



MOVIMIENTO CIUDADANO

PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES

**CNTYAI
UNIDAD DE DATOS PERSONALES**

ENERO DE 2022

CONTENIDO

PRESENTACIÓN	4
OBJETIVOS DEL PROGRAMA	5
RESPONSABILIDADES.....	6
ALCANCE.....	9
CUMPLIMIENTO DE OBLIGACIONES	10
1. DEBER DE SEGURIDAD.....	10
POLÍTICAS INTERNAS	11
FUNCIONES DE LOS QUE TRATAN DATOS PERSONALES.....	12
INVENTARIO	13
ANÁLISIS DE RIESGO, BRECHA Y PLAN DE TRABAJO.....	14
REVISIÓN Y VIGILANCIA.....	16
SISTEMA DE GESTIÓN.....	17
DOCUMENTO DE SEGURIDAD	18
2. DEBER DE CONFIDENCIALIDAD	19
3. PRINCIPIO DE LICITUD	20
4. PRINCIPIO DE LEALTAD.....	21
5. PRINCIPIO DE INFORMACIÓN	22
6. PRINCIPIO DE CONSENTIMIENTO	24
DATOS PERSONALES SENSIBLES.....	27
7. PRINCIPIO DE PROPORCIONALIDAD.....	28
8. PRINCIPIO DE FINALIDAD.....	29
9. PRINCIPIO DE CALIDAD.....	30
10. PRINCIPIO DE RESPONSABILIDAD.....	31
11. MEDIDAS COMPENSATORIAS.....	33
12. RELACIÓN CON LOS ENCARGADOS.....	34
13. COMPUTO EN LA NUBE	35
14. TRANSFERENCIAS.....	37
15. PORTABILIDAD	39

16.	SUPRESIÓN DE LOS DATOS PERSONALES	40
17.	EVALUACIÓN DE IMPACTO	41
18.	CAPACITACIÓN	42
19.	REVISIONES Y AUDITORIAS.....	43
20.	ACCIONES PARA LA MEJORA CONTINUA.....	45
	SANCIONES	46
	GLOSARIO.....	48

PRESENTACIÓN

El presente programa se elabora en cumplimiento a lo previsto por los artículos 30, fracciones I y II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y 47 de los Lineamientos Generales, donde se establece que entre las acciones que deberán realizar los responsables del tratamiento de datos personales para cumplir con el principio de responsabilidad, está la elaboración de políticas y programas de protección de datos personales, así como destinar los recursos necesarios para su implementación, las cuales son de carácter obligatorio.

Este Programa está basado en el Documento Orientador publicado por el INAI en el 2018, el cual sirvió como marco de referencia para definir las acciones a seguir en Movimiento Ciudadano para dar cumplimiento a las obligaciones que establecen la LGPDPPSO y sus Lineamientos Generales.

OBJETIVOS DEL PROGRAMA

1. Cumplir con las obligaciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales.
2. Establecer los elementos de operación y control que impliquen el tratamiento de datos personales, a fin de protegerlos de manera continua basado en el sistema de gestión PHVA (Planificar-Hacer, Verificar-Actuar).
3. Promover mejores prácticas en la protección de datos personales.

RESPONSABILIDADES

Del más alto nivel en Movimiento Ciudadano

Para lograr los objetivos planteados, se requiere del apoyo e impulso del más alto nivel de Movimiento Ciudadano, sin embargo, no podrá suplir ni afectar las funciones que otorga la LGPDPPSO a la Comisión Nacional de Transparencia y Acceso a la Información en su carácter de máxima autoridad en materia protección de datos personales.

De la Comisión Nacional de Transparencia y Acceso a la información

La Comisión Nacional de Transparencia y Acceso a la Información de Movimiento Ciudadano, en términos de lo dispuesto por los artículos 83 y 84, fracción I de la LGPDPPSO y 47, segundo párrafo, y 48 de los Lineamientos Generales, es la autoridad máxima en materia de protección de datos personales y tiene entre sus funciones:

- a) Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la LGPDPPSO y en aquellas disposiciones que resulten aplicables en la materia;
- b) Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;
- c) 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;
- d) Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la LGPDPPSO y en aquellas disposiciones que resulten aplicables en la materia;
- e) Supervisar, en coordinación con las unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;
- f) Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto y los organismos garantes, según corresponda;

- g) Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales, y
- h) Dar vista al órgano interno de control o instancia equivalente 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 los responsables.

Para los términos del presente programa sus funciones serán las siguientes:

- a) Aprobar, y dar a conocer el Programa de protección de datos personales a fin de que se tomen las medidas necesarias para su cumplimiento;
- b) Establecer un plan de trabajo para la implementación del Programa.
- c) Proponer cambios y mejoras al Programa;
- d) Asesorar a las Unidades Administrativas con el apoyo de la Unidad de Datos Personales en la implementación del Programa;
- e) Presentar un informe anual;
- f) Supervisar la correcta implementación del Programa;
- g) Establecer un programa de capacitación y actualización en materia de protección de datos personales.

De la Unidad de Protección de Datos Personales

La Unidad de Protección de Datos Personales, en términos de lo dispuesto por el artículo 121 y 122 de los Lineamientos Generales, tiene entre sus funciones:

- a) Asesorar a la Comisión Nacional de Transparencia y Acceso a la Información respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales;
- b) Proponer a la Comisión Nacional de Transparencia y Acceso a la Información políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la LGPDPPSO y los Lineamientos generales;
- c) Implementar políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la LGPDPPSO y los Lineamientos generales, previa autorización de la Comisión Nacional de Transparencia y Acceso a la Información;
- d) Asesorar permanentemente a las unidades administrativas en materia de protección de datos personales;

- e) Establecer procedimientos internos para gestionar de manera eficiente las solicitudes de derechos ARCO.
 - f) Auxiliar y orientar al titular en la elaboración de las solicitudes para el ejercicio de sus derechos ARCO, en todo momento, y en especial en aquellos casos en que el titular no sepa leer ni escribir, así como informar sobre la obligación del titular de acreditar su identidad y, en su caso, la identidad y personalidad de su representante, así como los costos a cubrir por la reproducción y envío de los datos personales.
- a) Las demás que determine el responsable y la normatividad que resulte aplicable.

Lo anterior, sin perjuicio de lo señalado en el artículo 85 párrafo segundo de la LGPDPSO.

