ITAIPUE

DEBER DE SEGURIDAD

GUÍA PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LOS

DATOS PERSONALES

índice:

GLOSARIO

- **Activo**: Información, bien, recurso o tipo de soporte, físico o electrónico, hardware o software, en el cual se almacenan los datos personales o que es empleado para realizar el tratamiento de datos personales y que tiene valor para el responsable.

- **Administrador**: Titular del área administrativa del responsable, designada por éste, y que bajo su responsabilidad el tratamiento de datos personales llevado a cabo.

- **Amenaza**: Posible evento o acontecimiento que pone en riesgo el sistema de seguridad, los activos del responsable y, por ende, la protección de los datos personales, y que se puede materializar en un daño.

- **Áreas**: Instancias de los responsables previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan con facultades y/o atribuciones para dar tratamiento a los datos personales.

- **Análisis de brecha**: Estudio que identifica las medidas de seguridad existentes y aquellas otras que resultan necesarias para la seguridad de los datos personales.

- **Análisis de riesgos**: Estudio que identifica las posibles amenazas y vulnerabilidades de los activos y recursos involucrados en el tratamiento de los datos personales y que se pueden materializar en un daño, causando así una vulneración de seguridad.

- **Ciclo de vida**: Serie de fases que se presentan en cada tratamiento de datos personales y que se encuentran compuestas de una o varias actividades u operaciones.

- **Crisis**: Situación que se suscita cuando una amenaza se materializa en un daño, causando una vulneración de seguridad.

- **Dato personal**: Cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, gráfica, fotográfica, acústica o en cualquier otro formato. Se considera que una persona es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información, siempre y cuando esto no requiera plazos, medios o actividades desproporcionadas.

- **Derechos ARCO**: Los derechos de acceso, rectificación y cancelación de datos personales, así como la oposición al tratamiento de los mismos.

- **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**: Prestador de servicios, que con el carácter de persona física o jurídica pública o privada, ajena a la organización del responsable, trata datos personales a nombre y por cuenta de éste.

- **Finalidad**: principio u obligación que constriñe al responsable a efectuar el tratamiento de datos personales para un objeto concreto, dado a conocer en el aviso de privacidad y que sea acorde con las atribuciones del responsable previstas en su normativa aplicable.

- **Inventario**: La acción interrelacionada prevista en los artículos 48, fracción III, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla y 18, fracción III, de los Lineamientos Generales en Materia de Protección de Datos Personales en Posesión de

Sujetos Obligados del Estado de Puebla, y que consiste en la elaboración de una relación de los diferentes tratamientos de datos personales llevados a cabo por el responsable, especificando ciertos elementos de los mismos.

- **Medidas de seguridad**: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan garantizar la confidencialidad, disponibilidad e integridad de los datos personales.

- **Oficial de protección de datos personales**: La figura prevista en los artículos 119 a 121 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla y que tiene como atribuciones, en síntesis, asesorar al Comité de Transparencia y a las áreas del responsable, así como diseñar, ejecutar, supervisar y evaluar políticas, programas, acciones y actividades que correspondan para el cumplimiento de la Ley y de las disposiciones que resulten aplicables en la materia, en coordinación con el Comité de Transparencia.

- **Perímetro de seguridad**: Conjunto de medidas de seguridad que delimitan un espacio de protección y aislamiento frente a intrusiones provenientes del exterior.

- **Responsable**: Cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, fideicomisos y fondos públicos, a los Ayuntamientos y partidos políticos del Estado de

Puebla, que decide y determina los fines, medios y demás cuestiones relacionadas con determinado tratamiento de datos personales.

- **Riesgo**: Posibilidad de que una amenaza se materialice y cause un daño.

- **Sistema de gestión de la seguridad de los datos personales**: Conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en los artículos 48 y 50 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Puebla.

- **Titular**: La persona física a quien hacen referencia o pertenecen los datos personales objeto del tratamiento.

- **Tratamiento**: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados aplicados a los datos personales, relacionadas, de manera enunciativa mas no limitativa, con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, transferencia y en general cualquier uso o disposición de datos personales.

- **Usuario**: El servidor público, integrante o colaborador del responsable que, por razones de sus atribuciones y funciones en la organización, debe acceder, usar y tratar datos personales.

