POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES DEL INSTITUTO MEXICANO DE LA PROPIEDAD INDUSTRIAL

Periférico Sur 3106, Jardines del Pedregal, Álvaro Obregón, 01900
Ciudad de México, Teléfono: 55 5624 0400 www.gob.mx/impi

PRESENTACIÓN.

La presente Política de Protección de Datos Personales del Instituto Mexicano de la Propiedad Industrial (IMPI), se elaboró en apego a lo previsto por el artículo 30, fracción II de la *Ley General de Protección de Datos Personales en posesión de Sujetos Obligados*, en el cual 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 de Protección de Datos Personales para el Sector Público*, que establece se deben 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.

En la redacción de esta Política se tomaron como referentes los criterios establecidos por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), a través de los materiales de apoyo dirigidos a los sujetos obligados del sector público, como son: la *Ley General de Protección de Datos Personales en posesión de Sujetos Obligados* (Ley General) los *Lineamientos Generales de Protección de Datos Personales para el Sector Público* (Lineamientos Generales), la *Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* (Guía) y el *Documento Orientador para la elaboración del Programa de Protección de Dato Personales*.

Con la instrumentación de este mecanismo se posibilita a las unidades administrativas que integran esta Entidad a realizar un tratamiento de datos personales, en estricto apego a los principios, deberes y obligaciones establecidos en la Ley General y demás disposiciones legales aplicables, lo cual permite garantizar su adecuada protección y el ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición por parte de sus titulares.

Asimismo, en esta Política se prevén actividades y mecanismos que facilitan a cada unidad administrativa acreditar el cumplimiento de los principios y deberes en materia de protección de datos. Incluso se consideró el establecer la obligación para las unidades administrativas de designar a una persona de nivel de mando y de nivel técnico operativo (apoyo) para fungir al interior de esta, así como ante la Unidad de Transparencia y el Comité de Transparencia, como **enlace responsable,** de las actividades en la protección de 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 el IMPI realice algún tratamiento de los mismos.

Alcance

La presente Política es de observancia general y obligatoria para todo el personal del IMPI que se involucre en el tratamiento de datos personales.

La aplicación de esta Política les corresponde a todas las unidades administrativas que tratan datos personales, en el ámbito de sus competencias y facultades, de conformidad con la Ley General, los Lineamientos Generales y demás disposiciones aplicables en materia de protección de datos personales.

Corresponde al Comité de Transparencia resolver cualquier controversia sobre la interpretación de sus alcances, así como el llevar a cabo y aprobar las modificaciones que se estimen pertinentes en cualquier momento, en aras de mejorar la operación, y se harán de conocimientos para los efectos conducentes.

Ordenamientos

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

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Documento Orientador del Programa de Protección de Datos.

CAPÍTULO I. DE LA IMPLEMENTACIÓN Y ACREDITACIÓN DE LA POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES DEL IMPI

I.1. DESIGNACIÓN DEL ENLACE RESPONSABLE

Artículo 1. Cada unidad administrativa designará a una persona servidora pública de nivel mando y técnico operativo (apoyo), para fungir al interior de ésta, así como ante la Unidad de Transparencia y el Comité de Transparencia, como enlace responsable de las actividades de protección de datos personales, con el fin de garantizar y evidenciar la operación y cumplimiento de esta Política ante el/la titular de los datos y el Instituto Mexicano de la Propiedad Industrial (IMPI).

Artículo 2. Las personas designadas como enlaces responsables cuentan con las funciones siguientes:

I. Implementar y acreditar en su unidad administrativa, el cumplimiento de los principios y deberes de acuerdo con las directrices señaladas por esta Política y el Comité de Transparencia, en su calidad de autoridad máxima en materia de datos personales al interior del IMPI.

II. Promover la capacitación del personal adscrito a su unidad administrativa y que se encuentre involucrado directamente en cualquier tratamiento de datos personales.

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

V. Gestionar al interior de su Unidad Administrativa, la debida atención de solicitudes relativas al ejercicio de los derechos ARCO que sean presentadas ante la Unidad de Transparencia.

VI. Las demás disposiciones normativas que determine el INAI o aquéllas que deriven de las resoluciones emitidas por el Comité de Transparencia.

CAPÍTULO II. DE LOS PRINCIPIOS

II.1. PRINCIPIOS GENERALES DE PROTECCIÓN DE DATOS PERSONALES EN EL IMPI

Artículo 3. Las unidades administrativas del IMPI responsables del tratamiento de datos personales deben observar los principios rectores, siguientes:

I. Licitud;

II. Finalidad;

III. Lealtad;

IV. Consentimiento;

V. Información;

VI Proporcionalidad;

VII. Calidad, y

VIII. Responsabilidad.

II.2. PRINCIPIO DE LICITUD

Artículo 4. El tratamiento de datos personales por parte de las unidades administrativas se sujeta a las atribuciones o facultades que les son conferidas en la normatividad que rige el actuar del IMPI y, en estricto apego a lo dispuesto en la Ley General, los Lineamientos Generales, la presente Política y demás disposiciones legales aplicables en materia de protección de datos personales.

II.2.1. Actividades vinculadas al principio de licitud

Artículo 5. Las unidades administrativas deben identificar 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 sus finalidades.

II.2.2. Mecanismos para acreditar el cumplimiento del principio de licitud

Artículo 6. Para el cumplimiento del principio de licitud, las unidades administrativas incluyen en el Aviso de Privacidad Integral y, en su caso, en el inventario, el fundamento legal que les faculta a tratar datos personales.

