ASF Auditoría Superior de la Federación

CÁMARA DE DIPUTADOS

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES DE LA AUDITORÍA SUPERIOR DE LA FEDERACIÓN

2TA3PD04

Versión 02

Diciembre, 2025

ÍNDICE

Sin texto

PRESENTACIÓN

La presente Política de Protección de Datos Personales de la ASF es la expresión de un ejercicio de revisión necesario para garantizar que la institución cuente con un marco normativo y procedimental adecuado para coadyuvar a la vigencia y efectividad del derecho fundamental a la protección de los datos personales reconocido en los artículos 6º y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos. La actualización de este instrumento refleja el compromiso institucional con la búsqueda de consolidar una cultura de respeto a la privacidad y de protección de los datos personales.

Es relevante anotar que el contenido de este documento es acorde con los cambios derivados de la reforma al artículo 6º, apartado A, fracciones II y VIII del texto constitucional, en materia de simplificación orgánica de diciembre de 2024, y con las disposiciones de la nueva Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General), publicada en marzo de 2025, que materializaron las disposiciones del Constituyente Permanente, de manera particular, en cuanto a la nueva estructura de tutela del derecho de protección de datos personales.

Esta versión de la Política tiene sustento en la experiencia acumulada a partir de sus dos versiones anteriores, correspondientes a los ejercicios 2020 y 2023, las cuales retomaron en su conformación diversos contenidos de los Lineamientos Generales de Protección de Datos Personales para el Sector Público[1] (Lineamientos Generales), y consideraron como referentes a los criterios establecidos por el entonces organismo garante, a través de los materiales de apoyo dirigidos a los sujetos obligados del sector público, como la Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y el Documento Orientador del Programa de Protección de Datos.

Las versiones anteriores de la Política constituyen documentos importantes en la construcción de un marco institucional sólido para la tutela del derecho fundamental a la protección de los datos personales, debido a que posibilitaron el establecimiento de mecanismos, responsabilidades y prácticas que han demostrado su eficacia en los distintos tratamientos de datos que se realizan en la ASF.

Con esta nueva versión se da continuidad al proceso de consolidación de la normativa, con base en la experiencia operativa y en los aprendizajes derivados de su aplicación. Su actualización busca puntualizar, ampliar y robustecer los contenidos que favorecen la actuación responsable de las personas servidoras públicas en el tratamiento de datos personales, conservando aquellos elementos que han probado su pertinencia y efectividad.

[1] Instrumento normativo que continúa vigente, de conformidad con lo dispuesto en el artículo Cuarto Transitorio del Decreto por el que se expiden la Ley General de Transparencia y Acceso a la Información Pública; la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; y se reforma el artículo 37, fracción XV, de la Ley Orgánica de la Administración Pública Federal, publicado en el Diario Oficial de la Federación el 20 de marzo de 2025.

De tal manera que, entre los principales ajustes realizados, se amplía el ámbito referencial normativo; se incorporan apartados relativos a la definición de funciones y responsabilidades de las instancias que participan en el cumplimiento de la Política; se agregan preámbulos explicativos en cada uno de los principios y deberes y, se adicionan algunos conceptos con la finalidad de contribuir a su mejor comprensión y apropiación; se establecen los componentes que debe contener el inventario de datos personales que se tratan en la institución; se detallan las acciones a cargo de las personas responsables del tratamiento en las UA de la ASF y se añade un nuevo apartado en el que se refiere la normativa aplicable a las conductas que pueden ser consideradas como incumplimiento a los principios y deberes en la materia.

Asimismo, se realizan ajustes en la estructura de la Política para reordenar su contenido, se fortalece su redacción y se incorpora el lenguaje incluyente, para lograr una mayor homogeneidad del documento.

Es pertinente señalar que se mantienen aspectos que han arrojado resultados positivos, como son el involucramiento de la Alta Dirección Institucional en las responsabilidades y toma de decisiones en materia de protección de datos personales, así como los aspectos procedimentales que han sido funcionales para el establecimiento de una comunicación fluida entre la Unidad de Transparencia y las UA.

Cabe mencionar que con la elaboración de esta Política de Protección de Datos Personales de la ASF se actúa conforme a lo previsto por los artículos 24, fracción II, y 27, fracción I, de la Ley General, en los cuales se prevé la creación de políticas internas como uno de los mecanismos adoptados por quienes tratan datos, para dar cumplimiento al Principio de Responsabilidad, así como de acuerdo con lo establecido en el artículo 47 de los Lineamientos Generales, que dispone el deber de elaborar e implementar políticas de protección de datos personales que tengan por objeto establecer los elementos y actividades de dirección, operación y control de todos sus procesos que, en el ejercicio de sus funciones y atribuciones, impliquen un tratamiento de datos personales. Asimismo, se consideró la debida alineación con el Plan Estratégico Institucional.

De esta manera, el proceso de mejora normativa conjuga la estabilidad de las disposiciones con su adecuación progresiva para garantizar la protección integral de los datos personales.

INTRODUCCIÓN

Objetivo

Acreditar y asegurar el cumplimiento de los principios y deberes en materia de protección de datos personales, así como establecer los elementos y actividades de dirección, operación y control en los procesos en los que la ASF realice algún tratamiento de los mismos.

Alcance

La presente Política es aplicable al personal de la ASF y a las UA involucradas en el tratamiento de datos personales.

La actualización de este documento es competencia de la Unidad de Enlace Legislativo, Planeación y Transparencia, por medio de la Dirección General de Transparencia, cuando se presenten reformas jurídicas que regulen los procesos internos y en materia de datos personales, o bien, para la implementación de mejoras en la operación.

El Comité de Transparencia, la Unidad de Enlace Legislativo, Planeación y Transparencia y la Dirección General de Transparencia son las instancias facultadas para supervisar su observancia y cumplimiento, así como para interpretar este documento y definir los criterios específicos aplicables en el caso de presentarse situaciones no previstas, en su respectivo ámbito de competencia.

Principales ordenamientos

El presente documento se encuentra alineado al marco jurídico y normativo siguiente:

- Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley de Fiscalización y Rendición de Cuentas de la Federación.
- Reglamento Interior de la Auditoría Superior de la Federación.
- Manual de Organización de la Auditoría Superior de la Federación.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Sin texto

CAPÍTULO I. DE LA DEFINICIÓN DE RESPONSABILIDADES

I.1. COMITÉ DE TRANSPARENCIA

Artículo 1. El Comité de Transparencia es una instancia colegiada que funge como máxima autoridad de la ASF en materia de protección de datos personales.

I.2. FUNCIONES DEL COMITÉ DE TRANSPARENCIA

Artículo 2. Para efectos de la presente Política, el Comité de Transparencia cuenta con las funciones siguientes:

I. Aprobar la presente Política, así como sus modificaciones.

II. Supervisar el cumplimiento de la Política por parte de las UA para garantizar la protección de los datos personales.

III. Realizar, en el ámbito de su competencia, las acciones necesarias para el adecuado cumplimiento de los principios y deberes por parte de las UA.

IV. Aprobar el Programa de Protección de Datos Personales.

V. Aprobar el Programa de Capacitación y Actualización en Materia de Protección de Datos Personales (PCAMPDP).

VI. Aprobar el Documento de Seguridad de la ASF.

VII. Supervisar, en coordinación con las UA, el cumplimiento de las acciones previstas en materia de seguridad de los datos personales, de conformidad con las disposiciones normativas aplicables.

VIII. Tomar conocimiento del informe que integre la UA responsable del tratamiento de datos personales con motivo de la vulneración a la seguridad de datos personales, así como determinar, en su caso, la implementación de acciones adicionales para reforzar las medidas de seguridad.

IX. Aprobar los criterios específicos y la normativa que resulte necesaria para la mejor observancia de la Ley General, de esta Política y de las disposiciones en la materia.

X. Las demás que determinen las disposiciones normativas aplicables, así como la Autoridad Garante o la Secretaría Anticorrupción y Buen Gobierno, en el ámbito de su competencia.

I.3. DESIGNACIÓN DE LA PERSONA ENLACE RESPONSABLE

Artículo 3. Cada UA designa a una persona servidora pública de mando superior para fungir al interior de ésta, así como ante la Unidad de Transparencia y ante el Comité de Transparencia, 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 la persona titular de los datos y la Autoridad Garante, en el ámbito de su competencia.

I.4. FUNCIONES DE LA PERSONA ENLACE RESPONSABLE

Artículo 4. La persona designada como enlace responsable tiene las funciones siguientes:

I. Implementar y acreditar en su UA el cumplimiento de los principios y deberes de acuerdo con las directrices señaladas por esta Política, la Autoridad Garante y el Comité de Transparencia en su calidad de autoridad máxima en materia de datos personales de la ASF.

II. Promover la capacitación del personal de la ASF adscrito a su UA que se encuentre involucrado directamente en el tratamiento de datos personales.

III. Participar en la integración y actualización de los documentos normativos previstos por la Ley General y demás disposiciones aplicables.

IV. Validar y, en su caso, actualizar semestralmente el Inventario de datos personales que, en el ámbito de su competencia, corresponda a su UA.

V. Vigilar que al interior de su UA se brinde la debida atención a las solicitudes relativas al ejercicio de los Derechos ARCO.

VI. Las demás que determinen las disposiciones normativas, así como la Autoridad Garante, la Secretaría Anticorrupción y Buen Gobierno y el Comité de Transparencia, en el ámbito de su competencia.

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES DE LA ASF

La Política de Protección de Datos Personales de la ASF es un instrumento que permite acreditar y asegurar el cumplimiento de los principios y deberes en materia de protección de datos personales al interior de la ASF, al establecer los elementos y actividades de dirección, operación y control en la materia.

La Política es de observancia general y obligatoria para todo el personal de la ASF involucrado con el tratamiento de datos personales.

FUENTE: Esquema de elaboración propia con base en lo señalado en el objetivo y alcance de esta Política, pág. 9.

