CULTURA
SECRETARÍA DE CULTURA

DOCUMENTO DE SEGURIDAD

Secretaría de Cultura

CULTURA
SECRETARÍA DE CULTURA

Contenido

Introducción

La protección de datos personales es un derecho humano, reconocido en los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos y para efectos de la reglamentación el 26 de enero de 2017 fue publicada en el Diario Oficial de la Federación la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en adelante Ley General) cuyo su objeto es establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados con la finalidad de regular su debido tratamiento

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 (en adelante Lineamientos Generales) cuyo objetivo es desarrollar las disposiciones previstas en la Ley General, y con ello, hacer más comprensible el cumplimiento de los principios, deberes y obligaciones exigidos en materia de protección de datos personales.

La Ley General de Datos dispone que el tratamiento de datos personales que realicen los sujetos obligados estará 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 el de confidencialidad y seguridad. Estos principios, deberes y derechos imponen una serie de obligaciones para los sujetos obligados cuya finalidad es que el tratamiento se realice garantizando la protección de los datos personales, con el objeto de respetar el derecho a la autodeterminación informativa de los titulares.

En específico, con relación al deber de seguridad, el artículo 31 de la Ley General de Datos señala que el responsable del tratamiento deberá establecer y mantener 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.

Al respecto, el artículo 35 de la Ley General establece como una obligación la elaboración de un documento de seguridad, que se define -según la fracción XIV del artículo 3 de la Ley General- 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.

De conformidad con el **artículo 35 de la Ley General**, el documento deberá contener, al menos, la siguiente información:

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.

En ese sentido, en cumplimiento de las obligaciones antes descritas, se presenta el documento de seguridad de la Secretaría de Cultura de conformidad con lo señalado en el artículo 35 de la Ley General de Datos.

Maco Normativo aplicable

Los principales instrumentos legislativos y normativos que rigen en la materia de datos personales son los siguientes:

- Artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf
- Lineamientos Generales de Protección de Datos Personales para el Sector Público, emitidos por el INAI. http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf

Abreviaturas y Denominaciones

Análisis de brecha: Concentración de elementos específicos que pueden existir entre lo deseable y lo actual.

Análisis de riesgo: Identificar peligros y estimar los riesgos, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento.

Archivo: 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 de forma física, electrónica o en cualquier formato, que es generado por el responsable y puesto a disposición de los titulares de los datos personales, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de estos.

Comité de Transparencia: El Comité de Transparencia de la Secretaría de Cultura.

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 riego 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 ARCOP: Derecho de Acceso, Rectificación, Cancelación Oposición y Portabilidad de datos personales.

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

Ley de Protección de Datos: Ley General de Protección de Datos Personales en posesión de los Sujetos Obligados.

Ley Federal: Ley Federal de Transparencia y Acceso a la Información Pública.

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

Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Publico publicados.

Normatividad aplicable: Los lineamientos y demás marco operativo que expida el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

OIC: Órgano Interno de Control de la Secretaría de Cultura.

Órgano Desconcentrado: Órganos administrativos desconcentrados, adscritos a la Secretaría de Cultura de conformidad con lo establecido en su Reglamento Interior que cumplen sus obligaciones. De transparencia a través de la Unidad de Transparencia de la Secretaría, a decir:

- INDAUTOR. - Instituto Nacional del Derecho de Autor
- RE. - Radio Educación

PNT: Plataforma Nacional de Transparencia.

SIPOT: Sistema de Portales de Obligaciones de Transparencia.

Secretaría: Secretaría de Cultura.

Sistema de Solicitudes de Información: El sistema autorizado por el Instituto, que contiene los formatos impresos y electrónicos para que los interesados presenten sus solicitudes de acceso a la información pública o de datos personales a través de medios electrónicos, y el sistema único para el registro y captura de todas las solicitudes recibidas por las dependencias y entidades en otros medios.

Sujetos Obligados: Se refiere a los sujetos obligados que cumplen sus obligaciones de transparencia a través del Comité y la Unidad de Transparencia de la Secretaría de Cultura:

- Instituto Nacional del Derecho de Autor;
- Radio Educación;
- Mandato del Fondo Nacional para la Cultura y las Artes;
- Fideicomiso Museo de Arte Popular Mexicano;
- Fideicomiso para Apoyar la Construcción del Centro Nacional de las Artes;
- Mandato Antiguo del Colegio de San lldefonso;
- Fideicomiso para la Cultura de la Comisión México-Estados Unidos para el Intercambio Educativo y Cultural F/22514 (Fonca);
- Fideicomiso para la Adaptación de los Museos Diego Rivera y Frida Kahlo;
- Fideicomiso para la Conservación de la Casa del Risco y Pinacoteca Isidro Fabela.

