SEGURIDAD
SECRETARÍA DE SEGURIDAD Y PROTECCIÓN CIUDADANA

PROTECCIÓN FEDERAL

POLÍTICAS INTERNAS PARA LA GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES DEL SERVICIO DE PROTECCIÓN FEDERAL

ÍNDICE

PRESENTACIÓN

Para la composición de estas ***Políticas Internas para la Gestión y Tratamiento de Datos Personales***, se tomaron como referencia la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Estas políticas, posibilitan a las áreas que integran al Servicio de Protección Federal a efecto de realizar un tratamiento de datos personales, en observancia a los principios y deberes establecidos en la Ley General y los Lineamientos Generales, lo cual permitirá garantizar una adecuada protección y el ejercicio de los Derechos ARCO, por parte de sus titulares.

I. OBJETO

Acreditar y asegurar el cumplimiento de los principios y deberes en materia de protección de datos personales, así como los roles y responsabilidades específicas de las unidades administrativas del Servicio de Protección Federal.

II. FUNDAMENTO LEGAL

- Constitución Política de los Estados Unidos Mexicanos.
- Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal.
- Ley Orgánica de la Administración Pública Federal.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.
- Ley Federal de Transparencia y Acceso a la Información Pública.
- Lineamientos Generales de Protección de Datos Persona les para el Sector Público.
- Reglamento del Servicio de Protección Federal.

III. ÁMBITO DE APLICACIÓN

Las presentes políticas son de observancia general y obligatoria para todas las personas servidoras públicas y unidades administrativas del Servicio de Protección Federal, que dan tratamiento a datos personales de conformidad con la Ley General y sus Lineamientos Generales.

IV. VIGENCIA Y DIFUSIÓN

Las presentes políticas estarán vigentes a partir del día hábil siguiente a su aprobación por el Comité de Transparencia del Servicio de Protección Federal, cuya difusión será a través del espacio virtual de "Protección de Datos Personales", que se encuentra en el portal Institucional: https://spf.gob.mx/sitio_transparencia/.

V. TÉRMINOS Y DEFINICIONES

- **Activos:** Los bienes tangibles o intangibles que posee el SPF, donde pueden ser almacenadas las bases de datos;
- **Aviso de privacidad:** Documento a disposición del titular de forma física, electrónica o cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos;
- **Bases de datos:** Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;
- **Bloqueo:** La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda;
- **Comité de Transparencia:** Autoridad máxima en materia de protección de datos personales a la que hacen referencia los artículos 43, de la Ley General de Transparencia Acceso a la Información Pública y 83, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
- **Consentimiento:** Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos;
- **Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;
- **Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;
- **Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al

tratamiento de datos personales;

- **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;
- **Fuentes de acceso público:** Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la presente Ley y demás normativa aplicable;
- **Instituto:** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), el cual es el organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados;
- **Ley General**: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
- **Lineamientos Generales:** Lineamientos Generales de Protección de Datos Personales para el Sector 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;
- **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;
- **Responsable del tratamiento de datos personales**: El Servicio de Protección Federal;
- **SPF**: Servicio de Protección Federal;
- **Persona Servidora Pública:** Las personas que nombren con tal carácter los titulares de las unidades administrativas del SPF, a efecto de atender los requerimientos que en materia de protección de datos personales, formulen la Unidad de Transparencia y/o el Comité de Transparencia del SPF;
- **Sistema de Gestión:** Conjunto de elementos y actividades interrelacionadas para establecer y mejorar el tratamiento y seguridad de los datos personales de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público;
- **Sistema de Datos:** Archivo físico o electrónico que contenga datos personales que

se hayan recabado para el ejercicio de las funciones de las Unidades Administrativas;

- **Solicitante:** Toda persona física o jurídica, nacional o extranjera, que formule al SPF, una solicitud relacionada con los derechos ARCO;
- **Supresión:** La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable;
- **Titular:** La persona física a quien corresponden los datos personales;
- **Transferencia:** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado;
- **Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales;
- **Unidades administrativas:** Áreas previstas en el artículo 8, del Reglamento del Servicio de Protección Federal, que cuentan o pueda contar, dar tratamiento, y ser responsables o encargadas de los datos personales;
- **Vulneraciones:** 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, y
- **Unidad de Transparencia**: Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

VI. PRINCIPIOS PARA LA PROTECCIÓN DE DATOS PERSONALES

PRIMERA: Las personas servidoras públicas vinculadas en el tratamiento de datos personales, deberán observar los principios de licitud, finalidad, consentimiento, información, proporcionalidad, calidad, responsabilidad y lealtad.

