Sistema de Gestión de Seguridad de Datos Personales

Fiscalía General de la República

Marco normativo

En la protección de datos personales al interior de la Fiscalía General de la República, resulta aplicable el siguiente marco normativo:

- Artículos 6, Apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- Lineamientos Generales de Protección de Datos Personales para el Sector Público • Publicados en el Diario Oficial de la Federación el 26 de enero de 2018.

Presentación

De conformidad con el artículo 34 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General), establece que las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.

Un sistema de gestión es el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en dicha legislación y las disposiciones que resulten aplicables en la materia.

Asimismo, el artículo 65 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales), estipula que el sistema de gestión deberá permitir planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales; tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad

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

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

Objetivo y alcance

Se tiene por objeto establecer los procedimientos para cumplir con la regulación y protección de los datos personales en posesión de la Fiscalía General de la República (FGR) en concordancia con los principios y deberes señalados en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás normatividad que resulte aplicable.

Este documento será de observancia general para todas las áreas responsables y personas servidoras públicas, al igual que para cualquier tratamiento de datos personales que obren en soportes físicos, electrónicos y mixtos dentro de las áreas responsables de la FGR.

Todas las áreas responsables y personas servidoras públicas de la FGR que intervengan en el tratamiento de datos personales, deberán garantizar la protección en el manejo de los mismos, por lo que no podrán comunicarlos a terceros, salvo en los casos previstos por la Ley General y demás normatividad que resulte aplicable en la materia; así mismo, no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de datos personales, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información de acuerdo a la normatividad aplicable; o bien que ello atienda a una obligación legal o a un mandato judicial, lo anterior de conformidad con lo dispuesto en el artículo 22, fracción III de la Ley General.

Las unidades administrativas y personas servidoras públicas de la FGR que posean, por cualquier título, bases que contengan datos personales, deberán hacerlo del conocimiento de la Unidad de Transparencia y Apertura Gubernamental (UTAG), quien coadyuvará para mantener el registro actualizado de los sistemas de tratamiento datos personales en posesión de la Institución de conformidad con la Ley General y demás normatividad que resulte aplicable en la materia.

La aplicación e interpretación del presente documento se hará conforme a lo dispuesto en la Ley General, sus Lineamientos Generales, así como las resoluciones y determinaciones que emita el Instituto Nacional de Trasparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI), favoreciendo en todo momento la protección más amplia a las personas, el derecho a la protección de datos personales y atendiendo a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

En cumplimiento, la UTAG implementará un documento de seguridad institucional en el que quedarán documentadas y contenidas las medidas de seguridad implementadas por las áreas para proteger los datos personales contra daño, pérdida, alteración destrucción o uso, acceso o tratamiento no autorizado, esto mediante la recopilación de los documentos de seguridad, y sus actualizaciones, elaborados por cada área.

Finalmente, es importante señalar que los casos no previstos en el presente documento serán resueltos por el Comité de Transparencia.

Visión general de los principios, deberes y obligaciones.

El tratamiento de datos personales que realicen las áreas de la FGR deberá regirse por los principios, deberes y obligaciones previstos en la Ley General, sus Lineamientos y demás disposiciones que otorguen la protección más amplia a sus Titulares.

PRINCIPIOS

En función de dar cumplimiento a las obligaciones en materia de protección de datos, las áreas deberán dirigir sus acciones conforme a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

Licitud Todo tratamiento de datos personales efectuado por el responsable debe sujetarse a las facultades o atribuciones que la normativa aplicable le ha conferido.

Se deberá 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.

El aviso de privacidad respectivo deberá incluir de manera precisa el fundamento legal que faculte a la instancia para llevar a cabo el tratamiento correspondiente.

Finalidad El responsable está obligado a determinar las finalidades concretas, lícitas, explícitas y legítimas que motivan cada tratamiento de datos personales que efectúe, las cuales deben ser acordes con las atribuciones que la normatividad aplicable le confiere.

Se entenderá que las finalidades son:

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

El responsable podrá tratar los datos personales en su posesión para finalidades distintas a aquéllas previstas en el aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en ley y solicite el consentimiento del titular.

Lealtad En todo momento el responsable debe privilegiar la protección de los intereses del titular y la expectativa razonable de privacidad; y por ningún motivo deberá obtener ni tratar datos personales a través de medios engañosos o fraudulentos.

Se tiene que verificar que los datos personales no se obtengan con dolo, mala fe o negligencia.

Llevar a cabo el tratamiento de los datos personales únicamente para los fines comunicados al titular en el Aviso de Privacidad, verificar que los Avisos de Privacidad respectivos, mantengan un contenido fiel a la realidad del tratamiento de los datos personales, así como que incluyan la totalidad de los elementos previstos para su elaboración en la Ley General y Lineamientos Generales, así como evitar que el tratamiento de los datos personales provoque a su titular discriminación, un trato injusto o arbitrario en su contra.

Consentimiento Para realizar el tratamiento de los datos personales, el responsable está obligado a recabar el consentimiento previo del titular, salvo que se actualice alguna de las siguientes causales de excepción, establecidas en el artículo 22 de la **LGPDPPSO.**

- Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidas por la Ley General; y en ningún caso, podrán contravenirla.
- Las transferencias que se realicen entre responsables sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales.
- Exista una orden judicial, resolución o mandato fundado y motivado de la autoridad competente.
- Se requiera para el reconocimiento o defensa de derechos del titular ante la autoridad competente.
- Los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable.
- Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes.
- Sean necesarios los datos personales para efectuar un tratamiento para la prevención, diagnóstico, o bien la prestación de asistencia sanitaria.
- Figuren los datos personales en fuentes de acceso público.
- Se sometan los datos a un procedimiento previo de disociación, o
- El titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

Calidad Las Unidades deberán adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales, principalmente cuando se obtuvieron de manera indirecta del titular.

Se entenderá que los datos personales son:

- Exactos y correctos: cuando los datos personales no presentan errores que pudieran afectar su veracidad.
- Completos: cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento
- Actualizados: cuando se realizan las acciones pertinentes para que los datos personales respondan fielmente a la situación actual del titular.

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

El responsable está obligado a establecer y documentar los procedimientos para la conservación, bloqueo y supresión de los datos personales.

Cabe destacar que esta obligación está íntimamente vinculada con los instrumentos de consulta y control archivístico de la FGR.

Del mismo modo, el responsable debe 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.

Proporcionalidad Sólo se deben 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.