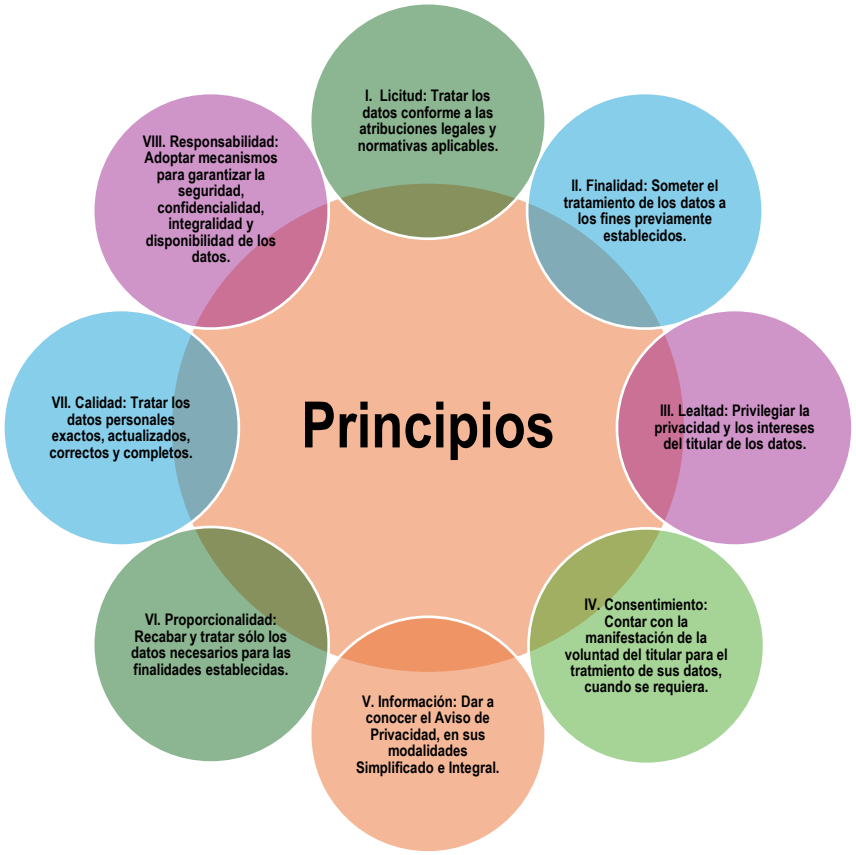
Sin texto

CAPÍTULO II. PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES EN LA ASF[2]

II.1. DE LOS PRINCIPIOS

Artículo 5. Las UA responsables del tratamiento de datos personales observan los principios rectores siguientes:

I. Licitud
II. Finalidad
III. Lealtad
IV. Consentimiento
V. Información
VI Proporcionalidad
VII. Calidad
VIII. Responsabilidad



FUENTE: Diagrama de elaboración propia tomando como referencia la definición de los principios de protección de datos personales referidos en esta Política, págs. 16 a 28.

[2] El contenido del presente Capítulo toma como referencia normativa lo establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 20 de marzo de 2025 y en los Lineamientos Generales de Protección de Datos Personales para el Sector Público, disponibles para su consulta en: https://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf, última modificación publicada en el Diario Oficial de la Federación el 14 de junio de 2024.

II.2. PRINCIPIO DE LICITUD

Artículo 6. Este principio asegura que el tratamiento de datos personales por parte de la UA se realice conforme a los límites fijados en el marco normativo que regula su ámbito de atribuciones, evitando su uso discrecional.

El tratamiento de datos personales por parte de la UA se sujeta a las atribuciones o facultades que les son conferidas en la normativa que rige el actuar de la ASF y en estricto apego a lo dispuesto en la Ley General, los Lineamientos Generales, la presente Política y demás disposiciones jurídicas aplicables en materia de protección de datos personales.

II.2.1. Actividad vinculada al Principio de Licitud

Artículo 7. La UA identifica el marco normativo que, en el ámbito de sus funciones, se encuentra relacionado con el tratamiento de datos personales, el tipo de datos objeto de tratamiento y las finalidades para ello.

II.2.2. Mecanismo para acreditar el cumplimiento del Principio de Licitud

Artículo 8. Para el cumplimiento del Principio de Licitud, la UA incluye en el Aviso de Privacidad Integral y en el Inventario, el fundamento legal que le faculta a tratar datos personales.

II.3. PRINCIPIO DE FINALIDAD

Artículo 9. Este principio permite proteger a la persona titular de los datos de cualquier uso excesivo o indeterminado de ellos, por lo que siempre está circunscrito al ámbito de incidencia establecido por el propósito, motivo o razón que justifica su obtención.

Como tal, el principio implica que todo tratamiento de datos personales efectuado por la UA está justificado por finalidades concretas, explícitas, lícitas y legítimas.

Para tal efecto, se entiende que las finalidades son:[3]

I. **Concretas:** cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en la persona titular.

II. **Explícitas:** cuando las finalidades se expresan y dan a conocer de manera clara en el Aviso de Privacidad.

III. **Lícitas:** cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades de la ASF en su calidad

[3] **Lineamientos Generales de Protección de Datos Personales para el Sector Público**, artículo 9.

de Responsable, conforme a lo previsto en la legislación mexicana y en el derecho internacional que le resulte aplicable.

IV. **Legítimas:** cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento de la persona titular, salvo que se actualice alguna de las causales de excepción a que se refiere la Ley General y la presente Política.

II.3.1. Actividades vinculadas al Principio de Finalidad

Artículo 10. Para el cumplimiento del Principio de Finalidad, la UA que trate datos personales debe:

I. Establecer en el Aviso de Privacidad todas las finalidades para las cuales se tratan los datos personales, de acuerdo con las atribuciones o facultades que tiene encomendadas.

II. Tratar los datos personales conforme a las finalidades concretas, lícitas, explícitas y legítimas expresadas en el Aviso de Privacidad.

III. Obtener el consentimiento de la persona titular para el tratamiento de sus datos personales, salvo las excepciones establecidas en la Ley General y en la presente Política.

IV. Informar a la persona titular las finalidades distintas a las que se someta el tratamiento de sus datos, en caso de que no hayan sido enteradas en el Aviso de Privacidad, siempre y cuando se tengan facultades o atribuciones para ello y se recabe su consentimiento, salvo que se actualice alguna de las excepciones establecidas en la Ley General y en esta Política para dicho consentimiento.

En el supuesto de la fracción IV, la UA considera lo siguiente:

a) La naturaleza de los datos personales.

b) Las consecuencias que, en su caso, se generen a la persona titular con motivo del tratamiento posterior de sus datos personales.

c) Las medidas adoptadas para que el tratamiento posterior de los datos personales cumpla con las disposiciones normativas aplicables.

d) La expectativa razonable de privacidad de la persona titular, consistente en la confianza depositada en la ASF para que los datos personales proporcionados sean tratados conforme a lo señalado en el Aviso de Privacidad.

II.3.2. Mecanismos para acreditar el cumplimiento del Principio de Finalidad

Artículo 11. Para acreditar el cumplimiento del Principio de Finalidad, la UA debe:[4]

I. Incluir en el Inventario las finalidades de cada tratamiento que se realice en su UA, así como verificar que éstas sean específicas o determinadas y acordes a las atribuciones o facultades de la ASF y en específico de la UA.

II. Vigilar que la persona servidora pública únicamente trate los datos personales de acuerdo con las finalidades informadas en el Aviso de Privacidad correspondiente.

III. Verificar que el Aviso de Privacidad informe todas las finalidades para las cuales se tratan los datos personales y que éstas sean descritas de manera clara.

IV. Informar a la persona titular sobre el tratamiento de los datos para finalidades distintas, en términos de las disposiciones aplicables.

V. Recabar el consentimiento de la persona titular, cuando proceda.

II.4. PRINCIPIO DE LEALTAD

Artículo 12. Este principio asegura que la actuación institucional esté delimitada al tratamiento de datos personales dentro de un esquema de buena fe y de honestidad que favorece la construcción de una relación de confianza entre la ASF y la persona titular.

Como tal, el Principio conlleva que la UA se abstenga de obtener y tratar datos personales por medios engañosos o fraudulentos, privilegiando la protección de los intereses de la persona titular y la expectativa razonable de privacidad.

Se entiende que un acto puede ser engañoso o fraudulento cuando la información que proporciona la UA a la persona titular sobre el tratamiento de sus datos personales es falaz, o cuando las finalidades no son informadas en el Aviso de Privacidad, o bien, cuando las señaladas en éste no corresponden con el tratamiento.[5]

II.4.1. Actividades vinculadas al Principio de Lealtad

Artículo 13. Derivado del Principio de Lealtad, la UA responsable del tratamiento de datos personales debe:

I. Obtener y tratar los datos personales sin que medie dolo, mala fe o negligencia.

[4] Sirve como referencia el Documento Orientador del Programa de Protección de Datos emitido por el entonces Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Ciudad de México, 2018, disponible para consulta en: https://inicio.inai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

[5] Sirve como referencia de estos conceptos lo establecido en las obligaciones generales del Principio de Lealtad, contenidas en la Guía para el Tratamiento de Datos Biométricos, emitida por el entonces Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Ciudad de México, 2018, pág. 23, disponible en: https://inicio.inai.org.mx/documentosdeinteres/guiadatosbiometricos_web_links.pdf

II. Privilegiar los intereses de la persona titular y evitar cualquier tipo de discriminación, trato injusto o arbitrario en su contra, con motivo del tratamiento de sus datos personales.

III. Respetar la expectativa razonable de privacidad.

II.4.2. Mecanismos para acreditar el cumplimiento del Principio de Lealtad

Artículo 14. Para acreditar el cumplimiento del Principio de Lealtad, la UA debe:

I. Contar con los avisos de privacidad conforme a lo establecido en la Ley General y en la presente Política.

II. Verificar que los tratamientos realizados no den lugar a discriminación, trato injusto o arbitrario en contra de la persona titular.

III. Constatar que el tratamiento de datos personales sólo se lleve a cabo para los fines informados en el Aviso de Privacidad.

II.5. PRINCIPIO DE CONSENTIMIENTO

Artículo 15. Este principio implica que la persona titular pueda ejercer plenamente su capacidad de decisión sobre sus datos personales.

Previo al tratamiento de los datos personales, la UA obtiene el consentimiento de la persona titular de manera libre, específica e informada, en términos de lo dispuesto en la Ley General.

Se entiende que el consentimiento es:

I. **Libre:** cuando corresponde con la manifestación de la voluntad de la persona titular.

II. **Específico:** cuando se refiere a una o varias finalidades que justifican el tratamiento de los datos personales.

III. **Informado:** cuando la persona titular tiene conocimiento del Aviso de Privacidad de manera previa al tratamiento al que se someten sus datos.

El consentimiento es expreso cuando por cualquier medio la persona titular manifiesta su voluntad acerca del tratamiento de sus datos personales.

El consentimiento es tácito cuando habiéndose puesto el Aviso de Privacidad a disposición de la persona titular, ésta no manifiesta su voluntad en sentido contrario.[6]

[6] **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**, artículo 15, segundo párrafo.

Por regla general, el consentimiento tácito es 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.

No se requiere consentimiento cuando se actualice alguna de las causales de excepción siguientes:[7]

I. Cuando una ley así lo disponga, en cuyo caso los supuestos de excepción deben ser acordes con las bases, principios y disposiciones establecidos en la Ley General.

II. Cuando las transferencias que se realicen entre la ASF 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.

III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente.

IV. Cuando el tratamiento de los datos personales es necesario para el reconocimiento o defensa de derechos de la persona titular ante una autoridad competente.

V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre la persona titular y la ASF.

VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a una persona de manera individual o en sus bienes.

VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico o la prestación de asistencia sanitaria.

VIII. Cuando los datos personales figuren en fuentes de acceso público.

IX. Cuando los datos personales se sometan a un procedimiento previo de disociación.

X. Cuando la persona titular de los datos personales sea reportada como desaparecida en términos de las disposiciones jurídicas en la materia.

La actualización de alguno de los supuestos anteriores no exime a la UA ni a la persona servidora pública responsable del tratamiento de los datos personales del cumplimiento de las demás obligaciones establecidas en la Ley General, en los Lineamientos Generales, en la presente Política y en las demás disposiciones aplicables.