Para los términos del presente programa sus funciones serán las siguientes:

- a) Elaborar y proponer el Programa de protección de datos personales;
- b) Proponer cambios y mejoras al Programa;
- c) Coordinar la implementación del Programa;
- d) Asesorar a las Unidades Administrativas con la implementación del Programa;
- e) Presentar un informe anual a la Comisión Nacional de Transparencia;

De las Unidades Administrativas Responsables

Las Unidades Administrativas tendrán la función y responsabilidad de cumplir con la implementación de los principios, deberes y obligaciones que establece el presente Programa.

ALCANCE

El presente Programa es de observancia obligatoria por todos los individuos que pertenezcan a Movimiento Ciudadano, sea cual fuere su nivel jerárquico y su situación en la institución; así como para las personas externas que debido a la prestación de un servicio, tengan acceso a los sistemas de datos personales o al sitio donde se ubican los mismos, que para términos del presente documento, éstos desempeñan la función de encargados ya sea de la administración de los sistemas de datos personales o desarrolladores de aplicaciones.

CUMPLIMIENTO DE OBLIGACIONES

1. DEBER DE SEGURIDAD

Obligaciones	Actividades para su cumplimiento
Establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad e impedir que cualquier tratamiento contravenga las disposiciones del marco normativo en la materia.	1. Establecer y mantener medidas de seguridad: administrativas, técnicas y físicas para la protección de los datos personales.
Tomar en cuenta otras disposiciones vigentes en materia de seguridad de la información emitidas por otras autoridades, cuando éstas contemplen una mayor protección para el titular o complementen lo dispuesto por la LGPDPPSO y los Lineamientos Generales.	2. Revisar el marco normativo que regula el tratamiento específico de los datos personales, a fin de identificar medidas de seguridad adicionales y analizar la procedencia de su implementación.
Unidad administrativa responsable del cumplimiento <ul style="list-style-type: none">• Unidades Administrativas responsables de implementar los controles de seguridad contenidos en el Documento de Seguridad.	
Medios para acreditar el cumplimiento <ol style="list-style-type: none">1. Programa de Protección de Datos Personales, y Documento de seguridad.2. Evidencia generada en la implementación de los controles de seguridad, y Marco normativo.	

POLÍTICAS INTERNAS

Obligaciones	Actividades para su cumplimiento
<p>Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o supresión.</p>	<ul style="list-style-type: none"> • Cumplir con todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la LGPDPPSO y sus Lineamientos generales; • Establecer roles y responsabilidades de los involucrados internos y externos, relacionados con el tratamiento de datos personales; • Establecer sanciones en caso de incumplimiento; • Identificar el ciclo de vida de los datos personales en función de las finalidades para las que fueron recabados; • Establecer un proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales; • Establecer un proceso general de atención de los derechos ARCO.
<p>Unidad administrativa responsable del cumplimiento</p> <ul style="list-style-type: none"> • Comisión Nacional de Transparencia y Acceso a la Información • Unidad de Protección de Datos Personales • Unidad Administrativa responsable del tratamiento 	
<p>Medios para acreditar el cumplimiento</p> <ul style="list-style-type: none"> • Programa de Protección de Datos Personales, y • Documentación que se genere con motivo de la implementación y evaluación del Programa. 	

FUNCIONES DE LOS QUE TRATAN DATOS PERSONALES

Obligaciones	Actividades para su cumplimiento
<p>Establecer y documentar las funciones, obligaciones y cadena de rendición de cuentas del personal involucrado en el tratamiento de datos personales.</p> <p>Establecer mecanismos para asegurar que el personal involucrado en el tratamiento conozca sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento.</p>	<p>Definir las funciones, obligaciones y cadena de mando a personal que trata datos personales, por unidad administrativa.</p> <p>Comunicar al personal la información antes señalada, así como capacitarlos en la materia.</p>
<p>Unidad administrativa responsable del cumplimiento</p> <ul style="list-style-type: none"> • Comisión Nacional de Transparencia y Acceso a la Información • Unidad de Protección de Datos Personales • Unidad Administrativa responsable del tratamiento 	
<p>Medios para acreditar el cumplimiento</p> <ul style="list-style-type: none"> • Documento en el que se establezcan las funciones, obligaciones y cadena de mando de cada servidor público, por unidad administrativa, que trate datos personales; • Documento mediante el cual se haya comunicado la información antes señalada, y • Constancias de capacitación al personal. 	

INVENTARIO

Obligaciones	Actividades para su cumplimiento
<p>Elaborar un inventario de datos personales y de los sistemas, considerar el ciclo de vida de los datos personales, conforme a lo siguiente:</p> <ul style="list-style-type: none"> • La obtención; • El almacenamiento; • El uso conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin; • La divulgación considerando las remisiones y transferencias que, en su caso, se efectúen; • El bloqueo, en su caso, y • La cancelación, supresión o destrucción de los datos personales. 	<p>Identificar lo siguiente:</p> <ul style="list-style-type: none"> • El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos; • Las finalidades de cada tratamiento; • El catálogo del tipo de datos personales que se traten, indicando si son sensibles o no; • El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales; • La lista de personal con acceso a los sistemas de tratamiento; • 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 • En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen.
<p>Unidad administrativa responsable del cumplimiento</p> <ul style="list-style-type: none"> • Unidad de Datos Personales • Unidad administrativa responsable del tratamiento 	
<p>Medios para acreditar el cumplimiento</p> <ul style="list-style-type: none"> • Inventario de tratamiento de datos personales. 	

ANÁLISIS DE RIESGO, BRECHA Y PLAN DE TRABAJO

Obligaciones	Actividades para su cumplimiento
Realizar un análisis de riesgo de los datos personales.	<p>1. Considerar lo siguiente:</p> <ul style="list-style-type: none"> • El valor de los datos personales de acuerdo a 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; • El riesgo inherente a los datos personales tratados, contemplando el ciclo de vida de los datos personales, las amenazas y vulnerabilidades existentes para los datos personales y los recursos o activos involucrados en su tratamiento, como pueden ser, hardware, software, personal o cualquier otro recurso humano o material, entre otros; • La sensibilidad de los datos personales tratados; • El desarrollo tecnológico; • Las transferencias de datos personales que se realicen; • El número de titulares; • Las vulneraciones previas ocurridas en los sistemas de tratamiento, y • 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.
Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes.	<p>2. Considerar lo siguiente:</p> <ul style="list-style-type: none"> • Las medidas de seguridad existentes y efectivas; • Las medidas de seguridad faltantes, y

Obligaciones	Actividades para su cumplimiento
	<ul style="list-style-type: none"> • La existencia de nuevas medidas de seguridad que pudieran reemplazar a uno o más controles implementados actualmente.
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes.	3. Elaborar el plan de trabajo priorizando las medidas de seguridad más relevantes y urgentes, considerando los recursos designados; el personal y fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.
Unidad administrativa responsable del cumplimiento <ul style="list-style-type: none"> • Unidad de Protección de Datos Personales • Unidades Administrativas responsables de implementar los controles de seguridad mencionadas en el Documento de Seguridad. 	
Medios para acreditar el cumplimiento <ol style="list-style-type: none"> 1. Análisis de riesgo documentado, y Documento de seguridad. 2. Análisis de brecha documentado, y Documento de seguridad. 3. Plan de trabajo elaborado, y Documentos de análisis de riesgo y análisis de brecha. 	