Lo anterior, se traduce en que se llevaran a cabo esfuerzos razonables para limitar los datos personales tratados al mínimo necesario, respecto de las finalidades que motivaron su tratamiento

Cada Unidad Administrativa deberá identificar los datos personales que se requieren para cada una de las finalidades del tratamiento.

Asimismo, deberá analizar y revisar que solo se soliciten aquellos que resultan indispensables para cumplir con las finalidades del tratamiento.

Cuando la normativa aplicable establezca con precisión los datos personales que deberán obtenerse para cumplir con la finalidad de que se trate, solo deberán solicitarse dichos datos.

Información Debe observarse en la etapa de obtención de los datos personales.

El responsable está obligado a informar al titular sobre la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a través del aviso de privacidad, a fin de que pueda tomar decisiones informadas al respecto.

El aviso de privacidad es el documento mediante el cual se materializa el principio de información, y en el cual se dan a conocer las características principales del tratamiento de los datos personales, a través de los elementos establecidos en la **LGPDPPSO** y Lineamientos Generales.

En ese sentido, el principio de información se constituye en el derecho de los titulares para conocer las características principales del tratamiento al que serán sometidos sus datos personales, a través del aviso de privacidad y, a su vez, en una obligación para el responsable de poner a disposición de los titulares dicho aviso.

Para cumplir con el principio de Información se deberán seguir las siguientes reglas:

- Redactar los avisos de privacidad que se requieran conforme a los tratamientos que lleven a cabo las unidades administrativas, como regla general, se requerirá un aviso de privacidad por tratamiento.
- Elaborar las dos modalidades para cada aviso de privacidad: simplificado e integral.
- De manera adicional, los avisos de privacidad deberán estar disponibles para su consulta en medio impreso (físico) en las instalaciones de la institución, 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.

Responsabilidad El responsable está obligado a implementar los mecanismos que considere convenientes para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la Ley General, así como rendir cuentas sobre el tratamiento de datos personales en su posesión al titular y al Instituto o a los organismos garantes, según corresponda.

Ahora bien, para cumplir con el principio de responsabilidad, el área deberá acreditar el apego a los principios, deberes y obligaciones establecidos en la Ley General y demás normatividad aplicable, así como implementar los mecanismos previstos en el artículo 30 de la referida Ley. Asimismo, deberá demostrar ante titulares y ante el INAI, que cumple con sus obligaciones en torno a la protección de los datos personales.

DEBERES

En función de dar cumplimiento a las obligaciones en materia de protección de datos, las áreas responsables deberán dirigir sus acciones conforme a los deberes de seguridad y confidencialidad,

Además, deberán informar, sin dilación alguna al titular de los datos, las vulneraciones que ocurran, conforme a lo previsto en el artículo 41 de la Ley General, esto en cuanto confirme que ocurrió la vulneración y una vez que hubiere empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación.

Lo anterior, con la finalidad de que los titulares puedan tomar las medidas correspondientes para la defensa de sus derechos de conformidad con el artículo 68 de los Lineamientos Generales.

Las Unidades Administrativas deberán hacer del conocimiento a la UTAG a través de su Enlace de Transparencia, las vulneraciones ocurridas, al mismo tiempo que notifiquen a los Titulares de las Unidades Administrativas, a efecto de que se informe lo conducente al INAI.

OBLIGACIONES

El responsable deberá establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales, conforme al sistema de gestión implementado.

Se deberá establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento.

Los servidores públicos involucrados en el sistema de datos personales deberán firmar de conocimiento en una lista anexa al documento de seguridad con la finalidad de que conozcan sus funciones asi como las probables consecuencias en caso de incumplimiento.

Con la finalidad de dar cumplimiento a las obligaciones en materia de Datos Personales, las Unidades Administrativas de la FGR deberán actualizar su documento de seguridad de manera **trimestral**, haciendo del conocimiento del Oficial de Protección de Datos de la UTAG, mediante el correo electrónico correspondiente:

- Si ha ocurrido algún cambio en la lista de servidores públicos que participan en el tratamiento de los datos personales (bajas o nuevos ingresos);
- Los resultados del análisis de brecha realizado en el trimestre correspondiente;
- Los avances en el plan de trabajo para la protección de los datos personales;
- Los resultados del monitoreo y revisión de las medidas existentes y efectivas y, en su caso, de las medidas implementadas; y en su caso
- Las vulneraciones ocurridas a los datos personales durante el trimestre correspondiente.

Asimismo, acorde a lo establecido en el artículo 36 de la **LGPDPPSO**, se deberá llevar a cabo una actualización cuando ocurran los siguientes eventos:

- 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.
- Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Las acciones antes mencionadas deberán ser realizadas por aquella persona que haya sido designado por el Enlace de datos personales como responsable del monitoreo y revisión de las medidas en el documento de seguridad.

Sistema de tratamiento de datos personales

Los sistemas de tratamiento de datos personales que posee cada Unidad Administrativa de la FGR incluyen el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas.

Asimismo, las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión. Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la Ley General.

Dicho sistema de tratamiento de datos personales deberá ser elaborado por la Unidad que, conforme a los dispuesto en la Ley General, realice cualquier tipo de 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, y deberá contener las medidas de seguridad administrativas, físicas y técnicas aplicables a sus sistemas de datos personales con la finalidad de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

Asimismo, deberá mantenerse siempre actualizado y ser de observancia obligatoria para todos los servidores públicos de las áreas, así como para las personas externas que debido a la presentación de un servicio tengan acceso a tales sistemas o al sitio donde se ubican los mismos.

Además de lo previsto en el párrafo anterior, el documento deberá ser actualizado en caso de que ocurra alguno de los siguientes eventos:

- En caso de que exista una implementación de acciones correctivas y preventivas ante una vulneración de seguridad.
- Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad; y
- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión.
- Implementación de acciones correctivas y preventivas ante una vulneración de seguridad

De conformidad con lo anterior, se considerarán medidas de seguridad:

- **Administrativas**: aquellas que hacen alusión a las 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.
- **Físicas:** aquellas de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

- **Técnicas:** aquellas que abarcan el 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.

El sistema de tratamiento de datos personales debe tener un contenido básico, acatando lo establecido en el artículo 35 de la Ley General, por lo cual el área de la Fiscalía que lo elabore debe cuidar que contenga, al menos, la siguiente información:

- Inventario de los datos personales y de los sistemas de tratamiento;
- Funciones y obligaciones de las personas o áreas que traten los datos personales;
- Análisis de riesgos;
- Análisis de brecha;
- Un plan de trabajo; y
- Los mecanismos de monitoreo y revisión de las medidas de seguridad.
- El programa general de capacitación.

