POLÍTICAS PARA LA PROTECCIÓN DE DATOS PERSONALES

INTRODUCCIÓN

La Secretaría de Desarrollo Social protegerá los datos personales proporcionados por las personas que acuden a esta dependencia, en los sucesivo SEDESSON, por esta razón, se da a conocer a sus usuarios las siguientes políticas, basadas en la normatividad vigente aplicable a la protección de datos personales.

La Política de Privacidad y Protección de Datos Personales, en adelante la Política de Privacidad, explica cómo se tratan y protegen los datos personales que sean recolectados; dándote la seguridad de que datos personales proporcionados serán almacenados en forma segura.

En todo tratamiento de datos personales que se realice en la SEDESSON, se deberán respetar los principios y deberes dispuestos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de conformidad con lo estipulado para ello en los Lineamientos Generales de Protección de Datos Personales para el Sector Público y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sonora, que establece las disposiciones en materia de protección de datos personales, considerando el ciclo de vida de tales datos personales.

OBJETIVO GENERAL

Garantizar el cumplimiento de los principios, deberes y obligaciones establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sonora, Además, se establecerán pautas de comportamiento para asegurar el tratamiento adecuado y la protección de los datos personales, manteniendo la seguridad de la información y garantizando el respeto a los derechos de los titulares.

ÁMBITO DE APLICACIÓN

El presente documento es de aplicación y observancia general y obligatoria para todas las personas servidoras públicas de la SEDESSON que conforme a sus atribuciones realicen tratamiento de datos personales.

MARCO JURÍDICO

Constitución Política de los Estados Unidos Mexicanos.
Ley General de Protección de Datos Personales en Posesión de los Sujetos.
Ley General de Transparencia y Acceso a la Información Pública.
Constitución Política del Estado Libre y Soberano de Sonora.
Ley Protección Datos Personales En Posesión Sujetos Obligados Estado Sonora.
Ley de Transparencia y Acceso a la Información Pública del Estado de Sonora.
Los Lineamientos Generales de Protección de Datos Personales para el Sector Publico.
Reglamento Interior de la Secretaría de Desarrollo Social para el Estado de Sonora.

PRINCIPIOS QUE RIGEN LA PROTECCIÓN DE LOS DATOS PERSONALES

El artículo 7 de los Lineamientos Generales de Protección de Datos Personales para el Sector Publico, establece que en todo tratamiento de datos personales se deberá observar los principios rectores de la protección de datos personales:

- **Licitud**

El responsable deberá tratar los datos personales que posea sujetándose a las atribuciones o facultades que la normatividad aplicable le confiera, así como con estricto apego y cumplimiento de lo dispuesto en dicho ordenamiento, los presentes Lineamientos generales, la legislación mexicana que le resulte aplicable y, en su caso, el derecho internacional, respetando los derechos y libertades de los titulares.

- **Finalidad**

El tratamiento de los datos personales deberá limitarse a las finalidades establecidas en el aviso de privacidad, para las cuales el titular otorgó su consentimiento.

- **Lealtad**

La instancia o Sujeto Obligado responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses de la persona titular y la expectativa razonable de privacidad.

- **Consentimiento**

El tratamiento de datos personales, salvo excepciones reguladas por ley, estará sujeto al consentimiento de los titulares. Dicho consentimiento podrá ser expreso o tácito en aquellas situaciones en los que las leyes lo permitan, sin embargo, tratándose de datos financieros, patrimoniales o sensibles, el consentimiento deberá ser expreso, salvo excepciones por ley. El consentimiento se podrá manifestar por cualquier medio que permita recabarlo de manera inequívoca.

- **Calidad**

La instancia responsable deberá adoptar las medidas necesarias para mantener exactos, completos, pertinentes, correctos y actualizados los datos personales en su posesión, a fin de que no se altere su veracidad.

Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por su titular y hasta que tal persona no manifieste y acredite lo contrario.

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

- **Proporcionalidad**

La instancia responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento. Se entenderá que los datos personales son adecuados, relevantes y estrictamente necesarios cuando son apropiados, indispensables y no excesivos para el cumplimiento de las finalidades que motivaron su obtención, de acuerdo con las atribuciones conferidas al responsable por la normatividad que le resulte aplicable.

