Programa de Protección de Datos Personales del Centro de Investigación en Alimentación y Desarrollo, A.C. (CIAD)

Contenido

I. Glosario de Términos Comunes

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva para determinar el grado de cumplimiento de los criterios preestablecidos para la misma.

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.

Bases de datos: Conjunto ordenado de datos personales bajo criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Centro: Centro de Investigación en Alimentación y Desarrollo, A.C. (CIAD)

Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública y 83 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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.

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

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

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

Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Programa: Programa de Protección de Datos Personales.

Responsable: Sujeto obligado de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que decide sobre el tratamiento de los datos personales.

Revisión: Actividad estructurada, objetiva y documentada, llevada a cabo con la finalidad de constatar el cumplimiento continuo de los contenidos establecidos en este Programa.

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

Sujeto Obligado: Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del ámbito federal.

Titular: 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.

Unidad Administrativa: Área a la que se le confieren atribuciones específicas en el Estatuto Orgánico del CIAD, incluidas las ponencias de los Comisionados.

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

II. Presentación

De conformidad con el artículo 34 de la LGPDPPSO, un sistema de gestión es un conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, así como, el cumplimiento de los principios, deberes y obligaciones previstos en dicha ley y las demás disposiciones que resulten aplicables en la materia.

El sistema de gestión del Centro desarrolla las siguientes cuatro fases: planificar, hacer, verificar y actuar (PHVA), de acuerdo con lo descrito en la tabla siguiente:

	Elemento	Fase del ciclo PHVA	Actividades
PROCESO		**P**lanificar	Identificar políticas, objetivos, riesgos, planes, procesos y procedimientos necesarios para obtener el resultado esperado por el responsable o encargado.
	Medios de acción	**H**acer	Implementar y operar las políticas, objetivos, planes, procesos y procedimientos establecidos en la fase anterior.
		Verificar	Evaluar y medir los resultados de lo implementado, a fin de verificar el adecuado funcionamiento del sistema de gestión y el logro de la mejora esperada.
		Actuar	Adoptar medidas correctivas y preventivas en función de los resultados y de la revisión realizada, o de otra información relevante, para lograr la mejora continua.

Para la elaboración del presente documento, se identificaron las obligaciones que establece la LGPDPPSO y los Lineamientos Generales y, a partir de ello, se definieron las acciones a seguir para su cumplimiento.

III. Objetivos del Programa

El Programa de Protección de Datos Personales del CIAD busca la realización de los siguientes objetivos:

1. Estipular los elementos, actividades, operación y procesos que realiza el Centro que permiten la protección continua de los Datos Personales en su posesión.
2. Establecer los mecanismos para cumplir con sus obligaciones conforme a la LGPDPPSO, así como demás normatividad aplicable.
3. Elaboración de programas de capacitación y actualización del personal del Centro, en materia de Protección de Datos Personales.
4. Fomentar la cultura de la Protección de Datos Personales en el Centro.
5. Implementar un sistema de gestión de seguridad de Datos Personales, el cual permita planificar, implementar, operar, monitorear y mejorar la seguridad en sus modalidades administrativa, físico y técnico.

IV. Responsabilidades

Con fundamento en lo dispuesto por los artículos 83 y 84, fracción I de la LGPDPPSO y 47, segundo párrafo, y 48 de los Lineamientos Generales, 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 la organización del responsable, dicho órgano tendrá las siguientes funciones con relación a este programa:

I. Elaborar, aprobar, coordinar y supervisar el Programa, en conjunto con las áreas técnicas que estime necesario involucrar o consultar;
II. Proponer cambios y mejoras al Programa, a partir de la experiencia de su implementación;
III. Dar a conocer el Programa al interior del sujeto obligado;
IV. Supervisar la correcta implementación del Programa;
V. Elaborar, aprobar, coordinar y supervisar el programa anual de capacitación, en conjunto con las áreas técnicas que estime necesario involucrar o consultar, y
VI. Las demás que de manera expresa señale el propio Programa.

V. Alcance del Programa

El presente programa aplicará a todas las unidades administrativas del CIAD que realicen tratamiento de datos personales en ejercicio de sus atribuciones, y a todos los tratamientos de datos personales que éstas efectúen en ejercicio de sus atribuciones.