Inventario de datos personales

Se establecen, sus medios de obtención, finalidad del tratamiento, tipo datos personales tratados, así como su categoría, formatos de almacenamiento y ubicación, numero de titulares contenidos, la identificación del personal que interviene en el tratamiento, así como el ciclo de vida de los datos personales.

Para la elaboración del inventario de datos personales y de los sistemas de tratamiento conforme a lo dispuesto en el artículo 58 de los Lineamientos Generales, se deberá incluir, la siguiente información:

- El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;
- Las finalidades de cada tratamiento de datos personales:
  Propósito que tiene el recabar los datos con relación a las facultades que les son proporcionadas por la ley, es una finalidad específica.
- El catálogo de los tipos 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:
  Se debe especificar qué datos personales se encuentran almacenados en cada lugar, junto a su ubicación, y en caso de que el almacenamiento sea por periodos especificarlos.
- La lista de servidores públicos que tienen acceso a los sistemas de tratamiento:
  Nombre completo y cargo de los servidores públicos que tengan acceso.
- En los casos aplicables, 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, así como las finalidades que las justifican.

Dentro del inventario se incluirá el **ciclo de vida de los datos personales**, conformado por lo siguiente:

- La obtención de los datos personales;
- El almacenamiento de los datos personales:
  Narración de cómo se resguardan, donde y que se resguarda ahí; es decir especificar qué datos se resguardan.
- El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin:
  Finalidades del uso de la información, limitada a sus facultades dentro del área.
- La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;
  Narración de a quién y el por qué dan esos datos,
- El bloqueo de los datos personales, en su caso, y
- La cancelación, supresión o destrucción de los datos personales:
  Narración de cómo se hace la destrucción de los datos personales, paso a paso.

Es importante señalar que para dar cabal cumplimento al ciclo de vida, este deberá ser narrado de forma que se describa puntualmente todos los procesos.

Funciones y obligaciones de las personas o áreas que traten los datos personales

Se definirán las funciones, y obligaciones por unidad administrativa, de cada servidor público que intervenga en el tratamiento de los datos personales durante su ciclo de vida. Además, se comunicará a cada uno de estos la información antes señalada, y se buscará su capacitación constante en la materia, lo anterior en términos del artículo 57 de los Lineamientos Generales.

Análisis de riesgos

Se debe identificar el daño que cause mayor impacto sobre los datos personales que se tratan a fin de identificar los controles más relevantes e inmediatos a implementar.

De conformidad con los artículos 33 fracción IV de la LGPDPPSO y 60 de los Lineamientos Generales, el análisis de riesgos se elaborará tomando en cuenta:

- Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;
- El valor de los datos personales de acuerdo con 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 su ciclo de vida, las amenazas y vulnerabilidades existentes y los recursos o activos involucrados en su tratamiento;
- 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.

Análisis de brecha

Esta sección es el proceso de evaluación de las medidas de seguridad que ya existen en el área del responsable contra las que sería conveniente tener. Los controles de seguridad, sin que sean limitativos se realizarán comparando las medidas de seguridad existentes y efectivas con las faltantes en la organización del responsable, de acuerdo con lo establecido en los artículos 33, fracción V de la LGPDPPSO y 61 de los Lineamientos Generales, será considerado lo siguiente:

- Identificar las medidas de seguridad existentes y efectivas:
  Mencionar las medidas con las que ya cuenta el área para el resguardo de los datos personales, haciendo una descripción de cada una de ellas, las cuales se dividen en administrativas, físicas y técnicas.
- Identificar las medidas de seguridad faltantes, y
- Considerar la existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente:

Mencionar las medidas que al área le gustaría implementar o requieran para que no suceda una vulneración a la seguridad de los datos personales.

Plan de trabajo

Es la herramienta con la que se organiza y simplifica las actividades necesarias para la implementación de medidas de seguridad faltantes.

En cumplimiento a lo dispuesto en los artículos 33, fracción VI de la LGPDPPSO y 62 de los Lineamientos, el plan de trabajo se elaborará después de contar con el análisis de riesgo y de brecha, priorizando las medidas de seguridad más relevantes y urgentes, considerando los recursos designados; el personal interno y externo en su organización, y estableciendo fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

Las fechas que se establezcan dentro del plan de trabajo deberán fijarse de manera específica con la finalidad de dar continuidad y cumplimiento a las acciones que se deben implementar derivado de la identificación del análisis de riesgo y análisis de brecha respectivamente.

Ejemplo:

Plan de trabajo				
Acción a implementar	**Meta o resultado esperado**	**Fecha de inicio**	**Fecha de término**	**Indicadores**
Cambio de contraseñas	Mitigar o reducir el riesgo de accesos no autorizados	Marzo 2023	Enero 2024	Certeza de que la contraseña únicamente la tiene el usuario designado.

Mecanismos de monitoreo y revisión de las medidas de seguridad

Uno de los objetivos planteados en este Sistema de Gestión de Seguridad, es documentar las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales, de conformidad con lo establecido en el artículo 34 de la Ley General y 65 de los Lineamientos Generales.

Al respecto, las medidas de seguridad administrativas, físicas y técnicas operadas por las instancias de la FGR son descritas de manera general en el Documento de Seguridad, el cual incluye los mecanismos que serán operados para su monitoreo, revisión, supervisión y auditoría.

De ese modo, las acciones relacionadas con las medidas de seguridad partirán del análisis de los reportes, dictámenes y directrices que se concluyan de la ejecución de dichos mecanismos.

Por tanto, una vez que los mecanismos sean operados, el presente sistema concentrará los resultados que se desprendan de su realización, a efecto de estar en oportunidad de planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad, de forma que resulten adecuadas para el contexto en que se desenvuelve el tratamiento de los datos personales.

En esta fase, se evalúan y miden los resultados de las políticas, planes, procesos y procedimientos implementados, a fin de verificar que se haya logrado la mejora esperada.

Para ello se estipularán mecanismos de monitoreo y revisión de manera periódica de las medidas de seguridad existentes y efectivas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, acorde a lo previsto en los artículos 33, fracción VII de la LGPDPPSO y 63 de los Lineamientos Generales se tomará en cuenta lo siguiente:

- Los nuevos activos que se incluyan en la gestión de riesgos;
- Las modificaciones necesarias a los activos;
- Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
- Las vulnerabilidades identificadas para determinar 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.

El modelo del documento de seguridad deberá ser generado a partir de lo dispuesto en los Lineamientos de Protección de Datos Personales y las Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales emitidas por el INAI, el cual será compromiso de la Unidad de Transparencia, que a su vez estará encargada de su actualización y divulgación al interior de la Fiscalía.

