del riesgo de desastres*, Ginebra, 2009 [en línea] http://www.unisdr.org/files/7817_UNISDRTerminologySpanish.pdf
[2] Comisión Económica para América Latina y el Caribe (CEPAL ONU), *Manual para la Evaluación de Desastres*, Santiago de Chile, 2014 [en línea] https://repositorio.cepal.org/bitstream/handle/11362/35894/S2013806_es.pdf

- Aluviones: Flujos de grandes volúmenes de lodo, agua, hielo, roces, originados por la ruptura de una laguna o deslizamiento de un nevado.
- Huaicos: Desprendimientos de lodo y rocas debido a precipitaciones pluviales, se presenta como un golpe de agua lodosa que se desliza a gran velocidad por quebradas secas y de poco caudal arrastrando piedras y troncos.

3. **Desastres generados por fenómenos meteorológicos e hidrológicos.**
   - Inundaciones: Invasión lenta o violenta de aguas de río, lagunas o lagos, debido a fuertes precipitaciones fluviales o rupturas de embalses, causando daños considerables. Se pueden presentar en forma lenta o gradual en llanuras y de forma violenta o súbita en regiones montañosas de alta pendiente.
   - Sequías: Deficiencia de humedad en la atmósfera por precipitaciones pluviales irregulares o insuficientes, inadecuado uso de las aguas subterráneas, depósitos de agua o sistemas de irrigación.
   - Heladas: Producidas por las bajas temperaturas, causando daño a las plantas y animales.
   - Tormentas: Fenómenos atmosféricos producidos por descargas eléctricas en la atmósfera.
   - Granizadas: Precipitaciones de agua en forma de gotas sólidas de hielo.
   - Tornados: Vientos huracanados que se producen en forma giratoria a grandes velocidades.
   - Huracanes: Son vientos que sobrepasan los 24 Km/h como consecuencia de la interacción del aire caliente y húmedo que viene del Océano Pacífico con el aire frío.

4. **Desastres de origen biológico.**
   - Plagas: Son calamidades producidas en las cosechas por ciertos animales.
   - Epidemias: Son la generalización de enfermedades infecciosas a un gran número de personas y en un determinado lugar.

DESASTRES TECNOLÓGICOS.

- Incendios.
- Explosiones.
- Derrames de sustancias químicas.
- Contaminación ambiental.
- Guerras.
- Subversión.
- Terrorismo.

En ese sentido, **¿qué es el registro de incidencias?**
Es el registro de las acciones que pudieran poner en riesgo la seguridad del sistema, consistente en la pérdida o destrucción no autorizada, robo, extravío o copia no autorizada, uso, acceso, o tratamiento no autorizado, daño, alteración o modificación de la información no autorizada, en cualquier modalidad de incidencia que pudiera presentarse.

Por lo anterior, en apego a lo que el artículo 31 de la Ley de Datos local establece, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos las siguientes:

- **Pérdida:** es aquella situación en la que se tiene la incapacidad de acceder a los datos desde una copia de seguridad o un sistema informático previamente en funcionamiento; así mismo, la eliminación accidental de archivos o la sobreescritura de datos o documentos.
- **Destrucción:** implica la destrucción no autorizada de la información, o de los medios de almacenamiento para que no se pueda acceder o hacer uso de los datos.

- **Robo:** es el acto de sustraer información en cualquier soporte en que se encuentre, físico o electrónico, sin consentimiento y/o autorización del titular o responsable.
- **Extravío:** cuando por un descuido, se desconoce u olvida dónde se encuentra el soporte que contiene la información, provocando la pérdida de los datos personales.
- **Copia no autorizada:** reproducción no autorizada de la información que contiene datos personales.
- **Uso, acceso o tratamiento no autorizado:** cuando son utilizados para finalidades distintas para las que fueron recabados o cuando se accede a ellos sin mediar autorización del responsable.
- **Daño, alteración o modificación no autorizada:** cuando la información sufre una transformación, perdiendo así su calidad e integridad, sin que medie la autorización del responsable.

De igual manera, **¿qué tiene que hacer el responsable del sistema de datos personales en caso de que ocurran incidencias?**

Deberá analizar las causas por la cuales se presentó la incidencia, con acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales, con el fin de que la vulneración no se repita, e informar al titular de los datos y al órgano garante para tomar las medidas de mitigación correspondientes.

Aunado a ello, el responsable del sistema de datos personales deberá llevar el registro de las vulneraciones a la seguridad del sistema de datos personales, las cuales implican la pérdida o destrucción no autorizada, robo, extravío o copia no autorizada, uso, acceso, o tratamiento no autorizado, daño, alteración o modificación no autorizada de la información.

Asimismo, **¿de qué manera se llevará el registro de las incidencias?**

Las incidencias se deben documentar mediante una bitácora, con el fin de permitir a las personas encargadas de la seguridad del sistema de datos personales dar respuesta a los incidentes, así como de contar con una base de conocimiento, que pueda ser utilizada para entrenar a los usuarios, o a nuevos integrantes del equipo de respuesta a incidentes, esto para la mejora continua.

De conformidad con el artículo 32 de la Ley de Datos local, para el caso de la bitácora, se recomienda considerar al menos los siguientes elementos[3]:

- Tipo de vulneración.
- La fecha y hora de ocurrencia.
- Motivos de la vulneración.
- Las acciones correctivas implementadas de forma inmediata y a largo plazo, derivadas de la incidencia.
- Nombre y cargo de quien reporta la vulneración.

Adicional a todo lo anterior, es pertinente considerar las siguientes interrogantes:

¿Qué obligación tendrá el responsable del sistema de datos personales en caso de una vulneración?

En caso de detectar una vulneración a la seguridad, deberá informar sin dilación alguna al titular y al Instituto en cuanto confirme que ocurrió la vulneración. Asimismo, deberá realizar las acciones necesarias para la revisión exhaustiva de la magnitud de la afectación.

[3] Para mayor referencia, se anexa a la presente, el formato que servirá de forma enunciativa más no limitativa, como guía para elaborar el registro de incidencias (Anexo 1).

¿Qué es lo que el responsable del sistema de datos personales debe de informar al titular de los datos personales?

En cuanto se detecte una vulneración a la seguridad deberá informar, por lo menos, la naturaleza del incidente, los datos personales comprometidos, los derechos del titular que puede adoptar para proteger sus datos, las acciones correctivas que realizó en forma inmediata y los medios en donde puede obtener más información.

¿Qué es lo que el responsable del sistema de datos personales debe de informar al Instituto una vez que ocurrió la vulneración?

Deberá informar, sin dilación alguna, las medidas de mitigación llevadas a cabo, los niveles de seguridad que tiene adoptados y el documento de gestión en donde el Instituto realizará las recomendaciones y medidas pertinentes para la protección de los datos personales.

¿Cuál es el plazo que deberá cumplir el responsable del sistema de datos personales para realizar las notificaciones?

El responsable del sistema de datos personales deberá informar, dentro de un plazo máximo de setenta y dos horas, al titular de los datos personales y al Instituto, en cuanto se confirme que ocurrió la vulneración, así mismo, deberá realizar acciones encaminadas a detonar un proceso de mitigación de la afectación.

El plazo a que se refiere el párrafo anterior comenzará a correr el mismo día natural en que el responsable confirme la vulneración de seguridad.

¿Qué tendrá que hacer el Instituto al momento de ser informado de una incidencia?

Realizará una verificación sobre las medidas adoptadas para mitigar el impacto, emitirá las recomendaciones para que sean solventadas en el término que establezca el Instituto[4].

[4] Para mayor referencia, se anexa a la presente, el formato que servirá de forma enunciativa más no limitativa, como guía para elaborar el acta circunstanciada de hechos ocurridos. (Anexo 2)

5.5. IDENTIFICACIÓN Y AUTENTIFICACIÓN.

Para el desarrollo del presente apartado, nos debemos preguntar:

¿Qué es la identificación y la autenticación?

La **identificación** es respecto a la persona (encargado y/o usuario) autorizada por el responsable para que acceda al sistema de datos personales. Es decir, es la capacidad de identificar de forma exclusiva a la persona autorizada para acceder al sistema.

La **autentificación** implica la capacidad de demostrar o comprobar la identidad de aquella persona autorizada para el tratamiento de datos personales. Es decir, el sistema reconoce que la persona (encargado y/o usuario) que accede o utiliza el sistema de datos personales es realmente quién asegura ser.