REVISIÓN Y VIGILANCIA

Obligaciones	Actividades para su cumplimiento
<p>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.</p>	<p>Implementar el plan de monitoreo periódico, considerando lo siguiente:</p> <ul style="list-style-type: none"> • Los nuevos activos que se incluyan; • Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras; • Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas; • La posibilidad de que vulnerabilidades nuevas sean explotadas por las amenazas correspondientes; • Las vulnerabilidades identificadas para determinar aquéllas 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, y • Los incidentes y vulneraciones de seguridad ocurridas.
<p>Unidad administrativa responsable del cumplimiento</p> <ul style="list-style-type: none"> • Unidad de Protección de Datos Personales • Centro de Documentación e Información • Unidades Administrativas responsables de implementar los controles de seguridad mencionadas en el Documento de Seguridad. 	
<p>Medios para acreditar el cumplimiento</p> <ul style="list-style-type: none"> • Plan de monitoreo periódico, y • Documentación que se genere a partir de la implementación del plan. 	

SISTEMA DE GESTIÓN

Obligaciones	Actividades para su cumplimiento
Implementar un sistema de gestión para la seguridad de los datos personales, que permita planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales.	Implementar el Programa de Protección de Datos Personales basado en un sistema de gestión PHVA.
Unidad administrativa responsable del cumplimiento <ul style="list-style-type: none">• Comisión Nacional de Transparencia y Acceso a la Información• Unidad de Protección de Datos Personales• Unidades Administrativas responsables de implementar los controles de seguridad mencionadas en el Documento de Seguridad.	
Medios para acreditar el cumplimiento <ul style="list-style-type: none">• Programa de Protección de Datos Personales, y• Documentación que se genere a partir de la implementación del Programa.	

DOCUMENTO DE SEGURIDAD

Obligaciones	Actividades para su cumplimiento
Elaborar un documento de seguridad	<p>El DSDP debe contener al menos lo siguiente:</p> <ul style="list-style-type: none"> • El inventario de datos personales y de los sistemas de tratamiento; • Las funciones y obligaciones de las personas que traten datos personales; • El análisis de riesgos; • El análisis de brecha; • El plan de trabajo; • Los mecanismos de monitoreo y revisión de las medidas de seguridad, y • El programa general de capacitación.
Mantener actualizado el documento de seguridad	<p>Actualizarlo cuando ocurra lo siguiente:</p> <ul style="list-style-type: none"> • Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo; • Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión; • Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, e • Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.
<p>Unidad administrativa responsable del cumplimiento</p> <ul style="list-style-type: none"> • Unidades de Protección de Datos Personales. • Todas las unidades administrativas que realicen tratamiento de datos personales. 	
<p>Medios para acreditar el cumplimiento</p> <ul style="list-style-type: none"> • Documento de seguridad. 	

2. DEBER DE CONFIDENCIALIDAD

Obligaciones	Actividades para su cumplimiento
<p>Establecer controles o mecanismos para que todas las personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad, obligación que subsistirá aún después de finalizar las relaciones</p>	<ol style="list-style-type: none"> 1. Incluir en las medidas de seguridad, controles para garantizar la confidencialidad de los datos personales 2. Implementar cláusulas de confidencialidad de protección de datos personales para todo el personal que trata datos personales. 3. Establecer cláusulas en los contratos con los encargados, que obliguen a la confidencialidad de los datos personales. 4. Implementar capacitación, a fin de generar conciencia sobre la importancia de guardar la confidencialidad de los datos personales que tratan.
<p>Unidad administrativa responsable del cumplimiento</p> <ul style="list-style-type: none"> • Comisión Nacional de Transparencia • Secretaría de Asuntos Jurídicos • Unidades de Protección de Datos Personales. • Unidades Administrativas responsables de implementar los controles de seguridad mencionadas en el Documento de Seguridad. 	
<p>Medios para acreditar el cumplimiento</p> <ol style="list-style-type: none"> 1. Documento de seguridad, Controles de confidencialidad de los datos personales, y 2. Evidencia de la aplicación de los controles. 3. Contratos celebrados con los encargados del tratamiento. 4. Documentación que acredite la capacitación brindada y tomada. 	

3. PRINCIPIO DE LICITUD

Obligaciones	Actividades para su cumplimiento
Sujetar el tratamiento de los datos personales a las atribuciones o facultades que la normatividad aplicable confiera, los Lineamientos Generales, la legislación mexicana que le resulte aplicable y, en su caso, el derecho internacional, respetando los derechos y libertades de los titulares.	Identificar el marco normativo (leyes, tratados o acuerdos internacionales, reglamentos, lineamientos, entre otros, con sus respectivos artículos) que faculta a la unidad administrativa a tratar los datos personales para cada una de las finalidades, y aquél que regula el tratamiento respectivo.
Unidad administrativa responsable del cumplimiento <ul style="list-style-type: none">• Comisión Nacional de Transparencia y Acceso a la Información• Unidad de Protección de Datos Personales• Todas las unidades administrativas que realicen tratamiento de datos personales.	
Medios que facilitan la acreditación del cumplimiento <ul style="list-style-type: none">• Marco normativo	

4. PRINCIPIO DE LEALTAD

Obligaciones	Actividades para su cumplimiento
No obtener ni tratar los datos personales a través de medios engañosos o fraudulentos.	1. Verificar que los datos personales no se obtengan con dolo, mala fe o negligencia.
Privilegiar los intereses y expectativa razonable de privacidad de los titulares. Esta obligación deberá observarse a lo largo de todo el ciclo de vida de los datos personales, desde la obtención de los mismos hasta su tratamiento y eliminación.	<p>2. Verificar que el tratamiento no dé lugar a discriminación o trato injusto o arbitrario en contra del titular.</p> <p>Elaborar avisos de privacidad con todos los elementos que establece la LGPDPPSO</p> <p>Incluir en los avisos de privacidad todas las finalidades de los tratamientos, las cuales deberán estar redactadas de forma clara y concreta, para que no haya lugar a confusión.</p> <p>Llevar a cabo el tratamiento de los datos personales sólo para los fines informados en el aviso de privacidad.</p>
<p>Unidad administrativa responsable del cumplimiento</p> <ul style="list-style-type: none"> Todas las unidades administrativas que realicen tratamiento de datos personales. 	
<p>Medios que facilitan la acreditación del cumplimiento</p> <ol style="list-style-type: none"> Medios para la obtención de los datos personales, y Resultado de las auditorías o procedimientos de revisión efectuados. Avisos de privacidad, Documentación que se genere durante el tratamiento, que permita acreditar que los datos personales se utilizaron conforme a lo señalado en el aviso de privacidad, y según lo dispuesto en la normatividad, y Resultado de las auditorías o procedimientos de revisión efectuados. 	

