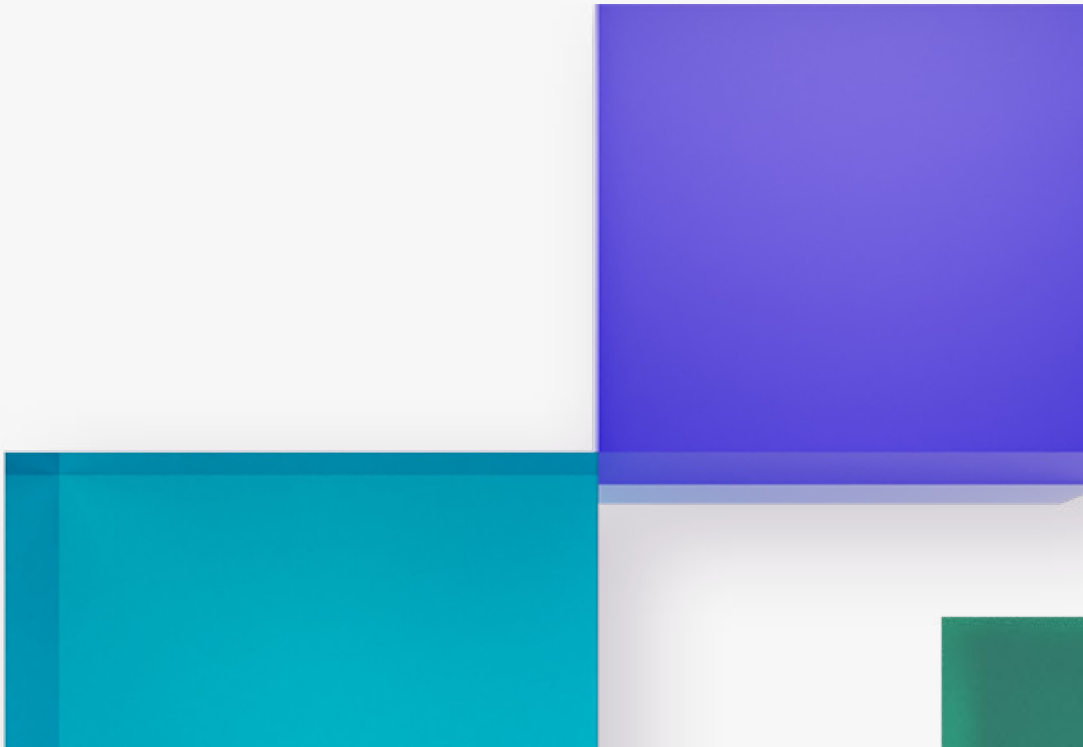
UNIDOS POR LAS AUDIENCIAS

Sistema Público de Radiodifusión del Estado Mexicano

Documento de Seguridad en materia de Protección de Datos Personales

2024



Índice

1. Introducción

La entrada en vigor de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[1] (en lo sucesivo LGPDPPSO), establece como uno de sus objetivos el proteger los datos personales en posesión de cualquier autoridad, entre ellos, el Sistema Público de Radiodifusión del Estado Mexicano (SPR)[2], como uno de los sujetos obligados o responsables en materia de protección de datos personales[3].

Además, establece las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales que estén en posesión de los sujetos obligados.

El SPR, como responsable, deberá implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la LGPDPPSO, la cual dispone que el tratamiento de datos personales realizado por los sujetos obligados está regido por ocho principios y dos deberes. Los ocho principios son: licitud, lealtad, información, consentimiento, finalidad, proporcionalidad, calidad y responsabilidad; mientras que los dos deberes son: confidencialidad y seguridad.

En este contexto, el Título Segundo, Capítulo II del referido ordenamiento, contempla que los sujetos obligados deben *establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad*[4].

En relación con las medidas de seguridad a que se refiere el párrafo anterior, el artículo 32 de la LGPDPPSO, establece que éstas deberán considerar: I. el riesgo inherente a los datos personales tratados; II. la sensibilidad de los datos personales tratados; III. el desarrollo tecnológico; IV. las posibles consecuencias de una vulneración para los titulares; V. las transferencias de datos personales que se realicen; VI. el número de titulares; VII. las vulneraciones previas ocurridas en los sistemas de tratamiento, y VIII. 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.

1 - Publicada en el Diario Oficial de la Federación el 26 de enero de 2017.
2 - Según lo dispuesto por el artículo 2, fracción V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
3 - En efecto, el artículo 1, párrafo 5 de la citada Ley dispone que *son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.*
4 - Artículo 31 de Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

A su vez, los artículos 33 y 34 del citado ordenamiento especifican una serie de actividades interrelacionadas que debe llevar a cabo el sujeto obligado, tendientes a establecer y mantener las medidas de seguridad para la protección de los datos personales, mismas que deben obrar en un sistema de gestión, entendido como el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

Ahora bien, de manera particular, es deber del SPR, en su calidad de sujeto responsable[5], elaborar un documento de seguridad que contenga al menos lo siguiente:

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

El documento de seguridad se define en el Artículo 3, fracción XIV de la LGPDPPSO, como *el 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*.

El 26 de enero de 2018, se publicaron en el Diario Oficial de la Federación los *Lineamientos Generales de Protección de Datos Personales para el Sector Público*[6] (en adelante Lineamientos Generales) cuyo objetivo es desarrollar las disposiciones previstas en la LGPDPPSO y, con ello, hacer más comprensible el cumplimiento de los principios, deberes y obligaciones exigidos en materia de protección de datos personales.

5 - En términos del artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
6 - Disponible en: https://dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018#gsc.tab=0

2. Glosario

Acervo: Al conjunto de documentos producidos y recibidos por los sujetos obligados en el ejercicio de sus atribuciones y funciones con independencia del soporte, espacio o lugar que se resguarden.

Administrador del Sistema: La persona servidora pública y/o prestadora de servicios profesionales que tiene a su cargo la responsabilidad de la administración del sistema y de los operadores.

Análisis de brecha: Permite identificar las medidas de seguridad actualmente implementadas, evaluar su efectividad en el tratamiento de los riesgos resultantes del proceso de análisis de riesgos; además nos permite definir nuevas medidas de seguridad para atender los riesgos, reforzando con ello la protección de los datos personales.

Análisis de riesgos: Permite identificar los peligros y evaluar el nivel de riesgo hacia los datos personales. Las metodologías de análisis de riesgo establecen un proceso sistemático que consiste en crear escenarios de riesgo, identificando y correlacionando todos los elementos que intervienen en él: activo (que en el presente contexto consiste en los datos personales), amenazas, vulnerabilidades, controles existentes e impactos o consecuencias. Una vez creados los escenarios de riesgo, se procede a evaluar cualitativa o cuantitativamente el riesgo mediante el establecimiento de parámetros como la probabilidad de ocurrencia y el nivel de impacto o de beneficio para el atacante.

Archivo: Al conjunto organizado de documentos producidos o recibidos por los sujetos obligados en el ejercicio de sus atribuciones y funciones, con independencia del soporte, espacio o lugar que se resguarden.

Aviso de privacidad: Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de estos.

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.

Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.

Catálogo de Disposición Documental (CADIDO): Formato en el que se registran todas las atribuciones de una institución (secciones documentales) y los procesos (series documentales) que ayudan a cumplir con estas atribuciones, en los cuales se produce documentación que se integra en expedientes. En este formato se indican los valores documentales (la utilidad o el uso que tiene el documento), la vigencia (durante cuánto tiempo tiene efecto) y los plazos y medidas de conservación (el tiempo que debe permanecer en el Archivo de Trámite y de Conservación, así como la manera en la que pasará al Histórico). Este formato se deriva del Cuadro General de Clasificación Archivística y es uno de los instrumentos de control archivístico.

Comité de Transparencia (CT): Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública.

Consentimiento: Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de estos.

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

Dato: Es el elemento primario de la información conformado por símbolos (letras, números, dibujos, señas, gestos) que reunidos pueden cobrar significación. Sólo o aislado el dato no posee relevancia, pero utilizado en las premisas de un razonamiento puede determinarse directa o indirectamente a través de cualquier información.

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

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

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

Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación de este.

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 conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

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

Expediente electrónico: Al conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan.

Evitar el riesgo: Acción para retirarse de una situación de riesgo o decisión para no involucrarse en ella.

Identificar el riesgo: Proceso para encontrar, enlistar y describir los elementos del riesgo.

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual es el organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización 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 deben considerar las siguientes actividades:

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

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Operador: Prestador(es) de servicios profesionales que opera(n) el sistema en el SPR.

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

Responsable: El SPR como sujeto obligado a que se refiere el artículo 1 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados a través del servidor público titular de la unidad administrativa o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales.

Riesgo: Combinación de la probabilidad de un evento y su consecuencia desfavorable.

Riesgo de seguridad: Combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas.

Riesgo inherente: Riesgo intrínseco al activo, sin considerar las medidas de seguridad implementadas.

Riesgo residual: El riesgo remanente después de tratar el riesgo.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades delimitadas por la normatividad aplicable.

Sistema: Conjunto de elementos relacionados entre sí que funcionan como un todo. Módulo ordenado de elementos que se encuentran interrelacionados y que interactúan entre sí. Conjunto de elementos con relaciones de interacción e interdependencia que le confieren entidad propia al formar un todo unificado.

SPR: Sistema Público de Radiodifusión del Estado Mexicano.

Sistema de Tratamiento de Datos Personales (SDP): Bases de datos personales, contenidos en un sistema informático, a las que se les aplica algún tratamiento.

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

Titular: 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 mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Unidades administrativas: Son las comprendidas en el Estatuto Orgánico del Sistema Público de Radiodifusión del Estado Mexicano y/o estructura orgánica básica de la Entidad, responsables de ejercer sus funciones y la asignación presupuestaria correspondiente.

Unidad de Transparencia (UT): Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

Usuario: Persona servidora pública o prestadora de servicios profesionales facultada por un instrumento jurídico o expresamente autorizada por el responsable que utiliza de manera cotidiana datos personales para el ejercicio de sus atribuciones, por lo que accede a los sistemas de datos personales, sin posibilidad de agregar o modificar su contenido, a menos que cuente con atribuciones o autorización por escrito para ello.