En términos simples, la identificación es indicar quién es la persona autorizada y la autentificación es demostrar que la persona es quien dice ser.

En ese aspecto, se deberán considerar los siguientes cuestionamientos:

- **¿Qué personas están autorizadas para acceder a los datos personales del sistema (encargados y/o usuarios)?**
- **¿De qué forma puedo comprobar la identidad de las personas autorizadas (encargados y/o usuarios)?**

Con base en ello, el responsable del sistema de datos personales deberá implementar los mecanismos de identificación y autentificación para el sistema de datos personales, los cuales, de manera enunciativa y no limitativa, podrán consistir en:

- Elaborar una relación actualizada de las personas servidoras públicas que tengan acceso autorizado al sistema de datos personales (se recomienda anexar la relación al documento de seguridad).

- Indicar en el presente documento el procedimiento de notificación o políticas de bajas respecto al personal autorizado para acceder al sistema.

- Establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de toda persona que intente acceder al sistema de datos personales (ejemplo: presentando identificación), el cual debe describirse en el presente apartado.

- Para el caso de los sistemas de datos personales automatizados, deberá implementar procedimientos para el acceso seguro mediante asignación de claves y contraseñas al personal autorizado, debiendo indicar el procedimiento de creación y modificación de claves y contraseñas, señalando longitud, formato y contenido, así como inactivación de cuentas por baja de personal.

Medidas de seguridad implementadas para controlar el acceso de personas

El responsable del sistema de datos personales deberá implementar medidas de seguridad para controlar el acceso de las personas a las instalaciones de la organización y, también, el espacio donde se almacena los soportes físicos o electrónicos del sistema.

A las instalaciones:

a) Identificarlo(a).
b) Autenticarlo(a).
c) Quién autoriza la identificación y la autenticación.
d) Quién autoriza el acceso.

Al interior:

Medidas de seguridad implementadas para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema. (Oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

a) Identificarlo(a).
b) Autenticarlo(a).
c) Quién autoriza la identificación y la autenticación.
d) Quién autoriza el acceso.

5.6. CONTROL DE ACCESO, GESTIÓN DE SOPORTES Y COPIAS DE RESPALDO Y RECUPERACIÓN

Para la construcción e identificación del presente apartado, es conveniente responder a los siguientes cuestionamientos:

¿Qué implica el control de acceso?

El control de acceso implica llevar el registro detallado de accesos al sistema, el cual permita de forma eficaz, aprobar o negar el paso de personas o grupo de personas a zonas restringidas en función de ciertos parámetros de seguridad, es decir, que solo el personal autorizado pueda tener acceso al sistema.

El control de acceso tiene como objetivos:

- Organizar y controlar el sistema respecto al personal autorizado (usuarios y/o encargados) por parte del responsable.
- Prohibir o permitir el acceso a las instalaciones, a los sistemas informáticos, a las bases de datos y otros servicios donde se encuentre la información, con el fin de evitar vulneraciones de seguridad.
- Detectar accesos no autorizados y, en su caso, implementar las medidas de seguridad adoptadas por el sujeto obligado.

En ese sentido, se deben describir las medidas de seguridad implementadas para controlar el acceso del personal autorizado al sistema de datos personales del que se trate, así como la forma en que se llevará el registro de accesos al mismo.

Ahora bien, **¿qué se entiende por gestión de soportes?**
La gestión de soportes implica garantizar la correcta conservación de los documentos, la localización y consulta de la información por el personal autorizado en el documento de seguridad, el cual debe de almacenar datos o documentos u objetos susceptibles de ser tratado en un sistema de información y se puedan grabar y recuperar datos en medios de almacenamiento (pendrive, discos duros externos, CD'S, DVD'S, memorias USB, scanner), inventariar, registrar las salidas y entradas de información aún de los correos electrónicos, el traslado de información, cifrado de datos, generar contraseñas y usuarios.

De igual manera preguntarse **¿qué información contienen los soportes físicos y electrónicos del sistema de datos personales?** Esta pregunta nos conlleva a llevar a cabo las siguientes acciones:

- Inventariar los soportes físicos y electrónicos que contienen información del sistema de datos personales.
- Identificar el tipo de información que contienen los soportes físicos y electrónicos, mediante el uso de etiquetas.
- Restringir o permitir el acceso a los soportes físicos y electrónicos, es decir, solo el personal autorizado (usuario y/o encargado) tendrá acceso a los mismos.
- En caso de proceder alguna acción cuyo objeto sea la disposición documental autorizada, en cualquier medio, por destrucción o baja de la misma, cualquier soporte que contenga datos de carácter personal deberá destruirse o borrarse, adoptando medidas eficaces que eviten completamente la recuperación de los datos contenidos en los dispositivos de almacenamiento, con el fin de evitar el

acceso a la información contenida en el mismo, aplicando técnicas físicas o electrónicas (ejemplo: destruir en trituradora por el personal autorizado, los documentos físicos que contengan datos personales, formatear las computadoras que contengan información con datos personales, etc.).

- Se puede tomar la decisión de considerar medidas adicionales, si a través de la evaluación del riesgo se determina que no hay necesidad inmediata de implementar controles adicionales o que estos controles se pueden implementar posteriormente (ejemplo: el equipo 26 de cómputo actual falla, pero se genera un respaldo de esa información al final del día, por lo que se decide retener ese riesgo durante un mes y esperar para cambiar el equipo de cómputo por uno nuevo).

Ahora bien, una vez identificadas las definiciones y acciones antes mencionadas, **¿qué medidas se deben implementar para llevar a cabo el traslado de los soportes que contienen la información del sistema de datos personales?**

Lo anterior resulta importante ya que nos permitirá establecer e implementar el procedimiento para realizar el traslado de información que contenga y resguarde el sistema de datos personales, por lo cual se debe considerar:

- Establecer el procedimiento para el traslado de información que contenga datos del sistema, debiendo adoptar medidas que eviten la sustracción, pérdida o acceso indebido a la misma, (ejemplo: sobre cerrado con el sello o leyenda de **CONFIDENCIAL** y solo deberá de ser trasladado por personal autorizado).
- Autorizar o negar la salida de las instalaciones u oficinas, de los soportes que contienen la información del sistema de datos personales, su salida sólo será autorizada por la persona responsable del sistema de datos personales.
- Llevar un registro de la salida de las instalaciones u oficinas, de los soportes que contienen la información del sistema de datos personales.

Finalmente, **el responsable del sistema de datos personales ¿tiene contratado, o se adhiere a servicios, aplicaciones e infraestructura de cómputo en la nube?**, y en caso de ser afirmativo se deberá atender a lo siguiente:

- Si tiene contratado o se adhiere a servicios, aplicaciones e infraestructura de cómputo en la nube, y otros servicios que impliquen el tratamiento de datos personales, el proveedor externo estará obligado a garantizar la protección de dichos datos con los principios y deberes establecidos en la Ley de Datos local y demás disposiciones que resulten aplicables en la materia.
- En su caso, deberá delimitar el tratamiento de los datos personales por parte del proveedor externo a través de cláusulas contractuales u otros instrumentos jurídicos, de conformidad con el artículo 57 de la Ley de Datos local.
- Realizar la descripción de perfiles del usuario y contraseñas implementados por el responsable para tener control de acceso mediante una red electrónica:

    a. Por el tipo de control de acceso:

        - Obligatorio.
        - Discrecional.
        - De acuerdo con el rol desempeñado.
        - De acuerdo con el grupo perteneciente.
        - De acuerdo con lo que establece el reglamento interior, o demás normativa interna del sujeto obligado.

    b. Por el perfil del usuario y contraseña para el manejo del sistema operativo podrá ser porque:

        - Cuenta con un sistema operativo de red instalado en su equipo.
        - Sistema operativo maneja rigurosos de perfiles de usuario y contraseñas.

- El sistema operativo solo reconoce los nombres de usuarios y las contraseñas cuando los almacena.

c. Por el perfil de usuario y contraseñas para el manejo del software podrá ser porque:

- El software maneja rigurosos de perfiles de usuario y contraseñas.
- El software solo reconoce los nombres de usuarios y las contraseñas cuando los almacena.

d. La administración de perfiles de usuario y contraseñas podrá ser por:

- Alta de nuevos perfiles.
- La creación de nuevos perfiles.
- Registro de la creación de nuevos perfiles.

e. Acceso remoto al sistema de datos personales podrá ser porque:

- Requieren los usuarios acceso remoto al equipo de cómputo para trabajar con el sistema.
- Requiere el administrador acceso remoto al equipo para realizar tareas de mantenimiento.