- **Información**

El titular de los datos personales deberá siempre ser informado de los datos personales a tratar, así como de las finalidades del tratamiento y los medios para ejercitar sus derechos; así mismo, deberá informarse de los cambios realizados en los medios, fines o tratamiento de los datos personales.

- **Responsabilidad**

La instancia responsable deberá adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley General y en la Ley local.

Los presenten principios serán los mínimos que deben observarse y ser incluidos en todas las actuaciones al respecto del tratamiento de datos personales que realiza el responsable o el encargado.

DEBERES QUE RIGEN LA PROTECCIÓN DE LOS DATOS PERSONALES

Los deberes que aplican y que se deben observar para el tratamiento de los datos personales son el de seguridad y el de confidencialidad:

Deber de seguridad: Se refiere a la obligación de establecer y mantener medidas de seguridad técnicas, físicas y administrativas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Para cumplir con este deber, las áreas deberán:

1. Establecer y mantener medidas de seguridad administrativas, físicas y técnicas.
2. No adoptar medidas de seguridad menores a aquéllas que mantengan para el manejo de su información.
3. Tomar en cuenta el riesgo inherente por tipo de dato personal; las posibles consecuencias para las personas titulares por una vulneración; la sensibilidad de los datos personales tratados y el desarrollo tecnológico.
4. Notificar a las personas titulares las vulneraciones de seguridad que se presenten, con la información y en los momentos antes señalados;
5. Llevar a cabo las acciones correctivas que sean necesarias.

Deber de confidencialidad: Este deber implica la obligación de guardar secreto respecto de los datos personales que son tratados. Este deber debe cumplirse para evitar causar un daño a su titular. De no ser así, un tercero no autorizado podría tener acceso a determinada información.

Para cumplir con este deber, las áreas deberán:

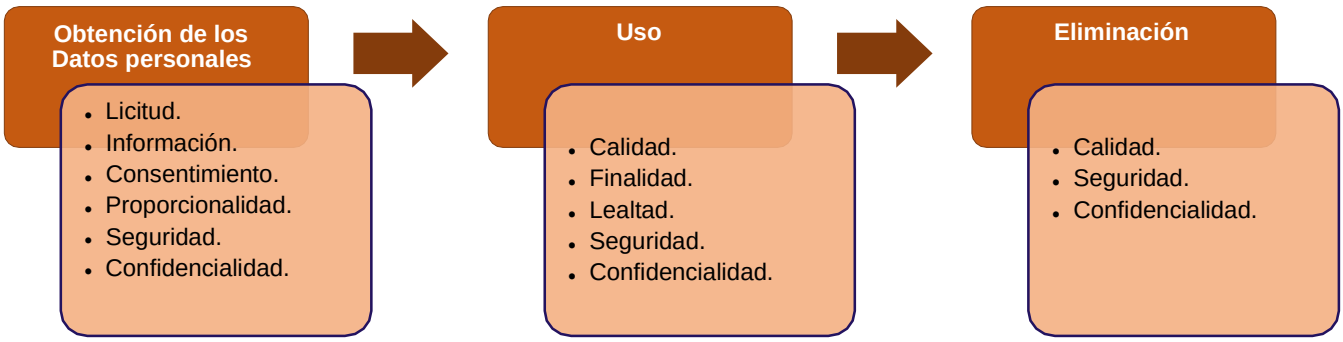
1. Guardar confidencialidad en cualquier fase del tratamiento de los datos personales, incluso después de finalizar la relación con la persona titular.
2. Verificar que los encargados también guarden confidencialidad de los datos personales que tratan a nombre y por cuenta del responsable, aun después de concluida la relación con éste.
3. Capacitar al personal para que conozca sus obligaciones con relación al tratamiento de datos personales.
4. Establecer procedimientos para evitar fuga de información o el acceso indebido a los datos personales.
5. Incluir en los contratos u otros instrumentos jurídicos que celebre con terceros, cláusulas de confidencialidad y para que quienes tengan acceso a los datos personales en posesión del responsable cumplan con esta obligación de confidencialidad.
6. Realizar verificaciones o supervisiones periódicas al trabajo realizado por los encargados, a fin de verificar que se cumplan con sus obligaciones en torno a la protección de los datos personales.