5. PRINCIPIO DE INFORMACIÓN

Obligaciones	Actividades para su cumplimiento
Poner a disposición del titular el aviso de privacidad, con independencia de que se requiera o no el consentimiento.	1. Redactar los avisos de privacidad que se requieran conforme a los tratamientos que lleven a cabo las unidades administrativas. Se requerirá un aviso de privacidad <u>por tratamiento</u> .
El aviso de privacidad debe ser sencillo, con la información necesaria, claro y comprensible, queda prohibido lo dispuesto en el artículo 28 de los Lineamientos Generales	2. Seguir la estructura que se propone en los modelos de aviso de privacidad de la Guía para Generar el Aviso de Privacidad, o bien, generar los avisos de privacidad en el Generador de Avisos de Privacidad del Sector Público.
El aviso de privacidad deberá redactarse en sus dos modalidades: simplificado e integral.	3. Redactar las dos modalidades para cada aviso de privacidad: simplificado e integral.
El aviso de privacidad simplificado deberá contener todos los elementos informativos listados en el artículo 27 de la LGPDPPSO	4. Incluir todos los elementos informativos que resulten aplicables en el aviso de privacidad simplificado.
El aviso de privacidad integral debe contener los elementos informativos, listados en el artículo 27 y 28 de la LGPDPPSO	5. Incluir todos los elementos informativos que resulten aplicables en el aviso de privacidad integral.
Implementar mecanismos para que el titular manifieste su negativa para el tratamiento de datos personales.	6. Diseñar mecanismos que permitan al titular manifestar su negativa previo al tratamiento o transferencia de sus datos personales, cuando se requiera su consentimiento para ello.
Proveer los mecanismos para que el titular pueda conocer el aviso de privacidad simplificado e integral de que se trate.	7. Poner a disposición los avisos de privacidad, en su modalidad simplificados e integrales, en el apartado virtual correspondiente, a fin de que se difunda por medios electrónicos. Los avisos de privacidad deberán estar disponibles para su consulta en medio impreso

Difundir el aviso de privacidad por medios electrónicos y físicos.	(físico), en donde resulte conveniente según el medio por el que se obtengan los datos personales y por el que se tenga contacto con los titulares.
Observar los momentos para dar a conocer el aviso de privacidad.	8. De manera previa a la obtención de los datos personales, cuando los mismos se obtengan directamente del titular, sin importar el formato y medio, o Al primer contacto con el titular o previo al aprovechamiento de los datos personales, cuando éstos se obtengan de manera indirecta del titular.
Poner a disposición del titular un nuevo aviso de privacidad, en sus dos modalidades.	9. Poner a disposición de los titulares un nuevo aviso de privacidad cuando se actualice cualquiera de los supuestos señalados en el artículo 44 de los lineamientos Generales

Unidad administrativa responsable del cumplimiento

- Todas las unidades administrativas que realicen tratamiento de datos personales.

Medios que facilitan la acreditación del cumplimiento

1. Aviso de privacidad, y Procedimiento o medio para la puesta a disposición de los avisos de privacidad.
2. Aviso de privacidad.
3. Aviso de privacidad.
4. Aviso de privacidad.
5. Aviso de privacidad.
6. Avisos de privacidad respectivos, y Mecanismos a disposición del titular para manifestar su negativa.
7. Lugares y medios en los que se difundieron y colocaron los avisos de privacidad.
8. Procedimientos para puesta a disposición de los avisos de privacidad, y Sitios donde estén publicados avisos de privacidad integrales.
9. Puesta a disposición del nuevo aviso de privacidad.

6. PRINCIPIO DE CONSENTIMIENTO

Obligaciones	Actividades para su cumplimiento
Contar con el consentimiento del titular, salvo que se actualice alguna de las excepciones previstas en el artículo 22 de la LGPDPPSO.	1. Identificar las finalidades para las cuales se requiere el consentimiento de los titulares.
El consentimiento debe ser libre, específico e informado , según lo dispuesto por el artículo 20 de la LGPDPPSO	2. Solicitar el consentimiento después de que se ponga a disposición del titular el aviso de privacidad. Redactar las solicitudes de consentimiento de forma tal que éste sea libre, específico e informado, y que las solicitudes sean concisas e inteligibles, estén en un lenguaje claro y sencillo acorde con el perfil del titular.
El consentimiento debe ser tácito o expreso, según el tipo de datos personales y siguiendo las reglas establecidas en el artículo 21 de la LGPDPPP	3. Documentar la puesta a disposición del aviso de privacidad para la obtención del consentimiento tácito. Cuando los datos sean sensibles y no se actualice alguna de las causales del artículo 22 de la LGPDPPSO, se requerirá el consentimiento expreso y por escrito , es decir, a través de la firma autógrafa o firma electrónica del titular, huella dactilar, o por medio del mecanismo de autenticación que para tal efecto se establezca.
Cuando los datos personales se recaben directamente del titular.	4. Solicitar el consentimiento previo a la obtención de los datos personales y después de la puesta a disposición del aviso de privacidad.