Es decir, en este apartado se deben describir las políticas, reglas, mecanismos implementados por el responsable para llevar el control sobre los soportes que detentan la información del sistema.

Ahora bien, para continuar con el desarrollo del presente apartado, se deberá atender a los siguientes cuestionamientos:

- **¿Qué implica hacer respaldos de la información contenida en el sistema de datos personales, y qué acciones se deben llevar a cabo?**
- **¿Qué es la digitalización?**
- **¿Qué se entiende por recuperación de la información?**

Con base en ello, el responsable del sistema de datos personales podrá identificar y deberá implementar las políticas y procedimientos correspondientes para realizar los respaldos y recuperación de la información.

En ese sentido, el **respaldo** implica la copia de archivos físicos y/o electrónicos a un sitio secundario para su preservación en caso de falla del equipo, catástrofe, desastre y que es fundamental para la recuperación de la información.

Para ello, se deberá señalar en este apartado la siguiente información:

- El procedimiento conforme a las políticas existentes, para realizar las copias de respaldo (desglosar el procedimiento correspondiente).

    - Cuando la información se encuentre en un soporte físico se debe proceder a la digitalización de los documentos, para su debido respaldo, l**a digitalización** es el proceso que permite la migración de documentos impresos a mensaje de datos, esto quiere decir que se permitirá migrar del papel al documento electrónico, para que este surta plenos efectos legales y que se le trate como si fuese el original.
    - Cuando se trate de información que consta en un soporte electrónico, su respaldo se realizará en discos, memorias externas, discos duros externos, o cualquier otro medio de almacenamiento.

- El periodo de realización (en qué momento se realizarán los respaldos, dicho periodo lo establecerá el sujeto obligado).

- La verificación por parte del responsable (se recomienda que sea al menos cada 6 meses).

Ahora bien, se entenderá como **recuperación** de la información al conjunto de técnicas y procedimientos utilizados para acceder y extraer la información almacenada en medios de almacenamiento digital que por daño o avería no pueden ser accesibles de manera usual ya sea por falla en el equipo, catástrofe o desastre natural.

En ese sentido, el responsable del sistema de datos personales deberá señalar los procedimientos conforme a la política interna para recuperar los datos contenidos en soportes electrónicos.

Finalmente, en caso de que el sujeto obligado, para el desarrollo u operación de sistemas de tecnología de la información, decida hacer uso de datos reales en sus pruebas, se deberá cuestionar sobre: **¿qué medidas se deben observar para realizar las pruebas con datos reales?**

Al desarrollar y operar sistemas de tecnologías de la información, generalmente se realizan pruebas con datos ficticios o anonimizados, no obstante, dependiendo de las circunstancias, en ocasiones puede ser necesario utilizar datos que contienen información personal real, que es fundamental para lograr el desarrollo o buen funcionamiento de la tecnología de la información de la que se trata.

Ante ello, las pruebas deben ser únicamente por lo que respecta a sistemas informáticos con previa copia de respaldo, debiendo llevar a cabo las siguientes acciones:

- Se debe verificar la correcta aplicación y funcionamiento de los procedimientos para obtener copias de respaldo y de recuperación de los datos.

- Previo a la realización de pruebas con datos reales, se debe elaborar una copia de respaldo.
- Realizar una evaluación correcta del riesgo que implica para los titulares de los datos personales.
- Que los datos utilizados sean los necesarios, es decir, que sean proporcionales a la prueba realizada, y este fundamentado y motivado su uso.
- Asegurar la eliminación necesaria de los datos personales una vez finalizada la prueba.

Por otro lado, las pruebas en nuevos sistemas informáticos diseñados para dar tratamiento al sistema, **no se realizarán con datos reales**, salvo que se asegure y garantice el nivel de seguridad correspondiente al tipo de datos tratados.

5.7. ANÁLISIS DE RIESGO.

Para el desarrollo del presente apartado, se considera pertinente responder a los siguientes cuestionamientos:

¿Qué es un riesgo?

Es la posibilidad de sufrir pérdidas; se relaciona con una ocurrencia que podría causar un resultado negativo, es una combinación de la probabilidad de un evento y su consecuencia desfavorable. De igual manera, son los proyectos e iniciativas de mejoras de la seguridad de información, en la que se debe de considerar las amenazas, vulneraciones y los recursos involucrados en su tratamiento.

¿Qué es la identificación de un riesgo?

Es el proceso para encontrar, enlistar y describir los elementos del riesgo. Comprender los riesgos en términos de la misión del responsable es el primer paso para la gestión de los riesgos.

¿Qué es la gestión de riesgos?

Es el proceso continuo de identificación de riesgos y de implementación de acciones para abordarlos. Cabe aclarar que, no existe la seguridad total; los riesgos y amenazas siempre existen, sin importar la cantidad de recursos que destine el responsable para su atención, por ello se debe realizar una gestión de riesgos acorde a los objetivos y capacidades del responsable.

¿Qué es una amenaza?

Circunstancia o condición externa, con la capacidad de causar daño a los activos (datos personales) explotando una o más de sus vulnerabilidades. Pueden ser de origen natural o humano, accidentales o deliberadas y además provenir de adentro o fuera de la organización.

¿Qué es una vulnerabilidad?

Circunstancia o condición propia de un activo, que puede ser explotada por una o más amenazas para causarle daño.

¿Qué es un análisis de riesgos?

Es el proceso para comprender la naturaleza del riesgo y/o determinar su magnitud aceptable o tolerable. Consiste en averiguar el nivel de riesgo que el responsable o sujeto obligado está soportando. Para ello, tradicionalmente las metodologías proponen que se realice un inventario de activos, se determinen las amenazas, las probabilidades de que ocurran y los posibles impactos.

En ese orden de ideas, también debemos tener en consideración que, en la fracción IV, del artículo 26 de la Ley de Datos local, se dispone que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable del sistema de datos personales deberá realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos

personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.

Asimismo, en el artículo 46 de los Lineamientos Generales se establece que para realizar el análisis de riesgos se deberá considerar lo siguiente:

- Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.
- El valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida.
- El valor y exposición de los activos involucrados en el tratamiento de los datos personales.
- Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.
- Los factores previstos en el artículo 25 de la Ley de Datos local. (Medidas y niveles de seguridad).

Ahora bien, los **factores para determinar las medidas de seguridad** son el conjunto de consideraciones que las organizaciones deben plantear como directrices para tratar el riesgo en función de sus alcances y objetivos.

Por otra parte, la **valoración respecto al riesgo** es el proceso de ponderación para identificar los escenarios de riesgo prioritarios y darles tratamiento proporcional, la cual contempla los siguientes pasos:

1. Identificar el tipo de nivel de seguridad y el valor de los datos personales, de acuerdo con su clasificación:
    - El incumplimiento con las obligaciones legales y contractuales relacionadas con el titular.
    - Vulneraciones de seguridad.
    - Daño a la integridad de los titulares de datos personales.
    - Daño a la reputación del sujeto obligado.

2. Identificar amenazas (el valor y exposición).

3. Identificar vulnerabilidades.

4. Identificar escenarios de vulneración y consecuencias.

- **Criterios de aceptación del riesgo.** El sujeto obligado podría aceptar o no ciertos niveles de riesgo, siempre y cuando la naturaleza del riesgo, sus consecuencias o su probabilidad, sean consideradas como muy poco significativas.

Se debe expresar el beneficio o el riesgo estimado para la organización, aplicando diferentes criterios de aceptación correspondientes al riesgo. Por ejemplo: riesgos que pueden resultar del incumplimiento a la Ley de Datos local que no pueden ser aceptados.