Capacitación

Este apartado se refiere a la capacitación que deberá otorgarse a los servidores públicos de la FGR en materia de protección de datos personales.

Para establecer y mantener las medidas de seguridad para la protección de los datos personales, conforme a lo establecido en los artículos 33, fracción VIII de la LGPDPPSO y 64 de los Lineamientos, se deberá diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales, el responsable tomará en cuenta lo siguiente:

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

La Unidad de Transparencia por conducto de la Dirección de Datos Personales y Capacitación, llevará a cabo las acciones necesarias para capacitar a los servidores públicos de esta FGR en materia de protección de datos personales a través de las siguientes modalidades:

- Modalidad presencial.

- Modalidad virtual, a través de la Plataforma Microsoft TEAMS

Los servidores públicos o unidades administrativas que lleven a cabo un sistema de tratamiento de datos personales deberán capacitarse en la materia, aplicando principalmente los siguientes cursos:

- **Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados** (LGPDPPSO)
- **Curso de Documento de Seguridad**
- **Taller para la elaboración de Documento de Seguridad**, en este último se, asesorará y dará acompañamiento al enlace designado durante la elaboración del sistema de tratamiento de datos personales del área correspondiente.

Sanciones

Debido a que la Fiscalía General de la República es un sujeto obligado competente en instancia de seguridad nacional y pública, así como de procuración y administración de justicia, la información contenida en los sistemas de datos personales de sus diferentes áreas es considerada de valor alto, por lo que se debe contar con las medidas de seguridad óptimas para garantizar su protección.

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

- 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 LGPDPPSO 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 LGPDPPSO;
- 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;
- 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;
- Incumplir el deber de confidencialidad establecido en el artículo 42 de la LGPDPPSO;
- No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la LGPDPPSO;
- 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;
- Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO;

- Obstruir los actos de verificación de la autoridad;
- Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la LGPDPPSO;
- No acatar las resoluciones emitidas por el Instituto, y
- 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.

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

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

Procedimiento para la atención a solicitudes para el ejercicio de Derechos ARCO.

(Acceso, Rectificación, Cancelación y Oposición)

Introducción

La protección a los datos personales es un derecho humano fundamental, reconocido en la Constitución Política de los Estados Unidos Mexicanos, específicamente en sus artículos 6, apartado A, fracción II y 16 párrafo segundo.
En virtud de lo anterior, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados es el ordenamiento jurídico cuyo objetivo se centra en establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección y tratamiento de sus datos personales, en posesión de sujetos obligados.
En tales consideraciones, las personas titulares o sus representantes podrán solicitar a esta Fiscalía General de la República el tratamiento de los datos personales que se encuentren en posesión de esta, ello a través de los denominados derechos ARCO (por las iniciales de Acceso, Rectificación, Cancelación u Oposición), los cuales versan en lo siguiente:

Acceder a sus datos personales, así como a conocer la información relacionada con las condiciones y generalidades de su tratamiento.
Rectificar sus datos personales. El titular tendrá derecho a solicitar la rectificación o corrección de sus datos personales cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados.
Cancelar sus datos personales. El titular tendrá derecho a solicitar la cancelación de sus datos personales que se encuentren en los archivos, registros, expedientes y sistemas de esta Fiscalía General de la República, a fin de que estos ya no obren en su posesión y dejen de ser tratados.
Oponerse al tratamiento de sus datos personales. La persona titular se podrá oponer al tratamiento de los datos personales cuando:

- Aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular o bien;

- Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

Por lo tanto, la presente Guía tiene como finalidad explicar, los procedimientos y requisitos para garantizar el ejercicio de los derechos ARCO sobre los datos personales en posesión de la Fiscalía General de la República.

Catálogo

Comité de Transparencia. Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública.

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.

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

FGR. Fiscalía General de la República

Interés jurídico. Aquel derecho subjetivo derivado de una ley que permite a una persona actuar a nombre de otra que por su situación le es imposible

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

PNT. Plataforma Nacional de Transparencia

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.

Titular. La persona física a quien corresponden los datos personales.

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

Procedimiento interno para la atención y trámite de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO).

Objetivo

Gestionar la atención de solicitudes de datos personales respecto a los datos que obren en posesión de la FGR para hacer efectivo los derechos ARCO de los solicitantes.

Reglas de operación

1. Se deberá verificar que la solicitud de derechos ARCO contenga los siguientes elementos:

- Nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones.
- Los documentos que acrediten la identidad del titular y en su caso la personalidad e identidad de su representante.
- De ser posible mencionar o dirigir al área responsable que trate los datos personales y ante el cual se presenta la solicitud.
- 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.
- La descripción del derecho ARCO que se pretende ejercer o bien, lo que solicite el titular.
- Cualquier otro elemento o documento que facilite la localización de los datos personales.

1.1. En el caso de las solicitudes de **acceso** a datos personales, el Titular deberá señalar la modalidad en la que prefiere que se otorgue el acceso a sus datos, salvo que exista una imposibilidad física o jurídica.

1.2. Tratándose de solicitudes de **rectificación**, el Titular en la medida de lo posible, señalará la base de datos en la que obran los datos personales y/o la finalidad para la que fueron recabados, y especificará la corrección o actualización solicitada, para lo cual deberá aportar la documentación que sustente su petición. En caso de que el Titular omita señalar la base de datos, ello no será impedimento para continuar con el desahogo de la solicitud;

1.3. En las solicitudes de **cancelación**, el Titular deberá señalar las causas que lo motiven a solicitar la supresión de sus datos personales en los archivos, registros o bases de datos de la FGR.

1.4. En el caso de la solicitud de **oposición**, el Titular deberá manifestar las causas legítimas o la situación específica que lo llevan a solicitar el cese en el tratamiento, así como el daño o perjuicio que le causaría la persistencia del tratamiento, o en su caso, las finalidades específicas respecto de las cuales requiere ejercer el derecho de oposición.

2. Si la solicitud de derechos ARCO no satisface alguno de los requisitos, o no se cuenta con elementos para subsanarla, se prevendrá al titular que pretenda llevar a cabo el ejercicio de derechos ARCO, dentro de los **cinco días** hábiles siguientes a la presentación de la solicitud por una sola ocasión, para que subsane las omisiones dentro de un plazo de **diez días hábiles** contados a partir del día hábil siguiente al de la notificación, no se omite señalar que la prevención tendrá el efecto de interrumpir el plazo para dar respuesta a la solicitud de ejercicio de los derechos ARCO.