- **Vulnerabilidad**: Punto débil en el sistema de seguridad o en cualquiera de los activos empleados para el tratamiento de datos personales, el cual puede ser aprovechado por una amenaza y, de esta manera, causar una vulneración a la seguridad.

- **Vulneración de seguridad**: Los eventos señalados en el artículo 53 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Puebla y que pueden consistir en: la pérdida o destrucción no autorizada de datos personales; el robo, extravío o copia no autorizada de datos personales; el uso, acceso o tratamiento no autorizado de datos personales, o el daño, la alteración o modificación no autorizada de datos personales.

INTRODUCCIÓN

¿Qué es el deber de seguridad de los datos personales y cómo dar cumplimiento al mismo?

En el ámbito del sector público del Estado de Puebla, el deber de seguridad es una obligación que debe observar todo responsable que realice un determinado tratamiento de datos personales.

Dicha obligación está prevista en los artículos 46 a 58 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, así como 17, fracción I, 18, 19 y 20 de los Lineamientos Generales en Materia de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Puebla.

Cabe destacar que el deber de seguridad está estrechamente relacionado con el principio de responsabilidad, previsto en los artículos 45 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Puebla y 13, 14, 15 y 16 de los Lineamientos Generales en Materia de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Puebla.

El objeto de esta obligación consiste en la creación, por parte del responsable, de un entorno o perímetro de seguridad de los datos personales manejados, el cual garantice la confidencialidad, integridad y disponibilidad de los mismos y permitan protegerlos contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado.

Los datos personales tienen un alto valor eminentemente económico –aunque no exclusivamente– para terceras personas, ajenas a la organización del responsable, las cuales buscan acceder y hacerse con dicha información con la finalidad de obtener un lucro, a través de su explotación comercial.

Para prevenir tal situación de riesgo de afectación a la privacidad de las personas, el responsable debe implementar un Sistema de Gestión de la Seguridad de los Datos Personales, sustentado en una serie de actividades que se encuentran interrelacionadas entre ellas, así como en medidas de carácter físico, técnico y administrativo, las cuales tendrán diferentes niveles de protección, dependiendo de distintos factores que subyacen en la naturaleza y cantidad de los datos personales tratados, así como del

número de titulares de datos personales involucrados por el tratamiento llevado a cabo y las características y condiciones que éstos poseen.

Para lograr lo anterior, el responsable habrá de observar y seguir ciertas pautas y quehaceres, los cuales se engloban en cuatro etapas distintas: Identificación, Desarrollo, Implementación y Monitorización y Mejoramiento.

De igual forma, el deber de seguridad implica la gestión de la crisis que, en su caso se suscite, derivado de una eventual vulneración al perímetro de seguridad, así como de las acciones que deberán llevarse a cabo. La transgresión al sistema de seguridad es una situación de la cual ningún responsable está exento a padecer; razón por la cual, todos los responsables deben implementar y mantener un nivel adecuado de protección de las bases en las cuales se encuentran contenidos los datos personales.

Fase 1: IDENTIFICACIÓN

Dentro de esta primera fase para la constitución e implementación de un Sistema de Gestión de la Seguridad de los Datos Personales, el responsable deberá conocer cuántos tratamientos de datos personales tiene en funcionamiento y, a partir de ello, elaborar un inventario. Asimismo, deberá identificar el ciclo de vida de los datos personales, identificar y definir las funciones y obligaciones del personal involucrado en cada tratamiento, y realizar un análisis de riesgos y otro de brecha.

Paso 1: Elaboración de un inventario de los diferentes tratamientos de datos personales llevados a cabo por el responsable.

Como primer paso, el responsable tiene que identificar cuáles son los tratamientos de datos personales que actualmente están siendo llevados a cabo en su organización. Para ello, el personal del responsable designado para tales efectos deberá mantener reuniones con los titulares de las áreas administrativas y demás personal que se estime necesario para allegarse de

los elementos necesarios que le permitan realizar tal inventario, a partir de la información y datos pertinentes que éstos suministren a los primeros.

De conformidad con el artículo 120, fracción II, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, el Oficial de Protección de Datos Personales tiene la atribución de diseñar, ejecutar, supervisar y evaluar políticas, programas, acciones y actividades que correspondan para el cumplimiento de la Ley y de las disposiciones que resulten aplicables en la materia, en coordinación con el Comité de Transparencia. No obstante lo anterior, se aconseja que en tales tareas se cuente con la participación activa de los titulares de las áreas administrativas del sujeto obligado y del personal involucrado en el tratamiento de datos personales.