SEGUNDA: Las unidades administrativas, en el tratamiento de datos personales, se sujetarán a las atribuciones o facultades que les son conferidas en la normatividad que rige el actuar del Servicio de Protección Federal, en estricto apego a lo dispuesto en la Ley General y los Lineamientos Generales, las presentes Políticas y demás disposiciones legales aplicables en materia de protección de datos personales.

Para cumplir con el principio de licitud, los servidores públicos vinculados a las unidades administrativas, incluirán en el aviso de privacidad, el fundamento legal que les faculta a tratar datos personales.

TERCERA: Las unidades administrativas tratarán datos personales sensibles y/o biométricos, siempre y cuando ello resulte adecuado, relevante y estrictamente necesario para la finalidad que justifica su tratamiento.

CUARTA: Todo tratamiento de datos personales efectuado por las personas servidoras públicas vinculadas a las unidades administrativas, deberá estar justificado por finalidades concretas, licitas, explicitas y legitimas.

Para dar cumplimiento al principio de finalidad, deberán:

- Incluir en el inventario, las finalidades de cada tratamiento que se realice en su unidad administrativa y verificar que éstas sean específicas o determinadas y acordes a las atribuciones o facultades del Desconcentrado y de su área.
- Vigilar que las personas servidoras públicas únicamente traten datos personales en términos de las finalidades informadas en el aviso de privacidad correspondiente.
- Verificar que en los avisos de privacidad se informen todas las finalidades para las cuales se tratan los datos personales, y que éstas sean descritas de manera clara.
- Informar a los titulares sobre el tratamiento de los datos para finalidades distintas.
- Recabar el consentimiento de los titulares, cuando este proceda.

QUINTA: Las personas servidoras públicas vinculadas a las unidades administrativas, se abstendrán de obtener y tratar datos personales a través de medios engañosos o fraudulentos, privilegiando la protección de los titulares y su privacidad.

Para acreditar el cumplimiento del principio de lealtad las personas servidoras públicas responsables del tratamiento de datos personales deberán:

a) Obtener y tratar los datos personales sin que medie dolo, mala fe o negligencia;
b) Privilegiar los intereses del titular y, evitar cualquier tipo de discriminación, trato injusto o arbitrario en contra de éstos, con motivo del tratamiento de sus datos, y
c) Respetar la expectativa razonable de privacidad.

SEXTA: Las personas servidoras públicas vinculadas a las unidades administrativas, previo al tratamiento de los datos personales, obtendrán el consentimiento del Titular de manera libre, específica e informada, salvo que se actualice alguna de las causales de excepción siguientes:

a) Cuando una ley así lo disponga, en cuyo caso, los supuestos de excepción deberán ser acordes con las bases, principios y disposiciones establecidos en la Ley General que, en ningún caso, podrán contravenirla.
b) Cuando las transferencias que se realicen entre la SPF y otro sujeto responsable sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o acordes con la finalidad que motivó el tratamiento de los datos personales.

c) Cuando exista una orden judicial, resolución o mandato fundado y motivado por una autoridad competente.
d) Para el reconocimiento o defensa de derechos del titular ante autoridad competente.
e) Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el SPF.
f) Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes
g) Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico o la prestación de asistencia sanitaria.
h) Cuando los datos personales figuren en fuentes de acceso público.
i) Cuando los datos personales se sometan a un procedimiento previo de disociación.
j) Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

Cabe precisar, que el consentimiento tácito será válido para llevar a cabo el tratamiento de datos personales, salvo aquellos supuestos en los cuales la Ley General o alguna disposición aplicable exija su obtención de forma expresa y, en su caso, por escrito, particularmente, cuando se refiera a datos sensibles.