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: Las unidades administrativas que conforman la Secretaría de Cultura, responsables de dar atención a los requerimientos en la materia.

Unidad de Transparencia (UT): Unidad de Transparencia de la Secretaría de Cultura.

Versión Pública del Documento: El documento a partir del que se otorga acceso a la información, en el que se testan partes o secciones clasificadas, indicando el contenido de éstas de manera genérica, fundando y motivando la reserva o confidencialidad, a través de la resolución que para tal efecto emita el Comité de Transparencia.

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

Vulneración de seguridad: En cualquier fase del tratamiento de datos, al menos, las siguientes: I. La pérdida o destrucción no autorizada; II. El robo, extravío o copia no autorizada; III. El uso, acceso o tratamiento no autorizado, o IV. El daño, la alteración o modificación no autorizada.

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

Como se señaló, de acuerdo con la fracción I del artículo 35 de la Ley General, el Inventario de datos personales y de los sistemas de tratamiento es un elemento del documento de seguridad, así mismo, el **artículo 33, fracción III de la Ley General** establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la elaboración de un inventario de datos personales y de los sistemas de tratamiento.

> ***Artículo 33.*** *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
> *I. (...)*
> *II. (...)*
> *III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;*

Al respecto, el artículo 58 de los Lineamientos Generales establecen lo siguiente:

> ***Artículo 58.*** *Con relación a lo previsto en el artículo 33, fracción III de la Ley General, el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos:*
>
> *I. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;*
> *II. Las finalidades de cada tratamiento de datos personales;*
> *III. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;*
> *IV. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;*
> *V. La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;*
> *VI. En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y*

VII. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.

En ese sentido, a efecto de identificar los procesos mediante los cuales esta Secretaría de Cultura trata datos personales, se solicitó a las Unidades Administrativas que conforman la Secretaría de Cultura un listado de todos los sistemas físicos y electrónicos donde se efectúe tratamiento de datos, esto para conformar el Inventario de Datos Personales y de los Sistemas de Tratamientos propuesto por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Derivado de la solicitud referida, las unidades administrativas de la Secretaría reportaron los Inventarios de los Sistemas de Tratamiento de Datos Personales que se encuentran en el Anexo 1 de este documento de seguridad, y que se encuentran identificados en el siguiente cuadro:

	Unidad administrativa	Área	Denominación del Inventario de Tratamiento de Datos Personales
I	Subsecretaría de Desarrollo Cultural	Centro Cultural los Pinos	Aviso de privacidad integral "Original" Encuentro de arte textil mexicano 2022
2	Dirección General de Culturas Populares, Indígenas y Urbanas	Museo Arte Popular Mexicano	Aviso de privacidad Museo Nacional de Culturas Populares
3	Subsecretaría de Desarrollo Cultural	Centro de Cultura Digital	Aviso de privacidad Centro de Cultura Digital
4	Dirección General de Culturas Populares, Indígenas y Urbanas	Dirección General de Culturas Populares, Indígenas y Urbanas	Aviso de privacidad integral Sistema de Datos Personales de la Convocatoria "Premio Nezahualcóyotl de Literatura en Lenguas Mexicanas"
5	Dirección General de Promoción y Festivales Culturales	Festival Internacional Cervantino	Aviso de Privacidad Integral Festival Internacional Cervantino
6	Subsecretaría de Desarrollo Cultural	Subsecretaría de Desarrollo Cultural	Aviso de Privacidad Integral Contigo a la Distancia
7	Subsecretaría de Desarrollo Cultural	Subsecretaría de Desarrollo Cultural	Aviso de Privacidad Integral Contigo a la Distancia Agentes Digitales: Directorio de Servicios Creativos Digitales
8	Dirección General de Asuntos Internacionales	Dirección General de Asuntos Internacionales	Aviso de Privacidad Integral "Plataforma Digital México Creativo"