Obligaciones	Actividades para su cumplimiento
<p>Cuando los datos personales se obtengan indirectamente del titular, y se requiera el consentimiento, no se podrán tratar los datos personales hasta que se cuente con la manifestación libre, específica e informada del titular, en la que autorice el tratamiento de sus datos personales de manera tácita o expresa, según corresponda.</p>	<p>5. Cuando los datos personales no los proporcione directamente el titular o su representante, se deberá enviar a los titulares el aviso de privacidad correspondiente al medio de contacto que tenga registrado. Asimismo, deberá informar que cuentan con un plazo de 5 días hábiles para en su caso manifestar su negativa para el tratamiento de sus datos personales para aquellas finalidades que requieran su consentimiento.</p> <p>En el caso del consentimiento expreso, es necesario que el mismo se solicite, ya sea en el cuerpo del aviso de privacidad o en un instrumento aparte. No se podrá tratar los datos personales si no cuenta con el consentimiento expreso del titular.</p>
<p>Atender las solicitudes de revocación del consentimiento, mismas que podrán ser presentadas por el titular en cualquier momento del tratamiento sin que se le atribuyan efectos retroactivos, a través del ejercicio de los derechos de oposición y cancelación.</p>	<p>6. Prever en el procedimiento interno para la atención de solicitudes de derechos ARCO lo relativo a la revocación del consentimiento, según los plazos, requisitos y procedimiento que se establecen para el ejercicio de los derechos de cancelación y oposición.</p>
<p>Unidad administrativa responsable del tratamiento</p> <ul style="list-style-type: none"> • Todas las unidades administrativas que realicen tratamiento de datos personales. • Unidad de Datos Personales 	

Obligaciones

Actividades para su cumplimiento

Medios que facilitan la acreditación del cumplimiento

1. Consentimiento expreso otorgado por los titulares, Aviso de privacidad, y Procedimiento para su puesta a disposición.
2. Procedimiento para la solicitud del consentimiento, Aviso de privacidad, Procedimiento para su puesta a disposición, y Consentimiento expreso otorgado.
3. Solicitud del consentimiento expreso, Consentimiento expreso otorgado por los titulares, y Puesta a disposición del aviso de privacidad.
4. Procedimiento para la solicitud del consentimiento, Aviso de privacidad y Procedimiento para su puesta a disposición, y Consentimiento expreso otorgado.
5. Aviso de privacidad, Constancia de envío del aviso de privacidad (Se sugiere utilizar un medio que permita acreditar la fecha en la que el titular recibió el aviso de privacidad), Respuesta por parte de los titulares, y Consentimiento expreso otorgado.
6. Procedimiento interno atención solicitud derechos ARCO.

DATOS PERSONALES SENSIBLES

Obligaciones	Actividades para su cumplimiento
No tratar datos personales sensibles, salvo que se cuente con el consentimiento expreso del titular o se trate de los casos establecidos en el artículo 22 de la LGPDPPSO.	<p>1. Revisar la necesidad y legalidad del tratamiento de datos personales sensibles para cumplir con la finalidad de que se trate, a fin de que quede debidamente justificada su obtención y uso.</p> <p>Revisar que se actualice alguno de los supuestos del artículo 22 de la LGPDPPSO, o bien, en caso contrario, solicitar el consentimiento expreso y por escrito del titular.</p>
No llevar a cabo tratamiento de datos personales que tengan como efecto la discriminación de los titulares por su origen étnico o racial, su estado de salud presente, pasado o futuro, su información genética, sus opiniones políticas, su religión o creencias filosóficas o morales y su preferencia sexual.	<p>2. Verificar que el tratamiento de datos personales no tenga como consecuencia la discriminación del titular.</p>
<p>Unidad administrativa responsable del cumplimiento</p> <ul style="list-style-type: none"> Todas las unidades administrativas que realicen tratamiento de datos personales. 	
<p>Medios para acreditar el cumplimiento</p> <ol style="list-style-type: none"> Marco normativo para el tratamiento de datos personales sensibles, y Consentimiento del titular, en su caso, o la actualización de alguno de los supuestos previstos en el artículo 22 de la LGPDPPSO. Documentación que se genere en torno al tratamiento. 	

7. PRINCIPIO DE PROPORCIONALIDAD

Obligaciones	Actividades para su cumplimiento
Tratar los datos personales sólo cuando resulten adecuados, relevantes y necesarios para la finalidad que justifica su tratamiento.	<p>Identificar qué datos personales se requieren para cada una de las finalidades.</p> <p>Analizar y revisar que se soliciten sólo aquellos datos personales que resultan indispensables para cumplir con las finalidades de que se trate.</p> <p>Cuando una normativa establezca con precisión los datos personales que deberán obtenerse para cumplir con la finalidad de que se trate, sólo deberán solicitarse dichos datos.</p> <p>Requerir el mínimo posible de datos personales para lograr las finalidades para las cuales se tratan.</p>
Unidad administrativa responsable del cumplimiento <ul style="list-style-type: none">• Todas las unidades administrativas que realicen tratamiento de datos personales.	
Medios para acreditar el cumplimiento <ul style="list-style-type: none">• Avisos de privacidad,• Documentos, expedientes, archivos o bases de datos correspondientes al tratamiento, y• Normatividad que establezca, en su caso, los datos personales que deberán solicitarse para el tratamiento específico.	

8. PRINCIPIO DE FINALIDAD

Obligaciones	Actividades para su cumplimiento
Justificar el tratamiento de los datos personales en finalidades concretas, lícitas, explícitas y legítimas.	1. Identificar las finalidades de cada tratamiento que se realice; Verificar que las mismas atiendan a fines específicos y acorde a las atribuciones de la unidad administrativa; Informan en el aviso de privacidad todas las finalidades para las cuales se tratan los datos personales, y describirlas de manera clara; Identificar qué finalidades requieren consentimiento y solicitarlo.
Las finalidades deben estar relacionadas con las atribuciones normativas de la unidad administrativa.	2. Identificar el marco normativo (ley, reglamento, lineamiento, entre otros, con sus respectivos artículos) que otorga las atribuciones a la unidad administrativa para tratar los datos personales.
Cuando se vayan a tratar los datos personales para finalidades distintas a las previstas en el aviso de privacidad, se requiere tener atribuciones legales para ello y el consentimiento del titular.	3. Identificar las finalidades que no fueron informadas en los avisos de privacidad y que se requieran llevar a cabo; Verificar que existan atribuciones legales para el tratamiento de los datos personales para estas finalidades adicionales; Solicitar el consentimiento de los titulares para estas finalidades adicionales, cuando se requiera; Implementar las medidas para cumplir con las obligaciones que establece la LGPDPPSO, con relación a las finalidades adicionales.
Unidad administrativa responsable del cumplimiento	
<ul style="list-style-type: none"> Todas las unidades administrativas que realicen tratamiento de datos personales 	
Medios para acreditar el cumplimiento	
<ol style="list-style-type: none"> Avisos de privacidad, Inventario de tratamientos de datos personales, y Documentos que se generen en el tratamiento. Marco normativo. Marco normativo ,y Consentimiento otorgado por los titulares o supuesto que se actualiza del artículo 22 de la LGPDPPSO. 	