Los titulares de las áreas administrativas y su personal, deberán colaborar activamente en todas y cada de las fases necesarias para la implementación del Sistema de Gestión de la Seguridad de los Datos Personales y en lo que respecta a este primer paso de la fase 1, deberán indicar cuántos y cuáles son los tratamientos de datos personales que tienen en funcionamiento, así como proporcionar otros datos y elementos necesarios para la confección del inventario.

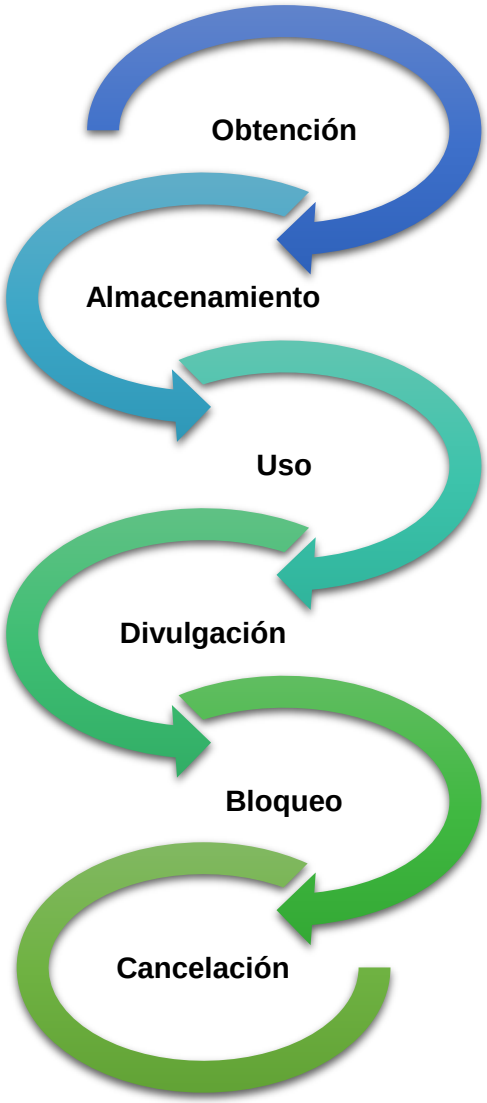
El inventario constituye un listado en el que debe anotarse el nombre de cada uno de los diferentes tratamientos de datos personales llevados a cabo por el responsable. Asimismo, y por cada tratamiento de datos personales, se deberá reflejar al menos los siguientes elementos:

- La o las finalidades de cada tratamiento de datos personales;
- Los medios físicos y electrónicos a través de los cuales se obtienen los datos personales;
- El formato (físico o electrónico) de almacenamiento, así como la descripción general de la ubicación (física y/o electrónica) de los datos personales;
- Los tipos de datos personales que son tratados, indicando si son sensibles o no;
- El ciclo de vida de los datos personales;
- El tiempo de conservación de los datos personales;
- Nivel de riesgo inherente por cada tipo de dato personal tratado;
- El o los servidores públicos que tienen acceso a los sistemas de tratamiento, y
- En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable.

El inventario es el elemento base que permitirá conocer las condiciones, circunstancias y actividades que entrañan el funcionamiento del tratamiento de datos personales para poder determinar su adecuación a las leyes aplicables en la materia, así como la realización de otras actividades interrelacionadas.

Paso 2: Identificación del ciclo de vida de los datos personales manejados en cada tratamiento de datos personales.

El responsable debe identificar el ciclo vital de los datos personal que integran el tratamiento, es decir, cuáles son las actividades que se realizan en cada etapa del tratamiento, desde que se obtienen hasta que se suprimen, conforme al siguiente esquema:



Paso 3: Identificación y evaluación del riesgo inherente a cada tipo y categoría de dato personal.