Valorar el riesgo: Proceso para asignar valores a la probabilidad y consecuencias del riesgo.

Vulnerabilidad: Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

3. Objetivos del Documento de Seguridad

El presente Documento de Seguridad tiene como objetivos, los siguientes:

1

Proveer el marco de trabajo necesario para la protección de los datos personales en posesión del Sistema Público de Radiodifusión del Estado Mexicano.

2

Cumplir con las obligaciones que establece la LGPDPPSO y los Lineamientos Generales.

3

Establecer los elementos y actividades de dirección, operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua, y

4

Promover la adopción de mejores prácticas en la protección de datos personales, de manera preferente una vez que se haya implementado de manera integral en el Sistema, o bien, cuando se estime pertinente la implementación de buenas prácticas en tratamientos específicos.

4. Marco normativo

Para efectos del presente documento, la normatividad aplicable es la siguiente:

- **Constitución Política de los Estados Unidos Mexicanos.**[7]
- **Convención Americana sobre Derechos Humanos.**[8]
- **Ley General de Protección de Datos Personales en posesión de Sujetos Obligados.**[9]
- **Ley General de Transparencia y Acceso a la Información Pública.**[10]
- **Ley General de Archivos.**[11]
- **Ley Federal de Transparencia y Acceso a la Información Pública.**[12]
- **Lineamientos Generales de Protección de Datos Personales para el Sector Público.**[13]
- **Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.**[14]
- **Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales.**[15]
- **Estándares de Protección de Datos Personales para los Estados Iberoamericanos.**

7 - Última reforma publicada el 6 de junio de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf
8 - Disponible en: https://www.dof.gob.mx/nota_to_imagen_fs.php?codnota=4645612&fecha=07/05/1981&cod_diario=199960
9 - Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017
10 - Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5391143&fecha=04/05/2015
11 - http://www.diputados.gob.mx/LeyesBiblio/pdf/LGA_150618.pdf
12 - Última reforma publicada el 27 de enero de 2017. Disponible en: http://inicio.inai.org.mx/doc/DGAJ/LGTA70FI/REGLAMENTOS/LEY%20FEDERAL%20DE%20TRANSPARENCIA.pdf
13 - Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018
14 - Disponible en: http://inicio.inai.org.mx/doc/DGAJ/LGTA70FI/1ERTRIM2018/120218%20Acuerdo%20de%20Portabilidad.pdf
15 - Disponible en: http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf

5. Responsabilidades

Con fundamento en lo dispuesto por los artículos 83 y 84 de la LGPDPPSO, que señalan que el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en posesión del SPR, dicho órgano tendrá las siguientes funciones:

1. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de datos personales.
2. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de solicitudes para el ejercicio de derechos ARCO.
3. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO.
4. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la Ley y en aquellas disposiciones que resulten aplicables en la materia.
5. Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad.
6. Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).
7. Establecer programas de capacitación y actualización para las personas servidoras públicas y/o personas prestadoras de servicios por honorarios en materia de protección de datos personales.
8. Dar vista al Órgano Interno de Control en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales; particularmente, en casos relacionados con la declaración de inexistencia que realicen las personas responsables.

Para que los objetivos planteados se logren con éxito, se requiere que el presente Documento de Seguridad, se difunda al interior del Sistema Público de Radiodifusión del Estado Mexicano, con la finalidad de impulsar su implementación, asimismo, es importante mencionar que será de observancia obligatoria para todas las personas prestadoras de servicios profesionales por honorarios que en ejercicio de sus funciones traten datos personales.

6. Ámbito de aplicación

En atención a los "Deberes" a que se refiere la LGPDPPSO, el presente documento es aplicable a todas las unidades administrativas del SPR que, en el ejercicio de sus atribuciones y funciones, administren bases de datos en sistemas de tratamiento de datos personales, ya sea que administren sistemas completos, o el tramo de información que le corresponda.

Asimismo, serán aplicables al tratamiento de datos personales que obren en soportes físicos y/o electrónicos, con independencia de la forma o modalidad de su creación, procesamiento, almacenamiento y organización. Los datos personales podrán ser expresados en forma numérica, alfabética, gráfica, alfanumérica, fotográfica, acústica o en cualquier otro formato.

Todas las personas servidoras públicas y/o prestadoras de servicios profesionales que tengan acceso a los datos personales, están obligados a conocer y aplicar las medidas de seguridad propias de cada Sistema en el que se concentren los datos y es aplicable en todas y cada una de las fases del tratamiento de los datos personales, iniciando desde la obtención de los mismos y finalizando su participación en el tratamiento de los datos personales porque hayan cambiado de funciones y aun cuando la relación laboral con el SPR haya concluido.

Además de las funciones y obligaciones de los servidores públicos y/o prestadores de servicios profesionales involucrados, establecidas de manera específica en el análisis de cada uno de los sistemas, de manera general deberán de observarse las siguientes:

Funciones genéricas en cualquier nivel de tratamiento

- Tratar los datos personales con responsabilidad y las medidas de seguridad que se hayan establecido para tal fin.

Obligaciones genéricas en cualquier nivel de tratamiento

- Guardar confidencialidad sobre la información que conozcan en el desarrollo de sus actividades.
- Estar capacitado en materia de tratamiento de datos personales.
- Dar aviso a los superiores jerárquicos, ante cualquier acción que pueda poner en riesgo los datos personales, y en general que puedan vulnerar la seguridad de los datos personales.

De manera particular y de conformidad con los cargos, encargos y/o designaciones de las personas servidoras públicas y/o prestadoras de servicios profesionales, se definen cuatro roles básicos en el tratamiento de datos personales.

- Responsable del SDP,
- Administrador del SDP,
- Operadores, y
- Enlace de datos personales.

Sus funciones son las siguientes:

Responsable del SDP: Siempre será la persona a cargo de la Unidad Administrativa donde se administre el Sistema de que se trata. Deberá:

» Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.
» Tratar los datos personales para finalidades concretas, licitas, explícitas y legítimas en ejercicio a las facultades y atribuciones que la normatividad aplicable le confiera.
» Evitar la obtención y tratamiento de datos personales, a través de medios engañosos o fraudulentos.
» Privilegiar la protección de los intereses del titular de los datos y la expectativa razonable de privacidad.
» Tratar los datos personales previo consentimiento, expreso o tácito, otorgado por el titular de manera libre, específica e informada; salvo cuando se actualice alguna de las causales de excepción previstas en el artículo 22 de la LGPDPPSO.
» Obtener el consentimiento expreso y por escrito del titular para su tratamiento, tratándose de datos personales sensibles, salvo en los casos previstos en el artículo 22 de la LGPDPPSO.
» Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.
» Establecer los plazos de conservación de los datos personales tomando en consideración las finalidades que justificaron su tratamiento y las disposiciones aplicables en materia de protección de datos personales, así como los aspectos administrativos, contables, fiscales, jurídicos e históricos de los mismos.
» Suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento, previo bloque, en su caso, y una vez que concluya el plazo de conservación de estos.
» Implantar mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos personales, incluyendo la revisión periódica sobre la necesidad de conservar los datos personales.
» Tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

- Informar a la persona titular, a través del aviso de privacidad, que deberá ser difundido por medios electrónicos y físicos, la existencia, características principales y finalidades del tratamiento al que serán sometidos sus datos personales.
- Instrumentar medidas compensatorias de comunicación masiva cuando resulte imposible dar a conocer a la persona titular el aviso de privacidad, de manera directa o ello exija esfuerzos desproporcionados.
- Establecer y mantener las medidas de seguridad de carácter administrativo, físicos y técnicos para la protección de los datos personales, que permitan salvaguardarlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.
- Dar aviso a la Unidad de Transparencia de los SDP que involucren tratamiento de datos personales, a cargo de dicha Unidad Administrativa.
- Designar al Administrador del SDP.
- Atender, dentro de los plazos establecidos, las solicitudes de ejercicio de los derechos ARCO que les sean turnadas por la Unidad de Transparencia.

Administrador del SDP o Encargados: Será la persona servidora pública o prestadora de servicios profesionales a quien designe de manera expresa el titular de la Unidad Administrativa. Tiene a su cargo la responsabilidad de la administración del sistema y de los operadores. Deberá:

- Tratar los datos personales para finalidades concretas, lícitas, explícitas y legítimas en ejercicio a las facultades o atribuciones que la normatividad aplicable le confiera o en cumplimiento a las instrucciones otorgadas por el Responsable del sistema de datos personales.
- Privilegiar la protección de los intereses del titular de los datos y la expectativa razonable de privacidad.
- Mantener actualizado el SDP.
- Determinar los servidores públicos que deben tener acceso a los datos personales, en función del tratamiento que debe aplicarse a los mismos.
- Autorizar los accesos a los prestadores de servicios profesionales, determinar los privilegios y limitantes y llevar un registro de estos.
- Tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento o en acatamiento a las instrucciones otorgadas por el Responsable del sistema de datos personales.
- Observar las indicaciones e instrucciones que el responsable del sistema de datos personales para la protección de estos y notificarle de inmediato en caso de que exista alguna vulneración al sistema o sistemas al que tenga acceso.
- Implementar las medidas de seguridad con la finalidad de evitar vulneraciones de la información.

Operador (es)

» Sus funciones quedan determinadas de acuerdo con el perfil que se haya asignado en el tratamiento de los datos personales de cada uno de los sistemas.

Enlace de datos personales

» Conocer el inventario de SDP que involucren tratamiento de datos personales y por cada uno, conocer el tipo de datos personales que se recaban y el nombre del Encargado por cada SDP.
» Dar seguimiento a las acciones de capacitación para los servidores públicos y/o prestadores de servicios profesionales involucrados en el tratamiento de los datos personales.
» Atender a los requerimientos de información que solicite la Unidad de Transparencia del SPR.

El incumplimiento a lo establecido en el Documento de Seguridad, así como a lo establecido por la LGPDPPSO y los Lineamientos Generales, causará la aplicación de medidas de apremio y/o sanciones, que se detallan en dichos instrumentos normativos.