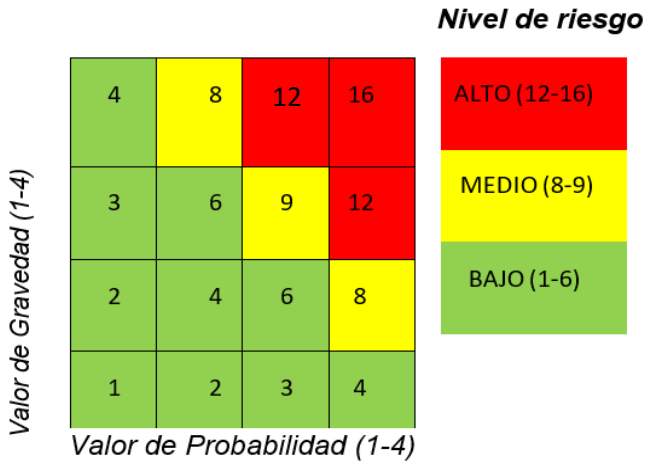
Se deben incluir múltiples umbrales, correspondientes a diferentes niveles de aceptación, previendo que los responsables acepten riesgos sobre esos niveles en circunstancias específicas.

En todo tratamiento de datos personales se debe realizar un análisis de riesgos, esto con la principal finalidad de establecer los controles y medidas de seguridad adecuadas que garanticen las libertades y los derechos de los titulares.

Expuesto lo anterior, a continuación, se presenta un ejemplo de matriz de riesgos que puede ayudar para realizar su análisis, así como un mapa de calor que permite determinar el nivel de riesgo aplicable, el cual se determina a través de valores numéricos:

NIVEL DE RIESGOS[5]				
IDENTIFICACIÓN	**ANÁLISIS**		**EVALUACIÓN**	
RIESGO	**PROBABILIDAD**	**GRAVEDAD**	**CALIFICACIÓN**	**NIVEL DEL RIESGO**
Mencione o describa claramente el o los posibles riesgos.	Establezca el valor de 1 a 4 según la probabilidad de ocurrencia del riesgo o riesgos anteriormente explicados. 1 siendo nada probable y 4 muy probable.	Establezca el valor de 1 a 4 según la gravedad del riesgo o riesgos mencionados anteriormente. 1 siendo nada grave y 4 muy grave.	Multiplique el valor de probabilidad por el valor de la gravedad.	Establezca el mismo de acuerdo con la calificación obtenida (alto, medio o bajo), esto de acuerdo con la tabla de colores verde, amarillo y rojo.

Con base en la tabla anterior, para determinar el nivel de riesgo en el siguiente mapa de calor hay que establecer el valor de la probabilidad y el valor de la gravedad del riesgo al que nos enfrentamos. Por ejemplo, si consideramos que el valor de probabilidad es tres y el valor de gravedad es cuatro, la calificación será de doce. Por lo cual, de acuerdo con el mapa de calor el nivel de riesgo es alto. Otro ejemplo, es si tenemos un valor de probabilidad de tres y un valor de gravedad de tres, la calificación será de nueve. Por lo tanto, el nivel de riesgo de acuerdo con el mapa es medio.



[5] Para mayor referencia, se anexa a la presente, el formato que servirá de guía de manera enunciativa más no limitativa, mismo que podrá utilizarse para llevar a cabo el análisis de riesgo, y el cual deberá de adaptarse a las condiciones de cada Sujeto Obligado (Anexo 3),

En ese sentido, una vez identificado el riesgo y su valor, podremos desarrollar el presente apartado a través de la descripción de los rubros que se presentan a continuación:

-**Origen del riesgo**

-Causa

-Posible consecuencia

-Nivel del riesgo

-Tratamiento o control (eliminación, prevención o reducción)

Ejemplo:

Origen del riesgo	Causa	Posibles consecuencias	Nivel de riesgo	Tratamiento o control
Incendio	Debido a que en las instalaciones del S.O. no existen restricciones en cuanto a las personas fumadoras	Destrucción, perdida de archivos físicos y digitales que se encuentran resguardados	Medio	Crear una política sobre no fumadores

5.8. ANÁLISIS DE BRECHA.

Para el desarrollo de este apartado, es importante preguntarnos: **¿qué es el análisis de brecha?**

El análisis de brecha[6] es el proceso de evaluación de las medidas de seguridad que ya existen en la organización contra las que sería conveniente tener, que resultan necesarias para la protección de datos personales. Asimismo, es el estudio comparativo de las medidas de seguridad existentes contra las medidas de seguridad faltantes; es decir donde estamos ahora y donde queremos estar (estado actual y el objetivo a alcanzar o que tenemos ahora y que nos hace falta).

[6] Para mayor referencia, se anexa a la presente, el formato que servirá de guía de manera enunciativa más no limitativa, mismo que podrá utilizarse para llevar a cabo el análisis de brecha, y el cual deberá de adaptarse a las condiciones de cada Sujeto Obligado (Anexo 4).

En ese orden de ideas, también debemos tener en consideración que, en la fracción V, del artículo 26 de la Ley de Datos local se dispone que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable del sistema de datos personales deberá realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.

Asimismo, en el artículo 47 de los Lineamientos Generales, se establece que, para realizar el análisis de brecha, se deberá considerar lo siguiente:

- Las medidas de seguridad existentes y efectivas.
- Las medidas de seguridad faltantes.
- La existencia de nuevas medidas de seguridad que pudieren remplazar a uno o más controles implementados actualmente.

Los controles de seguridad, sin que sean limitativos, deben considerar lo siguiente:

- Políticas del sistema de gestión del sistema de datos personales.
- Cumplimiento legal.
- Estructura organizacional de la seguridad.
- Clasificación y acceso de los activos.
- Seguridad del personal.
- Seguridad física y ambiental (áreas seguras y protección de equipamiento).
- Gestión de comunicaciones y operaciones.
- Control de acceso.
- Desarrollo y mantenimiento de sistemas.
- Vulneraciones de seguridad.
- Seguridad institucional (control de las transferencias de datos).
- Activos responsables (asignación de responsable y clasificación).
- Seguridad de sistemas de información (procesos de información, protección de archivos del sistema).

- Incidentes de seguridad en la información (regularidad con la que se dan).

En relación con el presente apartado, se propone la elaboración mediante la descripción de los siguientes rubros, mismos que se desarrollan en torno al análisis de riesgos y el apartado de tratamiento o control:

-**Categoría**
-Estado actual
-Estado objetivo
-Acción correctiva
-Prioridad (de acuerdo con el nivel de riesgo)

Ejemplo:

Categoría	Estado Actual	Estado Objetivo	Acción Correctiva	Prioridad
Prevención de pérdida de datos	Inexistentes procedimientos para realizar respaldos periódicos de la información en formatos digitales	Contar con la infraestructura que permita crear resguardos periódicos de la información en formato digital	Realizar mesas de trabajo con el área tecnológica e identificar los requerimientos mínimos para poder llevar a cabo los respaldos necesarios.	Alta

5.9. RESPONSABLE DE SEGURIDAD.

En este apartado del documento de seguridad, debemos tener claridad de: **¿quién es el responsable de seguridad?**

La normativa en la materia lo define como la persona designada formalmente por el responsable del sistema de datos personales para coordinar y controlar las medidas de seguridad del sistema:

I. Desde el nivel básico.
II. Técnico.
III. Organizativo.

IV. Vigilar los centros de tratamiento de datos locales.
V. Equipos.
VI. Sistemas.
VII. Programas.
VIII. Personas que intervienen.

Ahora bien, **¿cómo se debe realizar la designación del responsable de seguridad?** Se debe realizar la formalización mediante un oficio, signado por el responsable del sistema de datos personales, a través del cual se designará a la persona que será responsable de seguridad, en dicho documento se deberá hacer de conocimiento las funciones y obligaciones que tendrá.

Se sugiere que el acuse de entrega de dicho oficio se incluya como anexo a cada documento de seguridad[7].

En ese sentido, para el desarrollo del presente apartado de debe indicar la siguiente información del responsable de seguridad:

- Nombre
- Cargo
- Unidad administrativa
- Domicilio oficial
- Correo electrónico oficial
- Teléfono oficial

Ejemplo.

- Funciones:

[7] Un responsable de seguridad puede ser designado para todos los sistemas de datos personales que detente el responsable del sistema de acuerdo con la estructura, operatividad y naturaleza de los mismos.

I. Coordinar y controlar las medidas definidas en el documento de seguridad.
II. Controlar los mecanismos que permiten accesos autorizados al sistema.
III. Etc.

- Obligaciones:
  I. Supervisar la puesta en marcha de las medidas de seguridad establecidas en el presente documento de seguridad.
  II. Revisar la información acerca del control de accesos al sistema
  III. Etc.