[7] **Ibid.**, artículo 16.

II.5.1. Actividades vinculadas al Principio de Consentimiento

Artículo 16. En términos de los alcances del Principio de Consentimiento, la UA debe:

I. Obtener el consentimiento de la persona titular previo al tratamiento de los datos, salvo que se actualice alguno de los supuestos de excepción descritos en el artículo anterior.

II. Recabar el consentimiento expreso y, en su caso, por escrito cuando se refiera al tratamiento de datos sensibles, a través de formatos claros y sencillos, acorde con el perfil de la persona titular, en el cual se distingan los datos y finalidades del tratamiento que requieren de la manifestación de su voluntad.

III. Implementar medios sencillos y gratuitos para la obtención del consentimiento, independientemente de la modalidad en que éste se requiera.

IV. Habilitar, en su caso, en el Aviso de Privacidad casillas y/o espacios para que la persona titular exprese su consentimiento, respecto de cada una de las finalidades para las cuales son tratados sus datos.

II.5.2. Mecanismos para acreditar el cumplimiento del Principio de Consentimiento

Artículo 17. Para acreditar el cumplimiento del Principio de Consentimiento, la UA debe:

I. Identificar, en el Aviso de Privacidad, aquellos datos y finalidades que requieren del consentimiento de la persona titular para su tratamiento.

II. Mantener bajo su resguardo una copia del documento en el cual se haya manifestado el consentimiento de la persona titular para el tratamiento de sus datos, cuando proceda.

III. Documentar que se pone a disposición de la persona titular el Aviso de Privacidad, en aquellos casos en los cuales sea válido el consentimiento tácito.

II.6. PRINCIPIO DE INFORMACIÓN

Artículo 18. Este principio consiste en informar con oportunidad a la persona titular en qué consistirá el tratamiento de sus datos personales, así como las vías para el ejercicio de sus Derechos ARCO y, en su caso, de la portabilidad.

Independientemente de que se requiera o no el consentimiento de la persona titular para el tratamiento de los datos personales, la UA informa a ésta sobre la existencia y las características principales del tratamiento al que serán sometidos sus datos personales.

La UA que trate datos personales elabora y pone a disposición el Aviso de Privacidad Simplificado e Integral que corresponda al tratamiento que lleva a cabo, en los términos establecidos por la Ley General, los Lineamientos Generales, la presente Política y demás disposiciones aplicables.

En cualquier momento, la persona titular puede revocar el consentimiento que ha otorgado para el tratamiento de sus datos personales, sin que se le atribuyan efectos retroactivos a la revocación, a través del ejercicio de los derechos de cancelación y de oposición, de conformidad con lo dispuesto en la Ley General y en los Lineamientos Generales.

II.6.1. Actividades vinculadas al Principio de Información

Artículo 19. Para dar atención al Principio de Información, la UA que trate datos personales debe:

I. Redactar el Aviso de Privacidad que se requiera, en sus modalidades Integral y Simplificado, conforme al tratamiento que se lleva a cabo.

II. Poner gratuitamente a disposición de la persona titular el Aviso de Privacidad en los términos que fije la Ley General, los Lineamientos Generales y demás disposiciones aplicables, aunque no se requiera su consentimiento para el tratamiento de los datos personales.

III. Elaborar el Aviso de Privacidad con todos los elementos informativos que resulten aplicables, de manera clara, comprensible, así como con una estructura y diseño que facilite su entendimiento, considerando su accesibilidad para personas con algún tipo de discapacidad.

IV. Difundir el Aviso de Privacidad por medios electrónicos y físicos.

V. Ubicar el Aviso de Privacidad en un lugar visible y que facilite su consulta, con independencia del medio de difusión o reproducción que se utilice.

VI. Verificar que el Aviso de Privacidad sea redactado de conformidad con lo establecido por la Ley General, los Lineamientos Generales y demás disposiciones aplicables.

VII. Comunicar el Aviso de Privacidad a quienes se transfieran datos personales.

VIII. Prever la implementación de medidas compensatorias, en términos de lo dispuesto en la Ley General y demás disposiciones aplicables, para dar a conocer el Aviso de Privacidad a través de medios masivos de difusión (periódico oficial, página de internet, carteles o cápsulas informativas u otro similar), cuando resulte imposible hacerlo de manera directa a la persona titular o ello exija esfuerzos desproporcionados.

II.6.2. Mecanismos para acreditar el cumplimiento del Principio de Información

Artículo 20. Para acreditar el cumplimiento del Principio de Información, la UA debe:

I. Contar con los Avisos de Privacidad Integral y Simplificado por cada proceso de tratamiento de datos personales que se lleve a cabo.

II. Implementar un procedimiento gratuito para la puesta a disposición del Aviso de Privacidad.

III. Realizar las gestiones para que el Aviso de Privacidad, en sus modalidades Simplificado e Integral, sea publicado en la página de internet de la ASF, en la sección que se destine para ello, a fin de que se difunda por medios electrónicos.

IV. Incluir en el Inventario de datos personales la referencia al lugar y los medios en el que se difunde y coloca el Aviso de Privacidad.

V. Documentar la comunicación realizada del Aviso de Privacidad a quienes se transfieran los datos personales.

II.7. PRINCIPIO DE PROPORCIONALIDAD

Artículo 21. Este principio crea condiciones de equilibrio entre el cumplimiento de las atribuciones de la ASF y el uso de datos personales, dotando a la persona titular de la certeza de que únicamente se tratan los estrictamente necesarios.

La UA recaba aquellos datos personales que resulten adecuados, relevantes y necesarios para la finalidad que justifica su tratamiento.

Se entiende 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 UA de la ASF.

II.7.1. Actividades vinculadas al Principio de Proporcionalidad

Artículo 22. Para el cumplimiento al Principio de Proporcionalidad la UA responsable del tratamiento de datos personales debe:

I. Recabar y tratar sólo aquellos datos personales necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtienen.

II. Participar en la actualización de la normativa y los formatos internos con las áreas competentes de la ASF, relacionados con el ámbito de sus funciones, para reducir al mínimo necesario los datos personales que serán tratados, de acuerdo con las finalidades que lo motivan.

III. Limitar al mínimo posible el periodo de tratamiento de datos personales.

II.7.2. Mecanismos para acreditar el cumplimiento del Principio de Proporcionalidad

Artículo 23. Para acreditar el cumplimiento del Principio de Proporcionalidad, la UA debe:

I. Analizar y revisar que en su UA se soliciten sólo aquellos datos personales que resultan indispensables para cumplir con las finalidades de que se trate.

II. Promover que en su UA se requiera el mínimo de datos personales para lograr las finalidades para las cuales se tratan.

III. Promover prácticas que minimicen la obtención de datos personales y el periodo de su tratamiento y, en su caso, señalarlas en su documento de seguridad interno que dispone el artículo 41 de esta Política.

II.8. PRINCIPIO DE CALIDAD

Artículo 24. Este principio significa que los datos personales que son tratados por la UA son veraces y reflejan la realidad de la persona titular y, por lo tanto, son adecuados para el propósito legítimo para el cual se recaban.

La UA adopta las medidas señaladas en su documento de seguridad interno para mantener los datos personales exactos, correctos, completos y actualizados, a fin de que no se altere su veracidad.

Se entiende que los datos personales son:[8]

I. **Exactos y correctos**: Cuando no presentan errores que pudieran afectar su veracidad.

II. **Completos**: Cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y las atribuciones de la UA responsable.

III. **Actualizados**: Cuando los datos personales responden fielmente a la realidad de la persona titular.

Se presume que se cumple con la calidad de los datos personales cuando éstos son proporcionados directamente por la persona titular y cuando no manifieste lo contrario.[9]

Cuando los datos personales se hayan obtenido indirectamente de la persona titular, la UA debe adoptar las medidas referidas en su documento de seguridad interno para garantizar que los mismos respondan al Principio de Calidad, de acuerdo con su categoría, las condiciones y los medios del tratamiento.

En el supuesto de que los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el Aviso de Privacidad que motivaron su tratamiento, son suprimidos, previo bloqueo y una vez que concluya su plazo de conservación, de acuerdo con las disposiciones legales aplicables en materia archivística.

[8] **Lineamientos Generales de Protección de Datos Personales para el Sector Público**, artículo 21.
[9] **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**, artículo 17, segundo párrafo.

II.8.1. Actividades vinculadas al Principio de Calidad

Artículo 25. Para el cumplimiento del Principio de Calidad, la UA que trate datos personales debe:

I. Implementar medidas para que las actualizaciones efectuadas tengan impacto inmediato en las distintas bases de datos en las cuales obre la información de la persona titular.

II. Establecer plazos de conservación de la información, conforme a las disposiciones legales aplicables en materia archivística.

III. Observar los procedimientos para la conservación, bloqueo y supresión de los datos personales.

II.8.2. Mecanismos para acreditar el cumplimiento del Principio de Calidad

Artículo 26. Para acreditar el cumplimiento del Principio de Calidad, la UA debe:

I. Generar, en su caso, una relación de todas las bases de datos con que cuentan y el tipo de información personal tratada en cada una de ellas que, cuando proceda, permita vincularlas.

II. Documentar las acciones de actualización y supresión que realice.

III. Atender los procedimientos para la conservación, bloqueo y supresión de los datos personales.

II.9. PRINCIPIO DE RESPONSABILIDAD

Artículo 27. Este principio implica que la ASF, en su calidad de Responsable, establece las políticas, las prácticas o los mecanismos de supervisión y monitoreo exigibles a su interior, para garantizar el cumplimento de todos los principios y deberes en materia de protección de datos personales.

Conforme al Principio de Responsabilidad, la UA vela por el cumplimiento del resto de los principios, promueve la adopción de medidas necesarias para su aplicación y demuestra ante la persona titular y ante la Autoridad Garante o instancia competente, que se cumplen con las obligaciones en torno a la protección de los datos personales.

II.9.1. Actividades vinculadas al Principio de Responsabilidad

Artículo 28. Para dar cumplimiento al Principio de Responsabilidad, la UA debe:

I. Establecer entre el personal bajo su adscripción la obligatoriedad y exigibilidad de la Política y del Programa de Protección de Datos Personales que apruebe el Comité de Transparencia y, en su caso, prever los recursos necesarios para su instrumentación.

II. Incentivar la capacitación y actualización de las personas servidoras públicas de su adscripción sobre las obligaciones y demás deberes en materia de protección de datos personales.

III. Revisar periódicamente el Programa de Protección de Datos Personales y el Documento de Seguridad de la ASF para proponer, en su caso, las modificaciones que se requieran, así como su documento de seguridad interno para mantenerlo actualizado.

IV. Establecer los mecanismos necesarios para recibir y responder dudas o quejas de las personas titulares con relación al tratamiento de sus datos.

V. Observar lo previsto en el Programa de Protección de Datos Personales, así como la normativa interna que emita la UA competente, relacionada con la seguridad de la información y el uso servicios, sistemas o plataformas informáticas, o cualquier otra tecnología disponible que implique el tratamiento de datos personales, a fin de garantizar su protección de conformidad con la Ley General, los Lineamientos Generales, la presente Política y las demás disposiciones aplicables.