En caso de existir figura de “Encargado”, en la formalización de la prestación del servicio que implique la transferencia de datos para su tratamiento, deberá atenderse a lo previsto en el Artículo 59 de la LGPDDPSO y los artículos correspondientes de los Lineamientos Generales, que se refieren a la existencia de algún instrumento jurídico que incluya cláusulas sobre el tratamiento de datos personales conforme a las instrucciones del responsable, que prevean que los datos no se tratarán para finalidades distintas a las previstas, que establezcan que se implementarán medidas de seguridad, que se informará al responsable en caso de vulneración, que se guardará confidencialidad respecto de los datos personales, que éstos se suprimirán o devolverán al concluir la relación jurídica en atención a las normas jurídicas sobre su conservación y que se abstendrán de transferirlos salvo determinación del responsable en atención a la normatividad y al aviso de privacidad correspondiente.

7. Alcance del Documento de Seguridad

El presente Documento de Seguridad aplicará a todas las unidades administrativas que realicen tratamiento de datos personales en ejercicio de sus atribuciones. Se cumplirán todos los principios, deberes y obligaciones consagrados en los artículos 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41 y 42 de la LGPDPPSO; y 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 22, 24, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 46, 55, 56 de los Lineamientos Generales.

Las Unidades administrativas involucradas son:

UNIDAD ADMINISTRATIVA
Unidad de Administración y Finanzas Dirección de Recursos Humanos Dirección de Adquisiciones, Arrendamiento y Obra Pública Dirección de Servicios Generales y Conservación
Dirección General de Asuntos Jurídicos y Transparencia Dirección de lo Contencioso Dirección de Transparencia
Dirección General de Convergencia e Innovación Tecnológica
Dirección General de Canal Catorce Dirección de Producción Dirección de Noticias y Programas Informativos
Defensoría de las Audiencias
Dirección General de Comunicación y Redes Dirección de Comunicación Dirección de Investigación y Análisis Dirección de Redes Socio Digitales
Dirección General de Radio Dirección de Producción Dirección de Planeación y Programación de Radio Dirección de Modelos Radiofónicos
Presidencia Secretaría Técnica

8. Ciclo de vida de los Datos Personales

De conformidad con la fracción I del artículo 33 de la LGPDPPSO, para establecer y mantener las medidas de seguridad para la protección de los datos personales, se deberán crear políticas internas para su gestión y tratamiento que consideren el contexto en el que ocurren los tratamientos, así como el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior eliminación.

Debido a ello, la fracción IV del artículo 56 de los Lineamientos Generales, estipula que, en el diseño e implementación de las políticas internas para la gestión y el tratamiento de los datos personales, se deberá incluir la identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando su:

- **Obtención;**
- **Almacenamiento;**
- **Uso:**
  - » Acceso,
  - » Manejo,
  - » Aprovechamiento,
  - » Monitoreo,
  - » Procesamiento (incluidos los sistemas que se utilizan para tal fin);
- **Divulgación:**
  - » Remisiones,
  - » Transferencias**;**
- **Bloqueo;**
- **Cancelación, supresión o destrucción.**

Cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados.

Fuente: Guía de apoyo para la elaboración del Documento de Seguridad, INAI (2022)

De este modo, en cada tratamiento se deberá realizar lo siguiente:

1. Relacionar las operaciones que integran el tratamiento de los datos personales con las etapas del ciclo de vida.

a) Etapa de obtención: las concernientes a la forma en que se recaban los datos personales.
b) Etapa de uso: aquellas que permiten concretar la finalidad del tratamiento.
c) Etapa de archivo: las relativas al archivo del documento, en los términos previstos en el Catálogo de Disposición Documental[16] (CADIDO SPR).
d) Etapa de eliminación: las acciones relativas a la baja documental o, en su caso, su destrucción.

2. Definidas las etapas que preceden, el ciclo de vida de los datos personales de cada tratamiento estará determinado.

1 - Artículo 4, fracción XIII de la Ley General de Archivo lo define como el registro general y sistemático que establece los valores documentales, la vigencia documental, los plazos de conservación y la disposición documental.

De conformidad con el artículo 24 de la LGPDPPSO, cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento, deberán ser suprimidos, previo bloqueo, en su caso, y una vez que concluya su plazo de conservación.

El bloqueo de los datos personales consiste en la identificación y conservación de los datos una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con el periodo de su tratamiento, hasta que concluya el plazo de vigencia documental o, en su caso, de prescripción legal. Periodo en el que, los datos personales no podrán ser objeto de tratamiento.

Una vez transcurrido el bloqueo de los datos personales, se procederá a su eliminación, de conformidad con el procedimiento de baja archivística que se prevea para tal propósito. Cada unidad administrativa deberá mantener identificado el ciclo de vida de los datos personales que recabe y el periodo de bloqueo de la totalidad de los tratamientos que efectúen en ejercicio de sus funciones.

En términos de lo establecido en el artículo 23 de la LGPDPPSO, se deberán adoptar las medidas necesarias para mantener los datos personales exactos, completos, correctos y actualizados, a fin de que no se altere su veracidad.

No obstante, cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo, en su caso, y una vez que concluya su plazo de conservación.

Al respecto, el artículo 23 de los Lineamientos Generales estipula que se deberán establecer políticas, métodos y técnicas orientadas a la supresión definitiva de los datos personales, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima.

En el establecimiento de las políticas, métodos y técnicas a que se refiere el párrafo anterior, se deberán considerar los medios de almacenamiento físicos y/o electrónicos en los que se encuentren los datos personales, así como los atributos siguientes:

Irreversibilidad: que el proceso utilizado no permita recuperar los datos personales.
Seguridad y confidencialidad: que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la LGPDPPSO y los Lineamientos Generales.
Favorables al medio ambiente: que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.

9. Sistema de gestión de los Datos Personales

Para el tratamiento de los datos personales que lleva a cabo el Sistema Público de Radiodifusión del Estado Mexicano, se garantiza el tratamiento de estos como parte de sus funciones, desde su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación aplicable a los mismos. Se realiza mediante el establecimiento de políticas y métodos orientados a salvaguardar la confidencialidad, integridad y disponibilidad, conforme a los preceptos previstos en la LGPDPPSO y los Lineamientos Generales.

En tal virtud, el SPR inicio su proceso de planificación de los esquemas de protección de datos mediante la identificación de todos y cada uno de los procesos en los que, de acuerdo con el ámbito de sus funciones, las distintas áreas y unidades administrativas que conforman al Sistema, se involucra el tratamiento de datos personales. Para ello, se dispuso de un formato que permitió a las diversas unidades administrativas el levantamiento de inventarios de los datos personales que se encuentran bajo su responsabilidad, considerando los elementos mínimos que establecen los artículos 33, fracción II de la LGPDPPSO y el 58 de los Lineamientos Generales.

A través del desarrollo de un instrumento homogéneo y estandarizado, se llevó a cabo el levantamiento del Inventario de Datos Personales, con el propósito de identificar, entre otros aspectos, la categoría y tipo de datos que son sometidos a tratamiento, incluyendo los de carácter sensible; los medios a través de los cuales se obtienen dichos datos; el sistema físico y/o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; las características del lugar donde se ubican las bases físicas o electrónicas de datos; las finalidades del tratamiento, y el nombre, cargo y adscripción de las personas prestadoras de servicios profesionales por honorarios que tienen acceso al tratamiento, además de si son objeto de la transferencia y la identificación de los destinatarios o receptores de los mismos, así como las causas que la justifican.

En ese mismo sentido, el inventario ha contribuido desde el punto de vista operativo a considerar el ciclo de vida de los datos personales, de tal forma que las personas prestadoras de servicios profesionales por honorarios que intervienen en el tratamiento conocen que, una vez concluida la finalidad de los datos, éstos deben ser sometidos a un proceso de bloqueo y, en su caso, de cancelación, supresión o destrucción, lo que cobra especial relevancia en el marco del proceso de baja documental que las unidades administrativas realizan conforme a las disposiciones que regulan la gestión documental al interior del Sistema.

De igual forma, una vez integrado el Inventario de Datos Personales, se dispuso de la metodología para la elaboración del análisis de riesgos, en la cual, atendiendo a lo previsto en el artículo 33, fracción IV de la LGPDPPSO, las áreas responsables de los tratamientos identificaron el valor de los datos personales de acuerdo con su categoría y el ciclo de vida; el valor de exposición de los activos involucrados en el tratamiento; las consecuencias que pueden generarse para las personas titulares de los mismos con motivo de su posible vulneración y los factores de riesgo a los que eventualmente se encuentran expuestos.

También se han detectado nuevas medidas de seguridad que deberán desarrollarse para fortalecer algunos de los controles que actualmente son implementados; es decir, estarán contenidas en el análisis de brecha, a partir del cual será posible mitigar los riesgos a los que están expuestos los datos tratados.

Considerando que la identificación de vulnerabilidades tiene por objeto prevenir posibles dificultades en la seguridad de los datos bajo un enfoque proactivo; es decir, identificar áreas de oportunidad en materia de seguridad de los datos personales sin que éstas constituyan un daño efectivo, es que se enlistan como posibles vulnerabilidades las siguientes:

1. Control de acceso físico inadecuado a sistemas de archivos.
2. Deficiente conocimiento de procedimientos en materia de seguridad de los datos.
3. Inadecuada administración de autorizaciones de acceso a los datos personales (privilegios).
4. Falta de seguimiento y monitoreo a las políticas de seguridad.
5. Ausencia de mecanismos de confidencialidad por parte de los prestadores de servicios profesionales por honorarios.

Aunado a las anteriores vulnerabilidades, de manera enunciativa más no limitativa, se examinan algunos tipos de amenazas, que pueden ser intencionales o no, a las que podría enfrentarse el SPR y sus activos de información:

TIPOS DE AMENAZAS
Robo, extravío o copia no autorizada.
Uso, acceso o tratamiento no autorizado.
Daño, alteración o modificación no autorizado.
Pérdida o destrucción no autorizada.
Otras.