	Unidad administrativa	Área	Denominación del Inventario de Tratamiento de Datos Personales
9	Dirección General de Promoción y Festivales Culturales	Dirección General de Promoción y Festivales Culturales	Aviso de Privacidad "Contraloría Social para los Proyectos Beneficiados por el Apoyo a Festivales Culturales y Artísticos (PROFEST)"
10	Dirección General de Culturas Populares, Indígenas y Urbanas	Dirección General de Culturas Populares, Indígenas y Urbanas	Aviso de Privacidad "Contraloría Social para los Proyectos Beneficiados por el Apoyo a Instituciones Estatales de Cultura (AIEC)"
11	Dirección General de Culturas Populares, Indígenas y Urbanas	Dirección General de Culturas Populares, Indígenas y Urbanas	Aviso de Privacidad del Sistema de Datos Personales de la Convocatoria al "Premio Nezahualpilli"
12	Subsecretaría de Desarrollo Cultural	Centro Cultural los Pinos	Aviso de privacidad integral "Original" Encuentro de arte textil mexicano 2023
13	Dirección General de Culturas Populares, Indígenas y Urbanas	Dirección General de Culturas Populares, Indígenas y Urbanas	Aviso de Privacidad "Laboratorio de Cocreación Sociocultural"
14	Dirección General de Culturas Populares, Indígenas y Urbanas	Dirección General de Culturas Populares, Indígenas y Urbanas	Aviso de Privacidad del Sistema de Datos Personales "Acciones de Desarrollo Intercultural Bilingüe"
15	Dirección General de Promoción y Festivales Culturales	Festival Internacional Cervantino	Aviso de Privacidad del Sistema de Datos Personales "Sistema de Registros para el Festival Internacional Cervantino"

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

Como se señaló, de acuerdo con la fracción II del artículo 35 de la Ley General, el documento de seguridad debe señalar las funciones y obligaciones de las personas que tratan datos personales, así mismo, el artículo 33, fracción II de la Ley General establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la definición de las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.

> ***Artículo 33.*** *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
>
> *I. (...)*

> ***II.*** *Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;*
> *(...)*

Al respecto, el **artículo 57 de los Lineamientos Generales** señala lo siguiente:

> ***Artículo 57.*** *Con relación a lo dispuesto en el artículo 33, fracción II de la Ley General, el responsable deberá establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado.*
>
> *El responsable deberá establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales en su organización conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento.*

En cumplimiento a lo anterior, en relación con las funciones de los servidores públicos involucrados con el tratamiento de datos las Unidades administrativas de la Secretaría identificaron en los Inventarios de Tratamiento de Datos Personales el puesto de los servidores públicos que tienen acceso a la base de datos, el área de adscripción y la finalidad del acceso.

De igual forma, las funciones y obligaciones del personal de la Secretaría que trata datos personales se han identificado en el **Programa de Protección de Datos Personales**, en el cual se describen las obligaciones establecidas en la Ley General y los Lineamientos Generales, mismo que fue elaborado de acuerdo con lo señalado el Documento Orientador emitido por la Dirección General de Prevención y Autorregulación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales para tal efecto.

III, IV y V. Análisis de riesgos, análisis de brecha y Plan de Trabajo.

El artículo 33, fracciones IV, V y VI de la Ley General establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la realización del análisis de riesgo, análisis de brecha y plan de trabajo, en los siguientes términos:

> ***Artículo 33.*** *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*

> *I. (...)*
> ***IV.** Realizar un **análisis de riesgo** de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;*
> ***V.** Realizar un **análisis de brecha**, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;*
> ***VI. Elaborar un plan de trabajo** para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;*
> *(...)*

Como se señaló, de acuerdo con las fracciones III, IV y V del artículo 35 de la Ley General, los análisis de riesgo y brecha y el plan de trabajo forman parte del documento de seguridad.