II.9.2. Mecanismos para acreditar el cumplimiento del Principio de Responsabilidad

Artículo 29. Para acreditar el cumplimiento al Principio de Responsabilidad, la UA debe:

I. Cumplir con el PCAMPDP.

II. Llevar un registro de la atención de dudas o quejas que, en su caso, formulen las personas titulares sobre el tratamiento que la UA realice de sus datos.

III. Documentar la comunicación que se realice al interior de su UA para el conocimiento de la Política y del Programa de Protección de Datos Personales que al efecto se apruebe.

IV. Participar en la revisión y actualización del Programa de Protección de Datos Personales, del Documento de Seguridad de la ASF y de la normativa interna en la materia para proponer, en su caso, las modificaciones correspondientes, así como mantener actualizado su documento de seguridad interno conforme al tratamiento de datos personales que realice en el ámbito de sus funciones.

V. Guardar evidencia del cumplimiento de la presente Política.

Para efectos de lo previsto en la fracción II, se observa lo siguiente:

1) La recepción de una duda o de una queja que presente la persona titular relacionada con el tratamiento de sus datos personales, puede realizarse por los medios siguientes:

   a) **Unidad de Transparencia de la ASF:** ubicada en Carretera Picacho Ajusco número 167, Planta Baja, Colonia Ampliación Fuentes del Pedregal. Código Postal 14110, Demarcación Territorial Tlalpan, Ciudad de México,

en un horario de atención, de lunes a jueves de 9:00 a 16:00 horas y, viernes de 9:00 a 15:00 horas.

b) **Correo electrónico:** unidadtransparencia@asf.gob.mx

2) Son requisitos para la presentación de una duda o de una queja:

a) Nombre de la persona titular o, en su caso, de su representante y acreditación de su personalidad.

b) Domicilio o medio para recibir notificaciones.

c) Descripción clara y precisa de la duda o de la queja sobre el tratamiento de sus datos.

d) En el caso de la presentación de una queja, las pruebas que considere pertinentes para respaldar la misma.

De no señalarse el domicilio o medio para recibir notificaciones, la comunicación de la respuesta correspondiente a la persona titular se realiza a través de los estrados de la Unidad de Transparencia. De presentarse por correo electrónico, la notificación se lleva a cabo por el mismo medio.

En caso de no cumplir con alguno de los requisitos establecidos para la recepción de la duda o de la queja, la Unidad de Transparencia previene a la persona titular o a su representante, dentro de un plazo no mayor a tres días hábiles posteriores a su presentación, quedando interrumpidos los plazos para su trámite ante la UA. La persona interesada cuenta con un plazo máximo de diez días hábiles contados a partir de su notificación para desahogar la prevención; de no desahogarla en dicho plazo, se tendrá por no presentada la duda o la queja.

3) Una vez recibida la duda o la queja por parte de la Unidad de Transparencia, ésta la remite, en un plazo no mayor a dos días hábiles, a la UA responsable del tratamiento de los datos personales, para su registro y atención.

4) La UA da respuesta en un plazo que no exceda de 15 días hábiles contados a partir de la comunicación de la duda o de la queja.

5) La notificación a la respuesta a la persona titular se realiza a través de la Unidad de Transparencia, dentro de los tres días hábiles posteriores a su envío por parte de la UA competente.

En caso de que la duda o la queja corresponda a una solicitud para el ejercicio de los Derechos ARCO, la Unidad de Transparencia procede conforme a lo establecido en la Ley General. De referirse a un trámite diverso, orienta a la persona interesada para que acuda a la instancia competente.

La Unidad de Transparencia podrá elaborar las propuestas de formatos que sirvan de apoyo para la recepción y la atención de dudas o quejas, con independencia de que puede realizarse en escrito libre.

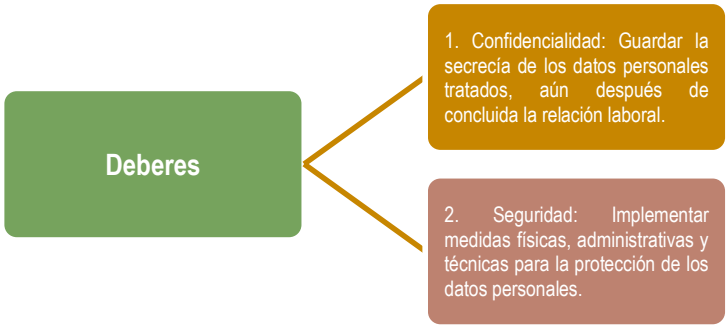
CAPÍTULO III. DEBERES PARA LA PROTECCIÓN DE DATOS PERSONALES EN LA ASF

III.1. DE LOS DEBERES

Artículo 30. Además de los principios señalados en el Capítulo anterior, las UA cumplen con lo siguiente:

I. Deber de Confidencialidad.

II. Deber de Seguridad.



FUENTE: Diagrama de elaboración propia tomando como referencia la definición de los deberes para la protección de datos personales de esta Política, págs. 29 y 30.

III.2. DEBER DE CONFIDENCIALIDAD

Artículo 31. El Deber de Confidencialidad es un elemento fundamental en la actuación del personal de la ASF para proteger los datos personales que son tratados en ejercicio de sus atribuciones y funciones, acorde con los fines para los cuales fueron recabados.

La UA establece controles o mecanismos de observancia obligatoria para que las personas que intervengan en cualquier fase del tratamiento de datos personales, guarden la confidencialidad de los mismos. Esta obligación subsiste aún después de finalizar su relación laboral con la ASF y sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.

III.2.1. Actividades vinculadas al Deber de Confidencialidad

Artículo 32. Para dar cumplimiento al Deber de Confidencialidad, la UA está obligada a:

I. Prever controles mediante los cuales se garantice la confidencialidad de los datos personales que son tratados.

II. 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.

III. Cumplir con el PCAMPDP, que fortalezca la sensibilización del personal sobre la importancia de la confidencialidad en la materia.

IV. Proponer, en su caso, la implementación de mejores prácticas al interior de la UA para garantizar la secrecía de los datos personales, de conformidad con sus atribuciones.

III.2.2. Mecanismos para acreditar el cumplimiento del Deber de Confidencialidad

Artículo 33. Para acreditar el cumplimiento del Deber de Confidencialidad, la UA está obligada a:

I. Incluir en su documento de seguridad interno, los controles y medidas de seguridad implementadas para garantizar la secrecía de los datos personales y guardar evidencia de su implementación.

II. Contar, de ser el caso, con los contratos o instrumentos jurídicos en los que se establezca la confidencialidad de datos, respecto de transferencias o remisiones.

III. Tener la evidencia documental de los cursos, talleres, seminarios o similares relacionados con la materia de protección de datos personales, en los que haya participado el personal de su adscripción.

IV. Documentar, de ser el caso, la implementación de mejores prácticas que garanticen la confidencialidad de los datos tratados.

III.3. DEBER DE SEGURIDAD

Artículo 34. El Deber de Seguridad constituye la obligación que tiene la ASF, en su carácter de Responsable, de implementar, mantener y supervisar las medidas de seguridad que son establecidas por la UA, para salvaguardar los datos personales que son tratados en sus respectivos ámbitos de competencia.

Corresponde a la UA adoptar e instrumentar las medidas de seguridad físicas, técnicas y administrativas para garantizar la protección de los datos personales tratados, a fin de evitar cualquier afectación a su titular.

III.3.1. Actividades vinculadas al Deber de Seguridad

Artículo 35. Para dar cumplimiento al Deber de Seguridad, la UA está obligada a:

I. Generar e implementar políticas de gestión, en las cuales se considere el tipo de datos personales recabados y el tratamiento que se les dará.

II. Determinar a las personas que pueden intervenir en el tratamiento de los datos personales, así como definir las funciones y obligaciones que les correspondan.

III. Elaborar el Inventario de datos personales y de los procesos en los que se lleva a cabo su tratamiento, conforme lo indica el Capítulo V de esta Política y demás disposiciones jurídicas aplicables.

IV. Realizar un análisis de riesgo de los datos personales tratados, así como de los sistemas físicos y/o electrónicos en el cual se desarrolle dicho tratamiento.

Para realizar el análisis de riesgo se considera al menos:[10]

a) Los requerimientos regulatorios, códigos de conducta o mejores prácticas aplicables al proceso de tratamiento de datos que se realice.

b) La determinación del valor o importancia de los datos personales de acuerdo con su tipo y su categoría, así como con su ciclo de vida.

c) La descripción de los activos involucrados en el tratamiento de los datos personales.

d) Las consecuencias negativas para la persona titular, que pudieran derivar de una vulneración ocurrida a la seguridad.

V. Realizar un análisis de brecha para identificar nuevas medidas de seguridad que pueden reemplazar uno o más controles implementados, a partir de comparar las medidas de seguridad existentes y las medidas de seguridad faltantes o recomendadas para el proceso de tratamiento de datos personales que realiza.[11]

VI. Desarrollar acciones de prevención y mitigación de amenazas o vulneraciones de datos personales.

VII. Monitorear y revisar las medidas de seguridad adoptadas para garantizar la protección de datos.

VIII. Incentivar la capacitación de las personas servidoras públicas involucradas en el tratamiento de datos personales, conforme al nivel de responsabilidad que ellas tengan asignado.

III.3.2. Mecanismos para acreditar el cumplimiento del Deber de Seguridad

Artículo 36. Para acreditar el cumplimiento del Deber de Seguridad, la UA está obligada a:

I. Contar con el Inventario de datos personales y de los procesos de tratamiento.

II. Comunicar al personal de su adscripción las políticas implementadas para la protección de datos personales y guardar evidencia de ello.

III. Llevar una bitácora en la cual se asiente cualquier amenaza o vulneración de datos personales suscitada, así como de las acciones realizadas para su mitigación.

IV. Instrumentar las medidas de seguridad físicas, técnicas y administrativas adoptadas para garantizar el tratamiento de los datos recabados, así como las

[10] **Lineamientos Generales de Protección de Datos Personales para el Sector Público**, artículo 60.
[11] **Ibid**., artículo 61.

acciones de monitoreo, análisis y revisión, a fin de mantenerlas actualizadas y, en su caso, detectar áreas de oportunidad para su desarrollo y ejecución.

V. Tener evidencia del cumplimiento del PCAMPDP por parte de las personas servidoras públicas de la UA.

CAPÍTULO IV. DOCUMENTO DE SEGURIDAD DE LA ASF

IV.1. OBJETO Y ALCANCES

Artículo 37. La ASF cuenta 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.

Artículo 38. El Documento de Seguridad de la ASF contiene como mínimo, lo siguiente: [12]

I. El Inventario de Datos Personales de la ASF y de los procesos de tratamiento.

II. Las funciones y obligaciones de las personas que traten datos personales.

III. El análisis de riesgos.

IV. El análisis de brecha.

V. El plan de trabajo.

VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad.