En relación con lo anterior, se plantean algunas de las funciones y obligaciones que dicha figura puede tener, en el entendido de que las acciones aquí plasmadas son enunciativas más no limitativas:

- Apoyar en la creación de políticas internas para la gestión y tratamiento de los datos personales, el ciclo de vida de los datos personales (obtención, uso y supresión).
- Coadyuvar para la definición de las funciones y obligaciones del personal involucrado.
- Apoyar en la elaborar del inventario de datos personales.
- Apoyar para la elaboración del análisis de riesgo considerando las amenazas y vulnerabilidades existentes.
- Realizar un análisis para solicitar los recursos involucrados en su tratamiento para la compra de hardware, software, contratación de personal del responsable.
- Apoyar en la elaboración del análisis de brecha.
- Apoyar en la elaboración del plan de trabajo considerando los análisis realizados.
- Apoyar en la definición e implementación de las medidas de seguridad faltantes, las políticas de gestión y tratamiento.

- Monitorear y revisar de manera periódica las medidas de seguridad implementadas, las amenazas y vulneraciones.
- Apoyar en el diseño y aplicación de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades.

5.10. REGISTRO DE ACCESO Y TELECOMUNICACIONES

Para el desarrollo del presente apartado, debemos realizarnos los siguientes cuestionamientos:

¿Quiénes tienen acceso al sistema de datos personales o a sus soportes (físicos o electrónicos)?
Se debe tomar en cuenta el listado del personal con acceso autorizado, el cual deberá estar identificado por figura (responsable de seguridad, usuario(s) y/o encargado(s)), e indicar aquellos datos y recursos a los cuales tendrán acceso para llevar a cabo el desarrollo de sus funciones.

Es de precisar que, solamente el responsable del sistema de datos personales podrá conceder, alterar o anular la autorización para el acceso y tratamiento a los datos personales del sistema.

¿Qué es el registro de acceso?
Es la constancia de ingresos al sistema mediante la identificación, autenticación y autorización, es decir, constancia de acceso no autorizado, constancia de seguridad en la conexión, constancia de eventos y actividades llevadas a cabo por los usuarios; en términos simples, implica llevar la constancia de quien tiene acceso o ingresa al sistema y soportes electrónicos en caso de que aplique.

En ese sentido, **¿cómo se debe llevar a cabo el registro de acceso?**
El registro de acceso se llevará a cabo mediante la implementación de bitácoras de acceso, por lo cual, en el presente apartado se debe establecer el procedimiento para el

uso de las bitácoras, considerando las acciones cotidianas llevadas a cabo en el sistema de datos personales.

Por lo anterior, dichas bitácoras deberán contener, por lo menos, la siguiente información:

- Nombre y cargo de quien accede al sistema.
- Identificación del sistema.
- Identificación del expediente (en su caso).
- Propósito del acceso.
- Fecha de acceso.
- Hora de consulta.
- Fecha de término de la consulta.
- Hora de término de la consulta.

Ejemplo:

Registro de acceso al Sistema de Datos….						
No.	***Nombre***	***Cargo***	***No. de expediente***	***Motivo de la consulta***	***Fecha y hora de la consulta***	***Fecha y hora término de la consulta***
1						
2						
3						

De manera adicional es pertinente plantearse las siguientes interrogantes:

¿Qué son las telecomunicaciones?

De conformidad con la Ley Federal de Telecomunicaciones en su artículo 3, fracción LXVIII, establece que se entenderá por telecomunicaciones a toda emisión, transmisión o recepción de signos, señales, datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos u otros sistemas electromagnéticos, sin incluir la radiodifusión.

¿Qué es el registro de telecomunicaciones?

Es la constancia de envío, recepción o almacenamiento de los datos personales del sistema a través de dispositivos de telecomunicación (fibra óptica, satélites de comunicaciones, conmutadores privados, redes de área local, módems, teléfonos móviles, teléfono fijo, máquinas de fax, buscapersonas, routers, entre otros).

¿Qué información del sistema puede ser transferida a través de los dispositivos de telecomunicación?

Para determinar qué información del sistema puede ser transferida a través de los dispositivos de telecomunicaciones, se debe tomar en cuenta:

- La manera en que se hará la transferencia de los datos, sin que puedan ser alterados o manipulados.
- El daño que puede ocasionar dicha transferencia.
- La información que va a transferirse, la cual puede implicar:
    - Sistemas.
    - Bases de datos.
    - Imágenes.
    - Videos.
    - Archivos.
    - Etc.

5.11. Mecanismo de monitoreo y revisión de medidas de seguridad.

Para el desarrollo del presente apartado nos debemos hacer las siguientes preguntas:

¿En qué consiste el mecanismo de monitoreo?

Control del desarrollo cuando se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo y como resultado de un proceso de mejora continua.

¿En qué consiste la revisión de las medidas de seguridad?

Implementación de acciones correctivas y preventivas periódicas ante una vulneración a la seguridad.

Ahora bien, de conformidad con lo establecido en el artículo 49 de los Lineamientos Generales, en relación con el artículo 26, fracción VII, de la Ley de Datos local, el responsable del sistema de datos personales deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.

Derivado de lo anterior, deberá monitorear continuamente lo siguiente:

- Los nuevos activos que se incluyan en la gestión de riesgos.
- Las modificaciones necesarias a los datos, como podría ser el cambio o migración tecnológica, entre otras.
- Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas.
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.
- Las vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.
- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en el nivel inaceptable de riesgo.
- Los incidentes y vulneraciones de seguridad ocurridas.

Aunado a lo previsto en las fracciones anteriores, el responsable del sistema de datos personales deberá contar con un programa para monitorear y revisar la eficacia del sistema de gestión.

A continuación, se presentan algunas acciones para revisar y mantener actualizadas las medidas de seguridad:

a) Desarrollo de política se seguridad.
b) Cumplimiento de la normatividad.
c) Organización de la seguridad en la información.
d) Clasificación e identificación de inventarios.
e) Administración de incidentes.
f) Continuidad en las operaciones.
g) Gestión de comunicaciones y operaciones.
h) Adquisición, desarrollo, uso y mantenimiento del sistema de información.
i) Soportes físicos.
j) Soportes electrónicos.

5.11. Plan de trabajo.

Ahora bien, **¿qué se entiende por plan de trabajo?**

El plan de trabajo es la herramienta con la que se organiza y simplifica las actividades necesarias para la implementación de medidas de seguridad faltantes para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.

En ese sentido, de conformidad con lo establecido en el artículo 48 de los Lineamientos Generales, en relación con el artículo 26, fracción VI, de la Ley de Datos local, el responsable del sistema de datos personales deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.

Lo anterior, considerando los recursos designados, el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nueva o faltante.

El plan de trabajo se elaborará de conformidad con el resultado del análisis de brecha, cuyos resultados faltantes pueden ser:

1. Fuga de información (prevención).
2. Disociación (cuando los datos pasen de un ambiente de riesgo menor a un ambiente de riesgo mayor).
3. Bloquear y dar de baja puertos y servicios innecesarios en los equipos de cómputo.
4. Ampliación de medidas de seguridad en caso de detectar faltantes.
5. Equipos de cómputo obsoletos.

5.13. Plan de capacitación.

El plan de capacitación está relacionado con el plan de trabajo. Para poder definir este apartado, hay que responder la siguiente pregunta:

¿En qué consiste programa general de capacitación?

Consiste en diseñar y aplicar diferentes niveles de capacitación del personal involucrado, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

En ese sentido, de conformidad con lo establecido en el artículo 50 de los Lineamientos Generales, en relación con el artículo 26, fracción VIII, de la Ley de Datos local, el responsable del sistema de datos personales deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos de su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.

Para los programas de capacitación, el responsable del sistema de datos personales deberá tomar en cuenta lo siguiente:

I. Los requerimientos y actualizaciones del sistema de gestión.
II. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de estos.
III. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales.
IV. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

Calendario programático para llevar a cabo:

A. Capacitaciones integrales del personal que opera el sistema.
B. Actualizaciones.
C. Fechas y duración de la capacitación.
D. Aéreas a capacitar.
E. Temas.
F. Mejoras implementadas.
G. Desaciertos y aciertos.
H. Oportunidades de mejora.

Retroalimentación.

6. ANEXOS

ANEXO 1. FORMATO DE REGISTRO DE INCIDENCIAS.