Por su parte, los artículos 60, 61 y 62 de los Lineamientos Generales establecen lo siguiente:

→ **Análisis de riesgos**

> ***Artículo 60.** Para dar cumplimiento al artículo 33, fracción IV de la Ley General, el responsable deberá realizar un **análisis de riesgos** de los datos personales tratados considerando lo siguiente:*
>
> ***I.** Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;*
> ***II.** El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;*
> ***III.** El valor y exposición de los activos involucrados en el tratamiento de los datos personales;*
> ***IV.** Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y*
> ***V.** Los factores previstos en el artículo 32 de la Ley General.*

→ **Análisis de Brecha**

> ***Artículo 61.** Con relación al artículo 33, fracción V de la Ley General, para la realización del **análisis de brecha** el responsable deberá considerar lo siguiente:*
>
> ***I.** Las medidas de seguridad existentes y efectivas;*
> ***II.** Las medidas de seguridad faltantes, y*
> ***III.** La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.*

→ **Plan de Trabajo**

> ***Artículo 62.*** *De conformidad con lo dispuesto en el artículo 33, fracción VI de la Ley General, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.*
>
> *Lo anterior, considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.*

Por su parte, el artículo 32 de la Ley General, citado en la fracción V del artículo 60 de los Lineamientos Generales, dispone lo siguiente:

> ***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 Jos 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.*

Por lo dispuesto en los artículos citados, dicho análisis de riesgo se lleva a cabo a partir de cuatro fuentes de información:

1. Análisis de riesgos de la infraestructura tecnológica y recursos de software y hardware;
2. Análisis de riesgos de hábitos de seguridad del personal de la Secretaría de Cultura;
3. Análisis de riesgos de vulneraciones, y
4. Análisis de riesgos vinculado con el cumplimiento de obligaciones normativas en materia de datos personales.

Los dos primeros análisis se realizan de manera general y aplican transversalmente, ya que el primero refiere a los distintos sistemas o medios en los que se llevan a cabo los diversos tratamientos que realiza la Secretaría, por lo que los riesgos y controles que se determinen aplican de manera directa a estos medios o sistemas; mientras que el segundo versa sobre los hábitos de seguridad del personal, de manera general y no asociados a un tratamiento en lo particular.

Por su parte, los análisis 3 y 4 se realizan, de manera específica, asociados a cada uno de los tratamientos, y tomando en cuenta sus particularidades.

Además, se ha realizado la estimación de las vulnerabilidades y amenazas que impactan a los tratamientos reportados en los inventarios, así como el nivel de riesgo que esto representa el cual se determinó con base en el tipo de datos personales, su riesgo inherente y el nivel de seguridad requerido, como sigue:

a) Datos personales con riesgo inherente bajo: Considera datos de identificación y contacto o información académica o laboral tal como nombre, teléfono, edad, sexo, Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), estado civil, correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo y lugar de trabajo, idioma o lengua, escolaridad, cédula profesional, información migratoria, entre otros que no se encuentren en incisos b) y c).

b) Datos personales con riesgo inherente medio: Contempla los datos que permiten conocer la ubicación física de la persona, tales como la dirección física, información relativa al tránsito de las personas dentro y fuera del país y/o cualquier otro que permita volver identificable a una persona a través de los datos que proporcione alguien más. Por ejemplo: dependientes, beneficiarios, familiares, referencias laborales, referencias personales, etc.
También son datos de riesgo inherente medio aquéllos que permitan inferir el patrimonio de una persona que incluye entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios, servicios contratados, incluye el número de tarjeta bancaria de crédito y/o débito.
Son considerados también los datos de autenticación con información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros) firma autógrafa y electrónica, fotografías, identificaciones oficiales, Inclusive escaneadas o fotocopiadas y cualquier otro que permita autenticar a una persona. Dentro de esta categoría se toman en cuenta los datos jurídicos tales como antecedentes penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

c) Datos con riesgo inherente alto: Se refiere a los datos personales sensibles. Que de acuerdo a la Ley incluyen datos de salud los cuales se refieren a la información médica donde se documente el estado de salud física y mental, pasado, presente o futuro; información genética; origen racial o étnico, ideología, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular.