El riesgo que de manera general puede presentarse en caso de que las amenazas señaladas exploten las vulnerabilidades, es el de facilitar el acceso a los datos personales de manera no autorizada con el fin de comprometer su confidencialidad, disponibilidad e integridad, por lo que las medidas de seguridad por parte de las áreas están orientadas a proteger los datos personales.

A partir de la identificación de vulnerabilidades y amenazas, se han establecido medidas de seguridad generales, que de acuerdo con la experiencia y mejores prácticas son monitoreadas para lograr la mejora continua por parte de todas las personas involucrados en el tratamiento. Como parte del sistema de gestión y política de seguridad institucional, se enmarcan las reglas generales siguientes:

a) Tratar datos personales de manera lícita, conforme a las disposiciones establecidas en la LGPDPPSO;
b) Sujetar el tratamiento de los datos personales al principio de consentimiento, salvo las excepciones previstas por la Ley;
c) Informar a las personas titulares del tratamiento de los datos y sus finalidades;
d) Procurar que los datos personales tratados sean correctos y estén actualizados;
e) Suprimir los datos personales cuando hayan dejado de ser necesarios para las finalidades para las cuales se obtuvieron;
f) Tratar los datos personales estrictamente para propósitos legales o legítimos del SPR;
g) Limitar el tratamiento de los datos personales al cumplimiento de las finalidades;
h) No obtener datos personales a través de medios fraudulentos;
i) Respetar la expectativa razonable de privacidad de la persona titular;
j) Tratar estrictamente los datos personales necesarios, adecuados y relevantes en relación con las finalidades;
k) Velar por el cumplimiento de los principios;
l) Establecer y mantener las medidas de seguridad;
m) Guardar la confidencialidad de los datos personales;
n) Identificar el flujo y ciclo de vida de los datos personales;
o) Mantener actualizado el Inventario de Datos Personales o de las categorías que maneja el SPR;
p) Respetar los derechos de las personas titulares en relación con sus datos personales;
q) Identificar a las personas prestadoras de servicios profesionales por honorarios del SPR responsables del tratamiento de datos personales, y;
r) Aplicar las excepciones contempladas en la normativa en materia de protección de datos personales.

Con base en lo anterior, el SPR determina las pautas de acción de las personas prestadoras de servicios profesionales por honorarios encarados del tratamiento de datos personales con miras a generar su correcto resguardo, buscando en todo momento actuar en apego a las directrices de la LGPDPPSO y los Lineamientos Generales, siempre en consideración de la salvaguarda del derecho a la privacidad y protección de datos de las personas.

10. Inventario de Datos Personales y de los Sistemas de Tratamiento

En términos de lo dispuesto por los artículos 33, fracción III; 35, fracción I de la LGPDPPSO; 58 y 59 de los Lineamientos Generales; el Inventario describe las gestiones que se llevan a cabo por cada unidad administrativa, en relación con el ciclo de vida de los datos personales.

Por Inventario de Datos Personales, se entiende el control documentado del conjunto de operaciones que realizan las unidades administrativas que integran al Sistema Público de Radiodifusión del Estado Mexicano con motivo de los datos que se recaban de las personas, a través de procedimientos automatizados o físicos, que van desde su obtención, registro, organización, conservación, utilización, cesión, difusión, interconexión, hasta la rectificación, cancelación y oposición, con motivo de la atención del ejercicio de estos derechos en el ámbito de sus atribuciones.

En una primera parte el Inventario describe de manera general atribuciones de la unidad administrativa y los procesos relacionados con el tratamiento, incluye el listado del tipo de datos personales que contiene el sistema, y cuestiones relativas a la primera etapa de ciclo de vida de los datos "obtención", la finalidad y el consentimiento que corresponda de acuerdo con el contexto de vida del dato:

1. Catálogo de los datos personales contenidos en el sistema de tratamiento.
2. Identifica cómo obtienen los datos personales.
3. Catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales.
4. Finalidades del tratamiento explícitas y concretas, distinguir si alguna requiere el consentimiento.
5. Se divulgan los datos personales, fundamento.

En tal virtud, en coordinación con las unidades administrativas y derivado del proceso de actualización de la información, se advirtió que, en general 8 de las 9 unidades administrativas que conforman la estructura del Sistema realizan tratamiento de datos personales. A partir de lo anterior, el SPR elaboró los inventarios de los distintos tratamientos de datos personales que realiza, como se muestra a continuación:

No.	Denominación del Inventario de Tratamiento de Datos Personales	Unidad administrativa responsable del tratamiento
1	Proveedores de bienes y servicios	Unidad de Administración y Finanzas
2	Expediente de personal	
3	Comité de ética	
4	Servicio social y prácticas profesionales	
5	Nómina	
6	Curriculum vitae	
7	Registro de entradas y salidas del inmueble	
8	Servicio Médico	
9	Representación y defensa jurídica en asuntos jurisdiccionales, contencioso-administrativo y ante toda clase de autoridad	Dirección General de Asuntos Jurídicos y Transparencia
10	Trámite de solicitudes de acceso a la información y de protección de datos personales	
11	Contacto con la Defensoría	Defensoría de las Audiencias
12	MXPlus TV	Dirección General de Convergencia e Innovación Tecnológica
13	Contacto Canal Catorce	Dirección General de Canal Catorce
14	Mensajería instantánea Canal Catorce	
15	Participantes de los programas de Canal Catorce y autorización expresa de uso de imagen y voz	
16	Programa para la producción de contenidos audiovisuales de productores y productoras nacionales independientes	
17	Taller de incubadoras sonoras	Dirección General de Radio
18	Contacto Altavoz Radio	
19	Participantes de los programas de Altavoz Radio y autorización expresa de uso de imagen y voz	
20	Convocatorias Toma el Altavoz y Hagamos Radio en Colectividad	
21	Mensajería instantánea Altavoz Radio	
22	Convocatoria Programa de Capacitación Periodismo Multimedia para los Medios Públicos	Secretaría Técnica
23	Fans y usuarios de las plataformas digitales vinculadas con la promoción y difusión del quehacer institucional del SPR.	Dirección General de Comunicación y Redes
24	Contacto con Infodemia Mx	
25	Representantes de medios de comunicación que cubren actividades del SPR	
26	Participantes, ponentes y asistentes en los proyectos multiplataforma vinculados con el acontecer informativo nacional, internacional e institucional del SPR	

Asimismo, durante el proceso de sistematización se observó que los datos personales cuyo tratamiento se lleva a cabo en los 26 procesos identificados, corresponden a las siguientes 3 categorías:

1. De identificación: nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros), CURP, RFC, año de nacimiento o edad, domicilio, firma, antecedentes laborales, cédula profesional, características físicas, correo electrónico, sexo, currículum vitae, datos académicos, datos de identificación, datos laborales, ocupación, nacionalidad, teléfono fijo o celular, datos personales contenidos en documento para acreditar personalidad del representante, datos personales contenidos en la identificación oficial presentada por la persona física, huella dactilar, huella digital, menor de edad, nivel educativo, imagen de la persona participante, voz de la persona participante, etcétera.

2. Patrimoniales: cuentas bancarias, estados de cuenta bancarias, CLABE interbancaria, institución bancaria, información fiscal, pensión alimenticia, descuentos por concepto de primas de seguros, etcétera.

3. Sensibles: datos de salud, tipo de sangre.

A partir de lo anterior, el Inventario de Datos Personales del Sistema Público de Radiodifusión del Estado Mexicano posibilitó la identificación de hallazgos en relación con el tratamiento de datos personales, aportando los elementos que permiten focalizar las áreas con mayor incidencia en el tratamiento de éstos y, con ello, enfocar los trabajos de atención para el cumplimiento de las disposiciones jurídicas en materia de protección de datos.

Sobre el particular, se identificó que por lo que hace al tratamiento de ***datos de identificación***, en las 8 unidades administrativas aludidas se llevan a cabo tratamiento de datos de esta naturaleza; por lo que hace a los ***patrimoniales*** en 1 de ellas se realiza tratamiento de éstos, y por lo que hace a los ***sensibles***, únicamente 1 unidad administrativa trata este tipo de datos.

Lo anterior, permite advertir que la categoría de datos personales con mayor número de áreas y procesos son los de ***carácter identificativo***, seguidos por los patrimoniales y, en casos muy específicos, los datos de naturaleza sensible. Sin embargo, es preciso indicar que se detectaron procesos en los que se realiza tratamiento de datos tanto identificativos y patrimoniales, otro con identificativos, patrimoniales y sensibles.

La Unidad de Administración y Finanzas posee el mayor número de procesos en las que intervienen tratamientos de datos personales, dada la naturaleza de sus funciones, toda vez que entre las áreas que la integran se encuentran aquellas

con atribuciones para administrar los recursos humanos y materiales del Sistema, por lo que el hallazgo en sí mismo representa un insumo imprescindible para el cumplimiento de sus funciones. Por tal motivo, las áreas de atención, oportunidad y verificación en materia de protección de datos deben contar con un enfoque de importancia en el desarrollo de las actividades de esta unidad administrativa.

Debe destacarse que, si bien la Unidad de Administración y Finanzas es la unidad administrativa con más operaciones en las que converge el tratamiento de datos, también lo es que todas las demás, en menor medida, cuentan con áreas en las que se implementa algún tipo de proceso de tratamiento de datos, por lo que la protección debe ser entendida como una acción de frecuencia generalizada.

Ante este contexto, es dable concluir que el Inventario de Datos Personales del SPR, a partir de los hallazgos identificados en su actualización, se constituye como un elemento del Sistema de Gestión de Datos Personales, que junto con las medidas de seguridad representa un instrumento de evidencia para la implementación de las directrices de la Política en Materia de Protección de Datos Personales. Asimismo, delinea las rutas para una capacitación focalizada en materia de protección de datos en aras de fortalecer la estructura de las personas que operan en cada uno de los procesos en que se tratan datos, buscando con ello sensibilizar y preparar a las personas responsables y encargadas de estos para que su tratamiento se lleve a cabo de conformidad con los estándares nacionales e internacionales en la materia.