Para ello, resulta fundamental que el Programa se conozca al interior del sujeto obligado, por lo que el Comité de Transparencia se encargará de difundirlo entre los servidores públicos.

Asimismo, en virtud de que uno de los objetivos del Programa es cumplir con las obligaciones establecidas en la LGPDPPSO, se cubrirán todos los principios, deberes y obligaciones que establece dicha norma para los responsables del tratamiento.

Quedan exceptuados de la aplicación de este programa, los datos personales que correspondan al cumplimiento de las obligaciones de transparencia a las que refieren el artículo 120 de la Ley General de Transparencia y Acceso a la Información Pública y numeral 117 de la Ley Federal de Transparencia y Acceso a la Información Pública.

Las unidades administrativas que forman parte de CIAD, y que deberán observar el Programa son las siguientes:

1. Dirección General
2. Dirección de Administración

3. Subdirección de Recursos Materiales y Servicios Generales:
4. Departamento de Mantenimiento y Obra Pública
5. Departamento de Adquisiciones
6. Departamento de Control Patrimonial y Servicios Generales

7. Departamento de Personal
8. Departamento de Contabilidad y Tesorería
9. Departamento de Presupuestos
10. Departamento Administrativo de Culiacán
11. Departamento Administrativo de Mazatlán
12. Departamento de Control y Sistemas Administrativos.
13. Departamento de Tecnologías de la Información y Comunicaciones.

14. Coordinación de Vinculación
15. Coordinación de Investigación
16. Coordinación de Programas Académicos

VI. Política de Gestión de los Datos Personales

El tratamiento de datos personales que realicen las unidades administrativas deberá cumplir con los principios, deberes y obligaciones que prevé la LGPDPPSO, para lo cual este programa establecerá el marco de trabajo mínimo que se deberá seguir para alcanzar dicho objetivo.

Para ello, se identificarán las obligaciones que se deberán cumplir en todos los tratamientos de datos personales que realicen las unidades administrativas, de acuerdo con lo que establece la LGPDPPSO y los Lineamientos Generales, y según el ciclo de vida de los datos personales.

Asimismo, el CIAD procurará la adopción de mejores prácticas para la protección de datos personales, en aquellos tratamientos que así lo permitan y según el nivel de madurez que exista.

VII. Inventario de Tratamiento de Datos Personales

El diagnóstico en mención se basa en la elaboración de un inventario con la información básica de cada tratamiento de datos personales que se realizan en el Centro.

Por "inventario de tratamientos de datos personales" se entenderá el control documentado que se llevará de los tratamientos que realizan las unidades administrativas del Centro, realizado con orden y precisión.

El inventario de datos personales al que hace referencia la LGPDPPSO en los artículos 33, fracción III, 35, fracción I, y 58 de los Lineamientos Generales, identificará los siguientes elementos relevantes:

1. ¿Qué tratamientos de datos personales realiza la unidad administrativa?
Hay que identificar cada uno de los procesos en los que la unidad administrativa trata datos personales.

2. ¿Qué unidad administrativa está a cargo de estos procesos y que por tanto sea la administradora de las bases de datos o archivos que se generen con motivo de dichos tratamientos?
Hay que identificar o definir si la unidad administrativa está a cargo del proceso en donde se tratan los datos personales, según las atribuciones o facultades normativas.

Podría ocurrir que una unidad administrativa trate datos personales recabados en el marco de un proceso del cual no es responsable. Por ejemplo, con motivo de una consulta, la unidad administrativa "X" podría tener acceso a datos de contacto del particular que realizó la consulta, sin embargo, la unidad administrativa que está a cargo del procedimiento de atención a consultas, y quien administra la base de datos de las consultas que recibe la institución es la unidad administrativa "Y".

Asimismo, podría darse el caso en que dos o más unidades administrativas estén a cargo de un proceso mediante el cual se recaban los datos personales y que administren las bases de datos correspondientes de manera conjunta.

En ese sentido, para definir quién está a cargo del proceso mediante el cual se recaban los datos personales y que, por tanto, administre las bases de datos o archivos correspondientes, es necesario analizar la función que realiza cada unidad administrativa dentro del proceso, y las atribuciones o facultades normativas que resulten aplicables.