Por lo anterior, para determinar el nivel de riesgo las unidades administrativas considerarán el criterio del riesgo inherente del dato personal, así como el nivel de seguridad requerido para éste, en adición a las vulnerabilidades y amenazas conforme a lo siguiente:

CRITERIOS DEL NIVEL DE RIESGO	
Riesgo inherente bajo	**Nivel de seguridad bajo**
Riesgo inherente medio	**Nivel de seguridad medio**
Riesgo inherente alto	**Nivel de seguridad alto**

Los elementos requeridos en los artículos 33, fracción IV de la Ley General y 60 de los Lineamientos Generales se atienden de la siguiente forma:

Elemento requerido	Fundamento
Tomar en cuenta amenazas y vulnerabilidades existentes.	33, fracción IV, de la Ley General.
Tomar en cuenta los recursos involucrados.	33, fracción IV, de la Ley General.
Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.	60, fracción I, de los Lineamientos Generales.
El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida.	60, fracción II, de los Lineamientos Generales.
El valor y exposición de los activos involucrados en el tratamiento de los datos personales	60, fracción III, de los Lineamientos Generales.
Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.	60, fracción IV, de los Lineamientos Generales.
El riesgo inherente a los datos personales tratados.	32, fracción I, de la Ley General.
La sensibilidad de los datos personales tratados.	32, fracción II, de la Ley General.
El desarrollo tecnológico.	32, fracción III, de la Ley General.
Las posibles consecuencias de una vulneración para los titulares.	32, fracción IV, de la Ley General.
Las transferencias de datos personales que se realicen.	32, fracción V, de la Ley General.
El número de titulares.	32, fracción VI, de la Ley General.
Las vulneraciones previas ocurridas en los sistemas de tratamiento.	32, fracción VII, de la Ley General.
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.	32, fracción VIII, de la Ley General.

Existen grandes retos a los que se enfrentan todas las instituciones tanto públicas como privadas, uno de ellos es el prever y evitar lo inesperado, especialmente en un escenario que involucra las constantes y novedosas tecnologías de la información.

Por tal motivo, la Ley General establece la necesidad de contar con un análisis de los riesgos a los cuales se puede enfrentar el tratamiento de los datos personales durante su ciclo de vida; en el documento denominado Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales, emitidas por el INAI, se indican los incidentes más comunes:

1. Robo de información en documentos y medios de almacenamiento desechados incorrectamente;
2. Empleados que acceden a datos personales sin la autorización correspondiente.
3. Empleados que revelan información a otras personas a través de engaños.
4. Robo o pérdida de equipos de cómputo, laptops, teléfonos inteligentes, tabletas, o memorias extraíbles con información personal, y
5. Acceso ilegal a las bases de datos personales por un externo.

El proceso del análisis de riesgos, en lo general. es el siguiente:

Fase Uno. Identificación de posibles riesgos y controles de seguridad preliminares

1. Cada una de las unidades administrativas a cargo de tratamientos de datos personales, responderán los cuestionarios relativos a los análisis de riesgos de hábitos de seguridad y de cumplimiento de obligaciones normativas.

   Se atenderá a un único formato de cuestionario de cumplimiento de obligaciones por tratamiento. todo el personal que esté involucrado con el tratamiento debe de responder un cuestionario sobre sus hábitos de seguridad.

   Una vez respondidos los cuestionarios, la unidad administrativa a cargo de tratamiento de datos personales analizará las respuestas para detectar posibles vulnerabilidades y amenazas a efecto de definir controles de seguridad preliminares.

2. La unidad administrativa a cargo de tratamientos de datos personales analizará los inventarios de datos personales. y en caso de detectar posibles vulnerabilidades y amenazas. definirá controles de seguridad preliminares.

3. La Dirección General de Tecnologías de Información y Comunicaciones (DGTIC) realizará el análisis de riesgos de la infraestructura y recursos impresos o electrónicos de acuerdo con la metodología que tiene definida.

Fase Dos. Entrevistas y determinación de riesgos y controles de seguridad

4. Una vez que la unidad administrativa a cargo de tratamiento de datos personales tenga identificadas las posibles vulnerabilidades y amenazas. Así como definidos los controles de seguridad preliminares -a partir del análisis realizado a los inventarios y los cuestionarios de hábitos de seguridad del personal y cumplimiento de obligaciones- preparará una entrevista con las distintas áreas responsables de los tratamientos a fin de intercambiar información con relación a los posibles riesgos identificados y los controles de seguridad necesarios para mitigarlos.

   En las entrevistas se deberán identificar qué controles de seguridad tiene implementados el área a cargo del tratamiento.

5. A partir de la información obtenida de las distintas entrevistas la unidad administrativa determinará los riesgos y los controles de seguridad necesarios para mitigarlos.

   Los riesgos vinculados a la infraestructura y recursos impresos o electrónicos serán definidos por la DGTIC.