VII. El programa general de capacitación.

IV.2. ACTUALIZACIONES

Artículo 39. En las actualizaciones que se realicen al Documento de Seguridad de la ASF participan todas las UA, por medio de la persona designada como enlace responsable a que se refiere el artículo 3 de la presente Política, quien en todo momento observa los principios y deberes a que se refiere la Ley General, los Lineamientos Generales, esta Política y demás disposiciones legales aplicables.

Para la formulación de propuestas de actualización del Documento de Seguridad de la ASF, la Unidad de Transparencia elabora los formatos, cuestionarios o cualquier otro documento de apoyo que resulte útil para el cumplimiento de dicha actividad.

El Documento de Seguridad de la ASF se actualiza en los supuestos siguientes:[13]

I. Cuando se produzcan modificaciones sustanciales al tratamiento de los datos personales que deriven en un cambio de nivel de riesgo.

[12] **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**, artículo 29.
[13] **Ibid**., artículo 30.

II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión con que se cuente.[14]

III. Derivado de un proceso de mejora para mitigar el impacto de vulneración a la seguridad ocurrida.

IV. Con motivo de la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Con independencia de los supuestos anteriores, el Documento de Seguridad de la ASF se actualiza cada tres años.

Artículo 40. Cuando una UA identifica que se actualiza alguno de los supuestos referidos en el artículo anterior, la persona designada como enlace responsable solicita por escrito al Comité de Transparencia las actualizaciones necesarias, quien resuelve lo conducente.

La persona designada como enlace responsable puede solicitar orientación técnica a la Unidad de Transparencia para la integración o cualquier acto relacionado con los alcances del Documento de Seguridad de la ASF.

IV.3. DOCUMENTO DE SEGURIDAD INTERNO

Artículo 41. Con independencia del Documento de Seguridad de la ASF, la UA integra su documento de seguridad interno, el cual, en correspondencia con el primero, establece las medidas de seguridad y controles que son implementados por las personas bajo su adscripción, de acuerdo con los procesos de tratamiento de datos personales que realiza en el ámbito de sus atribuciones.

El documento de seguridad interno permanece bajo el resguardo de cada UA.

La Unidad de Transparencia puede elaborar las propuestas de formatos que sirvan de apoyo para la integración o actualización del documento de seguridad interno, manteniendo la homogeneidad de sus elementos.

IV.3.1 Supervisión del documento de seguridad interno

Artículo 42. Corresponde a las personas titulares de las auditorías especiales y de las unidades, así como de las direcciones generales u homólogas, en su ámbito de competencia, supervisar el cumplimiento de las políticas para la gestión y tratamiento de datos personales.

La persona titular de la auditoría especial o de unidad puede solicitar en cualquier momento a quien haya designado como enlace responsable, los informes que se requieran sobre las acciones contenidas en el documento de seguridad interno, mismo

[14] Se entiende por sistema de gestión al conjunto de elementos y actividades para establecer, implementar y monitorear el tratamiento y seguridad de los datos personales conforme a lo previsto en **Ley General Protección de Datos Personales en Posesión de Sujetos Obligados,** artículo 28, segundo párrafo.

que debe integrarse en coordinación con las personas directoras generales o de área que corresponda, conforme a su ámbito de competencia.

IV.4. VULNERACIONES A LA SEGURIDAD DE LOS DATOS

Artículo 43. En caso de presentarse una vulneración de datos personales, la UA atiende a lo dispuesto en la Ley General, los Lineamientos Generales, el Protocolo general de la Auditoría Superior de la Federación para la prevención, identificación y actuación ante posibles vulneraciones a la seguridad de los datos personales (2TA3PD01), así como la normativa que resulte aplicable.

Artículo 44. Se consideran vulneraciones a la seguridad de los datos, las siguientes:[15]

I. La pérdida o destrucción no autorizada.

II. El robo, extravío o copia no autorizada.

III. El uso, acceso o tratamiento no autorizado.

IV. El daño, la alteración o modificación no autorizada.

Cuando la UA responsable del tratamiento de los datos personales confirme que aconteció una vulneración debe notificarlo a la Unidad de Transparencia para que, con el apoyo de ésta, se determine la procedencia o no de comunicar la vulneración a la persona titular de los datos involucrados, así como a la Autoridad Garante, en el ámbito de su competencia, en términos de la normativa aplicable.

Artículo 45. Si la vulneración afecta de forma significativa los derechos patrimoniales o morales de la persona titular, la UA involucrada genera dentro del plazo de 48 horas posteriores a que fue confirmada la vulneración, un informe detallado que contenga lo siguiente:[16]

I. La naturaleza del incidente.

II. Los datos personales comprometidos.

III. Las recomendaciones a la persona titular acerca de las medidas que puede adoptar para proteger sus intereses.

IV. Las acciones correctivas implementadas para mitigar la vulneración.

V. Los datos de contacto de la persona enlace responsable de la UA involucrada a la cual puede acudir la persona titular para obtener más información al respecto.

El informe se comunica a la persona titular por la UA responsable del tratamiento de los datos personales, a través de la Unidad de Transparencia, en un plazo no mayor a

[15] **Ley General Protección de Datos Personales en Posesión de Sujetos Obligados**, artículo 32.
[16] **Ibid.**, artículo 35.

72 horas, previo conocimiento del Comité de Transparencia, conforme a lo establecido en el Protocolo general de la Auditoría Superior de la Federación para la prevención, identificación y actuación ante posibles vulneraciones a la seguridad de los datos personales (2TA3PD01).

Adicionalmente, la UA prevé un informe dirigido a la Autoridad Garante y al Comité de Transparencia, en su ámbito de competencia, por conducto de la Unidad de Transparencia, en el que considera lo siguiente:[17]

I. La hora y fecha de la identificación de la vulneración.

II. La hora y fecha de la confirmación de la vulneración.

III. La hora y fecha del inicio de la investigación sobre la vulneración.

IV. La naturaleza del incidente o vulneración ocurrida.

V. La descripción detallada de las circunstancias en torno a la vulneración ocurrida.

VI. Las categorías de datos y número aproximado de las personas titulares afectadas.

VII. Los sistemas de tratamiento y datos personales comprometidos.

VIII. Las acciones correctivas realizadas de forma inmediata.

IX. La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida.

X. Las recomendaciones dirigidas a la persona titular.

XI. El medio a través del cual la persona titular pueda obtener más información al respecto.

XII. El nombre completo de la o las personas designadas y sus datos de contacto, para que puedan proporcionar más información a la Autoridad Garante, en caso de requerirse.

XIII. Cualquier otra información y documentación que considere conveniente hacer del conocimiento de la Autoridad Garante.

El referido informe se comunica a la Autoridad Garante dentro del término de 72 horas posteriores a que se haya confirmado la vulneración.

Artículo 46. Conforme a lo previsto en los Lineamientos Generales, se entiende que se afectan los derechos patrimoniales de la persona titular cuando la vulneración esté

[17] **Lineamientos Generales de Protección de Datos Personales para el Sector Público**, artículo 67.

relacionada con sus bienes, información fiscal, historial crediticio, ingresos o egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados u otros similares.

Para el caso de los derechos morales, se entiende que se afectan cuando la vulneración está relacionada, de manera enunciativa más no limitativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, aspecto físico, o cuando se menoscabe ilegalmente la libertad, integridad física o psíquica de la persona titular de los datos.

Artículo 47. En aquellos casos en los cuales no sea posible notificar directamente a la persona titular el informe a que hace referencia la presente Política o ello implique esfuerzos desproporcionados, la UA instrumenta las medidas compensatorias de comunicación que al efecto procedan, como: la publicación en periódico oficial, en la página de internet de la ASF, en carteles o cápsulas informativas u otro similar.

Artículo 48. El Comité de Transparencia puede determinar la implementación de acciones adicionales a las realizadas por la UA para evitar futuras vulneraciones y reforzar las medidas de seguridad aplicables.

Para tal efecto, el Comité de Transparencia se puede auxiliar de la asesoría, orientación o apoyo de otras UA, así como sugerir la suscripción de convenios de colaboración o la contratación de especialistas en la materia.

Sin texto

CAPÍTULO V. INVENTARIO DE DATOS PERSONALES DE LA ASF

V.1. DEL INVENTARIO DE DATOS PERSONALES

Artículo 49. El Inventario constituye el listado de procesos de tratamiento de datos que lleva a cabo la ASF, con motivo del ejercicio de sus facultades y atribuciones. A través de dicho instrumento la UA identifica y categoriza los distintos tipos de datos personales que son sometidos a tratamiento derivado del ejercicio de sus funciones, a fin de establecer las medidas de seguridad adecuadas para su protección.

V.2. DE SU INTEGRACIÓN O ACTUALIZACIÓN

Artículo 50. El Inventario que realiza la ASF en su calidad de Responsable, contiene al menos la información siguiente:[18]

I. Denominación del tratamiento.

II. UA tratante de los datos.

III. Catálogo de tipo de datos tratados.

IV. Catálogo de tipo de datos sensibles tratados, en su caso.

V. Finalidades del tratamiento.

VI. Catálogo de formatos de almacenamiento.

VII. Ubicación de los formatos de almacenamiento.

VIII. Medios o instrumentos a través de los cuales se recaban los datos.

IX. Personal de la ASF que tiene acceso a los procesos de tratamiento.

X. Denominación o nombre de la persona encargada e hipervínculo al instrumento jurídico que al efecto se determine.

XI. Personas a quienes se transfieren los datos y finalidades que lo justifican, en su caso.

[18] **Ibid**., artículo 58.

V.2.1. Casos en los que se requiere su actualización

Artículo 51. El Inventario se mantiene actualizado conforme a los tratamientos de datos personales que realiza cada UA.

La revisión y actualización se lleva a cabo cuando ocurre alguno de los supuestos siguientes:

I. Se traslade el proceso de tratamiento de datos personales a una nueva UA o ésta cambie su denominación, por disposición del Reglamento Interior de la ASF.

II. Se elabore un nuevo aviso de privacidad, de conformidad con la Ley General, los Lineamientos Generales y esta Política.

III. Se actualice o modifique el Documento de Seguridad de la ASF, o bien, el documento de seguridad interno de la UA, de acuerdo con los procesos de tratamiento de datos personales que lleva a cabo en el ejercicio de sus funciones.

IV. Se realicen modificaciones a la normativa relacionada con el ámbito de funciones de la UA, que incida en los elementos que conforman el Inventario de datos personales.

Artículo 52. Para la integración o actualización del Inventario, la persona enlace responsable de la UA se asegura que la información asentada en éste sea acorde con los procesos de tratamiento que lleve a cabo la UA en el ámbito de sus funciones.

CAPÍTULO VI. AVISOS DE PRIVACIDAD

VI.1. AVISOS DE PRIVACIDAD PARA CADA PROCESO

Artículo 53. Como parte de las acciones para cumplir con el principio de información y con independencia de que no se requiera del consentimiento de la persona titular para el tratamiento de sus datos personales, en la ASF se cuenta con un Aviso de Privacidad Integral y su correlativo Aviso de Privacidad Simplificado por cada proceso en que se traten datos personales.