10. Funciones y Obligaciones de las personas que traten datos personales

En relación con lo establecido en los artículos 33, fracción II de la LGPDPPSO y 57 de los Lineamientos Generales, se deben señalar y documentar los roles y responsabilidades del personal que, en el ejercicio de sus atribuciones y funciones, administren o realicen tratamientos de datos personales.

Serán aplicables al tratamiento de datos personales que obren en soportes físicos y/o electrónicos, con independencia de la forma o modalidad de su creación, procesamiento, almacenamiento y organización. Los datos personales podrán ser expresados en forma numérica, alfabética, gráfica, alfanumérica, fotográfica, acústica o en cualquier otro formato.

Todos las personas prestadoras de servicios profesionales que tengan acceso a los datos personales, están obligados a conocer y aplicar las medidas de seguridad propias de cada Sistema en el que se concentren los datos y es aplicable en todas y cada una de las fases del tratamiento de los datos personales, iniciando desde la obtención de los mismos y finalizando su participación en el tratamiento de los datos personales porque hayan cambiado de funciones y aun cuando la relación laboral con el SPR haya concluido.

Además de las funciones y obligaciones de las personas servidoras públicas y/o prestadoras de servicios profesionales involucrados, establecidas de manera específica en el análisis de cada uno de los sistemas, de manera general deberán de observarse las siguientes:

OBLIGACIONES

- Tratar los datos personales con responsabilidad y las medidas de seguridad que se hayan establecido para tal fin.
- Guardar confidencialidad sobre la información que conozcan en el desarrollo de sus actividades.
- Tomar capacitaciones en materia de protección de datos personales.
- Dar aviso a las personas superiores jerárquicas, ante cualquier acción que pueda poner en riesgo los datos personales, y en general que puedan vulnerar la seguridad de los datos personales.
- Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

- Tratar los datos personales para finalidades concretas, licitas, explícitas y legítimas en ejercicio a las facultades y atribuciones que la normatividad aplicable le confiera.
- Evitar la obtención y tratamiento de datos personales, a través de medios engañosos o fraudulentos.
- Privilegiar la protección de los intereses de la persona titular de los datos y la expectativa razonable de privacidad.
- Tratar los datos personales previo consentimiento, expreso o tácito, otorgado por la persona titular de manera libre, específica e informada; salvo cuando se actualice alguna de las causales de excepción previstas en el artículo 22 de la LGPDPPSO.
- Obtener el consentimiento expreso y por escrito de la persona- titular para su tratamiento, tratándose de datos personales sensibles, salvo en los casos previstos en el artículo 22 de la LGPDPPSO.
- Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.
- Establecer los plazos de conservación de los datos personales tomando en consideración las finalidades que justificaron su tratamiento y las disposiciones aplicables en materia de protección de datos personales, así como los aspectos administrativos, contables, fiscales, jurídicos e históricos de los mismos.
- Suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento, previo bloqueo, en su caso, y una vez que concluya el plazo de conservación de estos.
- Informar a la persona titular, a través del aviso de privacidad, que deberá ser difundido por medios electrónicos y físicos, la existencia, características principales y finalidades del tratamiento al que serán sometidos sus datos personales.
- Instrumentar medidas compensatorias de comunicación masiva cuando resulte imposible dar a conocer al titular el aviso de privacidad, de manera directa o ello exija esfuerzos desproporcionados.
- Establecer y mantener las medidas de seguridad de carácter administrativo, físicos y técnicos para la protección de los datos personales, que permitan salvaguardarlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.
- Dar aviso a la Unidad de Transparencia de los nuevos tratamientos de datos personales que se pretendan realizar.

El incumplimiento a lo establecido en el Documento de Seguridad, así como a lo establecido por la LGPDPPSO y los Lineamientos Generales, causará la aplicación de las medidas de apremio y/o sanciones, que se detallan en dichos instrumentos normativos.

12. Análisis de riesgos, análisis de brecha y plan de trabajo

El análisis de riesgo tiene fundamento en los artículos 6° y 16 de la Constitución Política de los Estados Unidos Mexicanos; 33, fracción IV, y 35, fracción III, de la LGPDPPSO; así como 59 y 60 de los Lineamientos Generales.

Bajo este marco normativo, el análisis de riesgos de los datos personales tratados considera lo siguiente:

- Los requerimientos regulatorios, 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 a los que se refiere el artículo 32 de la LGPDPPSO.[17]

METODOLOGÍA PARA EL ANÁLISIS DE RIESGOS

La seguridad de los datos personales se basa en el entendimiento de la naturaleza del riesgo al que están expuestos. En algún caso, el riesgo no se podrá erradicar completamente, pero sí minimizar a través de la mejora continua.

De manera general, el riesgo atiende a la combinación de la probabilidad de que una vulneración ocurra y las consecuencias desfavorables que genere, de modo tal que, al determinar el riesgo en el escenario de la organización del SPR, se podría evaluar el impacto y así realizar un estimado de las medidas de seguridad necesarias para preservar la información personal. Riesgo= Probabilidad de Amenaza x Magnitud de Daño.

17 - Artículo 32. Las medidas de seguridad adoptadas por el responsable deberán considerar:
I. El riesgo inherente a los datos personales tratados;
II. La sensibilidad de los datos personales tratados;
III. El desarrollo tecnológico;
IV. Las posibles consecuencias de una vulneración para los titulares;
V. Las transferencias de datos personales que se realicen;
VI. El número de titulares;
VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
VIII. 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.

En este contexto, los elementos para analizar los riesgos de los recursos involucrados en el tratamiento de datos personales son:

1) Identificación de activos de apoyo

Un activo es un recurso (ya sea material o físico, como documentos, servicios, prácticas, políticas, instalaciones; técnico como software o hardware, o humano como personas, etc.) que tiene valor para la organización del SPR y necesite por tanto ser protegido de potenciales riesgos. Los activos por evaluar serán aquellos que estén relacionados con el ciclo de vida de los datos personales previamente identificados y sus distintos tratamientos. Estos se deben revisar con suficiente nivel de detalle para proveer información que permita hacer la valoración del riesgo.

De acuerdo con el artículo 59 de los Lineamientos Generales se pueden identificar tres tipos de activos de apoyo:

- **Técnicos:**
  - Hardware (equipo de procesamiento de datos como computadoras, servidores, equipo móvil, periféricos).
  - Software (sistemas operativos como CPU, memoria, discos, procesos, aplicaciones; sistemas de servicio como antivirus, paquetería de software, administradores de bases de datos, mensajería instantánea, servidores web).
  - Redes y Telecomunicaciones (medios y equipos).
  - Soportes electrónicos (discos ópticos como CD´S y DVD´S, cintas de audio, videos y datos, discos duros removibles, memorias USB).

- **Material:**
  - Papel escrito a mano o impreso, transparencias, fotografías, expedientes, documentos.
  - Infraestructura adicional (edificios, coches, instalaciones, etc.).
  - Estructura organizacional (políticas, servicios, prácticas).

- **Humano:**
  - Personas servidoras públicas y/o prestadoras de servicios profesionales del SPR.

Después de identificar y describir los activos de apoyo, se podrán encontrar sus vulnerabilidades y posibles amenazas. Además, el custodio del activo (responsable del sistema de tratamiento) se quedará a cargo de proveer la adecuada rendición de cuentas de cada uno de ellos, señalando que el custodio del activo no podrá ejercer la propiedad de éste, pero tendrá responsabilidad sobre su mantenimiento y seguridad.

2) Identificación de amenaza

La amenaza tiene el potencial de dañar un activo y causar una vulneración a la seguridad. Las amenazas pueden ser de origen natural o humano, accidentales o deliberadas y provenir de adentro o de fuera del SPR. Las amenazas deben ser identificadas considerando que algunas pueden afectar a más de un activo al mismo tiempo.

Los responsables de los activos y sus usuarios pueden solicitar asesoría para identificar y estimar las amenazas relacionadas, por ejemplo, del área de recursos humanos, de los administradores de tecnologías y seguridad, profesionales en seguridad física, de asuntos jurídicos, externos como compañías de seguros. Los aspectos culturales también deben ser considerados dentro de las amenazas. Entre otras:

Amenazas a los activos	
Fuego	Alteración de hardware
Agua	Alteración de software
Contaminación	Rastreo de localización
Accidentes	Fallas del equipo
Polvo, corrosión, humedad, congelamiento	Mal funcionamiento del equipo
Fenómenos climáticos o meteorológicos	Saturación de los sistemas de información
Fenómenos sísmicos	Mal funcionamiento del software
Fenómenos volcánicos	Falla en el mantenimiento del sistema de información
Falla en el sistema de aire acondicionado o suministro de agua	Uso no autorizado de equipo
Pérdida de suministro eléctrico	Uso de software copiado o falsificado
Falla en los equipos de telecomunicaciones	Corrupción de datos
Intercepción e interferencia de señales	Procesamiento ilegal de los datos
Espionaje remoto	Error de uso
Escucha en comunicaciones	Abuso de privilegios
Robo de medios o documentos	Falsificación de privilegios
Robo de equipo	Denegación de acciones
Recuperación de medios desechados o reciclados	Indisponibilidad del personal
Revelación	Falta de capacitación
Fuentes poco confiables para la obtención de datos	Extorsión

3) Probabilidad de que ocurra una amenaza

No todas las amenazas tienen la misma posibilidad de que ocurran, debido a que habrá algunas que su presencia sea remota y otras que la probabilidad pueda ser alta. Por cada amenaza, la unidad administrativa, dada su experiencia y conocimiento de los activos y las amenazas, debe evaluar la posibilidad de ocurrencia de esta.

4) Conocimiento de vulnerabilidades por activo

La vulnerabilidad es la capacidad, las condiciones y características propias de los activos, que lo hacen susceptible a amenazas, con el resultado de sufrir un daño. Una vulnerabilidad es una debilidad en el funcionamiento o seguridad del activo y pueden ser identificadas en los siguientes ámbitos:

- Organizacionales.
- De procesos y procedimientos.
- De personal.
- Del ambiente físico.
- De la configuración de sistemas de información.
- Del hardware, software o equipo de comunicación.
- De la relación con prestadores de servicios.
- De la relación con terceros.