GENERALIDADES DEL CICLO DE VIDA DE LOS DATOS PERSONALES

En el respeto de los principios y el cumplimiento de los deberes previstos para el tratamiento de los datos personales, se deberán considerar las etapas que integran el ciclo de vida de los datos personales, las cuales son:

1. **Obtención** (los datos personales llegan a la instancia responsable);
2. **Uso** (registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento divulgación, transferencia o disposición); y,
3. **Eliminación** (concluye el ciclo del tratamiento de los datos personales).

Las etapas del ciclo de vida de los datos personales se concatenan con los principios y deberes de la forma que se indica a continuación:



Por tanto, las instancias deberán alinear cada etapa del ciclo de vida de acuerdo con el principio y deber respectivo.

PROHIBICIÓN DE TRATAMIENTOS QUE TENGAN COMO EFECTO CUALQUIER TIPO DE DISCRIMINACIÓN.

Queda prohibido el tratamiento de datos personales que tenga como efecto la discriminación de sus titulares por su origen étnico o racial, su estado de salud presente, futuro o pasado, su información genética, sus opiniones políticas, su religión o creencias filosóficas o morales o su preferencia sexual.

PRIVILEGIAR EL INTERÉS SUPERIOR DE LA NIÑA, NIÑO Y ADOLESCENTE.

Las instancias que, en ejercicio de sus funciones realicen el tratamiento de datos personales, deberán privilegiar el interés superior de la niña, niño y adolescente, en términos de lo establecido en la Ley General de los Derechos de Niñas, Niños y Adolescentes, así como lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los Lineamientos Generales de Protección de Datos Personales para el Sector Público y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sonora.

SANCIONES

Serán causas de sanción por incumplimiento a las obligaciones en materia de protección de datos personales, las establecidas en el artículo 193 de la LPDPPSOES:

I.- Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO o de la portabilidad de los datos personales;

II.- Incumplir los plazos de atención previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;

III.- Ampliar con dolo los plazos previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o la portabilidad de los datos personales;

IV.- 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;

V.- Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;

VI.- Mantener los datos personales inexactos cuando resulte imputable al responsable;

VII.- No efectuar la rectificación, cancelación u oposición al tratamiento de los datos personales que legalmente proceda, cuando resulten afectados los derechos de los titulares;

VIII.- No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refieren los artículos 38 y 39 de la presente Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;

IX.- Clasificar, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en Ley de Transparencia. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;

X.- Incumplir el deber de confidencialidad establecido en el artículo 60 de la presente Ley;

XI. No establecer las medidas de seguridad en los términos que establecen los artículos 47, 48 y 50 de la presente Ley;

XII.- Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 47, 48 y 50 de la presente Ley;

XIII.- Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley;

XIV.- Obstruir los actos de verificación de la autoridad;

XV.- Crear bases de datos personales en contravención a lo dispuesto por el artículo 8 de la presente Ley;

XVI.- No acatar las resoluciones emitidas por el Instituto;

XVII.- Aplicar medidas compensatorias en contravención de los criterios que tales fines establezca el Sistema Nacional;

XVIII.- Declarar dolosamente la inexistencia de datos personales cuando éstos existan total o parcialmente en los archivos del responsable;

XIX.- No atender las medidas cautelares establecidas por el Instituto;

XX.- Tratar los datos personales de manera que afecte o impida el ejercicio de los derechos fundamentales previstos en la Constitución Política de los Estados Unidos Mexicanos;

XXI.- No cumplir con las disposiciones previstas en los artículos 88, 93 y 94 de la presente Ley. XXII.- No presentar ante el Instituto la evaluación de impacto a la protección de datos personales en aquellos casos en que resulte obligatoria, de conformidad con lo previsto en la presente Ley y demás normativa aplicable;

XXIII.- Realizar actos para intimidar o inhibir a los titulares en el ejercicio de los derechos ARCO, y

XXIV.- Omitir l (sic) entrega del informe anual 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 día de manera extemporánea.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, XV, XVI, XVIII, XIX y XX, así como la reincidencia en las conductas previstas en el resto de las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa.