Para dar cumplimiento al principio de consentimiento, las unidades administrativas deberán:

a) Identificar en el aviso de privacidad, aquellos datos y finalidades que requieren del consentimiento del Titular, para su tratamiento.
b) Mantener bajo su resguardo una copia del documento en el cual se haya manifestado el consentimiento del Titular para el tratamiento de sus datos, cuando éste proceda.
c) Documentar la puesta a disposición del aviso de privacidad al Titular, en aquellos casos en los cuales sea válido el consentimiento tácito.

SÉPTIMA: Las personas servidoras públicas vinculadas a las áreas, deberán considerar que, independientemente de que traten datos personales, sin importar la función con la que se vincule, elaborarán y pondrán a disposición los avisos de privacidad simplificados e integrales que correspondan a los tratamientos llevados a cabo, en los términos establecidos por la Ley General y los Lineamientos Generales, así como en las presentes Políticas.

Para acreditar el cumplimiento del principio de información, las personas servidoras públicas realizarán las acciones siguientes:

a) Contar con los avisos de privacidad integral y simplificado por cada proceso de tratamiento de datos personales que se lleve a cabo.
b) Realizar las gestiones con la Unidad de Transparencia, para que los avisos de

privacidad, en sus modalidades simplificado e integral, sean publicados en el portal de Internet del Servicio de Protección Federal, en la sección que se destine para ello, a fin de que se difunda por medios electrónicos.

c) Documentar la comunicación realizada del aviso de privacidad a terceros a los que se transfieran los datos personales.

OCTAVA: Las personas servidoras públicas vinculadas a las unidades administrativas, recabarán aquellos datos personales que resulten adecuados, relevantes y necesarios para la finalidad que justifica su tratamiento.

Para dar cumplimiento al principio de proporcionalidad, las personas servidoras públicas deberán:

a) Recabar y tratar sólo aquellos datos personales necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.
b) Realizar esfuerzos razonables para actualizar la normativa y formatos internos, con el fin de limitar los datos personales tratados al mínimo necesario, considerando las finalidades que motivan su tratamiento.
c) Limitar al mínimo posible el periodo de tratamiento de datos personales.
d) Analizar y revisar que en su área se soliciten sólo aquellos datos personales que resultan indispensables para cumplir con las finalidades de que se trate.
e) Promover que en su área se requiera el mínimo posible de datos personales para lograr las finalidades para las cuales se tratan.
f) Fomentar prácticas que minimicen la obtención de datos personales y el periodo de su tratamiento, así como señalarlas en el documento de seguridad.

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 a las unidades administrativas del Servicio de Protección Federal.

NOVENA: Las personas servidoras públicas vinculadas a las unidades administrativas adoptarán las medidas señaladas en el documento de seguridad para mantener los datos personales exactos, correctos, completos y actualizados, a fin de que no se altere la veracidad de éstos.

Para acreditar el cumplimiento del principio de calidad, las personas servidoras públicas deberán realizar lo siguiente:

a) Generar una relación de todas las bases de datos con que cuentan y el tipo de información personal tratada en cada una de ellas que, en su caso, permita vincularlas.
b) Documentar las actualizaciones y supresiones realizadas.
c) Contar con los procedimientos para la conservación, bloqueo y supresión de los datos personales.

DÉCIMA: El Servicio de Protección Federal velará por el cumplimiento del principio de responsabilidad, adoptando medidas necesarias para su aplicación y demostrará ante los titulares y el Instituto que se cumple con las obligaciones en materia de protección de los datos personales.

Para ello, el Servicio de Protección Federal contará con un Programa de Protección de Datos Personales, aprobado por el Comité de Transparencia, cuyo objetivo es determinar las acciones generales bajo las cuales se llevarán a cabo las tareas institucionales orientadas a mantener la observancia en el cumplimiento de los principios y deberes, así como a garantizar el derecho a la protección de datos personales al interior de este sujeto obligado.

El Programa podrá ser sometido a su revisión, ajuste o actualización por parte del Comité de Transparencia, de conformidad con las facultades y atribuciones que le establece la normativa aplicable, en caso de considerarse necesario.