Excepcionalmente, cuando dos o más procesos de tratamiento de datos personales, atiendan a una misma finalidad o función, se puede contar con un mismo Aviso de Privacidad, en sus dos modalidades, siempre y cuando sea posible expresar con precisión y claridad las finalidades del tratamiento de datos personales, de tal suerte que no dé lugar a incertidumbre o ambigüedad a su titular.

Para cumplir con este principio informativo, la UA pone a disposición de la persona titular el Aviso de Privacidad, de conformidad con lo dispuesto en la Ley General, en los Lineamientos Generales, en los Criterios para la puesta a disposición del aviso de privacidad en la Auditoría Superior de la Federación (2TA3PD03), así como en la demás normativa que resulte aplicable.

VI.2. FORMATOS PARA SU ELABORACIÓN O ACTUALIZACIÓN

Artículo 54. Los formatos para la elaboración del Aviso de Privacidad Integral y Simplificado son acordes con los elementos que establece la Ley General, los Lineamientos Generales, esta Política y demás normativa que resulte aplicable.

Artículo 55. En la integración y elaboración de los avisos de privacidad, la UA prevé un formato que facilita su entendimiento por parte de la persona titular. La Unidad de Transparencia podrá elaborar las propuestas de formatos para su integración o actualización, manteniendo la homogeneidad de los elementos.

VI.3. DE SU REDACCIÓN

Artículo 56. Las UA se aseguran de que la información asentada en el Aviso de Privacidad se encuentre redactada en un lenguaje sencillo, claro y comprensible, considerando en todo momento el perfil de la persona titular al cual vaya dirigido, por lo que se abstienen de:[19]

I. Usar frases inexactas, ambiguas o vagas.

II. Incluir textos que induzcan a la persona titular a elegir una opción en específico.

III. Marcar previamente las casillas, en caso de que éstas se incluyan, para que la persona titular otorgue su consentimiento, o bien, incluir declaraciones orientadas a afirmar que ésta ha consentido el tratamiento de sus datos personales sin manifestación alguna de su parte.

[19] **Ibid**., artículo 28.

IV. Remitir a textos o documentos que no estén disponibles para la persona titular.

Artículo 57. Para la elaboración o actualización del Aviso de Privacidad, la persona enlace responsable puede, en todo momento, solicitar orientación técnica a la Unidad de Transparencia.

VI.4. NUEVO AVISO DE PRIVACIDAD

Artículo 58. Las UA consideran la elaboración de un nuevo Aviso de Privacidad, en sus dos modalidades, cuando ocurre alguno de los supuestos siguientes: [20]

I. Por disposición del Reglamento Interior de la ASF, el proceso de tratamiento de datos personales se traslade a una nueva área o ésta cambie su denominación.

II. Se requiere recabar datos sensibles distintos de aquellos informados en el Aviso de Privacidad original, los cuales no se obtengan de manera directa de la persona titular y se requiera de su consentimiento para el tratamiento de éstos.

III. Se cambien las finalidades señaladas en el Aviso de Privacidad original.

IV. Se modifiquen las condiciones de las transferencias de datos personales o se pretendan realizar otras no previstas inicialmente y el consentimiento de la persona titular sea necesario.

[20] La elaboración de un nuevo Aviso de Privacidad se entiende como el resultado de los cambios o actualizaciones que se realicen al mismo, conforme a lo establecido en los **Lineamientos Generales de Protección de Datos Personales para el Sector Público,** artículo 42.

CAPÍTULO VII. PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES

VII.1. OBJETO Y ALCANCES

Artículo 59. La ASF cuenta con un Programa de Protección de Datos Personales, aprobado por el Comité de Transparencia, cuyo objetivo es determinar las pautas 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.

VII.2. VIGENCIA Y ACTUALIZACIÓN

Artículo 60. El Programa de Protección de Datos Personales tiene una vigencia trianual, a fin de garantizar el desarrollo ininterrumpido de actividades, sin demérito de que puede ser sometido a su revisión o actualización por parte del Comité de Transparencia, de conformidad con las facultades y atribuciones que le establece la normativa aplicable, en caso de estimarse necesario.

Artículo 61. La Unidad de Transparencia elabora la propuesta de ajustes o actualizaciones al Programa de Protección de Datos Personales, la cual es presentada al Comité de Transparencia para su revisión y, en su caso, aprobación**.**

VII.3. CONTENIDO MÍNIMO

Artículo 62. El Programa de Protección de Datos Personales contiene al menos:

I. La vigencia del Programa.

II. El análisis de las necesidades o áreas de oportunidad detectadas para el cumplimiento de los principios y deberes en materia de protección de datos personales dentro de la ASF.

III. Las actividades propuestas para dar cumplimiento a las obligaciones en la materia, su viabilidad, así como los objetivos que se persiguen, los cuales están vinculados a la atención de las necesidades o áreas de oportunidad previamente identificadas.

IV. Los medios de verificación del cumplimiento de las actividades propuestas y las UA responsables de su atención.

VII.4. SUPERVISIÓN

Artículo 63. Corresponde a la Unidad de Transparencia coordinar el seguimiento a la ejecución de las actividades previstas en el Programa de Protección de Datos Personales e informar al Comité de Transparencia acerca de su cumplimiento, como instancia encargada de su supervisión.

Sin texto

CAPÍTULO VIII. PROGRAMA DE CAPACITACIÓN Y ACTUALIZACIÓN

Artículo 64. La ASF cuenta con un PCAMPDP, como uno de los mecanismos para dar cumplimiento al principio de responsabilidad, conforme a la legislación vigente y para coadyuvar al cumplimiento del marco normativo que garantiza el derecho a la protección de datos personales. Para su configuración, se definen niveles de capacitación en función de los roles y responsabilidades del personal que trata la información personal.

La planificación y gestión de las actividades de capacitación en materia de protección de datos personales se hace de manera conjunta con la correspondiente a transparencia y acceso a la información, dada la interrelación existente entre ambas temáticas. De tal forma, las acciones de capacitación del PCAMPDP están contenidas en el Programa de Capacitación en Transparencia, Acceso a la Información y Protección de Datos Personales.

VIII.1. ELABORACIÓN Y APROBACIÓN DEL PROGRAMA

Artículo 65. La Dirección General de Transparencia elabora anualmente la propuesta del PCAMPDP, en la cual se consideran las necesidades de capacitación de las UA y, en su caso, la oferta de formación de la Autoridad Garante. Dicha propuesta se somete a consideración del Comité de Transparencia para su aprobación.

VIII.2. OPERACIÓN DEL PROGRAMA

Artículo 66. La Dirección General de Transparencia es la encargada de dar seguimiento a la gestión e implementación del PCAMPDP.

Para ello, en atención a los procedimientos institucionales establecidos, el Instituto de Capacitación y Desarrollo en Fiscalización Superior (ICADEFIS) realiza las acciones necesarias para el registro y documentación de las actividades de capacitación y brinda el apoyo logístico necesario para su implementación.

DOCUMENTOS PARA LA PROTECCIÓN DE DATOS PERSONALES EN LA ASF PREVISTOS EN LOS CAPÍTULOS IV AL VIII

Documento de Seguridad de la ASF

Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por la ASF en su calidad de Responsable, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que trate.

Inventario de Tratamiento de Datos Personales de la ASF

Instrumento que identifica los tipos de datos personales, así como los procesos de tratamiento de éstos que lleva a cabo la ASF, en su calidad de Responsable, con motivo del ejercicio de sus facultades y sus atribuciones, a fin de establecer las medidas de seguridad que resultan adecuadas para su protección.

Avisos de Privacidad

Documento que se pone a disposición de la persona titular de forma física, electrónica o en cualquier formato generado por la ASF en su calidad de Responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle las finalidades del tratamiento de los mismos.

Programa de Protección de Datos Personales

Documento de planeación de la ASF, en el que se determinan las pautas generales bajo las cuales se llevan a cabo las tareas institucionales orientadas al cumplimiento de los Principios y Deberes en materia de protección de datos, a fin de garantizar el efectivo derecho a la autodeterminación informativa de las personas.[21]

Programa de Capacitación y Actualización en Materia de Protección de Datos Personales

Documento aprobado por el Comité de Transparencia, en el cual se definen niveles de capacitación en función de los roles y responsabilidades de las personas servidoras públicas que tratan la información personal al interior de la ASF, el cual forma parte del Programa de Capacitación en Transparencia, Acceso a la Información y Protección de Datos Personales.

FUENTE: Esquema de elaboración propia con base en lo señalado en esta Política, págs. 33 a 45.

[21] Es el "derecho fundamental que habilita a la persona para decidir, por sí sola, sobre la difusión y utilización de sus datos personales con un fin determinado y con independencia del tipo de soporte (físico o electrónico), en el que se encuentren los datos personales", en Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, **Diccionario de Protección de Datos Personales. Conceptos fundamentales**; Coordinado por Isabel Davara F. de Marcos, Ciudad de México, 2019; página 82, disponible en: https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf

CAPÍTULO IX. EJERCICIO DE LOS DERECHOS ARCO

IX.1. CONCEPTOS

Artículo 67. Para efectos del ejercicio de los Derechos ARCO, se consideran:

I. **Acceso**: Derecho de la persona titular para acceder a sus datos personales en posesión de la ASF, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento.

Cuando el tratamiento de los datos personales se realice por vía electrónica en un formato estructurado y comúnmente utilizado, la persona titular tendrá derecho a su portabilidad, de conformidad con lo establecido en la Ley General y demás normativa aplicable.[22]

II. **Rectificación**: Derecho de la persona titular para solicitar a la ASF la corrección de sus datos personales, cuando estos resulten inexactos, incompletos o no se encuentren actualizados.

III. **Cancelación**: Derecho de la persona titular para solicitar a la ASF que sus datos personales sean bloqueados y, posteriormente, suprimidos de los archivos, registros, expedientes y sistemas institucionales, a fin de que los mismos no se encuentren más en su posesión y, por lo tanto, dejen de ser tratados.

IV. **Oposición**: Derecho de la persona titular para solicitar a la ASF que se abstenga de utilizar información personal para ciertos fines o de requerir que se concluya su uso, a fin de evitar un daño o afectación a su persona.

[22] Para el ejercicio del derecho de portabilidad de datos personales, se atenderá a lo establecido en la **Ley General Protección de Datos Personales en Posesión de Sujetos Obligados**, artículo 51, primer párrafo, así como en los **Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales,** disponible para su consulta en: https://www.dof.gob.mx/nota_detalle.php?codigo=5512847&fecha=12/02/2018#gsc.tab=0, instrumento normativo que continúa vigente, de conformidad con lo dispuesto en el artículo Cuarto Transitorio del Decreto por el que se expiden la Ley General de Transparencia y Acceso a la Información Pública; la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; y se reforma el artículo 37, fracción XV, de la Ley Orgánica de la Administración Pública Federal, publicado en el Diario Oficial de la Federación el 20 de marzo de 2025.