3. Una vez que hayan sido identificados los tratamientos de los cuales está a cargo la unidad administrativa, será necesario determinar lo siguiente, de acuerdo con el ciclo de vida de los datos personales:

a. ¿Cómo se obtienen los Datos Personales?

- Directamente del titular
    - De manera personal, con la presencia física del titular de los datos personales o su representante, en su caso.
    - Vía telefónica
    - Por correo electrónico
    - Por internet o sistema informático
    - Por escrito presentado directamente en las oficinas del sujeto obligado
    - Por escrito enviado por mensajería

- Mediante una transferencia
    - Quién transfiere los Datos Personales y para qué fines
    - Medios por los que se realiza la transferencia.

- De una fuente de acceso público

b. ¿Qué tipo de Datos Personales se tratan? ¿son sensibles?

c. ¿Dónde se almacenan y realiza el tratamiento de los Datos Personales?

- Sección, serie y subserie de archivos
- Formato en que se encuentra la base de datos: físico y/o electrónico
- Ubicación de la base de datos

d. ¿Para qué finalidades se utilizan los datos personales?

Las finalidades son acciones más específicas de los procesos de los que derivan los tratamientos de datos personales. Por ejemplo, el procedimiento podría ser "contratación de personal" y las finalidades "evaluación de currículum para la selección de personal".

Será necesario identificar si se requiere el consentimiento o no de los titulares y el tipo de consentimiento (tácito o expreso y por escrito), y en caso de que no se requiera, definir qué supuestos (fracciones) del artículo 22 de la LGPDPPSO se actualizan.

Asimismo, se deberá señalar el marco jurídico que da facultades para el tratamiento de datos personales (disposición normativa, artículo, fracción, inciso, párrafo).

e. ¿Quién tiene acceso a la base de datos o archivos (sistemas de tratamiento) y a quién se comunican los datos personales al interior del sujeto obligado?

Se deberá identificar el catálogo de personas servidoras públicas al interior del sujeto obligado que tienen acceso a los datos personales y para qué fin.

f. ¿Intervienen encargados en el tratamiento de los datos personales?

Es necesario identificar el nombre del encargado y el número de contrato, pedido o convenio correspondiente.

g. ¿Qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad?

Hay que identificar las autoridades o terceros externos al Centro a quienes se comunican los datos personales y los fines de las transferencias.

Asimismo, es necesario señalar si se requiere el consentimiento para la transferencia, el tipo de consentimiento que se requiere en su caso (tácito o expreso y por escrito), y en caso de que no se requiera el consentimiento, se deberá definir qué supuestos (fracciones) de los artículos 22, 66 o 70 de la LGPDPPSO se actualizan.

h. ¿Se difunden los datos personales?
Hay que señalar si los datos personales se difunden y el fundamento jurídico para ello.

i. ¿Cuál es el plazo de conservación de los datos personales?
Este plazo tendría que estar definido en los instrumentos de clasificación archivística, por lo que es necesario identificar a qué serie documental pertenecen los archivos o bases de datos en los que están contenidos los datos personales.

Una vez que se haya realizado este diagnóstico inicial, estaremos preparados para cumplir de mejor manera con las obligaciones previstas en la LGPDPPSO y los Lineamientos Generales.

VIII. Tratamiento de Datos personales

La información dentro del Centro es transmitida en diversos medios, pudiendo ser impresa, escrita en papel, transmitida por correo, almacenada electrónicamente, utilizada por medios electrónicos, expuesta en una conversación o almacenada electrónicamente, independientemente del medio, dicha información debe ser protegida de forma adecuada.

El tratamiento de los Datos Personales se conforma por diversas etapas que permiten recabar los datos, registrarlos en una base de datos, lo que a su vez permite modificarlos, utilizarlos, comunicarlos, bloquearlos o destruirlos, por lo que es esencial la protección de los mismos.

Las etapas del Tratamiento de Datos Personales se integra de la siguiente manera:

1. **Obtención:** Momento en que se recaban los datos del titular, ya sea que él mismo los proporcione, o a través de un tercero, mediante el uso de diversos medios.