El riesgo inherente es el riesgo específico a cada tipo de dato personal, cuando no se toma ninguna acción para alterar la probabilidad de manifestación de una amenaza previamente identificada o la magnitud del impacto de un suceso. La eliminación absoluta del riesgo es imposible; sin embargo, se pueden adoptar diversas estrategias con el fin de abordar la manera en que se tratará el riesgo identificado. Algunas de estas opciones son reducir o mitigar el riesgo, evitar el riesgo, aceptar el riesgo, retener el riesgo, o compartir el riesgo. Cuando se opta por mitigar el riesgo, éste nunca podrá ser reducido a cero, por lo que siempre existirá un riesgo residual que será mayor o menor en la medida en la que la organización del responsable lo acepte y tolere.

Para la clasificación de los datos personales, en función de su riesgo inherente, el responsable habrá de estar a dos factores clave: la sensibilidad del dato personal y el número de titulares de datos personales potencialmente afectados en caso de manifestarse una amenaza que vulnere la seguridad del sistema.

De acuerdo con el artículo 5, fracción IX, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, los datos personales sensibles son aquéllos que se refieren a la esfera más íntima de privacidad del titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. Tradicionalmente, se consideran sensibles, de manera enunciativa mas no limitativa, los siguientes datos personales: origen racial o étnico, estado de salud (presente, pasado o futuro), creencias religiosas, filosóficas y morales, opiniones políticas, datos genéticos o datos biométricos, etc.

Como se ha dicho, el riesgo inherente dependerá del grado de sensibilidad que subyace en un dato personal recabado por la organización. En ese sentido, podemos clasificar el riesgo inherente en tres niveles distintos:

- Nivel bajo estándar (verde): datos de contacto, de identificación, académicos, laborales, etc. Son datos que simplemente pueden causar una ligera molestia en la esfera jurídica del titular.
- Nivel intermedio o sensible (amarillo): datos patrimoniales, ubicación física, jurídicos, etc. Son datos personales que inciden en la esfera más íntima del titular, pero sin llegar a ponerle en

una potencial situación de grave peligro, discriminación o afectación a otros intereses, derechos o libertades.

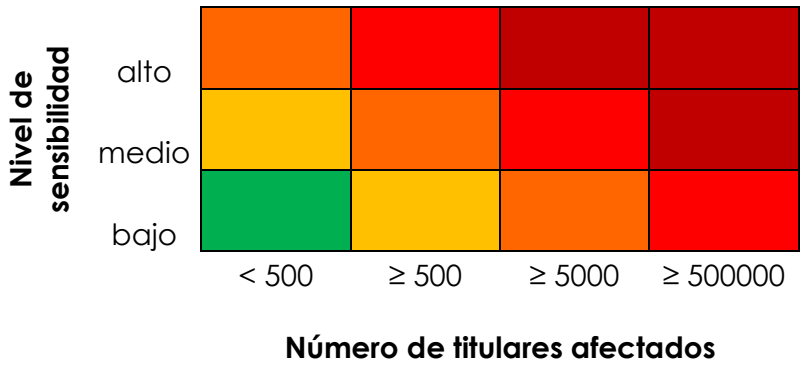
- Nivel alto o sensible especial (rojo): datos de salud, datos biométricos, datos genéticos, ideología, creencias religiosas, preferencias y orientación sexual, etc. Son datos personales que inciden en la esfera más íntima del titular, y llegan a ponerle en una potencial situación de grave peligro, discriminación o afectación a otros intereses, derechos o libertades.

En la tabla siguiente, se muestra un ejemplo de clasificación de categorías de datos personales en función del grado de sensibilidad:

Tipo de dato	Nivel
Datos de identificación	Estándar
Datos de contacto	Estándar
Datos laborales	Estándar
Datos sobre procedimientos judiciales o administrativos	Sensible
Datos clínicos	Especial

Por otro lado, el otro factor que determina la existencia de un mayor o menor riesgo inherente al dato personal, es el número de titulares posiblemente afectados.

La siguiente gráfica muestra el nivel de riesgo inherente de cada tipo de dato personal, en función de su sensibilidad y del número de titulares afectados.



La posición en un punto u otro de la gráfica evidenciará el nivel de protección que el responsable habrá de fijar para la custodia de los datos personales. En el supuesto que el dato personal manejado tenga un nivel de

sensibilidad bajo y el número de titulares de datos personales sea menor a quinientos, el riesgo inherente será bajo y, en consecuencia, el responsable podrá considerar implementar controles con un nivel de seguridad moderado. Por el contrario, si el dato personal manejado tiene un nivel de sensibilidad alto y el número de titulares de datos personales es de más de quinientos mil, entonces el riesgo inherente es muy alto y, en consecuencia, el responsable deberá implementar controles rigurosos de máximo nivel de seguridad.