IX.2. RECEPCIÓN DE SOLICITUDES PARA EL EJERCICIO DE LOS DERECHOS ARCO

Artículo 68. La presentación de solicitudes para el ejercicio de los Derechos ARCO puede realizarse a través de los medios de recepción siguientes:

I. **Unidad de Transparencia de la ASF:** ubicada en Carretera Picacho Ajusco número 167, Planta Baja, Colonia Ampliación Fuentes del Pedregal. Código Postal 14110, Demarcación Territorial Tlalpan, Ciudad de México.

II. **Correo electrónico**: unidadtransparencia@asf.gob.mx

III. **Plataforma Nacional de Transparencia:** http://www.plataformadetransparencia.org.mx/

Artículo 69. La Unidad de Transparencia es responsable de turnar las solicitudes del ejercicio de los Derechos ARCO que sean presentadas ante la ASF a la UA que, conforme a sus atribuciones, competencias o funciones, puede o debe tratar los datos personales, a fin de atenderla en los plazos y términos establecidos en la Ley General, los Lineamientos Generales y demás disposiciones aplicables en la materia.

Artículo 70. La UA lleva a cabo las acciones pertinentes para garantizar el efectivo ejercicio de los Derechos ARCO de la persona titular, acorde con los principios, deberes y obligaciones en materia de protección de datos personales.

Artículo 71. La UA podrá solicitar la asesoría técnica de la Unidad de Transparencia para atender la solicitud. En caso de que se interponga un recurso de revisión con motivo de la respuesta otorgada, la UA formula los alegatos correspondientes, en términos de la Ley General y demás disposiciones aplicables.

IX.3. ACATAMIENTO DE LA RESOLUCIÓN EMITIDA POR LA AUTORIDAD GARANTE

Artículo 72. La resolución que emita la Autoridad Garante es vinculante para la ASF y, una vez recibida, la Unidad de Transparencia lleva a cabo las gestiones que resulten necesarias ante la UA competente para dar cumplimiento a lo instruido.

ATENCIÓN DE SOLICITUDES PARA EL EJERCICIO DE LOS DERECHOS ARCO

La ASF, por medio de la Unidad de Transparencia, orienta a las personas sobre el ejercicio de sus derechos de protección de datos personales.

Si la ASF es la responsable de llevar a cabo el tratamiento de los datos personales, la persona titular puede ejercer sus Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), por cualquiera de las vías previstas para ello.

1

Unidad de Transparencia

UT
Unidad de Transparencia

Planta baja de la ASF, sede Ajusco

2

Correo electrónico

unidadtransparencia@asf.gob.mx

3

Plataforma Nacional de Transparencia

PLATAFORMA NACIONAL DE TRANSPARENCIA

http://www.plataformadetransparencia.org.mx/

Si la ASF determina la no procedencia del derecho solicitado, la persona titular no se encuentra satisfecha o no recibe respuesta a su solicitud, puede interponer un recurso de revisión ante la Autoridad Garante, para lo cual cuenta con 15 días hábiles después de recibida la contestación o ante la falta de atención a su requerimiento.

FUENTE: Esquema de elaboración propia con base en lo señalado en esta Política, págs. 47 y 48.

Sin texto

CAPÍTULO X. DE LAS REMISIONES Y TRANSFERENCIAS DE LOS DATOS PERSONALES EN POSESIÓN DE LA ASF

X.1. REMISIONES DE DATOS PERSONALES

Artículo 73. La remisión es toda aquella comunicación de datos personales realizada exclusivamente entre la ASF, en su calidad de Responsable y la persona encargada, dentro o fuera del territorio mexicano.

X.1.1 Relación entre la ASF y la persona encargada

Artículo 74. La ASF puede encargar el tratamiento de datos personales a personas físicas o morales ajenas a la institución, únicamente cuando sea consecuencia de la existencia de una relación formalizada mediante un instrumento jurídico suscrito por la persona servidora pública facultada para ello.

X.1.2. Obligación general de la persona encargada

Artículo 75. La persona encargada trata los datos personales a nombre y por cuenta de la ASF dentro del marco de actuación de la prestación del servicio que se formalice, conforme al ámbito de las atribuciones y funciones de la UA responsable del tratamiento y no ostenta poder alguno de decisión sobre el alcance y contenido del mismo, limitando en ese sentido, su encargo a los términos fijados en el instrumento jurídico respectivo.

X.1.3. Instrumento jurídico acorde con las finalidades informadas en el aviso de privacidad

Artículo 76. Cualquier acuerdo alcanzado y debidamente formalizado entre la ASF y la persona encargada se efectúa con base en lo previsto por la Ley General, los Lineamientos Generales, la presente Política, los Criterios para la formulación de cláusulas en contratos que tengan por objeto el tratamiento de datos personales (2TA3PD02) y el Aviso de Privacidad puesto a disposición de la persona titular en el cual quedaron definidas previamente las condiciones de su tratamiento.

X.1.4. Obligaciones específicas de la persona encargada contenidas en el instrumento jurídico

Artículo 77. El instrumento jurídico por el cual se formalice la relación jurídica entre la ASF y la persona encargada incluye para ésta última, al menos las obligaciones siguientes:[23]

I. Realizar el tratamiento de los datos personales conforme a las instrucciones de la ASF.

II. Impedir el tratamiento de los datos personales para finalidades distintas de las instruidas por la ASF.

III. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables.

[23] Las obligaciones previstas en esta disposición son acordes con lo establecido en la **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**, artículo 53 y, en los **Lineamientos Generales de Protección de Datos Personales para el Sector Público**, artículo 109.

IV. Informar a la ASF cuando ocurra una vulneración a los datos personales que trata por sus instrucciones.

V. Guardar confidencialidad respecto de los datos personales tratados.

VI. Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con la ASF, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.

VII. Evitar transferir los datos personales, salvo en el caso de que la ASF así lo determine, la comunicación derive de una subcontratación o por mandato expreso de la autoridad competente.

VIII. Permitir a la Autoridad Garante realizar verificaciones en el lugar o establecimiento donde se lleva a cabo el tratamiento de los datos personales.

IX. Colaborar con la Autoridad Garante en las investigaciones previas y verificaciones que lleve a cabo en términos de lo dispuesto en la Ley General y los Lineamientos Generales, proporcionando la información y documentación que se estime necesaria para tal efecto.

X. Colaborar con la UA para la atención de los Derechos ARCO, cuando éstos estén con el tratamiento de datos personales bajo su encargo.

XI. Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de las obligaciones señaladas en este artículo.

X.1.5. Subcontratación de servicios que impliquen el tratamiento de datos personales

Artículo 78. La subcontratación de servicios que impliquen el tratamiento de los datos personales previamente remitidos por la ASF sólo puede llevarse a cabo cuando en el instrumento jurídico suscrito por la ASF y la persona encargada se contemple dicha situación, debiendo formalizarse, a su vez, la relación jurídica con la persona subcontratada por medio de cualquier instrumento jurídico que permita acreditar su existencia, alcance y contenido, en términos de las disposiciones legales aplicables.

El instrumento jurídico de subcontratación, además de prever las cláusulas señaladas en el artículo anterior, también debe mencionar que la persona física o moral subcontratada asume las mismas obligaciones establecidas para la persona encargada.

X.1.6. Personas proveedoras de servicios de cómputo en la nube y otras materias

Artículo 79. En caso de que la ASF realice la contratación de servicios o se adhiera a servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias que impliquen el tratamiento de datos personales a través de internet, la UA verifica que la persona proveedora garantice las condiciones de seguridad de los datos y cuente con los mecanismos para ello, conforme a lo establecido en la Ley General.

Para dichos efectos, la UA contratante solicita el dictamen técnico a la Dirección General de Sistemas, de conformidad con sus atribuciones y la normativa interna en materia de tecnologías de la información, comunicación y seguridad informática en la ASF y suscribe el contrato o instrumento jurídico en el que se prevean las cláusulas generales que se refieren en este capítulo para garantizar la seguridad de los datos personales.

X.2. TRANSFERENCIAS DE DATOS PERSONALES

Artículo 80. La transferencia es toda comunicación de datos personales realizada a cualquier persona distinta de la titular, de la propia ASF en su calidad de Responsable y de la persona encargada.

Artículo 81. La ASF puede llevar a cabo transferencias nacionales o internacionales de los datos personales en su posesión, en los términos y bajo las condiciones que determina la Ley General.

X.2.1. Condiciones generales de las transferencias

Artículo 82. Toda transferencia de datos personales que lleve a cabo la ASF se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en la Ley General.[24]

Para tal efecto, la UA informa a la persona titular por medio del aviso de privacidad correspondiente las finalidades de la transferencia, así como su receptor.

Cuando la transferencia requiera del consentimiento expreso de la persona titular, se habilita los medios a través de los cuales ésta manifieste su voluntad.

La actualización de alguna de las excepciones previstas en la Ley General no exime a las UA de cumplir con las obligaciones previstas en la presente Política y demás disposiciones jurídicas aplicables.

[24] **Ley General Protección de Datos Personales en Posesión de Sujetos Obligados**, artículos 60, segundo párrafo, y 64.

X.2.2. Comunicación de avisos de privacidad a personas receptoras de datos personales

Artículo 83. En toda transferencia de datos personales la UA responsable comunica el aviso de privacidad respectivo a la persona receptora de las transferencias, así como documenta detalladamente dicha comunicación.

X.2.3. Formalización de la transferencia

Artículo 84. De acuerdo con lo previsto en la Ley General, toda transferencia de datos personales que realice la UA se formaliza mediante la suscripción de un instrumento jurídico que demuestre el alcance de su tratamiento, así como las obligaciones y responsabilidades contraídas por las partes.

La formalización referida no resulta aplicable en los casos siguientes:

I. Cuando la transferencia sea nacional y se realice en virtud del cumplimiento de una disposición legal o del ejercicio de las atribuciones expresamente conferidas.