2. **Uso:** Etapa donde los Datos Personales recabados se someten a diversos procedimientos, de manera que son registrados en una base de datos para ser modificados, consultados o utilizados en cualquier forma. El manejo de los datos puede ser hecha por el responsable autorizado para cumplir con el propósito por el que fueron recabados, o también siendo difundidos o distribuidos con un tercero, para la prestación de un servicio determinado al propio responsable.

3. **Eliminación, bloqueo, destrucción de los Datos Personales:** Etapa donde los Datos Personales han dejado de ser necesarios o han cumplido con las finalidades establecidas en el Aviso de Privacidad, por lo que, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya su plazo de conservación de los mismos.

El tratamiento de Datos Personales implica cualquier operación o conjunto de operaciones efectuadas mediante procedimientos informáticos, manuales, digitales o electrónicos, enfocados en la obtención, registro, organización, conservación, utilización, cotejo, interconexión o cualquier forma que permita la obtención de información y facilite al interesado el acceso, rectificación, cancelación u oposición de sus datos.

Para el cumplimiento de las obligaciones establecidas en la Ley de la materia, se deberá observar lo siguiente:

- **Obtención de Datos Personales:**

  Los Datos Personales podrán ser recabados de forma enunciativa, más no limitativa, por los siguientes medios:

  - Visita a las instalaciones.
  - Llenado de formatos.
  - Formularios electrónicos.
  - Presentación de un escrito.

Los medios por los cuales se obtenga y traten los Datos Personales deberán ser lícitos, privilegiando en todo momento la protección de los intereses del titular y la expectativa razonable de privacidad, evitando utilizar medios engañosos o fraudulentos.

Previo al tratamiento de Datos Personales, se deberá obtener el consentimiento del titular, de manera libre, especifica e informada, se considerará que el consentimiento del titular es tácito, cuando habiéndose puesto a su disposición el Aviso de Privacidad, aquel no manifieste su voluntad en sentido contrario.

En el caso de Datos Personales Sensibles, se deberá obtener el consentimiento expreso y escrito por el titular para su tratamiento, a través de firma autógrafa, electrónica o cualquier mecanismo de autenticación que al efecto se establezca.

- **Uso y almacenamiento de Datos Personales**

El responsable deberá adoptar las medidas necesarias para mantener exactos, pertinentes, completos, correctos y actualizados los Datos Personales en su posesión, a fin de que se no se altere la veracidad de éstos.

El tratamiento de Datos Personales que lleven a cabo las distintas áreas administrativas del Centro deberá sujetarse a establecido por los artículos 9 de los Lineamientos Generales y 18 de la LGPDPPSO, por lo que todo tratamiento de Datos Personales que se efectúe deberá estar justificado por finalidades:

I. Concretas: cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular;
II. Explícitas: cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad;
III. Lícitas: cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable, y
IV. Legítimas: cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento del titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General.

En el tratamiento de Datos Personales, se deberán mantener mecanismos efectivos de seguridad de carácter administrativo, físico y técnico para la protección de los mismos, con el objetivo de impedir, que se contravenga las disposiciones de la normatividad en la materia. Dichos mecanismos deberán permitir:

- Mantener identificada, clasificada y controlada la información propiedad del Centro a fin de garantizar su confidencialidad, integridad y disponibilidad.
- Establecer normas y controles internos durante la recolección, procesamiento, almacenamiento, acceso y disposición de la información.
- Identificar, evaluar y tomar medidas que disminuyan riesgos en la administración de la información y garantizar la continuidad en los procesos.
- Implantar y mantener un modelo de seguridad de la información, eficiente, tolerante a fallas y fácil de monitorear, que involucren a todo el Centro.
- Proteger al Centro de posibles responsabilidades legales derivadas del uso indebido de los activos de información.
- Implantar y mantener un modelo de seguridad para conservar la confidencialidad e integridad de la información que se genere en el Centro y se transmita a través de medios electrónicos o redes ya sean internas o externas.
- Implantar mecanismos necesarios que permitan conservar la integridad de los documentos y transacciones generados y entregados en el Centro o fuera a terceras personas.
- Implantar mecanismos para almacenamiento y recuperación de la información en casos de desastre.