Fase Tres. Análisis de brecha

6. Una vez determinados los riesgos y los controles de seguridad necesarios para mitigarlos se realizará el análisis de brecha que consiste en identificar cuáles son los controles que hacen falta implementar a partir de aquéllos definidos como necesarios.

Fase Cuatro. Ponderación de los riesgos y elaboración del Plan de Trabajo

7. Una vez que se han identificado los riesgos potenciales y determinado los controles necesarios para mitigarlos la unidad administrativa con apoyo de la UT y la DGTIC presentarán ante el Comité de Transparencia una ponderación de los riesgos a fin de determinar cuáles se mitigarán, eliminarán, transferirán o aceptarán, así como priorizar las medidas de seguridad a implementar, cuando se actualicen las causales del artículo 36 de la Ley General.

   En la ponderación se deberán tomar en cuenta las posibles consecuencias de una vulneración para los titulares el número de titulares y el riesgo por el valor potencial

cuantitativo o cualitativo que pudieran tener los datos personales tratados por una tercera persona no autorizada para su posesión.

Esta definición se podrá consultar y poner a consideración de las unidades administrativas encargadas de los tratamientos.

8. Ya que se ha realizado la ponderación la UT elaborará el **Plan de Trabajo** en el cual se definirán las acciones a implementar priorizando las medidas de seguridad más relevantes e inmediatas.

9. En el Plan de Trabajo se deberán identificar los responsables de las acciones, así como las fecha compromiso.

Forman parte integral de este documento de seguridad el análisis de riesgos de la infraestructura tecnológica, software y hardware, los cuestionarios respondidos por cada unidad administrativa y la identificación de vulnerabilidades, amenazas, controles de seguridad y brechas.

El Plan de Trabajo y la ponderación de riesgos en materia de protección de datos personales son parte integral del Documento de Seguridad.

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

Como se señaló, de acuerdo con la fracción VI del artículo 35 de la Ley General, el documento de seguridad debe señalar los mecanismos de monitoreo y revisión de las medidas de seguridad, así mismo, el artículo 33, fracción VII de la Ley General establece 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

> ***Artículo 33.*** *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
> *I. (...)*
> *II. (...)*
> *III. (...)*
> *IV. (...)*

V. (...)
VI. (...)
***VII.** Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y*
(...)

Así, respecto a los mecanismos de monitoreo y revisión de las medidas de seguridad, el artículo 63 de los Lineamientos Generales señala lo siguiente:

***Artículo 63.** Con relación al artículo 33, fracción VII de la Ley General, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.*

Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:

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

Aunado a lo previsto en las fracciones anteriores del presente artículo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

De lo anterior es posible identificar que el monitoreo y revisión de las medidas de seguridad tiene el objetivo de fortalecer, a través de un ciclo de mejora continua, la protección de los datos personales que resguarda esta Secretaría de Cultura.

A continuación, se desarrollan las acciones de monitoreo y supervisión periódica para las medidas de seguridad de la Secretaría de Cultura:

Mecanismos de Monitoreo de las unidades administrativas que están a cargo del tratamiento de datos personales

Para los tratamientos de datos personales se consideran los siguientes tipos de monitoreo:

1. **Revisión de cumplimiento de las políticas de la Secretaría de Cultura por parte de las unidades administrativas, relacionadas con el tratamiento de datos personales.** Su objetivo es asegurar que los servidores públicos realicen los tratamientos de datos personales en relación con lo dispuesto en la Ley General, los Lineamientos Generales, y demás normatividad que resulte aplicable en materia de protección de datos personales.

Para ello, cuando se identifique algún cambio en los instrumentos normativos mencionados, 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 los inventarios de datos personales, según corresponda.
c) Evaluar si hubo 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 riego.** Tiene el objetivo de identificar modificaciones a los riesgos identificados en los tratamientos de datos personales para ello, se implementarán los siguientes monitoreos **de las unidades administrativas que están a cargo del tratamiento de los datos personales:**

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 SC,
   (ii) Control de acceso a través de bitácoras para visitantes y personal de la SC que no cuenta con credencial,
   (iii) Control de asistencia a través de huella digital, y

(iv) Circuito cerrado de cámaras de vigilancia.

b) **Monitoreo del entorno electrónico.** Para la detección continua de amenazas y vulnerabilidades, la DGTIC cuenta con herramientas automatizadas de monitoreo (activo y pasivo).