REGISTRO DE INCIDENCIAS DEL SISTEMA (NOMBRE DEL SISTEMA DE DATOS PERSONALES).

Versión del anexo			
Elaborado por:	Fecha elaboración	Aprobado por:	Fecha de aprobación:
I. Tipo de incidencia: (Precisar si se trata de pérdida, destrucción, robo, extravío, copia, uso, acceso o tratamiento, daño, alteración o modificación no autorizada)			
II. Motivo (posible o identificado) de la incidencia: (el motivo se relaciona con identificar las acciones u omisiones de cualquier persona que pudieran haber provocado la vulneración y sea posible distinguirlas en ese momento.)			
III. Tipo de soporte (X): Físico ☐ Automatizado ☐ Mixto ☐			
IV. Momento en que se produjo: Fecha__/__/__ Hora __:__			

V. Valoración de la serie documental vinculada al sistema de datos personales afectado (X):

a) Valor primario: Legal ☐ Fiscal ☐ Contable ☐ Administrativo ☐

b) Valor secundario: Informativo ☐ Testimonial ☐ Evidencial ☐

c) Tiempo de conservación de los datos personales contenidos en el sistema:

Etapa de ciclo vital	SÍ(X)	Tiempo de conservación
En medio automatizado		
En archivo de trámite		
En archivo de concentración		
En archivo histórico		

Número de hoja: 1

VI. Tipos de datos personales afectados:

Categoría de datos personales	Si (X)	Especificar el(los) tipo(s) de dato(s) personal(es)
Datos identificativos		
Datos electrónicos		
Datos laborales		
Datos patrimoniales		
Datos sobre procedimientos administrativos y/o jurisdiccionales		
Datos académicos		
Datos de tránsito y movimientos migratorios		
Datos sobre la salud		
Datos biométricos		
Datos especialmente protegidos (sensibles)		
Datos personales de naturaleza pública		
Otro		

Número aproximado de titulares afectados:

VII. Lugar en que se produjo:

VIII. Nombre y cargo de quien notifica la incidencia: (Indicar el nombre y cargo de la persona que tuvo conocimiento por primera vez)

IX. Nombre y cargo de quien recibe la notificación: (Indicar nombre y cargo de la persona responsable de seguridad del sistema de datos personales)

X. Descripción de los hechos: (La descripción detallada de las circunstancias en torno a la vulneración ocurrida).

Número de hoja: 2

XI. Efectos que derivan de la incidencia:
XII.Acciones correctivas implementadas de forma inmediata y definitivas, que derivan de la incidencia:
XIII. Nombre y cargo de quien autorizó la recuperación de datos:
XIV. Comentarios adicionales:
XV. Firma de las personas que intervinieron: _____ **Nombre y firma** Responsable del sistema de datos personales _____ **Nombre y firma** Responsable de seguridad ____(en caso que aplique)____ **Nombre y firma** Encargado _____ **Nombre y firma** Persona que notifica la incidencia Número de hoja: 3

ANEXO 2. FORMATO DE ACTA CIRCUNSTANCIADA DE INCIDENCIAS.

ACTA CIRCUNSTANCIADA DE INCIDENCIAS DEL SISTEMA DE DATOS PERSONALES (citar el nombre del sistema de datos personales).

En la Ciudad de México, siendo las _(1)_ horas, del _(2)_ de _(3)_ de _(4)_ se reunieron en las oficinas del **(indicar el nombre del sujeto obligado)** ubicadas **(indicar el domicilio del sujeto obligado)**, estando presentes: **quien notificó la incidencia de seguridad**, el(la) C. (5) que se identifica con (6) con domicilio en (7), el (la) C. (8) asignado (a) como responsable de seguridad que se identifica con (9) con domicilio en (10), el (la) C. (11) designado (a) como responsable del sistema de datos personales que se identifica con (12) con domicilio en (13), y el(la) C. (14) en su carácter de enlace en materia de protección de datos personales ante el INFO CDMX, que se identifica con (15) con domicilio en (16).

_____HECHOS_____

I. Tipo de incidencia

_____(17)_____

II. Tipo de soporte

_____(18)_____

III. Momento en que se produjo la incidencia

_____(19)_____

IV. Lugar en que se produjo la incidencia

_____(20)_____

V. Nombre de quien notifica la incidencia

_____(21)_____

VI. Nombre y cargo de quien recibe la notificación de la incidencia

_____(22)_____

VII. Descripción de los hechos

_____(23)_____

VI. Efectos que derivan de la incidencia

_____(24)_____

VII.Acciones implementadas que derivan de la incidencia

_____(25)_____

X. Otros hechos

_____
_____(26)_____

La/El C. (27), responsable del sistema de datos personales manifiesta haber proporcionado todos los elementos necesarios para la formulación de esta acta circunstanciada, y que no fue omitido asunto alguno, información, documentación, o cualquier aspecto importante relativo a su gestión.

Los anexos que se mencionan en esta acta, constantes de (28) fojas útiles, forman parte integrante de la misma y se firman en todas sus hojas para su identificación y los efectos legales a que haya lugar.

La presencia del enlace en materia de protección de datos personales sólo tiene como finalidad verificar que la celebración del acta se realice conforme a la normatividad aplicable; por consiguiente, no avala su contenido, ni el de sus anexos, lo que queda bajo responsabilidad del personal involucrado en la incidencia, conforme a la normatividad aplicable en la materia.

La presente acta, no implica liberación alguna de responsabilidades que pudieran determinarse por la autoridad competente con posterioridad.

El/La C. (29) detenta todos los recursos y documentos que se precisan en el contenido de la presente acta y sus anexos ----------Cierre de acta----------Previa lectura de la presente y no habiendo más que hacer constar, se da por concluida a las (30) horas del (31) , firmando para constancia en todas sus hojas los que en ella intervinieron.---------

_____	_____
Nombre y Firma	**Nombre y Firma**
Persona que notifica la incidencia	Responsable de seguridad
_____	_____
Nombre y Firma	**Nombre y Firma**
Responsable del sistema de datos personales	Enlace en materia de datos personales

ANEXO 3. CUESTIONARIO DE AYUDA PARA EL ANÁLISIS DE RIESGO.

Análisis de Riesgo Amenazas, vulnerabilidades y recursos involucrados				
Código	**Pregunta o Control**	**¿Existe? SI**	**¿Existe? NO**	**Observaciones (acciones a realizar en caso de no contar con:**
1	*¿Tienes identificado los tipos de datos personales que recabas?*			
2	*¿Tienes clasificados por categorías los datos personales que recabas?*			
3	*¿Tienes establecido e identificado el ciclo de vida de los datos personales?*			
4	*¿Tienes definido el tratamiento que se le da a cada uno de los datos personales?*			
5	*¿Tienes identificado el procedimiento sobre qué hacer en caso de que los datos personales sean vulnerados?*			
6	*¿Tienes claridad sobre las consecuencias negativas para los titulares de los datos personales en caso de una vulneración?*			
7	*¿Tienes un plan reactivo en caso de sufrir una vulneración a la seguridad de los datos personales?*			
8	*¿Tienes una bitácora de las amenazas a los datos personales que pudieras presentar?*			

Análisis de Riesgo Amenazas, vulnerabilidades y recursos involucrados				
Código	**Pregunta o Control**	**¿Existe? SI**	**¿Existe? NO**	**Observaciones (acciones a realizar en caso de no contar con:**
9	*¿Tienes una bitácora sobre vulneraciones sufridas en los datos personales?*			
10	*¿Cuentas con un procedimiento regulatorio en caso de vulneración a los datos personales?*			
11	*¿Tienes una política a seguir en caso de daño al sistema de datos personales por una vulneración de los datos personales?*			
12	*¿Tienes delimitadas las funciones, obligaciones y códigos de conducta del personal que trata datos personales?*			
13	*¿Tienes claro el beneficio para el atacante al obtener los datos personales?*			
14	*¿Tienes un registro de todas y cada una de las consecuencias que surgieron a raíz de la vulneración del sistema de datos personales?*			
15	*En caso de que aplique, ¿tienes un software para descubrir la anonimidad del atacante que vulnera los datos personales?*			
16	*¿Tienes respaldos en el caso de sufras alguna vulneración a la seguridad de los datos personales?*			

Análisis de Riesgo Amenazas, vulnerabilidades y recursos involucrados				
Código	**Pregunta o Control**	**¿Existe? SI**	**¿Existe? NO**	**Observaciones (acciones a realizar en caso de no contar con:**
17	*¿Tienes hardware y software para respaldar los datos personales?*			
18	*¿Tienes personal capacitado para llevar a cabo los respaldos hardware y software que contendrán los datos personales?*			
19	*¿Tienes calendario, con fechas para dar servicio y mantenimiento a los sistemas, computadoras, discos duros, hardware y software en los que se almacenan datos personales?*			
20	*¿Tienes asesoría externa para dar servicio y mantenimiento a los sistemas, computadoras, discos duros, hardware y software en los que se almacenan datos personales?*			

ANEXO 4. CUESTIONARIO DE AYUDA PARA EL ANÁLISIS DE BRECHA.