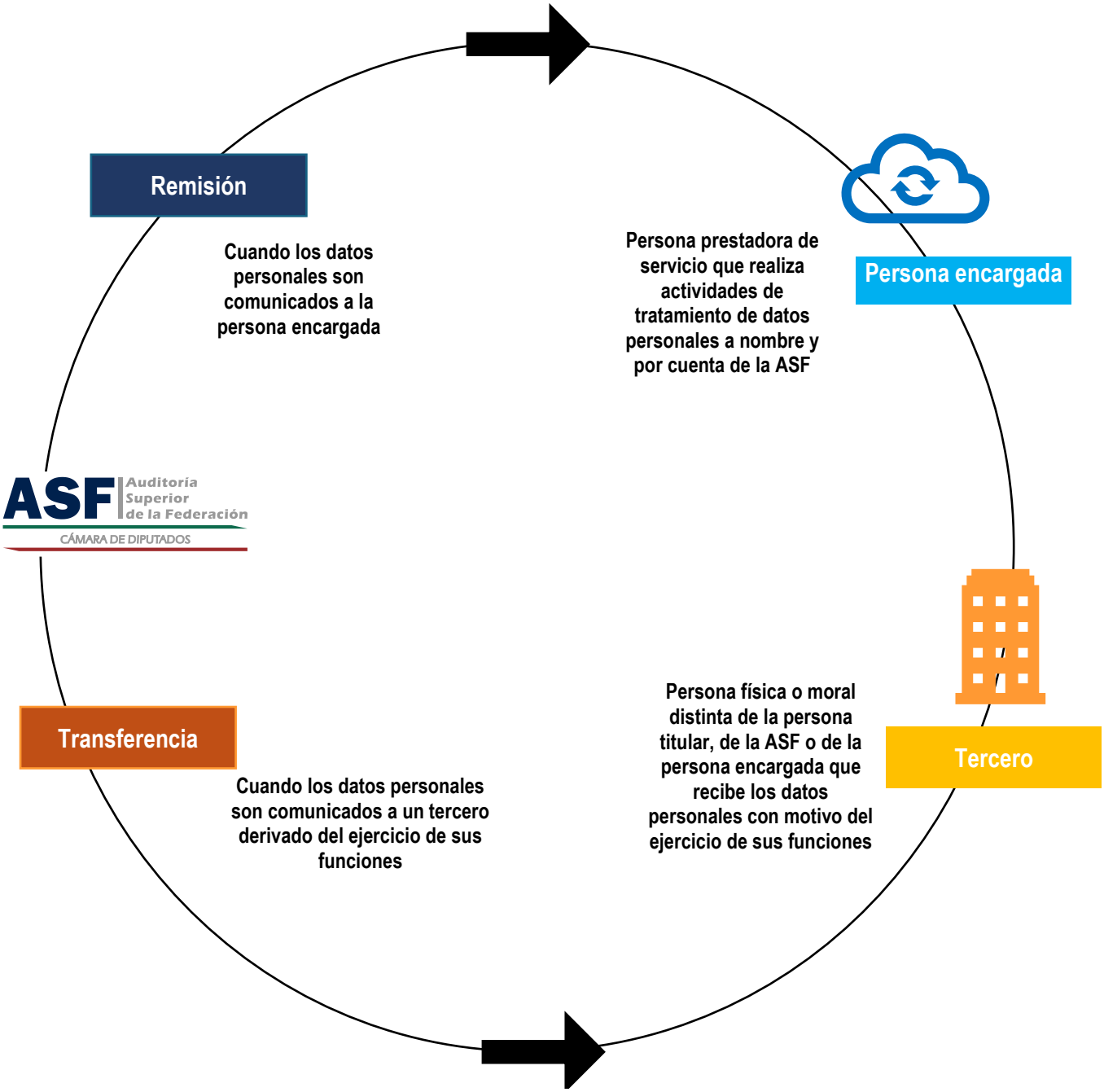
II. Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre la ASF y quien recibe sean homólogas o las finalidades que motivan la transferencia sean equivalentes o compatibles respecto de aquéllas que dieron origen al tratamiento por parte de la ASF.

X.2.4. Transferencias internacionales

Artículo 85. Cuando la comunicación de datos personales se realice fuera del territorio nacional, previo a su transferencia, la ASF se asegura que quien sea receptor se obligue a proteger los datos personales conforme a los principios, deberes y obligaciones similares o equiparables a las previstas en la Ley General y demás normativa mexicana aplicable en la materia, así como a los términos previstos en el Aviso de Privacidad que le es comunicado por la ASF.

La ASF puede solicitar a la Autoridad Garante la opinión respecto de las transferencias internacionales que se le susciten, en términos de lo dispuesto en los Lineamientos Generales.

TRANSFERENCIAS Y REMISIONES DE DATOS PERSONALES



FUENTE: Esquema de elaboración propia con base en lo señalado en esta Política, págs. 51 a 54.

Sin texto

CAPÍTULO XI. DEL INCUMPLIMIENTO A LOS PRINCIPIOS Y DEBERES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Artículo 86. Las UA son responsables de dar cumplimiento a los principios y deberes en materia de protección de datos personales, conforme a lo dispuesto en esta Política y demás disposiciones aplicables.

Artículo 87. En caso de actualizarse alguna conducta que sea considerada como un incumplimiento a las obligaciones previstas en esta Política, se estará a lo dispuesto en el Título Décimo Primero de la Ley General.

Sin texto

GLOSARIO

SIGLAS Y ACRÓNIMOS	DENOMINACIONES
ASF	Auditoría Superior de la Federación
PCAMPDP	Programa de Capacitación y Actualización en Materia de Protección de Datos Personales
UA	Unidad Administrativa /Unidades Administrativas

TÉRMINOS	DEFINICIONES
ACTIVO	Es cualquier componente, recurso o mecanismo de valor que sea importante para el tratamiento de los datos personales que realice la ASF en su calidad de Responsable, a través de sus UA.
AUTORIDAD GARANTE	El órgano interno de control o equivalente al que se refiere el artículo 3, fracción II, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
AVISO DE PRIVACIDAD	Es el documento que se pone a disposición de la persona titular de forma física, electrónica o en cualquier formato generado por la UA, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle las finalidades del tratamiento de los mismos. Sus dos modalidades son: **Simplificado**: Es la modalidad del instrumento en el cual se señalan los elementos mínimos que debe conocer la persona titular de los datos personales en torno al tratamiento que se dará a éstos. **Integral**: Es la modalidad del instrumento que complementa la información proporcionada a la persona titular en torno al tratamiento de sus datos personales y la forma en la que puede ejercer sus Derechos ARCO o, en su caso, de portabilidad.
BITÁCORA DE VULNERACIONES	Es un registro que lleva la UA de las vulneraciones a la seguridad de los datos personales que tratan.
COMITÉ DE TRANSPARENCIA	Es la autoridad máxima en materia de protección de datos personales al interior de la ASF.
DERECHOS ARCO	Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.
DOCUMENTO DE SEGURIDAD INTERNO	Es el documento integrado por cada UA en el que establece las medidas de seguridad de datos personales (4TA3PD01-02), de acuerdo con los procesos del tratamiento que realiza en el ámbito de sus funciones.
DOCUMENTO DE SEGURIDAD DE LA ASF	Es el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por la ASF para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que trate.
INVENTARIO DE DATOS PERSONALES	Es el instrumento que identifica los tipos de datos personales, así como los procesos de tratamiento de éstos que lleva a cabo la ASF, en su calidad de Responsable, con motivo del ejercicio de sus facultades y sus atribuciones.
LEY GENERAL	La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

TÉRMINOS	DEFINICIONES
LINEAMIENTOS GENERALES	Los Lineamientos Generales de Protección de Datos Personales para el Sector Público.
MEDIDAS COMPENSATORIAS	Son los mecanismos alternos para dar a conocer a las personas titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance.
MEDIDAS DE SEGURIDAD	Son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.[25] Se entienden por: **Administrativas**: aquellas relacionadas a las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel institucional; la identificación, clasificación y borrado seguro de la información, y la sensibilización y capacitación de personal en la materia. **Técnicas**: el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con el hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. **Físicas**: el conjunto de acciones y mecanismos implementados para proteger el entorno físico de los datos personales y los recursos involucrados en su tratamiento.
PERSONA ENCARGADA	Es la persona física o jurídica, pública o privada, ajena a la ASF, que sola o juntamente con otras trate datos personales a nombre y por cuenta de la ASF en su calidad de Responsable.
PERSONA ENLACE RESPONSABLE	Es la persona servidora pública de mando superior con nivel mínimo de dirección general u homólogo designada por la persona titular de Auditoría Especial o Unidad para gestionar los asuntos en materia de datos personales al interior de la misma, así como ante la Unidad de Transparencia y el Comité de Transparencia.
PERSONA TITULAR	Es la persona física a quien corresponden los datos personales.
PERSONAL DE LA ASF	Son las personas servidoras públicas de base y de confianza, y prestadoras de servicios profesionales por honorarios, capítulo 1000.
POLÍTICA	La Política de Protección de Datos Personales de la ASF.
PROGRAMA DE CAPACITACIÓN Y ACTUALIZACIÓN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES	Es el documento aprobado por el Comité de Transparencia, en el cual se prevén actividades de capacitación para todo el personal que forma parte de la estructura de la ASF, atendiendo los roles y responsabilidades que tienen al interior de la institución.
PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES	Es el documento de planeación de la ASF, en el que se determinan las pautas generales bajo las cuales se llevan a cabo las tareas institucionales orientadas al cumplimiento de los Principios y Deberes en materia de protección de datos, a fin de garantizar el efectivo derecho a la autodeterminación informativa de las personas.
REMISIÓN	Se refiere a toda comunicación de datos personales realizada exclusivamente entre la ASF en su calidad de Responsable y la persona encargada, dentro o fuera del territorio mexicano.

[25] Para su definición se toma como referencia lo establecido en la **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**, artículo 3, fracciones XIX, XX y XXI.

TÉRMINOS	DEFINICIONES
RESPONSABLE	La ASF en su calidad de sujeto obligado que decide sobre el tratamiento de datos personales**.**
SISTEMA DE GESTIÓN	Es el conjunto de elementos y actividades para establecer, implementar y monitorear el tratamiento y seguridad de los datos personales.
TRANSFERENCIA	Es toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta de la persona titular, de la ASF en su calidad de Responsable o de la persona encargada.
TRATAMIENTO	Es 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.[26]
UNIDAD ADMINISTRATIVA/ UNIDADES ADMINISTRATIVAS	Son las áreas que se señalan en el artículo 3o del Reglamento Interior de la ASF que lleven a cabo el tratamiento de datos personales.
UNIDAD DE TRANSPARENCIA	Es la instancia a la que hacen referencia los artículos 41 de la Ley General de Transparencia y Acceso a la Información Pública y 3, fracción XXXII de la Ley General. Su titularidad recae en la Unidad de Enlace Legislativo, Planeación y Transparencia, en términos de lo previsto en el artículo 20, fracción X del Reglamento Interior de la ASF.

[26] **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**, artículo 3, fracción XXXI.

Sin texto

AUTORIZACIONES

Conforme a lo dispuesto en los artículos 20, fracciones X del Reglamento Interior de la Auditoría Superior de la Federación, se emite la versión **02** de la **Política de Protección de Datos Personales de la Auditoría Superior de la Federación (2TA3PD04)**, el 18 de diciembre de 2025.

Esta Política fue aprobada por **unanimidad de votos** de las personas integrantes del Comité de Transparencia de la Auditoría Superior de la Federación, como autoridad máxima en materia de protección de datos, en su Cuadragésima sesión extraordinaria 2025, celebrada el 18 de diciembre de 2025, mediante Acuerdo 40SE/CT/ASF/18122025.02.

El presente documento entra en vigor el día siguiente de su publicación en el Sistema de Control de Documentos de la ASF (SCD) y deja sin efectos la **Política de Protección de Datos Personales de la Auditoría Superior de la Federación (2TA3PD04)**, versión **01**, aprobada el **13** de **julio** de **2023**.

Autorizó

Dr. Jaime Bolaños Cacho Guzmán
Titular de la Unidad de Enlace Legislativo,
Planeación y Transparencia

Elaboró

Mtro. Ricardo Chincoya Zambrano
Director de Transparencia, Acceso
a la Información y Protección de Datos

Revisó

Lcda. Areli Cano Guadiana
Directora General de Transparencia