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 DGTIC y el Comité de Transparencia.

d) **Revisión de avances del plan de trabajo.** A través de los mecanismos que determine la DGTIC y el Comité de Transparencia, se hará una revisión de los avances en el 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, la DGTIC y el Comité de Transparencia se coordinarán para decidir sobre las acciones pertinentes para mitigar dicho incidente.

A continuación, se describen los mecanismos de monitoreo y revisión de la Secretaría de Cultura:

Elemento por revisar	Fundamento	Acciones
Los nuevos activos que se incluyan en la gestión de riesgos;	63, fracción I, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas de la SC, relacionadas con el tratamiento de datos personales.
Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;	63, fracción II, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas de la SC, relacionadas con el tratamiento de datos personales.

Elemento por revisar	Fundamento	Acciones
Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;	63, fracción III, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas de la SC, relacionadas con el tratamiento de datos personales. 2.a. Monitoreo del entorno físico. 2.b. Monitoreo del entorno electrónico.
La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;	63, fracción IV, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas de la SC, relacionadas con el tratamiento de datos personales. 2.a. Monitoreo del entorno físico. 2.b. Monitoreo del entorno electrónico.
Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;	63, fracción V, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas de la SC, relacionadas con el tratamiento de datos personales. 2.a. Monitoreo del entorno físico. 2.b. Monitoreo del entorno electrónico.
El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo	63, fracción VI, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas de la SC, relacionadas con el tratamiento de datos personales. 2.c. Actualización del plan de trabajo. 2.d. Revisión de avances del plan de trabajo.
Los incidentes y vulneraciones de seguridad ocurridas.	63, fracción VII, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas de la SC, relacionadas con el tratamiento de datos personales. 2.f. Vulneraciones a la seguridad de los datos personales.

Mecanismos de supervisión o revisión

Además del monitoreo continuo de las medidas de seguridad, se estará a lo dispuesto en el artículo 30 fracción V de la Ley General.

De conformidad con lo establecido en el artículo 151 de la Ley General y 218 de los Lineamientos Generales. este Sujeto Obligado Responsable podrá solicitar voluntariamente la realización de una auditoría al INAI con el objeto de verificar la adaptación adecuación y eficacia de los controles medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la presente Ley y demás normativa que resulte aplicable.

Hasta el momento no se han realizado auditorías específicas en materia de protección de datos personales a los tratamientos de la Secretaría de Cultura.

Los resultados de las auditorías se considerarán para realizar adecuaciones al análisis de riesgos de la SC y, por lo tanto, al plan de trabajo.

VII. El programa general de capacitación

Como se señaló, de acuerdo con la fracción VII del artículo 35 de la Ley General, el documento de seguridad debe integrar el programa general de capacitación así mismo, el artículo 33, fracción VII de la Ley General establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el diseño y aplicación de diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

> ***Artículo 33.*** *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
>
> *I. (...)*
> *II. (...)*
> *III. (...)*
> *IV. (...)*
> *V. (...)*
> *VI. (...)*
> *VII. (...)*
> ***VIII.*** *Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.*

Por su parte, el artículo 64 de los Lineamientos Generales señala lo siguiente:

> ***Artículo 64.*** *Para el cumplimiento de lo previsto en el artículo 33, fracción VIII de la Ley General, el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.*

En el diseño e implementación de los programas de capacitación a que se refiere el párrafo anterior del presente artículo, el responsable deberá tomar en cuenta lo siguiente:

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

A partir de lo anterior, la Secretaría desarrolló su programa general de capacitación, mismo que forma parte integral de este documento de seguridad.

VIII. Actualización del documento de seguridad

El **artículo 36** de la Ley General establece la obligación de la actualización del documento de seguridad cuando ocurran los siguientes eventos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y
IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

En ese sentido, el Comité de Transparencia deberá estar atento a la actualización de alguno de los supuestos antes citado, para, en su caso, actualizar el presente documento de seguridad.

Las unidades administrativas informarán a la UT las modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo: aquellos resultados de un proceso de mejora continua. derivado del monitoreo y revisión del sistema de gestión: los resultados de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida y las acciones correctivas y preventivas ante una vulneración de seguridad a fin de que sean sometidas ante el Comité de Transparencia para la debida actualización del presente documento.