9. PRINCIPIO DE CALIDAD

Obligaciones	Actividades para su cumplimiento
Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales, principalmente cuando se obtuvieron de manera indirecta del titular.	1. Implementar medidas para que los datos personales se actualicen y, en su caso, corrijan o completen de manera inmediata, en todas las bases de datos.
Establecer plazos de conservación de los datos personales. Considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos.	2. Establecer los plazos de conservación de los datos personales, para cada uno de los tratamientos, lo cual deberá ser congruente con los plazos de conservación establecidos en los instrumentos de clasificación archivística.
Establecer y documentar los procedimientos para la conservación y supresión de los datos personales, en los cuales se incluyan los periodos de conservación y realizar una revisión periódica sobre la necesidad de conservar los datos personales.	3. Elaborar los procedimientos para la conservación y supresión de los datos personales, así como documentarlos, éstos podrán ser los establecidos en materia de archivos
Unidad administrativa responsable del cumplimiento <ul style="list-style-type: none"> • Todas las unidades administrativas que realicen tratamiento de datos personales. • Coordinación Nacional de Archivo 	
Medios para acreditar el cumplimiento <ol style="list-style-type: none"> 1. Constancias o anotaciones sobre la rectificación realizada, en aquellos casos en que la misma haya sido procedente, y Base de datos actualizada y correcta 2. Instrumentos de clasificación archivística. 3. Procedimientos desarrollados, y Documentación y evidencia que se genere. 	

10. PRINCIPIO DE RESPONSABILIDAD

Obligaciones	Actividades para su cumplimiento
Elaborar políticas y programas de protección de datos personales obligatorios y exigibles, tomando en cuenta el desarrollo tecnológico y las técnicas existentes; la naturaleza, contexto, alcance, finalidades del tratamiento, atribuciones y facultades del responsable	1. Prever presupuesto para la instrumentación de programas y políticas de protección de datos personales. Elaborar un programa de protección de datos personales que contemple el cumplimiento de las obligaciones.
Poner en práctica un programa de capacitación del personal sobre las obligaciones y demás deberes en la materia.	2. Elaborar y aplicar un programa de capacitación y actualización del personal.
Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.	3. Establecer un sistema de supervisión y vigilancia para comprobar el cumplimiento del programa, incluyendo las medidas de seguridad.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares	4. De fácil acceso y con la mayor cobertura posible; considerando el perfil de los titulares y la forma en que se mantiene contacto o comunicación directa o cotidiana con ellos, así como estar, en todo momento, habilitado.
Diseñar e implementar las políticas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales.	5. Se deberán aplicar las medidas de carácter administrativo, técnico, físico o cualquier otra que resulten necesarias. de forma tal que prevean la privacidad por diseño y por defecto.
Implementar mecanismos para evidenciar el cumplimiento de los principios, deberes y obligaciones ante los titulares y el Instituto, tanto de tratamiento propio como de aquéllos realizados por los	6. En todos los casos generar pruebas para acreditar el cumplimiento de los principios, deberes y obligaciones que establece la LGPDPPSO, los Lineamientos Generales y demás disposiciones que resulten aplicables.

Obligaciones	Actividades para su cumplimiento
encargados y en las transferencias nacionales e internacionales.	
<p>Unidad administrativa responsable del cumplimiento</p> <ul style="list-style-type: none"> • Tesorería Nacional • Comisión Nacional de Transparencia y Acceso a la Información. • Centro de Documentación e Información • Unidad de Datos Personales • Todas las unidades administrativas que realicen tratamiento de datos personales. 	
<p>Medios para acreditar el cumplimiento</p> <ol style="list-style-type: none"> 1. Presupuesto del ejercicio en curso, y Programa de Protección de Datos personales. 2. Programa de capacitación. 3. Programa de supervisión y vigilancia, y resultados obtenidos. 4. Procedimiento para recibir y responder dudas y quejas de los titulares. 5. Políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología. 6. Pruebas generadas según lo establecido en la columna de “Medios para acreditar el cumplimiento” de todos los cuadros de este Programa. 	

11. MEDIDAS COMPENSATORIAS

Obligaciones	Actividades para su cumplimiento
<p>Instrumentar medidas compensatorias cuando resulte imposible dar a conocer al titular el aviso de privacidad simplificado de manera directa, o ello exija esfuerzos desproporcionados.</p>	<p>Dar a conocer el aviso de privacidad simplificado a través de la implementación de medidas compensatorias cuando</p> <p>Resulte imposible dar a conocer al titular el aviso de privacidad de manera directa, o Ello exija esfuerzos desproporcionados.</p> <p>Se debe evaluar si se requiere o no la autorización expresa del INAI para la implementación de medidas compensatorias</p> <p>Implementar las medidas compensatorias de conformidad con lo dispuesto por los Criterios Generales para la instrumentación de medidas compensatorias.</p>
<p>Unidad administrativa responsable del cumplimiento</p> <ul style="list-style-type: none"> • Todas las unidades administrativas que realicen tratamiento de datos personales. 	
<p>Medios que facilitan la acreditación del cumplimiento</p> <ul style="list-style-type: none"> • Evidencia de la difusión del aviso de privacidad por el medio de comunicación masiva utilizado para la medida compensatoria implementada, y • En su caso, autorización del INAI y evidencia de su difusión. 	

12. RELACIÓN CON LOS ENCARGADOS

Obligaciones	Actividades para su cumplimiento
Formalizar las relaciones con los encargados mediante contrato o instrumento jurídico, que permita acreditar su existencia, alcance y contenido.	Incluir en el instrumento jurídico, al menos, las siguientes obligaciones del encargado: <ul style="list-style-type: none"> • Las numeradas en el artículo 59 de la LGPDPPSO; • Permitir al INAI o al responsable, realizar verificaciones en el lugar o establecimiento donde se lleva a cabo el tratamiento de los datos personales; • Colaborar con el INAI en las investigaciones previas y verificaciones que lleve a cabo en términos de lo dispuesto en la LGPDPPSO y los Lineamientos Generales, proporcionando la información y documentación que se estime necesaria para tal efecto, así como • Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones.
Autorizar las subcontrataciones que realicen los encargados y que involucren el tratamiento de datos personales.	Incluir en los contratos originales con los encargados una cláusula que haga referencia a lo que procederá en caso de que el encargado desee subcontratar servicios que involucren el tratamiento de datos personales. Las autorizaciones se podrán otorgar desde el contrato original, cuando el encargado ya prevea subcontrataciones específicas, y garantice que las mismas se realizarán en las condiciones señaladas.
Unidad administrativa responsable del cumplimiento	
<ul style="list-style-type: none"> • Secretaría de Asuntos Jurídicos. • Centro de Documentación e Información • Unidad Administrativa que trate datos personales y lo requiera. 	
Medios para acreditar el cumplimiento	
<ul style="list-style-type: none"> • Cláusula tipo, y • Contratos o instrumentos jurídicos. 	