Transcurrido el plazo sin desahogar la prevención se tendrá por no presentada la solicitud para el ejercicio de los derechos ARCO.

Ahora bien, en el supuesto de que el Titular atienda satisfactoriamente el requerimiento de información, el plazo para dar respuesta a la solicitud empezará a correr al día hábil siguiente al del desahogo.

3. Se deberá verificar que las solicitudes para el ejercicio de los Derechos ARCO sean presentadas por el titular de los datos personales o su representante.[1]

Por lo anterior, la acreditación de la identidad del titular y en su caso, de su representante, así como la personalidad de este último, se realizará previo a hacer efectivo el derecho correspondiente.

Para notificar la procedencia o no procedencia del ejercicio de derechos ARCO se deberá solicitar acreditar la titularidad de los datos personales o, en su caso la identidad y personalidad del representante.

El titular podrá acreditar su identidad a través de los siguientes medios:

- Identificación oficial;
- Instrumentos electrónicos o mecanismos de autenticación permitidos por otras disposiciones legales o reglamentarias que permitan su identificación fehacientemente, o
- Aquellos mecanismos establecidos por el responsable de manera previa, siempre y cuando permitan de forma inequívoca la acreditación de la identidad del titular

En su caso, el representante acreditará su identidad y personalidad de acuerdo con lo siguiente:

- Copia simple de la identificación oficial del titular;
- Identificación oficial del representante, e
- Instrumento público; carta poder simple firmada ante dos testigos anexando copia simple de las identificaciones oficiales de quienes intervengan en la suscripción de este, o declaración en comparecencia personal del titular.

La acreditación de la identidad y personalidad se deberá llevar a cabo presentando los documentos originales, en el caso de que el titular o su representante acudan directamente ante la Unidad de Transparencia.

En la constancia que acredite el ejercicio del derecho de que se trate, se señalará que el titular o su representante acreditaron su identidad y personalidad en el caso de este último, mediante la presentación de documentos originales, describiendo estos.

4. Cuando se trate de **menores de edad y personas en estado de interdicción o incapacidad** de conformidad con las leyes civiles. se estará a las reglas de representación dispuestas en la misma legislación,[2]así como a lo dispuesto en el artículo 81 de los Lineamientos Generales de Protección de datos Personales para el Sector Público.

[1] De conformidad con lo establecido en el artículo 49 de la LGPDPPSO
[2] Acorde al artículo 49 de la LGPDPPSO

Para el ejercicio de los derechos ARCO será necesario acreditar la identidad del titular y, en su caso, la identidad y personalidad con la que actúe el representante.

El ejercicio de los derechos ARCO por persona distinta a su titular o a su representante, será posible, excepcionalmente, en aquellos supuestos previstos por disposición legal, o en su caso, por mandato judicial.

4.1. Ahora bien, el titular podrá acreditar su identidad a través de los siguientes medios:[3]

- Identificación oficial;
- Instrumentos electrónicos o mecanismos de autenticación permitidos por otras disposiciones legales o reglamentarias que permitan su identificación fehacientemente, o
- Aquellos mecanismos establecidos por el responsable de manera previa, siempre y cuando permitan de forma inequívoca la acreditación de la identidad del titular.

4.2. En el caso de la identidad de los menores de edad se podrá acreditar mediante:

- Acta de nacimiento,
- Clave Única de Registro de Población,
- Credenciales expedidas por instituciones educativas o instituciones de seguridad social,
- Pasaporte, o
- Cualquier otro documento oficial utilizado para tal fin.

Acreditación de menores de edad cuando sus padres ejercen la patria potestad.

Cuando el titular sea un menor de edad y sus padres sean los que ejerzan la patria potestad y los que pretendan ejercer los derechos ARCO de éste, además de acreditar la identidad del menor, se deberá acreditar la identidad y representación de los padres mediante los siguientes documentos:

- Acta de nacimiento del menor de edad, y
- Documento de identificación oficial del padre o de la madre que pretenda ejercer el derecho.

Acreditación de menores de edad cuando una persona distinta a sus padres ejerce la patria potestad

- Cuando el titular sea un menor de edad y su patria potestad la ejerce una persona distinta a los padres y ésta sea quien presente la solicitud para el ejercicio de los derechos ARCO, además de acreditar la identidad del menor se deberá acreditar la identidad y representación de la persona mediante los siguientes documentos:
- Acta de nacimiento del menor de edad;
- Documento legal que acredite la posesión de la patria potestad, y
- Documento de identificación oficial de quien ejerce la patria potestad.

Acreditación de menores de edad cuando son representados por un tutor.

[3] Conforme a lo dispuesto en el artículo 76 de los Lineamientos Generales

Cuando el titular sea un menor de edad y la solicitud para el ejercicio de los derechos ARCO la presente su tutor, además de acreditar la identidad del menor, el tutor deberá acreditar su identidad y representación mediante los siguientes documentos:

- Acta de nacimiento del menor de edad;
- Documento legal que acredite la tutela, y
- Documento de identificación oficial del tutor.

4.3. Por lo que hace a la identidad de personas en estado de interdicción o incapacidad declarada por ley se podrá acreditar mediante:

- Acta de nacimiento
- Clave Única de Registro de Población
- Pasaporte
- Cualquier otro documento o identificación oficial expedida para tal finalidad.

Acreditación de personas en estado de interdicción o incapacidad declarada por ley o por autoridad judicial.

Cuando el titular sea una persona en estado de interdicción o incapacidad declarada por ley o por autoridad judicial, además de acreditar la identidad de la persona, su representante deberá acreditar su identidad y representación mediante los siguientes documentos:

- Instrumento legal de designación del tutor, y
- Documento de identificación oficial del tutor.

4.4. Cuando el titular ejerza sus derechos ARCO a través de su representante, éste deberá acreditar la identidad del titular y su identidad y personalidad presentando ante el responsable lo siguiente:

- Copia simple de la identificación oficial del titular;
- Identificación oficial del representante, e
- Instrumento público; carta poder simple firmada ante dos testigos anexando copia simple de las identificaciones oficiales de quienes intervengan en la suscripción de este, o declaración en comparecencia personal del titular.

6. Costos de reproducción

El ejercicio de los derechos ARCO será gratuito. Sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío, conforme a la normatividad que resulte aplicable:[4]

- Los costos de reproducción, certificación o envío deberán ser cubiertos por el Titular de manera previa a la entrega de los datos personales.
- Cuando el Titular proporcione el medio magnético, electrónico o el mecanismo necesario para reproducir los datos personales, éstos deberán ser entregados sin costo.