Cabe destacar que la identificación del riesgo inherente sirve de pauta para examinar qué medidas de seguridad habrán de establecerse. Sin embargo, en esta etapa del procedimiento para la implementación del Sistema de Gestión de la Seguridad de los Datos Personales, únicamente habrá de plantearse este cuestionamiento a los únicos efectos de determinar el nivel de riesgo inherente; la relación de las medidas de seguridad que, de manera concreta, habrán de implementarse, corresponde a una fase ulterior del procedimiento.

Paso 4: Definición de los roles, permisos y funciones, facultades, atribuciones, y obligaciones del personal involucrado en cada uno de los tratamientos de datos personales anotados en el inventario.

Una vez se tienen identificados cuáles son los diferentes tratamientos de datos personales existentes, el responsable debe proceder a definir cuáles son las funciones y los permisos en base a los cuales el personal involucrado en cada tratamiento de datos personales podrá acceder y usar los datos personales para el cumplimiento de sus funciones y tareas.

Para ello, el responsable deberá elaborar una matriz en la que expongan los roles de cada una de las personas que habrán de intervenir en el tratamiento de datos personales, junto con los permisos con los que cuentan. Los roles que podrán manejarse son los de administrador y usuario.

Matriz de roles y permisos del personal involucrado en cada tratamiento de datos personales			
	Cargo	**Rol**	**Permisos**
Persona A	Titular	Responsable	Cr
Persona B	Director	Administrador	UDBCR
Persona C	Analista	Operador	OAU

Leyenda: Cr: creación; O: obtención; U: uso; D: divulgación; A: almacenamiento; R: resguardo; B: bloqueo; C: cancelación. Etc.

Asimismo, el responsable deberá hacer constar las facultades y atribuciones previstas en su normativa aplicable, con las que cuenta el personal para

intervenir en el tratamiento de datos personales; lo anterior, en base al principio de licitud, previsto en el artículo 15 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla.

Por último, el responsable deberá establecer un elenco de obligaciones generales que deberán observar las personas de su organización que, por razones de su cargo, deban acceder a las bases de datos y usar los mismos. Dicha relación deberá ser acompañada de un régimen de sanciones para el caso de que alguna de las personas autorizadas a acceder a los datos personales incumpla alguna de las obligaciones previstas.

Fase 2: DESARROLLO

En esta segunda fase, el responsable desarrollar los análisis de riesgo y de brecha, en base a los cuales se podrá determinar cuáles son las amenazas para los datos personales y las vulnerabilidades que presentan los activos en los cuales se encuentran resguardados los datos personales.

Paso 1: Elaboración de un análisis de riesgo.

El responsable deberá realizar un análisis de los riesgos que pueden llegar a perjudicar los datos personales, como activo intangible, pero también los activos tangibles en los cuales se encuentran almacenados los datos personales, tales como archivos, libros, expedientes, documentos, dispositivos de almacenamiento masivo (discos duros, USBs, discos compactos, etc.).

Para ello, el responsable habrá de plasmar en un hipotético escenario las amenazas y vulnerabilidades existentes para los datos personales y los recursos empleados para su tratamiento. Asimismo, en tal escenario habrá de señalarse cuáles son los activos que se emplean en el tratamiento de los datos personales, distinguiendo entre los activos intangibles o de información (datos personales) y los activos tangibles o de apoyo (objeto en el cual se guardan los datos personales, les sirven de protección o están

estrechamente vinculados con el tratamiento). Así también habrá de indicarse el daño que puede ocurrir en caso de que se presente la amenaza identificada y la probabilidad de que ésta suceda.

Tratamiento de datos personales				
Escenario de vulneración				
Activo	**Amenazas**	**Vulnerabilidad**	**Daño**	**Probabilidad**
Disco duro	• Falla técnica o malfuncionamiento • Descarga eléctrica • Virus o *malwares*	• Componente con muchos años de uso • Existencia de variación de voltaje y cortes espontáneos de suministro de energía eléctrica • Componente instalado en una computadora conectada a redes internas e internet y que no tiene instalado *software* de seguridad	• Pérdida de información • Avería o descompostura • Alteración, sustracción o acceso no autorizado	Alta debido a que el equipo está anticuado, tiene muchos año de uso, existe inestabilidad en el suministro eléctrico, y no se ha adquirido *software* de antivirus.