13. COMPUTO EN LA NUBE

Obligaciones	Actividades para su cumplimiento
<p>Contratar servicios de cómputo en la nube y similares con proveedores que garanticen políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la LGPDPPSO, los Lineamientos Generales y demás disposiciones que resulten aplicables en la materia.</p> <p>En caso de que los contratos se hayan celebrado antes de la entrada en vigor de la LGPDPPSO, será necesario que, para su modificación o renovación, se revise que los mismos cumplen con las condiciones antes señaladas, pues de lo contrario no podrán renovarse ni modificarse en los mismos términos.</p>	<p>Sólo contratar servicios de cómputo en la nube que garanticen que el servicio cumpla al menos, con lo siguiente:</p> <ul style="list-style-type: none"> • Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la LGPDPPSO y demás normativa aplicable; • Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; • Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y • Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.
<p>Contratar sólo servicios de cómputo en la nube que cuenten con ciertos mecanismos:</p>	<p>Mecanismos para:</p> <ul style="list-style-type: none"> • Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; • Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; • Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio; • Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable y que este último haya podido recuperarlos.

Obligaciones	Actividades para su cumplimiento
<p>Cuando el responsable tenga la posibilidad de convenir con el proveedor las condiciones y términos del servicio, además de observar las obligaciones específicas para servicios de cómputo en la nube.</p>	<p>Incluir en el instrumento jurídico las obligaciones generales de cualquier encargado.</p>
<p>Unidad administrativa responsable del cumplimiento</p> <ul style="list-style-type: none"> • Secretaría de Asuntos Jurídicos. • Unidad Administrativa que lo requiera. • Centro de Documentación e Información 	
<p>Medios para acreditar el cumplimiento</p> <ul style="list-style-type: none"> • Contratos o instrumentos jurídicos. 	

14. TRANSFERENCIAS

Obligaciones	Actividades para su cumplimiento
Formalizar las transferencias nacionales e internacionales mediante instrumento jurídico, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.	1. Elaborar instrumento jurídico, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes cuando se requiera.
Comunicar el aviso de privacidad respectivo al tercero receptor en las transferencias nacionales e internacionales que se realicen.	2. Cuando inicien las transferencias, comunicar el aviso de privacidad correspondiente.
Solicitar el consentimiento para las transferencias nacionales e internacionales	3. Identificar las transferencias que requieren consentimiento de los titulares e informarlo en el aviso de privacidad y solicitarlo a los titulares previo a la transferencia, cuando éste sea necesario y según la modalidad que se requiera (tácito o expreso y por escrito).
En caso de que se requiera el consentimiento expreso.	4. Establecer los medios para solicitar el consentimiento expreso, previo a la transferencia.
Sólo tratar los datos que hayan sido transferidos al responsable para las finalidades para las cuales le hayan sido comunicados, según lo establecido en el aviso de privacidad proporcionado, así como garantizar la confidencialidad de los datos personales.	5. Implementar los controles de seguridad establecidos para la confidencialidad de los datos personales, no tratar los datos personales para finalidades distintas.
Unidad administrativa responsable del cumplimiento <ul style="list-style-type: none"> • Todas las unidades administrativas que realicen tratamiento de datos personales y realicen transferencias. • Secretaría de Asuntos Jurídicos • Centro de Documentación e Información 	

Obligaciones**Actividades para su cumplimiento****Medios para acreditar el cumplimiento**

1. Cláusulas contractuales, convenios de colaboración u otros instrumentos jurídicos.
2. Evidencia de la comunicación del aviso de privacidad.
3. Consentimiento de los titulares.
4. Medios establecidos para solicitar el consentimiento, en caso de requerirse.
5. Controles implementados.

15. PORTABILIDAD

Obligaciones	Actividades para su cumplimiento
Otorgar al titular una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.	Atender las solicitudes del ejercicio del derecho de portabilidad según los criterios y parámetros establecidos por la LGPDPPSO y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.
Unidad administrativa responsable del cumplimiento <ul style="list-style-type: none">• Unidad de Datos Personales• Todas las unidades administrativas que realicen tratamiento de datos personales.	
Medios para acreditar el cumplimiento <ul style="list-style-type: none">• Documentación que se genere para atender las solicitudes de ejercicio del derecho de portabilidad.	

16. SUPRESIÓN DE LOS DATOS PERSONALES

Obligaciones	Actividades para su cumplimiento
Suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades y una vez que concluya su plazo de conservación establecido.	<p>1. Tener identificados los plazos de conservación de las series documentales que contienen datos personales.</p> <p>Realizar la eliminación de los documentos correspondientes a dichas series documentales cuando haya concluido el plazo de conservación respectivo.</p>
Previo a la supresión procederá el bloqueo.	2. Considerar en el plazo de conservación, la etapa de bloqueo de los datos personales.
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.	3. Considerar los atributos de irreversibilidad; seguridad y confidencialidad y favorable al medio ambiente.
<p>Unidad administrativa responsable del cumplimiento</p> <ul style="list-style-type: none"> • Coordinación Nacional de Archivo • Centro de Documentación e Información • Unidad de Datos Personales • Todas las unidades administrativas que realicen tratamiento de datos personales. 	
<p>Medios para acreditar el cumplimiento</p> <ol style="list-style-type: none"> 1. Instrumentos de clasificación archivística, Evidencia generada en la eliminación de los documentos, y Inventario de datos personales 2. Procedimiento de archivo que incluye el bloqueo. 3. Políticas, métodos y técnicas desarrolladas, y Documentación y evidencia que se genere con su implementación. 	

17. EVALUACIÓN DE IMPACTO

Obligaciones	Actividades para su cumplimiento
<p>Realizar una evaluación de impacto en la protección de datos personales, y presentarla ante el área establecida por el INAI cuando se pretenda poner en operación o modificar sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen el tratamiento intensivo o relevante de datos personales.</p>	<p>1. Establecer un procedimiento que prevea lo siguiente:</p> <ul style="list-style-type: none"> • Los mecanismos para detectar los casos en que se requiera la realización de la Evaluación de Impacto en la Protección de Datos Personales. • Los mecanismos para la elaboración y presentación de las Evaluaciones de Impacto en la Protección de Datos Personales.
<p>Atender el plazo para presentar la evaluación ante el INAI: 30 días anteriores a la fecha en que se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología.</p>	<p>2. Presentar en tiempo y forma las Evaluaciones que se requieran ante el área que establezca el INAI.</p> <p>Atender las observaciones que en su caso realice el INAI, y justificar cuando ello no sea posible.</p>
<p>Unidad administrativa responsable del cumplimiento</p> <ul style="list-style-type: none"> • Comisión Nacional de Transparencia y Acceso a la Información. • Todas las unidades administrativas que realicen tratamiento de datos personales. • Unidad de Protección de Datos Personales 	
<p>Medios para acreditar el cumplimiento</p> <ol style="list-style-type: none"> 1. Procedimiento. 2. Documentación que se genere con motivo de la presentación de la Evaluación ante el INAI y la atención de las observaciones que en su caso emita el Instituto. 	