Las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

PROCESO GENERAL PARA EL ESTABLECIMIENTO, ACTUALIZACIÓN, MONITOREO Y REVISIÓN DE LOS MECANISMOS Y MEDIDAS DE SEGURIDAD.

El artículo 48, fracción VII de la LPDPPSOES establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

De acuerdo con la fracción XVIII del artículo 52 de la LPDPPSOES, los mecanismos de monitoreo y revisión forman parte del documento de seguridad. Así, respecto a los mecanismos de monitoreo y revisión de las medidas de seguridad, el artículo 63 de los Lineamientos Generales señala lo siguiente:

"***Monitoreo y supervisión periódica de las medidas de seguridad implementadas***

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

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

I. Los nuevos activos que se incluyan en la gestión de riesgos;

II. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;

III. Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;

IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;

V. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;

VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y

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

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

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

Mecanismos de Monitoreo

Para los tratamientos de datos personales la SEDESSON, considera los siguientes tipos de monitoreo:

1) Revisión de cumplimiento de las políticas internas de la SEDESSON, relacionadas con el tratamiento de datos personales. Tiene el objetivo de asegurar que las personas servidoras públicas realicen los tratamientos de datos personales en concordancia con lo dispuesto en la LGPDPPSO, LPDPPSOES, los Lineamientos Generales, y demás normatividad que resulte aplicable.

Para ello, cuando se identifica algún cambio en los instrumentos antes mencionados, se deberán realizar las siguientes actividades:

a) Revisar y, en su caso, actualizar los procesos involucrados en el tratamiento de datos personales.

b) Revisar y, en su caso, actualizar los avisos de privacidad, las funciones y obligaciones del personal y los inventarios de datos personales, según corresponda.

c) Evaluar si hubo cambios en las amenazas, vulnerabilidades o impacto de los riesgos relacionados con las modificaciones a la normativa, para actualizar los análisis de riesgos, análisis de brecha y plan de trabajo.

d) Revisar y, en su caso, adecuar los sistemas de tratamiento para cumplir con los cambios normativos.

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

a) **Monitoreo del entorno físico:** Para la detección continua de amenazas y vulnerabilidades en el entorno físico, se cuenta con:

- Personal de vigilancia en los accesos al edificio de la SEDESSON,
- control de acceso a través de bitácoras para visitantes y personal de la SEDESSON que olvidó su credencial,
- circuito cerrado de cámaras de vigilancia.

b) **Monitoreo del entorno electrónico**: Para la detección continua de amenazas y vulnerabilidades, la SEDESSON cuenta con herramientas de monitoreo.

c) **Actualización del plan de trabajo:** Derivado del monitoreo del entorno físico o electrónico, se pueden realizar actualizaciones en el plan de trabajo en caso de que se identifiquen cambios en las amenazas, las vulnerabilidades o el impacto de los riesgos identificados. Estos cambios se pondrán a consideración del área que apoya en el análisis de riesgos.

d) **Revisión de avances del plan de trabajo:** A través de los mecanismos que determine el área que apoya en el análisis de riesgos, se hará una revisión de los avances en el plan de trabajo, identificando las acciones, fechas compromiso y, en su caso, las causas por las cuales no se está cumpliendo el plan de trabajo, para hacer los ajustes correspondientes al mismo.

e) **Vulneraciones a la seguridad de los datos personales:** En caso de identificar un incidente de seguridad que involucre datos personales, el área que apoya en el análisis de riesgos, se coordinarán para decidir sobre las acciones pertinentes para mitigar dicho incidente. Mecanismos de supervisión o revisión Además del monitoreo continuo de las medidas de seguridad, se requiere realizar una supervisión periódica de las medidas de seguridad, a través de auditorías, las cuales pueden ser internas o externas.