En base a este ejercicio, el responsable podrá llegar a identificar las amenazas que ponen en peligro la confidencialidad, integridad y disponibilidad de los datos personales. La amenaza tiene el potencial de dañar la información sometida a tratamiento y causar una vulneración de seguridad. La vulneración puede definirse como la violación de la seguridad en la que se copian, transmiten, visualizan, roban, destruyen, alteran o usan de forma no autorizada datos personales, protegidos o confidenciales, los cuales pueden estar almacenados o ser transmitidos o procesados de cualquier otra forma. Esto puede ser causado por amenazas que provienen tanto del interior de la organización como del exterior, y pueden ser de origen natural o humano, y accidentales o deliberadas.

Paso 2: Elaboración de un análisis de brecha.

El responsable deberá realizar un análisis de brecha en el que se comparen las medidas de seguridad existentes y que cumplen su propósito, contra las faltantes para así lograr un estado idóneo de protección a los datos personales. En ese sentido, el responsable habrá de estudiar la normativa

aplicable y comprender los requerimientos regulatorios para estar en situación de cumplir cabalmente con la misma.

Para la adopción de una medida de seguridad u otra, el responsable habrá de considerar lo siguiente:

I. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión;

I. II. La sensibilidad de los datos personales tratados;
II. El desarrollo tecnológico;
III. Las posibles consecuencias de una vulneración para los titulares;
IV. Las transferencias de datos personales que se realicen;
V. El número de titulares, y
VI. Las vulneraciones previas ocurridas en los sistemas de tratamiento.

De esta manera, el análisis de brecha mostrará las medidas de seguridad vigentes y que, por ser efectivas, vale la pena mantener y, por otro lado, las medidas de seguridad que hacen falta para cubrir el *gap* entre el estado actual de seguridad y un estado idóneo.

Paso 3: Creación de una política interna de tratamiento de datos personales.

El responsable deberá elaborar y aplicar una política interna en la que, al menos, contemple lo siguiente:

I. Los controles para garantizar que se valida la confidencialidad, integridad y disponibilidad de los datos personales;
II. Las acciones para restaurar la disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente físico o técnico;
III. Las medidas correctivas en caso de identificar una vulneración o incidente en los tratamientos de datos personales;
IV. El proceso para evaluar periódicamente las políticas, procedimientos y planes de seguridad establecidos, a efecto de mantener su eficacia;
V. Los controles para garantizar que únicamente el personal autorizado podrá tener acceso a los datos personales para los finalidades concretas, lícitas, explícitas y legítimas que originaron su tratamiento, y
VI. Las medidas preventivas para proteger los datos personales contra su destrucción accidental o ilícita, su pérdida o alteración y el

almacenamiento, tratamiento, acceso o transferencias no autorizadas o acciones que contravengan las disposiciones de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Puebla y demás ordenamientos que resulten aplicables.

Además de lo anterior, el responsable podrá, igualmente, incluir como contenido de su política interna, la manera en que serán protegidos ciertos activos en los que se encuentran almacenados los datos personales, tales como discos duros, expedientes, dispositivos de almacenamiento masivo, etc.), normas éticas o de conducta en relación al manejo de los datos personales, etc.

También el responsable podrá adoptar los mejores estándares, nacionales e internacionales, existentes para la protección de información sensible de las organizaciones o contemplar un procedimiento más sencillo y expedito para la atención de solicitudes para el ejercicio de derechos ARCO (acceso, rectificación, cancelación y oposición).

En este mismo instrumento el responsable podría incluir lo anteriormente referido al régimen de obligaciones generales que deberán observar las personas de su organización que, por razones de su cargo, deban acceder a las bases de datos y usar los mismos, junto con el régimen de sanciones para el caso de que alguna de ellas incumpla alguna de las obligaciones previstas.

Fase 3: IMPLEMENTACIÓN

Paso uno: Elaboración de un plan de trabajo.

Dentro de esta fase, el responsable habrá de elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas internas de tratamiento de datos personales.