- Implantar mecanismos para prevención y corrección contra ataque de virus informáticos, códigos, maliciosos y demás variantes.
- Recomendar y/o sugerir cambios o mejoras en el establecimiento de seguridad física dentro de las instalaciones del Centro.
- Implantar y mantener mecanismos necesarios para determinar los accesos a los recursos del Centro, como lo son impresoras, equipos, etc.

El responsable deberá informar a los titulares a través del Aviso de Privacidad, la existencia y las características principales del tratamiento al que serán sometidos sus datos personales.

IX. Vulneraciones

El responsable deberá llevar una bitácora de las vulneraciones a la seguridad en la que se describa ésta, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

Se considera como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

- La pérdida o destrucción no autorizada;
- El robo, extravío o copia no autorizada;
- El uso, acceso o tratamiento no autorizado o,
- El daño, la alteración o modificación no autorizada

El responsable deberá informar en un plazo máximo de **setenta y dos hora** al titular y al Comité de Transparencia, las vulneraciones que afecten de forma significativa los **derechos patrimoniales** (de forma enunciativa más no limitativa relacionado con sus bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, AFORES, fianzas, servicios contratados o las cantidades o porcentajes relacionados con la situación económica del titular) o **morales** (de manera enunciativa, más no limitativa, relacionados con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspectos físicos, menoscabo ilegalmente de la libertad o integridad), en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados, puedan tomar las medidas para la defensa de sus derechos.

Conforme al artículo 67 de los Lineamientos Generales, la notificación de vulneración de seguridad al Comité de Transparencia deberá contener los siguientes elementos:

I. La hora y fecha de la identificación de la vulneración;
II. La hora y fecha del inicio de la investigación sobre la vulneración;
III. La naturaleza del incidente o vulneración ocurrida;
IV. La descripción detallada de las circunstancias en torno a la vulneración ocurrida;

V. Las categorías y número aproximado de titulares afectados;
VI. Los sistemas de tratamiento y datos personales comprometidos;
VII. Las acciones correctivas realizadas de forma inmediata;
VIII. La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida;
IX. Las recomendaciones dirigidas al titular;
X. El medio puesto a disposición del titular para que pueda obtener mayor información al respecto;
XI. El nombre completo de la o las personas designadas y sus datos de contacto, para que puedan proporcionar mayor información al Centro, en caso de requerirse, y
XII. Cualquier otra información y documentación que considere convenientes hacer del conocimiento del Centro.

- **Eliminación de datos personales**

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 el plazo de conservación de los mismos.

Los plazos de conservación de los Datos Personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los Datos Personales.

Se deberán establecer métodos y técnicas para la supresión definitiva de los Datos Personales, de tal manera que la posibilidad de recuperarlos o reutilizarlos sea nula; para lo cual se deberán considerar los medios de almacenamiento físicos y/o electrónicos en los que se encuentren los Datos Personales, así como los siguientes atributos:

- **Irreversibilidad:** Que el proceso utilizado no permita recuperar los Datos Personales.
- **Seguridad y confidencialidad:** En la eliminación definitiva de los Datos Personales, se deberán observar los deberes de confidencialidad y seguridad establecidos en la ley de le la materia.
- **Favorable al medio ambiente:** Que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten al medio ambiente.

X. Obligaciones de las Unidades Administrativas

Con la finalidad de mejorar el tratamiento y seguridad de los datos personales, así como, el cumplimiento de los principios, deberes y obligaciones previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, las unidades administrativas deberán elaborar y mantener actualizado, de conformidad con lo señalado en los puntos anteriores y la normativa aplicable, lo siguiente:

1. Inventario de datos personales
2. Aviso de privacidad
3. Bitácora de vulneraciones.
4. Análisis de Riesgos de Activos
5. Proponer y establecer medidas de seguridad al interior del área en materia de seguridad de la información en su posesión.
6. Promover la capacitación de los servidores públicos que integran la unidad administrativa.
7. Atender las sugerencias y recomendaciones del Comité de Transparencia.
8. Las demás que señale la normativa correspondiente.