DÉCIMA PRIMERA: Para acreditar el cumplimiento al principio de responsabilidad, las unidades administrativas deberán:

a) Contar con las constancias de capacitación de su personal en temas relacionados con la materia de protección de datos personales.
b) Documentar la comunicación hacia su personal de la presente Política y del Programa de protección de datos que al efecto sea aprobado.
c) Guardar evidencia del cumplimiento a las presentes Políticas.

DÉCIMA SEGUNDA: Las unidades administrativas del Servicio de Protección Federal se abstendrán de obtener y tratar datos personales a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

Para acreditar el cumplimiento al principio de lealtad, las unidades administrativas deberán:

a) Contar con avisos de privacidad que cumplan con lo establecido en la Ley General y las presentes Políticas.
b) Implementar instrumentos que permitan verificar que los tratamientos realizados no den lugar a discriminación, trato injusto o arbitrario en contra del titular.
c) Constatar que el tratamiento de datos personales sólo se lleve a cabo para los fines informados en el aviso de privacidad.

VII. DEBERES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

DÉCIMA TERCERA: Además de los principios señalados anteriormente, las personas servidoras públicas cumplirán con lo siguiente:

- Deber de confidencialidad.
- Deber de seguridad.

DÉCIMA CUARTA: Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

El titular de la unidad administrativa responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico, así como garantizar su confidencialidad, integridad y disponibilidad.

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.
d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure la disponibilidad e integridad.
e) Prevenir el acceso a las bases de datos o a la información, así como a los recursos sea por usuarios identificados y autorizados.
f) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.
g) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.
h) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

DÉCIMA QUINTA: Para cumplir con el deber de confidencialidad, las personas servidoras públicas establecerán controles o mecanismos de observancia obligatoria que intervendrán en cualquier fase del tratamiento y guardarán confidencialidad de los datos personales, obligación que subsistirá aún después de finalizar su relación laboral con el SPF y sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.

Para el debido cumplimiento del deber de confidencialidad, las unidades administrativas deberán:

a) Prever controles mediante los cuales se garantice la confidencialidad de los datos

personales que son tratados.

b) Incluir en el documento de seguridad, los controles y medidas de seguridad implementadas para garantizar la secrecía de los datos personales.
c) Establecer cláusulas en los contratos para que los sujetos obligados del ámbito público o privado a los cuales les sean transferidos o remitidos datos personales se obliguen a la confidencialidad de éstos, durante y posterior a la vigencia del instrumento jurídico.
d) La Unidad de Transparencia implementará campañas de sensibilización para las personas servidoras públicas, en materia de protección de datos personales y sobre la importancia de la confidencialidad de los datos personales.
e) Tener la evidencia documental de los cursos, talleres, seminarios o similar en los que haya participado el personal y se encuentre relacionado con la materia de protección de datos personales.
f) Incentivar la capacitación de los servidores públicos involucrados en el tratamiento de datos personales, conforme al nivel de responsabilidad que éstos tengan asignado.

DÉCIMA SEXTA: Para el debido cumplimiento del deber de seguridad, las personas servidoras públicas llevarán a cabo, al menos, lo siguiente:

a) Contar con un inventario de datos y de los sistemas de tratamiento.
b) Comunicar al personal las políticas implementadas para la protección de datos y guardar evidencia de ello.
c) Llevar una bitácora en la cual se asiente cualquier amenaza o vulneración de datos personales suscitada, así como las acciones realizadas para su mitigación.
d) Instrumentar las medidas de seguridad físicas, técnicas y administrativas adoptadas para garantizar el tratamiento de los datos recabados, así como las acciones de monitoreo, análisis y revisión a implementar, a fin de mantenerlas actualizadas y, en su caso, detectar áreas de oportunidad para su desarrollo y ejecución.
e) Tener la evidencia documental de los cursos, talleres, seminarios o similar en los que haya participado el personal de la unidad administrativa y se encuentre relacionado con la materia de protección de datos personales.