[4] De conformidad con el artículo 50 de la LGPDPPSO

- La información será entregada sin costo, cuando los datos personales estén contenidos en hasta veinte hojas simples o certificadas.
- No se puede establecer para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio que implique un costo al titular.

6.1 La Unidad de Transparencia podrá exceptuar el pago de reproducción, certificación o envío atendiendo a las circunstancias socio económicas del Titular. Si el titular no pudiera cubrir los costos de reproducción y/o envío deberá manifestarlo en su solicitud, cuando esto se manifieste, se deberá realizar el análisis correspondiente, a fin de determinar si procede la excepción del pago.

7. En caso de que la Unidad de Transparencia advierta que la solicitud para el ejercicio de los derechos ARCO corresponda a un derecho diferente de los previstos en la presente Guía, deberá reconducir la vía haciéndolo del conocimiento al Titular.

Procedimiento interno para atención a solicitudes de derechos ARCO

1. En caso de las solicitudes para el ejercicio de derechos ARCO que sean presentadas de manera presencial en el Módulo de Atención Ciudadana de la Fiscalía General de la República, un servidor público adscrito a la unidad asistirá de manera particular al titular para que pueda ejercer su derecho, a través de un formulario, mismo que deberá estar debidamente llenado y sellado. Posteriormente la solicitud será ingresada a la Plataforma Nacional de Transparencia para asignarle un folio con el que se le dará trámite para continuar con su proceso correspondiente.

Acuse

2. Las personas que formulen solicitudes a través del módulo electrónico de la PNT tendrán acceso directo al acuse que para tales efectos genere dicho sistema, en tal caso no será necesario desahogar gestiones adicionales, toda vez que la propia plataforma notifica el acuse a través de la cuenta del titular.

En el caso de solicitudes recibidas por un medio diferente a la PNT, ya sea por escrito libre a través del Módulo de Atención Ciudadana o vía correo electrónico, una vez registradas en la plataforma, la Unidad de Transparencia enviará el acuse correspondiente que genere el sistema a la persona solicitante, a través del medio señalado para oír y recibir notificaciones, posterior a su recepción, el cual indicará la fecha de recepción, el folio que corresponda y los plazos de respuesta aplicables.

A efecto de dar trámite a todas las solicitudes de ejercicio de Derechos ARCO, una vez recibida la solicitud, la Unidad de Transparencia deberá turnarla al área que corresponda el tratamiento, resguardo o posesión de los datos personales en materia, posterior a su recepción.

3. Cuando las disposiciones aplicables a determinados tratamientos de datos personales establezcan un **trámite o procedimiento específico** para solicitar el ejercicio de los derechos ARCO, se deberá informar al titular sobre la existencia del mismo, en un plazo no mayor a cinco días hábiles siguientes a la presentación de la solicitud para el ejercicio de los derechos ARCO, a efecto de que este último decida si ejerce sus derechos a través del trámite específico, o bien, por medio del procedimiento que el responsable haya institucionalizado para la atención de solicitudes para el ejercicio de los derechos ARCO.

El titular tendrá un plazo de cinco días hábiles contados a partir del día siguiente de recibir la respuesta del responsable, para indicar si ejerce sus derechos ARCO a través del trámite específico o del procedimiento de la LGPDPPSO. Si el titular no responde, se entenderá que señala el procedimiento general.

4. Tratándose de las solicitudes de acceso a datos personales, la acreditación de la identidad del Titular o, en su caso, la identidad y personalidad del representante, deberá realizarse al momento de la entrega de la información, y en el caso de las solicitudes de rectificación, cancelación y oposición, al momento de notificar la respuesta de la procedencia del ejercicio del derecho correspondiente.

4.1. Posterior a la notificación de la procedencia del derecho al Titular o a su representante, la Unidad de Transparencia deberá informarlo al área correspondiente, para que ésta haga efectivo el derecho de rectificación, cancelación u oposición que proceda, siempre y cuando haya quedado acreditada la identidad y, en su caso, la personalidad del Titular o su representante, según sea el caso. Dicha área deberá remitir a la Unidad de Transparencia el documento que haga constar el ejercicio del derecho respectivo, a efecto de que ésta lo notifique al Titular.

De ser procedente el acceso a los datos personales, el área deberá entregarlos en formato comprensible e informar al Titular o a su representante, de ser el caso, los costos de reproducción de la información requerida, los cuales deberán pagarse de manera previa a su entrega.

5. Cuando la solicitud del ejercicio de los derechos ARCO no sea procedente, el Área de la FGR que haya recibido la solicitud deberá remitir al Comité, por conducto de la Unidad de Transparencia, un oficio en el que funde y motive su determinación, acompañando, en su caso, las pruebas que resulten pertinentes y el expediente correspondiente, para que el Comité resuelva si confirma, modifica o revoca la improcedencia manifestada.

Sólo se podrá **negar** el ejercicio de los derechos ARCO cuando se actualicen algunas de las siguientes causas, previstas en el artículo 55 de la LGPDPPSO:

- Cuando el titular o su representante no estén debidamente acreditados para ello;
- Cuando los datos personales no se encuentren en posesión del responsable;
- Cuando exista un impedimento legal;
- Cuando se lesionen los derechos de un tercero;
- Cuando se obstaculicen actuaciones judiciales o administrativas;
- Cuando exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de estos;
- Cuando la cancelación u oposición haya sido previamente realizada;
- Cuando el responsable no sea competente;
- Cuando sean necesarios para proteger intereses jurídicamente tutelados del titular
- Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular;
- Cuando en función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado Mexicano; o
- Cuando los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del sujeto obligado hayan proporcionado a

éste, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades.

Cuando se niegue el ejercicio de los derechos ARCO, la negativa deberá constar en una resolución del Comité de Transparencia en la que confirme la improcedencia.

Se deberá informar al titular el motivo de la negativa, en el plazo de hasta veinte días, por el mismo medio en que se llevó a cabo la solicitud, acompañando en su caso, las pruebas que resulten pertinentes.

El plazo referido en el párrafo anterior podrá ser ampliado por una sola vez hasta por **diez días** hábiles cuando así lo justifiquen las circunstancias, y siempre y cuando se le notifique al Titular dentro del plazo de respuesta.

6. Cuando los datos personales no obren en los archivos, registros, sistemas o expedientes del área correspondiente a la que le fue turnada la solicitud o ésta señale su **incompetencia**, se tendrá que hacer de conocimiento al solicitante cuando el responsable no sea competente para atender la solicitud para el ejercicio de derechos ARCO dentro de los **3 días hábiles siguientes** a su presentación y en caso de poderlo determinar, orientarlo hacia el sujeto obligado competente, sin que sea necesaria una resolución del Comité de Transparencia.