Análisis de brecha **Medidas de seguridad existentes y medidas de seguridad faltantes**				
Código	**Pregunta o Control**	**¿Existe? SI**	**¿Existe? NO**	**Observaciones**
1	*¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?*			
2	*¿Cuentas con una política de escritorio limpio?*			
3	*¿Cuentas con hábitos de cierre y resguardo?*			
4	*¿Cuentas con impresoras, escáneres, copiadoras y buzones limpios?*			
5	*¿Cuentas con bitácoras para la gestión de los usuarios y accesos?*			
6	*¿Tienes mecanismos para eliminar de manera segura la información?*			
7	*¿Realizas la destrucción segura de documentos?*			
8	*¿Realizas la eliminación segura de información en equipo de cómputo y medios de almacenamiento electrónico?*			
9	*¿Cuentas con periodos de retención y destrucción de información?*			
10	*¿Has establecido y documentado los compromisos respecto a la protección de datos?*			

Análisis de brecha **Medidas de seguridad existentes y medidas de seguridad faltantes**				
Código	**Pregunta o Control**	**¿Existe? SI**	**¿Existe? NO**	**Observaciones**
11	*¿Informan al personal sobre sus funciones y obligaciones de seguridad en materia de protección de datos personales?*			
12	*¿Aseguran la protección de datos personales en subcontrataciones?*			
13	*¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?*			
14	*¿Tienes claro el procedimiento de notificación derivado de una vulneración?*			
15	*¿Contemplas la realización de monitoreos a los datos y a las medidas de seguridad?*			
16	*¿Realizas respaldos periódicos de los datos personales?*			
17	*¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?*			
18	*¿Cuentas con registros del personal con acceso autorizado?*			
19	*¿Tienes medidas de seguridad para evitar el robo?*			
20	*¿Cuidas el movimiento de información al interior de tu área?*			
21	*¿Cuentas con un procedimiento de aprobación de salida de documentos, equipo de*			

Análisis de brecha Medidas de seguridad existentes y medidas de seguridad faltantes				
Código	**Pregunta o Control**	**¿Existe? SI**	**¿Existe? NO**	**Observaciones**
	cómputo y/o medios de almacenamiento electrónico?			
22	*¿Realizas actualizaciones al equipo de cómputo?*			
23	*¿Revisas periódicamente el software instalado en el equipo de cómputo?*			
24	*¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?*			
25	Uso de contraseñas y/o cifrado			
26	Uso de contraseñas solidas			
27	Bloqueo y cierre de sesiones			
28	Administrar usuarios y accesos			
29	*¿Revisas la configuración de seguridad del equipo de cómputo?*			
30	*¿Tienes medidas de seguridad para navegar en entornos digitales?*			
31	Instalar herramientas antimalware y de filtrado de tráfico			
32	Reglas de navegación segura			
33	Reglas para la divulgación de información			
34	Uso de conexiones seguras			
35	*¿Cuidas el movimiento de información en entornos de trabajo digitales?*			

Análisis de brecha **Medidas de seguridad existentes y medidas de seguridad faltantes**				
Código	**Pregunta o Control**	**¿Existe? SI**	**¿Existe? NO**	**Observaciones**
36	Validación del destinatario de una comunicación			
37	Seguridad de la información enviada y recibida			

ANEXO 5. FORMATO DE LA ESTRUCTURA DEL DOCUMENTO DE SEGURIDAD.

<table>
<tr><td rowspan="4">Logo del sujeto obligado</td><td colspan="2">DOCUMENTO DE SEGURIDAD</td></tr>
<tr><td colspan="2">Nombre del sistema de datos personales</td></tr>
<tr><td>Fecha de elaboración</td><td>Fecha de la última actualización</td></tr>
<tr><td>Elaboró el documento</td><td>Aprobó</td></tr>
<tr><td>(Nombre y firma)</td><td>(Nombre y firma)</td></tr>
</table>

I. DATOS GENERALES DEL SISTEMA

Nombre del sistema: [Indicar el nombre del sistema de datos personales].

Fecha de publicación en la GOCDMX del acuerdo de creación: [Indicar la fecha de publicación en la GOCDMX del acuerdo de creación del sistema de datos personales y adjuntarlo como anexo al final (en caso de que aplique)].

Fecha de inscripción en el RESDP: [Indicar la fecha de inscripción del sistema de datos personales en el RESDP].

Folio de inscripción en el RESDP: [Indicar el número de folio señalado en el acuse de Registro del sistema de datos personales y adjuntarlo como anexo al final].

Fecha de publicación en GOCDMX del Acuerdo de Modificación: [Indicar la fecha de publicación en la GOCDMX del acuerdo de modificación del sistema de datos personales y adjuntarlo como anexo (en caso de que aplique)].

Fecha de última modificación en el RESDP: [Indicar la fecha de modificación del sistema de datos personales en el RESDP y adjuntarlos como anexos].

Normatividad aplicable para el tratamiento
[Indicar la normativa aplicable al sistema de datos personales, de acuerdo con la publicación en la GOCDMX y el RESDP, enlistándola con artículos y fracciones].

Logo del sujeto obligado	**DOCUMENTO DE SEGURIDAD**	
	Nombre del sistema de datos personales	
	Fecha de elaboración	Fecha de la última actualización
	Elaboró el documento	Aprobó
	(Nombre y firma)	(Nombre y firma)

II. INVENTARIO DE DATOS PERSONALES

Obtención

Las personas sobre las que se pretenden obtener datos de carácter personal son… **(indicar el grupo de personas objetivo).**

La recolección de los datos personales que contiene es de carácter **(enlistar los medios y agregar como anexo, así mismo, indicar los medios por los cuales se recaba la información, ya sean físicos, electrónicos o mixtos).**

Modo de tratamiento: El procesamiento de los datos personales se llevará a cabo a través de procedimientos **(indicar físicos, electrónicos o mixtos).**

Medio de actualización: la actualización de los datos personales se llevará a cabo **(indicar si es a petición del interesado, revisión periódica o mediante oficio).**

Finalidades del tratamiento

Finalidad y uso previsto: las finalidades de cada tratamiento de datos Personales **(indicar la finalidad o finalidades y usos previstos del sistema de datos personales, como en la GOCDMX y/o el RESDP).**

Remisiones (responsable – encargados)

[Enlistar a la(s) persona(s) física(s) o jurídica(s), pública(s) o privada(s) ajena(s) al responsable y que tratan datos personales, a nombre y por cuenta del responsable, y anexar copia del contrato, según sea el caso].

Logo del sujeto obligado	**DOCUMENTO DE SEGURIDAD**	
	Nombre del sistema de datos personales	
	Fecha de elaboración	Fecha de la última actualización
	Elaboró el documento	Aprobó
	(Nombre y firma)	(Nombre y firma)

Transferencias

[Enlistar los terceros receptores, a los que una normativa faculta la transferencia de datos personales, así como las finalidades que la justifican. Cuando las transferencias se realicen entre sujetos obligados se encuentre de manera expresa en una ley o tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos]**.**

[En su caso indicar aquellas transferencias que se formalizaron mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad aplicable al responsable].

Interrelación

(Señalar si el sistema de datos personales se interrelaciona con otro sistema de datos personales del mismo sujeto obligado, indicando nombre y finalidad de la interrelación).

El catálogo de los tipos de datos personales

[Enlistar y agrupar los tipos de datos personales que recaban en el sistema de datos personales, en cada una de las categorías, indicando si tratan datos sensibles].