DÉCIMA SÉPTIMA: El SPF debe contar con un Documento de Seguridad como parte de los mecanismos implementados para asegurar el cumplimiento al deber de seguridad, cuyo objeto es establecer, de manera general, las medidas de seguridad técnicas, físicas y administrativas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales tratados.

DÉCIMA OCTAVA: El Documento de Seguridad deberá contener como mínimo, lo siguiente:

- El inventario de datos personales y de los sistemas de tratamiento.
- Las funciones 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.
- El programa general de capacitación.

DÉCIMA NOVENA: En las actualizaciones que se realicen al Documento de Seguridad, deberán participar todas las unidades administrativas, a través de las personas servidoras públicas designadas a que se hace referencia la presente Política, quienes en todo momento observarán los principios y deberes a que se refiere la Ley General y los Lineamientos Generales

La Unidad de Transparencia, elaborará formatos o cualquier otro instrumento de apoyo que resulte útil para el cumplimiento de estas Políticas y demás disposiciones aplicables en la materia.

VIGÉSIMA: El Documento de Seguridad se actualizará en los supuestos siguientes:

a) Se produzcan notificaciones sustanciales al tratamiento de los datos personales que deriven en un cambio de nivel de riesgo.
b) Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión con que se cuente.
c) Derivado de un proceso de mejora para mitigar el impacto de vulneración a la seguridad ocurrida.
d) Con motivo de la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

VIGÉSIMA PRIMERA: Cuando alguna de las unidades administrativas se encuentre en los supuestos referidos, la persona servidora pública designada solicitará por escrito a la Unidad de Transparencia, las actualizaciones correspondientes, quien resolverá lo conducente.

La persona servidora pública, designada podrán solicitar orientación técnica a la Unidad de Transparencia, para la integración o cualquier acto relacionado con los alcances del Documento de Seguridad.

VIGÉSIMA SEGUNDA: En términos de lo previsto en la Ley General, se consideran vulneraciones a la seguridad de los datos, las siguientes:

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

VIGÉSIMA TERCERA: Cuando las vulneraciones afecten de forma significativa los derechos patrimoniales o morales de los Titulares, las unidades administrativas involucradas, deberán generar un informe detallado que contenga al menos lo siguiente:

- La naturaleza del incidente.
- Los datos personales comprometidos.
- Las recomendaciones al titular acerca de las medidas que éste puede adoptar para proteger sus intereses.
- Las acciones correctivas implementadas para mitigar la vulneración.
- Los datos de contacto del enlace responsable o personal al cual puede acudir el titular para obtener más información al respecto.

El referido informe será remitido a la Unidad de Transparencia, en un plazo no mayor a dos días naturales posteriores a la fecha en que se haya confirmado la vulneración, para que ésta lo haga del conocimiento de los titulares de los datos involucrados y del Comité de Transparencia.

Adicional a lo anterior, las unidades administrativas deberán prever en el informe a notificarse al Instituto, por parte de la Unidad de Transparencia, lo siguiente:

- La hora y fecha de la identificación de la vulneración.
- La hora y fecha del inicio de la investigación sobre la vulneración.
- La naturaleza del incidente o vulneración ocurrida.
- La descripción detallada de las circunstancias en torno a la vulneración ocurrida.
- Las categorías y número aproximado de titulares afectados.
- Los sistemas de tratamiento y datos personales comprometidos.
- La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida.
- Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.

VIGÉSIMA CUARTA: Se entenderá que se afectan los derechos patrimoniales del titular, cuando la vulneración esté relacionada con sus bienes, información fiscal, historial crediticio, ingresos, egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados u otros similares.

Para el caso de los derechos morales, se entenderán aquellos relacionados, de manera enunciativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, aspecto físico; que en su caso menoscabe ilegalmente la libertad, integridad física o psíquica del Titular de los datos, de conformidad con lo dispuesto por el artículo 66 de los Lineamientos Generales.

VIII. ROLES Y RESPONSABILIDAD ESPECÍFICA DE LOS INVOLUCRADOS INTERNOS

VIGÉSIMA QUINTA: Cada unidad administrativa responsable de un Sistema de Datos Personales deberá adoptar las medidas necesarias para mantener seguros, exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de estos.