La presencia de vulnerabilidades por sí misma no causa daño, se requiere de una amenaza que la explote. Una vulnerabilidad que no se encuentre expuesta a una amenaza identificada posiblemente no requiera la implementación de un control, pero debe ser reconocida y monitoreada constantemente, o bien cuando surja algún cambio.

Por su parte, las medidas de seguridad usadas incorrectamente o con una mala implementación son una causa de vulnerabilidad. Una medida puede ser efectiva o no, dependiendo del contexto en el cual opera. Las vulnerabilidades pueden estar relacionadas a propiedades de los activos que a su vez pueden ser usadas para propósitos distintos a los que se habían destinado originalmente.

En este sentido, en un primer ejercicio, respecto a vulnerabilidades atinentes a procesos, organización, procedimientos y a fin de complementar el análisis de riesgos, es necesaria una revisión de las **prácticas, actividades, servicios, procedimientos o políticas** que se utilicen en cada sistema de tratamiento, a fin de advertir en éstos, aspectos que pudieran comprometer la privacidad o protección (confidencialidad, disponibilidad y/o integridad) de los datos personales involucrados.

5) Estimado del impacto a los activos a través de la identificación del posible daño (evaluación del riesgo).

El riesgo se evalúa contemplando dos elementos básicos. El primero es el estimado del impacto negativo, bajo, medio o alto, a los activos, y el segundo es la identificación del posible daño. Se pretende determinar el daño que el riesgo pudiera causar a los activos, si es tolerable o debe mitigarse.

Se considera que el determinar el riesgo inherente a los datos personales tratados es un deber de los sujetos obligados en la adopción de medidas de seguridad, para lo que deben realizar un análisis que considere las amenazas y vulnerabilidades para los datos, así como los recursos involucrados en el tratamiento.

Derivado de lo anterior, la valoración de los riesgos de los datos personales forma parte de los elementos mínimos que debe contener el instrumento que describe y da cuenta, en lo general, sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas (Documento de Seguridad), en este caso, por el Sistema, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de ese tipo de datos bajo su posesión.

Aunado a lo anterior, el análisis de riesgos de los datos personales tratados debe contemplar los siguientes aspectos:

- 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.
- Las consecuencias negativas para los titulares de los datos personales, que puedan derivar en una vulneración de seguridad.
- El riesgo inherente, la sensibilidad, las posibles consecuencias de vulneración para las personas titulares, las transferencias y vulneraciones previas ocurridas sobre los datos personales, así como el número de titulares de éstos y el riesgo por su valor potencial, además del desarrollo tecnológico.

Análisis de la información

Estado actual de riesgo de datos personales, en general se tiene que el SPR cuenta con 8 unidades administrativas en las que se da tratamiento de datos personales mediante 26 procesos, tal y como se visualiza a continuación:

Unidad administrativa	Tratamientos
Unidad de Administración y Finanzas	8
Dirección General de Asuntos Jurídicos y Transparencia	2
Dirección General de Convergencia e Innovación Tecnológica	1
Dirección General de Canal Catorce	4
Dirección General de Radio	5
Dirección General de Comunicación y Redes	4
Defensoría de las Audiencias	1
Secretaría Técnica	1
TOTAL	**26**

Bajo esta premisa, para analizar los riesgos de los datos personales que son objeto de tratamiento en el SPR, se aplicó un instrumento para clasificar los datos utilizados, a partir de la categorización existente en la ley:

1. De identificación o contacto: que se refieren a información por la que se identifica a una persona y/o permiten su contacto como, por ejemplo, el nombre, domicilio, correo electrónico, teléfono, firma, estado civil, lugar y fecha de nacimiento, nacionalidad, Registro Federal de Contribuyentes, Clave Única de Registro de Población, etcétera.

2. Patrimoniales: que comprenden la información que se encuentra vinculada al patrimonio de una persona como, por ejemplo, el salario, los créditos, las tarjetas de débito, historial crediticio, información fiscal, egresos, seguros, afores, sueldos y salarios.

3. Sensibles: que consideran la información concerniente a la esfera más íntima de su titular o que su uso puede dar origen a discriminación o conlleva un riesgo grave para éste como, por ejemplo, el origen étnico, estado de salud (presente o futuro), creencias religiosas, filosóficas o morales, afiliación sindical, opinión política, preferencia sexual, etcétera.

Para la determinación del riesgo sobre esa tipología de datos personales se valoró la probabilidad e impacto de que, en su obtención, almacenamiento, tratamiento, transferencia o remisión, bloqueo y/o eliminación (ciclo de vida), en correspondencia con la cantidad de datos involucrados, se materialice uno o más factores que pueden causar un daño a su titular (amenaza).

Para el desarrollo del análisis, se recuperaron cuatro tipos de amenazas sustentados en la Ley:

- Robo, extravío o copia no autorizada.
- Uso, acceso o tratamiento no autorizado.
- Daño, alteración o modificación no autorizado.
- Pérdida o destrucción no autorizada.

Esto es, se tomó en cuenta la probabilidad baja, media o alta de que la amenaza suceda en las distintas etapas de vida de los datos personales. Así, se consideró la consecuencia desfavorable leve, moderada o grave que a la persona titular provoca en caso de que la amenaza ocurra (impacto). La identificación y valoración del riesgo en cada proceso en que se tratan datos personales por las unidades administrativas que integran el SPR se basaron en una escala de 1 al 3, representándose de la siguiente forma:

Tipo de dato	Riesgo inherente	Nivel de riesgo
Datos identificativos	Bajo	1
Datos patrimoniales, laborales, procedimientos administrativos	Medio	2
Datos sensibles	Alto	3

Los riesgos que se identifican y las medidas de seguridad[18] que se definan quedan documentados, con el objetivo de evidenciar la evaluación de riesgos realizada y tener una base de trabajo ante futuras revisiones del análisis, derivadas de cambios en las actividades de tratamiento. Por último, una adecuada gestión de riesgos requiere un proceso de identificación, evaluación y tratamiento de los riesgos y vulneraciones a los que está expuesta una actividad de tratamiento. Una vez que se presente una vulneración a la seguridad de los datos personales que obren bajo su resguardo deberá atender el procedimiento ante vulneraciones a la seguridad de datos personales, sobre lo que además de la LGPDPPSO y los Lineamientos Generales, también deben consultarse las Recomendaciones para el manejo de incidentes de seguridad de datos personales, emitidas por el INAI, en junio 2018.

MATRIZ PARA EL ANÁLISIS DE RIESGOS[19]

TABLA PARA ESTIMAR LA PROBABILIDAD	
VALOR	**DESCRIPCIÓN**
Bajo (1)	La amenaza se materializa a lo sumo una vez cada año.
Medio (2)	La amenaza se materializa a lo sumo una vez cada mes.
Alto (3)	La amenaza se materializa a lo sumo una vez cada semana.
TABLA PARA ESTIMAR EL IMPACTO	
VALOR	**DESCRIPCIÓN**
Bajo (1)	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para los derechos del titular.
Medio (2)	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para los derechos del titular.
Alto (3)	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para los derechos del titular.
CRITERIOS DE ACEPTACIÓN DEL RIESGOt	
VALOR	**DESCRIPCIÓN**
Riesgo <= 4	La organización considera el riesgo poco reseñable.
Riesgo > 4	La organización considera el riesgo reseñable y debe proceder a su tratamiento.

18 - Medidas de seguridad se documentan en el respectivo inventario de sistema de tratamiento respectivo, así como en las respectivas matrices de medidas administrativas, físicas y técnicas.
19 - **NOTA:** En relación con los riesgos administrativos o normativos, es relevante señalar que, en el transcurso de los trabajos relativos al desarrollo de la gestión de riesgos, se advirtió la importancia de revisar las prácticas, la gestión relativa al uso de los datos frente al cumplimiento de la normativa en materia de datos personales. De cuyo resultado se obtiene como medida correctiva la necesidad de emitir políticas o procedimientos para un debido tratamiento de datos.

Etapa de mayor y menor vulnerabilidad

La identificación de la etapa de mayor o menor vulnerabilidad es el resultado de la valoración que se haga al distribuir porcentajes a las etapas de tratamiento (obtención, tratamiento, almacenamiento, transferencia, bloqueo y eliminación), analizando cuál es el riesgo para cada etapa, de acuerdo con las medidas de seguridad implementadas a los diferentes entornos.

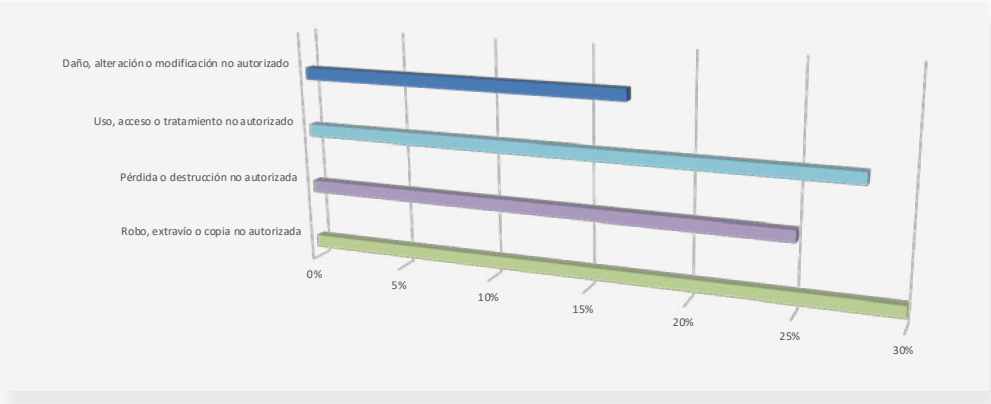
Al respecto, hay que señalar además que la etapa del ciclo de vida (obtención, tratamiento, almacenamiento, trasferencia, bloqueo y eliminación) en la que los datos personales se encuentran más vulnerables, es en el periodo de almacenamiento en un 30%; mientas que el periodo que implica menor riesgo es el de bloqueo con 3%, como se aprecia a continuación:

Obtención	20%
Tratamiento	22%
Almacenamiento	30%
Transferencia	20%
Bloqueo	3%
Eliminación	5%
Total	**100%**

Las amenazas a las que se ven expuestos son básicamente:

- Robo, extravío o copia no autorizada.
- Uso, acceso o tratamiento no autorizado.
- Daño, alteración o modificación no autorizado.
- Pérdida o destrucción no autorizada.