XI. Revisiones

Con la finalidad de establecer y mantener las medidas de seguridad para los Datos Personales, el Comité de Transparencia evaluará y medirá los resultados de las políticas, planes, proceso y procedimientos implementados en materia de seguridad y tratamiento de datos, a fin de verificar el cumplimiento de los objetivos planteados, se deberá monitorear continuamente los siguientes aspectos:

- Los nuevos activos que se incluyan en la gestión de riesgos
- Las modificaciones necesarias a los activos
- Las nuevas amenazas que podrían estar activas dentro y fuera del Centro y que no han sido valoradas.
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes
- Las vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.
- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.
- Los incidentes y vulneraciones ocurridos.

XII. Acciones para la mejora continua del Programa

En esta fase del Programa, se adoptarán las medidas preventivas y correctivas que hayan resultado de las revisiones realizadas, o bien que se hayan obtenido de otras fuentes de información relevantes.

Los puntos de mejora de la implementación del Programa pueden ser de dos tipos:

1. Acciones preventivas: El objetivo de las acciones preventivas es disminuir la probabilidad de ocurrencia.

2. Acciones correctivas: El objetivo de las acciones correctivas es eliminar la causa de la no conformidad, o bien, reducir su grado de prevalencia.

El Comité de Transparencia deberá establecer un plazo límite para que se corrijan las no conformidades detectadas.

El Comité de Transparencia deberá documentar las medidas preventivas o correctivas realizadas para la mejora continua en la implementación de este Programa.

Obligaciones	**Actividades para su cumplimiento**	**Unidades administrativas/ponencias responsables del cumplimiento**	**Medios para acreditar el cumplimiento**
El responsable deberá implementar acciones para evitar o corregir cualquier no conformidad.	1. Elaborar un procedimiento para la gestión de las acciones preventivas y correctivas.	Comité de Transparencia	• Procedimiento para la gestión de acciones preventivas y correctivas. • Documentación que acredite las acciones preventivas o correctivas implementadas, así como los resultados y revisiones de las acciones una vez implementadas.

XIII. Sanciones por Incumplimiento

Cuando el Comité de Transparencia tenga conocimiento del incumplimiento de alguna obligación prevista en este Programa, deberá realizar a la unidad administrativa correspondiente un exhorto para que lleve a cabo las acciones que resulten pertinentes con objeto de modificar dicha situación y evitar incumplimientos futuros o situaciones de riesgo que los pudieran ocasionar.

De manera adicional, es importante que las personas servidoras públicas que están a cargo del tratamiento de datos personales tengan presente que de conformidad con el artículo 163 de la LGPDPPSO serán causas de sanción por incumplimiento de las obligaciones establecidas en dicha ley, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;
II. Incumplir los plazos de atención previstos en la LGPDPPSO para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;
III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la LGPDPPSO;
V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la LGPDPPSO, según sea el caso, y demás disposiciones que resulten aplicables en la materia;
VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;
VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la LGPDPPSO;
VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la LGPDPPSO;
IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la LGPDPPSO;
X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO;
XI. Obstruir los actos de verificación de la autoridad;
XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la LGPDPPSO;

XIII. No acatar las resoluciones emitidas por el Centro, y

XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV, así como la reincidencia en las conductas previstas en el resto de las fracciones, serán consideradas como graves.

Asimismo, de conformidad con el artículo 105 de los Lineamientos Generales, cuando alguna unidad administrativa se niegue a colaborar con la Unidad de Transparencia en la atención de las solicitudes para el ejercicio de los derechos ARCO, ésta dará aviso al superior jerárquico para que le ordene realizar sin demora las acciones conducentes.

Si persiste la negativa de colaboración, la Unidad de Transparencia lo hará del conocimiento del Comité de Transparencia para que, a su vez, dé vista al Órgano interno de Control Específico y, en su caso, dé inicio el procedimiento de responsabilidad administrativo respectivo.

Cabe destacar que las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

Las responsabilidades que resulten de los procedimientos administrativos correspondientes son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

El Comité de Transparencia tomará las medidas necesarias para que las personas servidoras públicas del sujeto obligado conozcan esta información.

Fecha de autorización
30 de mayo de 2024