VIGÉSIMA SEXTA: Las actualizaciones de los Sistemas de Datos Personales deberán realizarse por las unidades administrativas responsables de su administración, el Titular de estas, remitirá a la Unidad de Transparencia en el formato que establezca para tal efecto la modificación, actualización o cancelación de dichos Sistemas.

VIGÉSIMA SÉPTIMA: Cada unidad administrativa designará a una persona servidora pública para fungir al interior de esta, como enlace responsable de las actividades de dirección en la protección de datos personales, con el fin de garantizar y evidenciar la operación y cumplimiento de esta Política ante el titular de los datos y el Instituto.

Las personas servidoras públicas designadas como enlaces, contarán con las funciones siguientes:

a) Implementar y acreditar en su unidad administrativa, el cumplimiento de los principios y deberes de acuerdo con las directrices señaladas por esta Política y el Comité de Transparencia, en su calidad de autoridad máxima en materia de datos personales al interior de la SPF.
b) Promover la capacitación de las personas servidoras públicas adscritas a su unidad administrativa y que se encuentren involucradas directamente en el tratamiento de datos personales.
c) Participar en la integración y actualización de los documentos normativos exigidos por la ley y demás disposiciones aplicables.
d) Validar y, en su caso, actualizar semestralmente el inventario de datos personales que, en el ámbito de su competencia, correspondan a su unidad administrativa.
e) Gestionar al interior de su unidad administrativa, la debida atención de solicitudes relativas al ejercicio de los Derechos ARCO que sean presentadas ante la Unidad de Transparencia.
f) Las demás que determinen las disposiciones normativas, el Instituto o, aquellas que deriven de las resoluciones emitidas por el Comité de Transparencia.

Para tal efecto, el Comité de Transparencia tiene la facultad de exhortar a las personas servidoras públicas, con el propósito de que cumplan con los principios, deberes, bases y procedimientos que rigen el tratamiento de datos personales, debiendo atender con celeridad y eficiencia los requerimientos específicos que les sean formulados, respetando estrictamente los plazos y términos establecidos en la Ley General y los Lineamientos Generales.

Cuando alguna persona servidora pública se niegue a atender los requerimientos del Comité de Transparencia de la Unidad de Transparencia, se dará vista al Titular de la unidad administrativa de su adscripción, solicitándole que lo conmine a realizar sin demora las acciones conducentes, con independencia de que pueda darse vista al Órgano Interno de Control, en caso de que se presuma alguna causal de responsabilidad.

IX. DE LAS SANCIONES

VIGÉSIMA OCTAVA: Las personas servidoras públicas vinculadas a las unidades administrativas, podrán ser sancionadas por incumplimiento a las obligaciones establecidas en la Ley General, mismas que pueden ser las siguientes:

- Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO.
- Incumplir los plazos de atención previstos en la Ley General, para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate.
- 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.
- Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la Ley General y en las presentes Políticas.

X. IDENTIFICACIÓN DEL CICLO DE VIDA DE LOS DATOS PERSONALES

VIGÉSIMA NOVENA: Las personas servidoras públicas vinculadas a las unidades administrativas, deberán adoptar las medidas necesarias para mantener seguros, exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de estos.

TRIGÉSIMA: En la elaboración de los inventarios de datos personales, las unidades administrativas deberán determinar el ciclo de vida respecto de cada tratamiento que se efectué, considerando la obtención, almacenamiento, uso, procesamiento, divulgación, bloqueo, cancelación, supresión, destrucción o cualquier otra operación realizada en función de las finalidades para las que fueron recabados los datos personales.

TRIGÉSIMA PRIMERA: 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 aquellos 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.

TRIGÉSIMA SEGUNDA: Las personas servidoras públicas responsables de sus sistemas y/o bases de datos personales, deberán establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleven a cabo, en los cuales se incluyan los periodos de conservación de los mismos, de conformidad con lo dispuesto en el artículo 23 de la Ley General.

En los procedimientos a que se refiere el párrafo anterior, las unidades administrativas responsables de sistemas y/o bases datos personales deberán incluir mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos personales, así como para realizar una revisión periódica sobre la necesidad de conservar los datos personales en la SPF.