18. CAPACITACIÓN

Obligaciones	Actividades para su cumplimiento
Establecer un programa anual de capacitación y actualización en materia de protección de datos personales	Establecer un programa anual de capacitación y actualización en materia de protección de datos personales, considerando los roles y responsabilidades asignadas y el perfil del puesto.
Unidad administrativa responsable del cumplimiento <ul style="list-style-type: none">• Comisión Nacional de Transparencia y Acceso a la Información• Unidad de Datos Personales.	
Medios para acreditar el cumplimiento <ul style="list-style-type: none">• Programa anual de capacitación.	

19. REVISIONES Y AUDITORIAS

Obligaciones	Actividades para su cumplimiento
<p>Contar con un programa de auditoría, interno y/o externo, y/o revisiones administrativas para monitorear y revisar la eficacia y eficiencia del sistema de gestión.</p>	<p>1. Elaborar un programa de aplicación de las revisiones administrativas y auditorías.</p> <p>Como resultado de las auditorías se deberá obtener el nivel de madurez de la protección de datos personales bajo resguardo, a fin de tenerlo como referencia para la mejora continua.</p>
	<p>2. Realizar al menos una auditoría integral una vez al año, incluir la revisión del cumplimiento de las obligaciones que tiene la Comisión Nacional de Transparencia en cuanto a la aplicación del presente Programa;</p> <p>Incluir, cifras, indicadores y estadísticas relacionadas con los procedimientos puestos en operación, y contener recomendaciones para hacer más efectivo y eficiente el cumplimiento del Programa.</p>
	<p>3. Llevar a cabo revisiones administrativas, las cuales deberán estar documentadas, y tendrán como objetivo supervisar:</p> <ul style="list-style-type: none"> • El adecuado desarrollo y efectividad del Programa; • El debido tratamiento en los cambios que afecten aspectos significativos en la protección de datos personales, como nueva normatividad, tecnología, o procesos o procedimientos. <p>Las revisiones administrativas deben basarse en:</p> <ul style="list-style-type: none"> • La retroalimentación por parte de las unidades administrativas; • Los riesgos identificados en el análisis de riesgos; • Los resultados de auditorías; • Los resultados de las revisiones anteriores;

Obligaciones	Actividades para su cumplimiento
	<ul style="list-style-type: none"> • Las actualizaciones o cambios en la tecnología, normatividad y procesos implementados; • Nuevos requerimientos por parte de autoridades; • Las quejas, y • Las vulneraciones de seguridad. <p>4. Las auditorías voluntarias, serán realizadas a través del INAI según el artículo 151 de la LGPDPPSO.</p>
<p>Unidad administrativa responsable del cumplimiento</p> <ul style="list-style-type: none"> • Comisión Nacional de Transparencia y Acceso a la Información • Unidad de Datos Personales. • Auditores internos y externos • Todas las unidades administrativas que realicen tratamiento de datos personales. 	
<p>Medios para acreditar el cumplimiento</p> <ol style="list-style-type: none"> 1. Programa de aplicación de revisiones administrativas y auditorías 2. Reportes de las auditorías que permitan identificar el nivel de madurez con relación a la protección de datos personales. 3. Documentos que acrediten la realización de la revisión administrativa. 4. Documentos que acrediten la realización de la auditoría voluntaria. 	

20. ACCIONES PARA LA MEJORA CONTINUA

Obligaciones	Actividades para su cumplimiento
<p>Implementar acciones preventivas y correctivas resultado de las auditorias y revisiones realizadas para corregir el no cumplimiento de las obligaciones.</p>	<p>Acciones preventivas: encaminadas a evitar cualquier “no cumplimiento”:</p> <ul style="list-style-type: none"> • Revisión de las posibles causas de no cumplimiento; • Determinar el no cumplimiento que podría desencadenarse a partir de situaciones de riesgo para el tratamiento de datos personales; • Evaluar las acciones para evitar que el no cumplimiento ocurra; • Revisar la eficacia de las acciones preventivas tomadas. <p>Acciones correctivas: encaminadas a eliminar las causas de “no cumplimiento”:</p> <ul style="list-style-type: none"> • Analizar el no cumplimiento; • Determinar las causas que dieron origen al no cumplimiento; • Evaluar las acciones necesarias para evitar que el no cumplimiento vuelva a ocurrir; • Implementar estas acciones; • Documentar los resultados de las acciones tomadas, y • Revisar la eficacia de las acciones correctivas tomadas. <p>Establecer un plazo límite para que se corrija el no cumplimiento detectado.</p>
<p>Unidad administrativa responsable del cumplimiento</p> <ul style="list-style-type: none"> • Comisión Nacional de Transparencia y Acceso a la Información • Unidad de Datos Personales 	
<p>Medios para acreditar el cumplimiento</p> <ul style="list-style-type: none"> • Procedimiento para la gestión de acciones preventivas y correctivas, y • Documentación que acredite las acciones preventivas o correctivas implementadas y sus resultados. 	

SANCIONES

La Comisión Nacional de Transparencia y Acceso a la Información, en caso de incumplimiento de alguna obligación prevista en el presente trabajo, realizará a la Unidad Administrativa identificada un exhorto para que lleve a cabo las acciones pertinentes con objeto de modificar dicha situación y evitar incumplimientos futuros o situaciones de riesgo que pudieran resultar.

Si persiste la negativa de colaboración, la Comisión Nacional de Transparencia y Acceso a la Información dará inicio el procedimiento de responsabilidad administrativo respectivo.

Es importante tener 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 Instituto, 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 Datos Personales 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 Datos Personales lo hará del conocimiento de la Comisión Nacional de Transparencia y Acceso a la Información de Movimiento Ciudadano para que, dé inicio el procedimiento de responsabilidad respectivo.

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

GLOSARIO

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 los mismos.

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.

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

LGPDPPO: 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.

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.

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

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.

Titular: Persona física a quien corresponden los datos personales.

Transferencias: 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.