Siendo la más alta, la de robo, extravío o copia no autorizada y la de menor riesgo es daño, alteración o modificación no autorizada, como se muestra en la siguiente tabla:



La unidad administrativa que observa mayor estado de vulnerabilidad y riesgo de los datos personales es la Dirección de Recursos Humanos con un riesgo de 2, después la Dirección General de Canal Catorce y la Dirección General de Asuntos Jurídicos y Transparencia, ambas con un riesgo de 1.5.

Finalmente, como parte del análisis es posible establecer que el nivel de riesgo es mayormente bajo debido que se trabaja sobre todo con datos de identificación, en algunos casos con datos patrimoniales y solo en un tratamiento se solicitan datos sensibles.

Asimismo, los datos personales corresponden a menos de 100 personas, lo que reduce el nivel de riesgo y se mantienen a resguardo en computadoras personales con contraseña y en archiveros con llave para ampliar el margen de seguridad.

Para el caso concreto del SPR, se puede deducir que si bien existen medidas físicas, técnicas y administrativas para la protección de los datos personales, también se concluye que varios de las personas responsables de los sistemas desconocen las obligaciones que establece la LGPDPPSO, sus atribuciones y funciones; por ello señalan que corresponde a otros y no a ellos ser garantes de las medidas de seguridad; también se aprecia que hay una percepción limitada respecto al ámbito de aplicación de las medidas de seguridad, ya que se considera que éstas son responsabilidad de la persona Encargada, y, por ende, solamente las medidas administrativas les resultan aplicables.

Esta situación genera riesgos porque, evidentemente, el desconocimiento de las normas y las medidas de seguridad acrecienta la probabilidad de que ocurra un incidente, lo que inevitablemente puede causar un impacto con un determinado daño en los sistemas de datos personales y entre ellos deben considerarse los siguientes:

Código de identificación del riesgo (CIR)	Descripción del riesgo	Nivel de impacto si el riesgo se materializa	Probabilidad de que se materialice
CIR 1	Tratar datos personales con motivos distintos de la finalidad para los que fueron recabados o sin contar con las atribuciones o funciones para ello.	Alto	Media
CIR 2	Obtener un consentimiento que no cumpla con los requisitos que establece la LGPDPPSO, para el tratamiento de datos personales.	Medio	Media
CIR 3	Acceso a los datos personales por parte de personas no autorizadas o sin atribuciones para ello.	Medio	Baja
CIR 4	Carencia o falta de supervisión de las medidas de seguridad de los sistemas de datos personales.	Medio	Media
CIR 5	Modificación, alteración o sustracción de datos personales por parte de personas no autorizadas o sin atribuciones para ello.	Alto	Alta
CIR 6	Desconocimiento de la necesidad de realizar procesos de Disociación para responder solicitudes de acceso a la información.	Medio	Baja
CIR 7	Elaboración de un contrato incompleto con la(s) persona(s) Encargada(s), en el que no se estipulen todos los apartados necesarios y las garantías adecuadas para la protección de los datos personales o la cláusula de confidencialidad.	Bajo	Baja
CIR 8	Dificultar el ejercicio de los derechos ARCO.	Bajo	Baja
CIR 9	Deficiente definición de funciones y competencias de la(s) persona(s) responsable(s), Encargado(s) y Usuaria(s).	Bajo	Alta
CIR 10	Falta de información a las personas prestadoras de servicios profesionales que tienen acceso a los sistemas de datos personales sobre las medidas de seguridad que están obligadas a observar y las consecuencias ante su omisión.	Medio	Alta
CIR 11	Falta de acciones para desincentivar la posibilidad de transmitir datos personales de manera ilícita por su valor (económico, político, social, laboral, etcétera) para terceros no autorizados.	Alto	Baja
CIR 12	Percepción errónea de capacidad legal para el tratamiento o cesión de datos personales, incluso entre responsables sin las formalidades que requiere la Ley.	Medio	Baja

El análisis de brecha, en términos de los artículos 33, fracción V, y 35, fracción IV, de la LGPDPPSO; así como el artículo 61 de los Lineamientos Generales es el que consiste en identificar soluciones para reducir, mitigar o aceptar el riesgo, y, por tanto, garantizar una protección integral de los datos personales. Es decir, se

trata de una herramienta que permite conocer el estado actual de las medidas de seguridad; si son suficientes para solucionar el riesgo identificado, o bien se requiere implementar otra medida.

La brecha permite precisamente identificar cuán lejos se está de donde se quiere llegar para obtener la solución. Una vez identificada la solución, es necesario planear cómo y con qué se va a cerrar esa brecha para lograr el objetivo.

En este sentido, al haberse conocido los riesgos en la seguridad de los sistemas de datos personales, es importante identificar las acciones necesarias para implantar las medidas que permitan evitar, eliminar o mitigar la probabilidad de que se materialicen y, por ende, impedir o reducir el impacto que podría generarse. En el SPR se identificaron los siguientes:

(CIR)	Descripción del riesgo	Medidas	Acciones
CIR 1	Tratar datos personales con motivos distintos de la finalidad para los que fueron recabados o sin contar con las atribuciones o funciones para ello.	Concientizar a las áreas y unidades administrativas responsables que realizan tratamiento de datos personales, la obligatoriedad de cumplir con el Principio de Finalidad.	-Elaborar el Documento de Seguridad, difundirlo en el SPR. -Brindar capacitación y asesoría de acompañamiento de manera permanente. -Supervisar el cumplimiento de las medidas de seguridad.
CIR 2	Obtener un consentimiento que no cumpla con los requisitos que establece la LGPDPPSO, para el tratamiento de datos personales.	Concientizar a las áreas y unidades administrativas responsables que realizan tratamiento de datos personales, la obligatoriedad de cumplir con el Principio de Lealtad.	-Elaborar el Documento de Seguridad, difundirlo en el SPR. -Brindar capacitación y asesoría de acompañamiento de manera permanente. -Supervisar el cumplimiento de las medidas de seguridad.
CIR 3	Acceso a los datos personales por parte de personas no autorizadas o sin atribuciones para ello.	Concientizar a las áreas y unidades administrativas responsables que realizan tratamiento de datos personales, la obligatoriedad de cumplir con el Principio de Responsabilidad.	-Elaborar el Documento de Seguridad, difundirlo en el SPR. -Brindar capacitación y asesoría de acompañamiento de manera permanente. -Supervisar el cumplimiento de las medidas de seguridad.
CIR 4	Carencia o falta de supervisión de las medidas de seguridad de los sistemas de datos personales.	Concientizar a las áreas y unidades administrativas responsables que realizan tratamiento de datos personales, la obligatoriedad de cumplir con el Principio de Responsabilidad.	-Elaborar el Documento de Seguridad, difundirlo en el SPR. -Brindar capacitación y asesoría de acompañamiento de manera permanente. -Supervisar el cumplimiento de las medidas de seguridad.
CIR 5	Modificación, alteración o sustracción de datos personales por parte de personas no autorizadas o sin atribuciones para ello.	Concientizar a las áreas y unidades administrativas responsables que realizan tratamiento de datos personales, la obligatoriedad de cumplir con el Principio de Responsabilidad.	-Elaborar el Documento de Seguridad, difundirlo en el SPR. -Brindar capacitación y asesoría de acompañamiento de manera permanente. -Supervisar el cumplimiento de las medidas de seguridad.

(CIR)	Descripción del riesgo	Medidas	Acciones
CIR 6	Desconocimiento de la necesidad de realizar procesos de Disociación para responder solicitudes de acceso a la información pública	Concientizar a las áreas y unidades administrativas responsables de que la LGPDPPSO son de orden público y por ende se debe garantizar la observancia de los principios de protección de datos personales.	-Elaborar el Documento de Seguridad, difundirlo en el SPR. -Brindar capacitación y asesoría de acompañamiento de manera permanente.
CIR 7	Elaboración de un contrato incompleto con el Encargado, en el que no se estipulen todos los apartados necesarios y las garantías adecuadas para la protección de los datos personales o la cláusula de confidencialidad	Concientizar a las áreas y unidades administrativas responsables de que la LGPDPPSO son de orden público y por ende se debe garantizar la observancia de los principios de protección de datos personales.	-Elaborar el Documento de Seguridad, difundirlo en el SPR. -Brindar capacitación y asesoría de acompañamiento de manera permanente.
CIR 8	Dificultar el ejercicio de los derechos ARCO	Concientizar a las áreas y unidades administrativas responsables de que la LGPDPPSO son de orden público y por ende se debe garantizar la observancia de los principios de protección de datos personales.	-Elaborar el Documento de Seguridad, difundirlo en el SPR. -Brindar capacitación y asesoría de acompañamiento de manera permanente. -Supervisar el cumplimiento de las medidas de seguridad.
CIR 9	Deficiente definición de funciones y competencias del responsable, encargado y usuario(s)	Concientizar a las áreas y unidades administrativas responsables que realizan tratamiento de datos personales, la obligatoriedad de cumplir con el Principio de Licitud.	-Elaborar el Documento de Seguridad, difundirlo en el SPR. -Brindar capacitación y asesoría de acompañamiento de manera permanente. -Supervisar el cumplimiento de las medidas de seguridad.
CIR 10	Falta de información a los prestadores de servicios profesionales que tienen acceso a los sistemas de datos personales sobre las medidas de seguridad que están obligados a observar y las consecuencias ante su omisión.	Concientizar a las áreas y unidades administrativas responsables que realizan tratamiento de datos personales, la obligatoriedad de cumplir con el Principio de Responsabilidad.	-Elaborar el Documento de Seguridad, difundirlo en el SPR. -Brindar capacitación y asesoría de acompañamiento de manera permanente. -Supervisar el cumplimiento de las medidas de seguridad.
CIR 11	Falta de acciones para desincentivar la posibilidad de transmitir datos personales de manera ilícita por su valor (económico, político, social, laboral, etcétera) para terceros no autorizados.	Concientizar a las áreas y unidades administrativas responsables que realizan tratamiento de datos personales, la obligatoriedad de cumplir con los Principios de Responsabilidad, Licitud y Calidad.	-Brindar capacitación y asesoría de acompañamiento de manera permanente. -Supervisar el cumplimiento de las medidas de seguridad.
CIR 12	Percepción errónea de capacidad legal para el tratamiento de datos personales incluso entre responsables sin la formalidad que requiere la Ley.	Concientizar a las áreas y unidades administrativas responsables que realizan tratamiento de datos personales, la obligatoriedad de cumplir con el Principio de Responsabilidad.	-Elaborar el Documento de Seguridad, difundirlo en el SPR. -Brindar capacitación y asesoría de acompañamiento de manera permanente. -Supervisar el cumplimiento de las medidas de seguridad.