Los datos personales del sistema **(en físico, automatizado o mixto)** se encuentran contenidos **(señalar donde se encuentran contenidos, series documentales. Anexar Catálogo de Disposición Documental del sujeto obligado).**

Ciclo de vida de los datos
[Describir el tiempo de conservación de los datos personales con lo que señala el Catálogo de Disposición Documental del sujeto obligado).

- En medio automatizado:
- En archivo de trámite:
- En archivo de concentración:

- [En caso de que aplique se debe señalar si se contempla la transferencia de información al archivo histórico].

<table>
<tr><td rowspan="4">Logo del sujeto obligado</td><td colspan="2">DOCUMENTO DE SEGURIDAD</td></tr>
<tr><td colspan="2">Nombre del sistema de datos personales</td></tr>
<tr><td>Fecha de elaboración</td><td>Fecha de la última actualización</td></tr>
<tr><td>Elaboró el documento</td><td>Aprobó</td></tr>
<tr><td></td><td>(Nombre y firma)</td><td>(Nombre y firma)</td></tr>
</table>

Nivel de seguridad: [Indicar el nivel de seguridad aplicable de acuerdo con el tipo de datos recabados, este puede ser básico, medio o alto].

Medidas de seguridad: [Indicar las medidas de seguridad adoptadas, aplicables conforme a lo establecido en la Ley de Datos local, estas pueden ser administrativas, físicas y/o técnicas].

Catálogo de las formas de almacenamiento:

Los expedientes del sistema de datos personales denominado **[Indicar el nombre del sistema],** se encuentran resguardados en el inmueble localizado en **[Indicar el domicilio de ubicación].**

[De igual forma se sugiere indicar la descripción general de la ubicación física y/o electrónica de los datos personales. Se puede hacer uso de mapas, planos etc., para señalar la ubicación específica donde se resguarda el sistema de datos personales en sus diferentes destinos, es decir, archivo de trámite, archivo de concentración, histórico y resguardo automatizado].

Lista de las personas servidoras públicas que tienen acceso al sistema de datos personales. [Indicar el nombre y cargo del responsable del sistema de datos personales y de los usuarios involucrados en el tratamiento].

Solo los siguientes servidores públicos, podrán acceder a los datos personales del sistema, en cumplimiento al desarrollo de las funciones y atribuciones que les han sido conferidas.

1. **Nombre**
   Cargo
2. **Nombre**
   Cargo

[Se sugiere agregar el organigrama correspondiente].

<table>
<tr><td rowspan="5">Logo del sujeto obligado</td><td colspan="2">DOCUMENTO DE SEGURIDAD</td></tr>
<tr><td colspan="2">Nombre del sistema de datos personales</td></tr>
<tr><td>Fecha de elaboración</td><td>Fecha de la última actualización</td></tr>
<tr><td>Elaboró el documento</td><td>Aprobó</td></tr>
<tr><td>(Nombre y firma)</td><td>(Nombre y firma)</td></tr>
</table>

III. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE INTERVENGAN EN EL TRATAMIENTO DEL SISTEMA DE DATOS PERSONALES

Funciones y obligaciones del responsable del sistema de datos personales:

[Enlistar el nombre, cargo, domicilio oficial, correo oficial, teléfono oficial, así mismo se deberán indicar las funciones y obligaciones que tiene el responsable del sistema en materia de protección de datos personales].

Funciones y obligaciones del (los) usuario (s) del sistema de datos personales:

[Enlistar en un anexo el nombre y cargo de todos los usuarios, junto con los acuses de notificación a estos como parte del sistema, de igual forma se deberá indicar de acuerdo con las atribuciones del sujeto obligado las funciones y obligaciones que le competen a los usuario del sistema, en materia de protección de datos personales, considerando las facultades que cada uno tiene].

Funciones y obligaciones del encargado del sistema de datos personales:

[Enlistar los datos de identificación del encargado como: denominación nombre, domicilio oficial, correo oficial, teléfono oficial; así mismo, indicar las funciones y obligaciones que de acuerdo a las atribuciones del sujeto obligado, le competen, estas deben coincidir con lo establecido en el los artículos 55 y 56 de la Ley de Datos local, así como, en el documento jurídico por el que se haya formalizado la relación con el responsable].

Establecer las obligaciones generales no incluidas en las categorías señaladas al principio de este apartado.

[Establecer las políticas generales de seguridad que aplican a todo el personal o a persona ajena a la unidad administrativa responsable del sistema de datos personales].

Logo del sujeto obligado	**DOCUMENTO DE SEGURIDAD**	
	Nombre del sistema de datos personales	
	Fecha de elaboración	Fecha de la última actualización
	Elaboró el documento	Aprobó
	(Nombre y firma)	(Nombre y firma)

IV. REGISTRO DE INCIDENCIAS

[Indicar el procedimiento o aspectos a considerar en caso de que ocurra una vulneración/incidencia; se sugiere incluir como anexos los formatos, reporte de incidencia y acta de hechos, los cuales podrá encontrar como anexos en la presente guía].

V. IDENTIFICACIÓN Y AUTENTIFICACIÓN

[Indicar el procedimiento o aspectos a considerar respecto de:
- Mecanismos de identificación y autentificación
- Medidas de seguridad implementadas para controlar el acceso de personas (en este caso puede ser para el acceso a las instalaciones o al interior del sujeto obligado)].

VI. CONTROL DE ACCESO, GESTIÓN DE SOPORTES Y COPIAS DE RESPALDO Y RECUPERACIÓN.

[Indicar el procedimiento o aspectos a considerar respecto a:

- Control de acceso
- Gestión de soportes
- Respaldo y recuperación

Para este apartado se pueden apoyar de su área tecnológica]

VII. ANÁLISIS DE RIESGOS

[Identificar Amenazas: El valor y exposición; identificar vulnerabilidades; e identificar escenarios de vulneración y consecuencias.

Se sugiere realizar una tabla en donde se describan los elementos antes mencionados].

<table>
<tr><td rowspan="5">Logo del sujeto obligado</td><td colspan="2">DOCUMENTO DE SEGURIDAD</td></tr>
<tr><td colspan="2">Nombre del sistema de datos personales</td></tr>
<tr><td>Fecha de elaboración</td><td>Fecha de la última actualización</td></tr>
<tr><td>Elaboró el documento</td><td>Aprobó</td></tr>
<tr><td>(Nombre y firma)</td><td>(Nombre y firma)</td></tr>
</table>

VIII. ANALISIS DE BRECHA

[Se sugiere realizar una tabla en donde se describan los elementos faltantes para cubrir sus medidas de seguridad].

IX. RESPONSABE DE SEGURIDAD

[Indicar el nombre, cargo, domicilio oficial, correo oficial, teléfono oficial del responsable de seguridad, así como las funciones y obligaciones que este tiene en materia de protección de datos personales].

X. REGISTRO DE ACCESO Y TELECUMUNICACIONES

[Agregar como anexo el registro de quien tiene acceso al sistema, así mismo, se deberá elaborar una bitácora.

Indicar si se consideran transferencias telemáticas de datos, es decir, que datos o de qué forma pueden transferirse de manera que no puede ser manipulada.

Solamente el responsable del sistema de datos personales podrá conceder, alterar o anular la autorización para el acceso al sistema de datos personales].

XI. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

[Indicar las acciones o los procedimientos a considerar para mantener actualizadas las medidas de seguridad y revisión de estas, lo anterior en cumplimiento al artículo 25 de la Ley de Datos local].

<table>
<tr><td rowspan="5">Logo del sujeto obligado</td><td colspan="2">DOCUMENTO DE SEGURIDAD</td></tr>
<tr><td colspan="2">Nombre del sistema de datos personales</td></tr>
<tr><td>Fecha de elaboración</td><td>Fecha de la última actualización</td></tr>
<tr><td>Elaboró el documento</td><td>Aprobó</td></tr>
<tr><td>(Nombre y firma)</td><td>(Nombre y firma)</td></tr>
</table>

XII. PLAN DE TRABAJO

[Elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer; considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes].

XIII. PLAN DE CAPACITACIÓN

[Indicar, de acuerdo con la naturaleza del sistema de datos personales, las temáticas de interés sobre las que se quiere o pretende sensibilizar al personal involucrado en el tratamiento de datos personales, así como, incluir, temporalidad y especificar quienes son los que deben dar cumplimiento.

Para este apartado se puede considerar lo acordado en su programa anual de capacitación institucional, para ello, se sugiere incluir como anexo el mismo de manera íntegra].