Si el responsable es competente para atender parcialmente la solicitud, deberá dar respuesta en el ámbito de su competencia en el plazo de 20 días. hábiles

El plazo referido en el párrafo anterior podrá ser ampliado por una sola vez hasta por **diez días** hábiles cuando así lo justifiquen las circunstancias, y siempre y cuando se le notifique al Titular dentro del plazo de respuesta.

7. En caso de que el responsable declare la **inexistencia** de los datos personales, dicha declaración deberá constar en una resolución del Comité de Transparencia que confirme la inexistencia de los datos personales, y en la que se informen los elementos mínimos para que permitan al titular tener la certeza de que se utilizó un criterio de búsqueda exhaustivo; se señalen las circunstancias de tiempo, modo y lugar que generaron la inexistencia y se identifique la unidad administrativa competente para contar con los datos personales.

8. Cuando la respuesta del área correspondiente determine la procedencia de la entrega de la información, la misma deberá reproducirse o certificarse dentro de los siguientes días hábiles a aquel en que la Unidad de Transparencia notifique sobre el pago correspondiente.

Una vez realizado el pago de derechos por el Titular, la Unidad de Transparencia deberá entregar la información requerida, siempre que se haya acreditado la identidad del Titular o bien, la personalidad del representante, según sea el caso.

9. La **respuesta** a las solicitudes de derechos ARCO deberá notificarse al Titular, o en su caso, al representante, a través de la Unidad de Transparencia, en un plazo que no deberá exceder de **veinte días** hábiles contados a partir del día siguiente a la recepción de la solicitud.

El plazo referido en el párrafo anterior podrá ser ampliado por una sola vez hasta por **diez días** hábiles cuando así lo justifiquen las circunstancias, y siempre y cuando se le notifique al Titular dentro del plazo de respuesta.

En caso de resultar procedente el ejercicio del derecho ARCO, el mismo se hará efectivo en un plazo que no podrá exceder de quince días hábiles contados a partir del día hábil siguiente en que se haya notificado la respuesta al Titular o a su representante, según sea el caso, y se haya acreditado su identidad o personalidad, respectivamente.

En la respuesta a una solicitud para el ejercicio de los derechos ARCO, se deberá señalar:

- Los costos de reproducción, certificación y/o envío de los datos personales o de las constancias que acrediten el ejercicio efectivo de los derechos ARCO que, en su caso, correspondan;
- El plazo que tiene el titular para realizar el pago, el cual no podrá ser menor de tres días hábiles contados a partir del día siguiente de que se notifique la repuesta; señalando que una vez que el titular o, en su caso, su representante realice el pago deberá remitir copia del recibo correspondiente, con la identificación del número de folio de la solicitud para el ejercicio de los derechos ARCO que corresponda, a más tardar al día siguiente de realizarse el pago a través del medio que señaló para oír y recibir notificaciones, o bien, presentando personalmente una copia ante la Unidad de Transparencia del responsable,
- El derecho que le asiste al titular para interponer un recurso de revisión ante el INAI en caso de inconformidad por la respuesta recibida.

La respuesta puede ser notificada a través de los siguientes medios:

- Unidad de Transparencia; en el Módulo de Atención Ciudadana de la FGR, ubicado en Av. Insurgentes No. 20, de la Glorieta de Insurgentes, Col. Roma Norte, Alcaldía Cuauhtémoc, CDMX, CP 06700.
- Plataforma Nacional de Transparencia (no procede notificación a través de representante).
- Correo certificado, a la dirección proporcionada por el titular de los datos personales (Sólo procederá el envío por correo certificado de los datos personales o de las constancias del ejercicio efectivo de los derechos ARCO, cuando la solicitud sea presentada personalmente por el titular ante el responsable, no medie representación alguna del titular, y no se trate de menores de edad o de datos personales de fallecidos).

10. Cuando el titular o su representante hayan acreditado su identidad y personalidad directamente ante la Unidad de Transparencia, mediante la presentación de documentos originales, la respuesta podrá ser notificada a través de los medios electrónicos que haya determinado el titular cuando acudió directamente ante la Unidad de Transparencia.

11. Se tendrá a disposición del titular y, en su caso, de su representante los datos personales en el medio de reproducción solicitado y/o las constancias que acrediten el ejercicio efectivo de los derechos ARCO durante un plazo máximo de 60 días, contados a partir del día siguiente en que se hubiere notificado la respuesta de procedencia al titular.[5]

12. Transcurrido dicho plazo, el responsable dará por concluida la atención a la solicitud para el ejercicio de los derechos ARCO y proceder a la destrucción del material en el que se reprodujeron los datos personales o de las constancias que acrediten el ejercicio efectivo de los derechos ARCO.

[5] De conformidad con el artículo 98 de los Lineamientos Generales

Lo anterior, dejando a salvo el derecho que le asiste al titular de presentar una nueva solicitud de derechos ARCO ante el responsable.

Medidas fácil acceso a personas con discapacidad.

La Unidad de Transparencia y Apertura Gubernamental de la Fiscalía General de la Republica en virtud de garantizar a todas las personas el acceso a la información así como la protección a sus datos personales cuenta con medidas implementadas en sus instalaciones para garantizar el fácil acceso a personas con discapacidad que pretendan o se encuentren llevando a cabo la tramitación a solicitudes de acceso a la información y solicitudes para el ejercicio de Derechos ARCO, contando con un módulo de Atención Ciudadana, situado en planta baja del inmueble de la Fiscalía General de la República, ubicado en Insurgentes Sur 20, Colonia Roma Norte, Código Postal 06700 Ciudad de México.

Asimismo, se cuenta con rampas de acceso situadas a los costados del inmueble, las cuales permiten la libre movilidad a personas con problemas de discapacidad permanente o temporal para ingresar de manera eficiente y accesible a las instalaciones de esta FGR.
Adicionalmente dentro de las instalaciones del inmueble de esta FGR, se cuentan con las señalizaciones pertinentes para personas con discapacidad.

Procedimiento para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de datos personales (derechos arco), concernientes a personas fallecidas.

Interés jurídico.

El interés jurídico es aquel que tiene una persona física que, con motivo del fallecimiento de la persona titular, pretende ejercer los derechos ARCO de ésta, para el reconocimiento de derechos sucesorios, atendiendo a la relación de parentesco por consanguinidad o afinidad que haya tenido con la persona titular, el cual se acreditará en términos de las disposiciones legales aplicables.