En relación a las medidas de seguridad faltantes, el responsable habrá de priorizar aquéllas que sean más relevantes y urgentes a establecer, en función de los indicadores arrojados en los análisis de riesgo y de brecha y de los recursos, humanos y financieros, disponibles.

El plan de trabajo deberá indicar las medidas de seguridad que habrán de implementar a corto, mediano y largo plazo; lo anterior, bajo un esquema de calendarización de cumplimiento de metas.

En el plan de trabajo se deberá indicar el nombre y cargo del administrador de cada tratamiento de datos personales; en él se dejará la responsabilidad de implementar, de manera material, las medidas de seguridad faltantes, en coordinación con el Oficial de Protección de Datos Personales y las demás áreas que hayan de intervenir. Si existieran varias áreas que manejaran la información personal, se deberá designar un conjunto de personas de las mismas que funjan como responsables a tales efectos.

Paso dos: Elaboración de un documento de seguridad.

De conformidad con el artículo 51 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, el responsable debe elaborar un documento de seguridad que contenga, al menos, lo siguiente:

I. El inventario de datos personales y de los sistemas de tratamiento;

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

III. El análisis de riesgos;

IV. El análisis de brecha;

V. El plan de trabajo;

VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad;

VII. El programa general de capacitación, y

VIII. Nombre y cargo del personal del responsable o encargado.

Fase 4: MONITORIZACIÓN Y MEJORAMIENTO

Paso único: Monitorización y revisión de las medidas de seguridad, y capacitación al personal involucrado.

Una vez las medidas de seguridad han sido implementadas, sea de una sola vez o de manera progresiva, el responsable habrá atender las pautas previstas en su política interna para monitorear y revisar de manera periódica dichas medidas de seguridad, así como las amenazas, vulnerabilidades y vulneraciones que pudieran surgir o llegar a presentarse.

El objeto de estas acciones es corroborar que las medidas implementas son efectivas y sirven para el propósito para el cual fueron implementadas –es decir, la protección de los datos personales–, y que no hayan surgido nuevas amenazas que pudieran poner en jaque el sistema de seguridad existente o la aparición de puntos débiles en el mismo o en los activos que contienen los datos personales. De advertirse alguna de estas circunstancias, el responsable deberá realizar unos nuevos análisis de riesgo y de brecha y, posteriormente, un nuevo plan de trabajo para corregir las desviaciones en el sistema de seguridad.

Estas acciones deberán realizarse de manera recurrente, de conformidad con la periodicidad fijada en las políticas internas de tratamiento de datos personales, y podrán abarcar gestiones tales como auditorías, revisión de riesgos internos y externos, generación de indicadores o el establecimiento controles de seguimiento como, por ejemplo, capacitaciones.

Asimismo, el responsable debe actualizar el documento de seguridad cuando ocurran eventos tales como modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo; como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión; como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad

ocurrida, y se implementen acciones correctivas y preventivas ante una vulneración de seguridad ocurrida.

Por otro lado, como parte del mejoramiento al Sistema de Gestión de la Seguridad de los Datos Personales, el responsable habrá de fijar un programa de capacitación que tenga como público objetivo aquél personal que se encuentre involucrado en los diferentes tratamientos de datos personales existentes en la organización. La capacitación en materia de protección de datos personales debe centrarse en contenidos que doten a los asistentes de las herramientas necesarias para que se encuentren en situación de cumplir con los principios, deberes y obligaciones previstos en las leyes de la materia y, también, en el cumplimiento de las medidas de seguridad implementadas para cada uno de los diferentes tratamientos de datos personales. En ese sentido, la oferta de capacitación tiene que ser periódica, de manera que se mantenga actualizado al personal involucrado en los tratamientos de datos personales. Asimismo, se debe capacitar al personal de nuevo ingreso para que éste conozca desde el inicio cuáles son sus obligaciones y las posibles consecuencias en caso de incumplimiento.

El contenido de las capacitaciones tiene que ser enfocado a las circunstancias del tratamiento de datos personales, en específico, así como a las atribuciones, facultades, obligaciones y roles del personal involucrado.

Para determinar la eficiencia y eficacia de los cursos de capacitación en la materia, se debe realizar una evaluación a los participantes que permita dilucidar el grado de comprensión de los contenidos expuestos.