XI. MONITOREO Y SUPERVISIÓN PERIÓDICA DE LAS MEDIDAS DE SEGURIDAD IMPLEMENTADAS

TRIGÉSIMA TERCERA: Para cumplir con el monitoreo y supervisión de las medidas de seguridad, las personas servidoras públicas vinculadas a las unidades administrativas deberán monitorear continuamente lo siguiente:

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

XII. PROCEDIMIENTO DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN (ARCO) AL TRATAMIENTO DE DATOS PERSONALES

TRIGÉSIMA CUARTA: En la solicitud para el ejercicio de los derechos ARCO no podrán imponerse mayores requisitos que los siguientes:

a) El nombre del Titular y su domicilio o cualquier otro medio para recibir notificaciones;
b) Los documentos que acrediten la identidad del Titular y, en su caso, la personalidad e identidad de su representante;
c) De ser posible, la unidad administrativa responsable que trata los datos personales y ante la cual se presenta la solicitud;
d) La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso;
e) La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el Titular;
f) Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso. Tratándose de una solicitud de acceso a datos personales, el Titular o su representante deberá señalar la modalidad en la que prefiere que estos se reproduzcan, y
g) Las unidades administrativas deberán atender la solicitud en la modalidad requerida por el Titular, salvo que exista una imposibilidad física o jurídica que lo limite a reproducir los datos personales en dicha modalidad, en este caso deberá ofrecer otras modalidades de entrega de los datos personales fundando y motivando dicha actuación.

En caso de que la solicitud de protección de datos no satisfaga alguno de los requisitos a que se refiere el párrafo anterior y el SPF no cuente con elementos para subsanarla, se prevendrá al Titular dentro de los cinco días siguientes a la presentación de la solicitud de ejercicio de los derechos ARCO, por una sola ocasión, para que subsane las omisiones dentro de un plazo de diez días contados a partir del día siguiente al de la notificación. Transcurrido dicho plazo sin que el Titular o su representante desahoguen la prevención se tendrá por no presentada la solicitud de ejercicio de los derechos ARCO.

Los plazos y procedimientos para dar trámite a las solicitudes del ejercicio de los derechos ARCO en la SPF, deberán desahogarse dentro del plazo máximo de veinte días hábiles determinados por el artículo 51 de la Ley General, atendiendo a lo dispuesto por el artículo 50 de la misma y su correlativo 141 de la Ley General de Transparencia y Acceso a la Información Pública.

Dentro de dicho plazo se entenderá comprendida la notificación al particular a través de la Unidad de Transparencia o las personas servidoras públicas vinculadas según corresponda.

TRIGÉSIMA QUINTA: Las resoluciones del Comité de Transparencia que confirmen, modifiquen o revoquen la inexistencia de datos personales, o la improcedencia total o parcial de la rectificación, cancelación u oposición de estos, deberán estar fundadas y motivadas y se harán constar en Acuerdos asentados en las actas de las Sesiones del Comité de Transparencia del SPF.

Así lo resolvieron por unanimidad, los integrantes del Comité de Transparencia del Servicio de Protección Federal, en la Décima Tercera Sesión Extraordinaria, el veintiséis de septiembre de dos mil veintidós.

Comisario Jefe
Lic. Jean Paul Verduzco Fuentes
Titular de Unidad de Transparencia y
Presidente del Comité de Transparencia

Comisaria Jefa
Mtra. Violeta Millan Zamora
Directora General de Administración y
Vocal del Comité de Transparencia

Dr. Jorge Armando Mora Beltrán
Titular del Órgano Interno de Control en el
Servicio de Protección Federal y Vocal del
Comité de Transparencia

Oficial Rebeca Odilia Zarco Gutiérrez
Jefa de Departamento de Transparencia

Elaboró

Subinspectora Alejandra Elizabeth Mendoza Calva
Subdirectora de Transparencia y Atención a Quejas y Recomendaciones en Materia de Derechos Humanos

Revisó

Inspectora Cynthia Fabiola Morales López
Directora de lo Consultivo, Transparencia y Derechos Humanos

Validó