Podrán alegar interés jurídico, de manera enunciativa más no limitativa, el albacea, los herederos, los legatarios, las o los familiares en línea recta sin limitación de grado y en línea colateral hasta el cuarto grado, o cualquier persona que haya sido designada previamente por la persona titular para ejercer los derechos ARCO en su nombre, lo que se acreditará con copia simple del documento delegatorio, pasado ante la fe de notario público o suscrito ante dos testigos.

1. Personas facultadas para ejercer los derechos ARCO de personas fallecidas.

Tratándose de datos personales concernientes a personas fallecidas, la persona que acredite tener un interés jurídico, de conformidad con las leyes aplicables, podrá ejercer los derechos ARCO, siempre que la persona titular hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato judicial para dicho efecto. En caso de que la persona fallecida no hubiere expresado fehacientemente su voluntad, bastará que la persona que pretende ejercer los derechos ARCO acredite su interés jurídico en los términos previstos en la normativa aplicable.[6]

---

[6] De conformidad con el artículo 49, párrafo 4, de la LGPDPPSP, así como 75 y 82 de los Lineamientos Generales.

2. Medios para acreditar el interés jurídico.

2.1 Personas vinculadas a fallecidas.

La persona que pretenda ejercer los derechos ARCO deberá anexar a su solicitud copia simple de los siguientes documentos:

- Identificación oficial de la persona a quien pertenecían los datos.
- Acta de nacimiento o Clave Única de Registro de Población (CURP) de la persona fallecida.
- Acta de defunción.
- Documento(s) que acrediten el interés jurídico, en su caso:
  El documento donde la persona titular hubiere expresado fehacientemente su voluntad de que esta persona ejerza los derechos ARCO con relación a sus datos personales o
  El mandato judicial para dicho efecto.
- Identificación oficial de quien presenta la solicitud.

3.2 Familiares.

Las o los familiares de la persona fallecida deberán acreditar el parentesco por consanguineidad o afinidad con la persona fallecida.

El parentesco por consanguineidad es el que existe entre personas que descienden de una misma persona progenitora, para acreditarlo, la persona interesada deberá anexar a su solicitud copia simple de las actas de nacimiento de ascendientes y descendientes.

El parentesco por afinidad es el que se contrae por el matrimonio, para acreditarlo deberá presentar copia simple de la respectiva acta de matrimonio.

3.3 Personas menores de edad.

En el supuesto de que la persona titular sea menor de edad, el interés jurídico se acreditará con copia simple de los siguientes documentos:

- Acta de defunción.
- Acta de nacimiento.
- Identificación de la persona menor.
- Identificación de quien ejercía la patria potestad y/o tutela.

3.4 Personas en estado de interdicción o incapacidad.

En el supuesto de que la persona titular hubiese sido una persona en estado de interdicción o incapacidad declarada por ley o por autoridad judicial, el interés jurídico se acreditará con copia simple de la siguiente documentación:

- Acta de defunción.
- Identificación oficial de la persona titular (fallecida).
- Identificación de quien ejercía la tutela.
- Instrumento legal de designación del tutor.

Procedimiento para generar las constancias que acrediten la ejecución de los derechos de acceso, rectificación, cancelación y oposición de datos personales en posesión de la Fiscalía General de la República.

Objeto.

Este procedimiento tiene por objeto establecer las bases que permitan a las áreas de la FGR cumplir con la obligación de otorgar acceso a los datos personales y generar las constancias que acrediten la ejecución de los derechos de rectificación, cancelación y oposición de datos personales, en términos de las leyes aplicables.

Elementos para garantizar el derecho de acceso a datos personales.

El derecho de acceso a datos personales se tendrá por garantizado cuando la UTAG ponga a disposición de la persona titular, previa acreditación de su identidad y, en su caso, la identidad y personalidad de su representante, los datos personales materia de la solicitud, proporcionado por el área de la FGR, a través de consulta directa, en el sitio donde se encuentren, o mediante la expedición de copias simples, copias certificadas, medios magnéticos, ópticos, sonoros, visuales u holográficos, o cualquier otra tecnología que determine la persona titular, así como previa acreditación del pago de los derechos correspondientes.

La solicitud se atenderá en la modalidad requerida por la persona 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.

Emisión de constancias correspondientes a los derechos de rectificación, cancelación y oposición.

Tratándose de los derechos de rectificación, cancelación y oposición de datos personales, una vez que la UTAG haya notificado la procedencia del derecho que corresponda, previa acreditación de la identidad de la persona titular o la identidad y personalidad de su representante deberá remitir dicha notificación al área responsable de la FGR para que emita la constancia que acredite la rectificación, cancelación u oposición objeto de la solitud, según sea el caso.

El área responsable de la FGR deberá remitir a la UTAG la constancia señalada en el párrafo anterior en un plazo máximo de 5 días hábiles, para que esta realice la entrega a la persona titular o, bien, a su representante.

Las constancias que emitan los órganos responsables deberán contener, según sea el caso, los siguientes elementos:

Constancia de **rectificación** de datos personales

- El nombre completo de la persona titular,
- Los datos personales corregidos, y
- La fecha a partir de la cual fueron rectificados los datos personales en sus registros, archivos, sistemas de información, expedientes, bases de datos o documentos en su posesión.

Constancia de **cancelación** de datos personales

- Los documentos, bases de datos personales, archivos, registros, expedientes y/o sistemas de tratamiento donde se encuentren los datos personales objeto de cancelación;
- El periodo de bloqueo de los datos personales, en su caso;
- Las medidas de seguridad administrativas, físicas y técnicas implementadas durante el periodo de bloqueo, en su caso, y
- Las políticas, métodos y técnicas utilizadas para la supresión definitiva de los datos personales, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima.

Constancia de **oposición** de datos personales

- Un informe pormenorizado que acredite la obligación de cesar el tratamiento en los datos personales objeto de la solicitud, identificando, en su caso, las finalidades específicas respecto de las cuales la persona titular solicitó el derecho de oposición.

Notificación de la ejecución de los derechos ARCO

La Unidad de Transparencia deberá entregar a la persona titular o, en su caso, a su representante, en el caso del derecho de acceso a datos, la información requerida en la modalidad solicitada y, en el caso de los derechos de rectificación, cancelación u oposición, la constancia que acredite la ejecución del derecho, según sea el caso, dentro del plazo de 15 días hábiles contados a partir del día siguiente en que se haya notificado la respuesta al titular.