Plan de trabajo

Una vez que se cuenta con la medida de seguridad que se considera controlará el riesgo, de acuerdo con lo dispuesto en los artículos 33, fracción VI y 35, fracción V, de la LGPDPPSO, así como el 62 de los Lineamientos Generales, las unidades administrativas desarrollaron el Plan de Trabajo que prevé, además del plazo, los recursos personales y económicos que se requieren para implementarla.

En este sentido, para cada tratamiento dependiendo del análisis de brecha, se elabora un Plan de Trabajo para la implementación de las medidas de seguridad faltantes.

El plan de trabajo se elabora 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.

Para lo anterior, se consideraron los recursos designados, el personal interno en la organización de la unidad administrativa, y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

13. Mecanismos de monitoreo y revisión de las medidas de seguridad

Los artículos 33, fracción VII, 35, fracción VI de la LGPDPPSO y el 63 de los Lineamientos Generales establecen como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales; dichos mecanismos de monitoreo y revisión forman parte del documento de seguridad.

Cuando se genera, procesa, transfiere y almacena información referente a una persona identificada o identificable, es necesario garantizar su debida protección, por ello se deben implementar controles que aseguren la integridad, confidencialidad y disponibilidad de la información de datos personales. A continuación, se desarrollan las acciones de monitoreo y supervisión periódica para las medidas de seguridad del SPR:

Mecanismos de Monitoreo

Para los tratamientos de datos personales del SPR, se consideran los siguientes tipos de monitoreo

1) Revisión de cumplimiento del tratamiento de datos personales. Tiene el objetivo de asegurar que las personas servidoras públicas y/o prestadoras de servicios profesionales por honorarios realicen los tratamientos de datos personales en concordancia con lo dispuesto en la LGPDPPSO, los Lineamientos Generales, y demás normatividad que resulte aplicable.

Para ello, cuando se identifica algún cambio en la normatividad antes mencionada, se deberán realizar las siguientes actividades:

a. Revisar y, en su caso, actualizar los procesos involucrados en el tratamiento de datos personales.
b. Revisar y, en su caso, actualizar los avisos de privacidad, las funciones y obligaciones del personal y el Inventarios de Datos Personales, según corresponda.
c. Evaluar si hay cambios en las amenazas, vulnerabilidades o impacto de los riesgos relacionados con las modificaciones a la normativa, para actualizar los análisis de riesgos, análisis de brecha y plan de trabajo.
d. Revisar y, en su caso, adecuar los sistemas de tratamiento para cumplir con los cambios normativos.

2) Revisión del riesgo. Tiene el objetivo de identificar modificaciones a los riesgos identificados en los tratamientos de datos personales, para ello, se implementarán los siguientes monitoreos:

a. Monitoreo del entorno físico. Para la detección continua de amenazas y vulnerabilidades en el entorno físico, se cuenta con: (i) personal de vigilancia en los accesos al edificio del SPR, (ii) control de acceso de las personas prestadoras de servicios profesionales, (iii) control de acceso a través de bitácoras para visitantes y (iv) circuito cerrado de cámaras de vigilancia.

b. Monitoreo del entorno electrónico. Para la detección continua de amenazas y vulnerabilidades, la Dirección General de Convergencia e Innovación Tecnológica (DGCIT) cuenta con herramientas automatizadas de monitoreo (activo y pasivo), así como con bitácoras de los sistemas informáticos del SPR.

c. Actualización del plan de trabajo. Derivado del monitoreo del entorno físico o electrónico, se pueden realizar actualizaciones en el plan de trabajo en caso de que se identifiquen cambios en las amenazas, las vulnerabilidades o el impacto de los riesgos identificados. Estos cambios se pondrán a consideración de la DGCIT y el Comité de Transparencia.

d. Revisión de avances del plan de trabajo. La DGCIT y el Comité de Transparencia, revisarán los avances al plan de trabajo, identificando las acciones, fechas compromiso y, en su caso, las causas por las cuales no se está cumpliendo el plan de trabajo, para hacer los ajustes correspondientes al mismo.

e. Actualización tecnológica. Cuando se integren nuevos equipos de cómputo, servidores, aplicaciones o tenga lugar una migración tecnológica, se realizará una actualización del análisis de riesgo, análisis de brecha y plan de trabajo.

f. Vulneraciones a la seguridad de los datos personales. En caso de identificar un incidente de seguridad que involucre datos personales, el área que apoya en el análisis de riesgos, la DGCIT y el Comité de Transparencia se coordinarán para decidir sobre las acciones pertinentes para mitigar dicho incidente.

14. Programa de capacitación

En atención a lo dispuesto en los artículos 33, fracción VII, 35, fracción VII de la LGPDPPSO, así como el artículo 64 de los Lineamientos Generales, todo Documento de Seguridad debe incluir un programa general de capacitación que actualice de forma permanente a las y los servidores públicos involucrados en el tratamiento de datos personales.

En ese contexto, las personas integrantes del Comité de Transparencia aprueban el Programa Anual de Capacitación en materia de Transparencia, Acceso a la Información, Protección de Datos Personales y temas relacionados. La capacitación se llevará a cabo en dos vertientes: básica y especializada.

Capacitación básica

El propósito de esta capacitación es que las personas conozcan los aspectos teóricos, conceptuales y normativos fundamentales en materia de protección de datos personales.

En este rubro, se considera el curso introductorio de la LGPDPPSO, mismo que será **OBLIGATORIO, para todas las personas servidoras públicas o prestadoras de servicios profesionales por honorarios del Sistema, con nivel de jefatura de departamento hasta mandos superiores,** sin perjuicio de que, sea **extensivo para el resto de las personas** que forman parte del Organismo.

Este curso tiene el propósito de difundir el conocimiento sobre los aspectos relevantes de la normatividad emitida en la materia y versará sobre la siguiente temática:

1. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales

- La LGPDPPSO, sus objetivos y ámbitos de aplicación;
- Conceptos y figuras claves en la LGPDPPSO; y
- Reglamentación de la LGPDPPSO (Lineamientos Generales).

2. Principios y deberes de protección de datos personales

- Principios de protección de datos personales;
- Deberes de seguridad y confidencialidad;
- Obligaciones específicas: encargados, régimen de transferencias y evaluaciones de impacto en la protección de datos personales; y
- Responsabilidades administrativas en caso de incumplimiento.

3. Derechos arco, medios de impugnación y facultad de verificación.

- Derechos de acceso, rectificación cancelación, oposición y portabilidad;
- Formas y plazos señalados por la LGPDPPSO para el ejercicio de estos derechos;
- Recursos de revisión y de inconformidad y sus etapas de sustanciación;
- Facultades que el Instituto tiene para verificar el cumplimiento de la LGPDPPSO; y
- Medidas cautelares y de apremio para hacer cumplir las resoluciones y determinaciones de la LGPDPPSO.

Capacitación especializada

La capacitación especializada está dirigida a atender necesidades o problemáticas sobre aspectos particulares de la normatividad en materia de datos personales.

En este rubro, se consideran los cursos relacionados con el cumplimiento de obligaciones, principios, deberes y derechos ARCO.

1. Aviso de privacidad;
2. Tratamiento de datos biométricos y manejo de incidentes de seguridad de datos personales;
3. Sistema de gestión de seguridad de datos personales en el sector público;
4. Auditorias voluntarias en materia de protección de datos personales;
5. Esquemas de mejores prácticas en materia de protección de datos personales; y
6. Temas especializados en materia de protección de datos personales y gestión y administración de archivos electrónicos en el sector público.

La capacitación especializada será determinada en función de las necesidades que se pretendan cubrir por cada una de las áreas que realizan tratamientos de datos personales.

15. Actualización del Documento de Seguridad

El Documento de Seguridad del SPR, de acuerdo con lo dispuesto en el artículo 36 de la LGPDPPSO se deberá actualizar cuando ocurran los siguientes eventos:

1. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
2. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida;
3. Derivado de la implementación de acciones correctivas y preventivas ante una vulneración de seguridad; y/o
4. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión para la seguridad de los datos personales que en su momento se emita para el SPR.

Todos los sistemas de tratamiento que integran el documento de seguridad del SPR deben mantenerse actualizados; sin embargo, las modificaciones que éstos presenten únicamente implicarán la necesidad de actualizar el documento de seguridad existente del Organismo cuando de dichas modificaciones en el tratamiento se altere el nivel de riesgo de los activos respectivos y, por ende, se deban modificar las medidas de seguridad implementadas.

Aprobación del documento de Seguridad: 19 de junio de 2020
Primera actualización. Fecha de aprobación: 30 de enero de 2024

SPR

Sistema Público de Radiodifusión
del Estado Mexicano

UNIDOS POR LAS
AUDIENCIAS

Camino de Santa Teresa 1679, Col. Jardines del Pedregal
Alcaldía Álvaro Obregón, C.P. 01900, Ciudad de México

Tel. 55 5533 0730 | www.spr.gob.mx | @SPRMexico