II.3. PRINCIPIO DE FINALIDAD

Artículo 7. Todo tratamiento de datos personales efectuado por las unidades administrativas debe estar justificado por finalidades concretas, lícitas, explícitas y legítimas. Se entiende que las finalidades son:

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 el/la 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 del responsable, conforme a lo previsto en la legislación mexicana y 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 del/de la titular, salvo que se actualice alguna de las causales de excepción a que se refiere la Ley General y la presente Política.

Periférico Sur 3106, Jardines del Pedregal, Álvaro Obregón, 01900
Ciudad de México, Teléfono: 55 5624 0400 www.gob.mx/impi

II.3.1. Actividades vinculadas al principio de finalidad

Artículo 8. Como consecuencia del principio de finalidad, las unidades administrativas que traten datos personales deben:

I. Establecer detalladamente en el aviso de privacidad todas las finalidades para las cuales se tratan los datos personales, las cuales deben ser acordes a las atribuciones o facultades que tienen 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 las personas titulares de los mismos, para el tratamiento de sus datos personales cuando así se requiera, salvo las excepciones establecidas en la Ley General y la presente Política.

IV. Informar a los/las titulares sobre el tratamiento de sus datos personales, para finalidades distintas a las previstas en el aviso de privacidad, siempre y cuando, se tengan facultades o atribuciones para ello y se recabe el consentimiento de éstos, con excepción de lo establecido en la Ley General.

V. Además, debe considerarse lo siguiente:

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

b) La naturaleza de los datos personales.

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

II.3.2. Mecanismos para acreditar el cumplimiento del principio de finalidad

Artículo 9. Para acreditar el cumplimiento del principio de finalidad, las unidades administrativas deben:

I. Verificar que las finalidades de cada tratamiento que realicen éstas, sean específicas o determinadas y acordes a las atribuciones o facultades del IMPI y de su área.

II. Vigilar que las personas servidoras públicas únicamente traten datos personales en términos de las finalidades informadas en el aviso de privacidad correspondiente.

III. Verificar que en los avisos de privacidad se informen todas las finalidades para las cuales se tratan los datos personales y que éstas sean descritas de manera clara, evitando textos que generen confusión.

IV. Informar a los/las titulares sobre el tratamiento de los datos para finalidades distintas.

V. Recabar el consentimiento de las personas titulares de los datos personales, cuando este proceda.

II.4. PRINCIPIO DE LEALTAD

Artículo 10. Las unidades administrativas se abstendrán 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.

II.4.1. Actividades vinculadas al principio de lealtad

Artículo 11. Derivado del principio de lealtad, las unidades administrativas responsables del tratamiento de datos personales deben:

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

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

III. Respetar la expectativa razonable de privacidad.

II.4.2. Mecanismos para acreditar el cumplimiento del principio de lealtad

Artículo 12. Para acreditar el cumplimiento del principio de lealtad, las unidades administrativas deben:

I. Contar con avisos de privacidad que cumplan con lo establecido en la Ley General y la presente Política.

II. Implementar instrumentos que permitan verificar que los tratamientos realizados no den lugar a discriminación, trato injusto o arbitrario en contra de la persona titular de los datos personales.

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 13. Previo al tratamiento de los datos personales, las unidades administrativas deben obtener el consentimiento (tácito, expreso, escrito o verbal, según proceda) de la persona la titular de manera libre, específica e informada, en términos de lo dispuesto en la Ley General, salvo que se actualice alguna de las causales de excepción siguientes:

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 que, en ningún caso, puede contravenirla.

II. Cuando las transferencias que se realicen entre el IMPI 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. Para el reconocimiento o defensa de derechos del/de la titular ante 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 de los datos y el IMPI.

VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona 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 el/la titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

La actualización de alguno de los supuestos no exime a la unidad administrativa y a las personas servidoras públicas responsables del tratamiento de datos personales del cumplimiento de las demás obligaciones establecidas en la Ley General, los Lineamientos Generales y la presente Política.

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.

II.5.1. Actividades vinculadas al principio de consentimiento

Artículo 14. En términos de los alcances del principio de consentimiento, las unidades deben:

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

Periférico Sur 3106, Jardines del Pedregal, Álvaro Obregón, 01900
Ciudad de México, Teléfono: 55 5624 0400 www.gob.mx/impi

II. Recabar el consentimiento expreso y, en su caso, por escrito, a través de formatos claros y sencillos, cuando así proceda, debiendo ser acorde con el perfil de la persona titular de los datos personales, en los cuales 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 este se requiera, cuando así proceda.

IV. En su caso, habilitar 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 personales.

II.5.2. Mecanismos para acreditar el cumplimiento del principio de consentimiento

Artículo 15. Para acreditar el cumplimiento del principio de consentimiento, las unidades administrativas deben:

I. Identificar en el aviso de privacidad, aquellos datos y finalidades que requieren del consentimiento de la persona titular de los datos personales, para su tratamiento.

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

III. Documentar que se pone a disposición de la persona titular de los datos personales el aviso de privacidad, en aquellos casos en los cuales sea válido el consentimiento tácito.

II.6. PRINCIPIO DE INFORMACIÓN

Artículo 16. Independientemente de que se requiera o no el consentimiento de la persona titular de los datos personales para su tratamiento, las unidades administrativas deben informar de forma clara sobre la existencia y las características principales del tratamiento al que serán sometidos sus datos personales.

Las unidades administrativas que traten datos personales, sin importar la función con la que se vincule, deben elaborar y poner a disposición los avisos de privacidad simplificados e integrales que correspondan a los tratamientos llevados a cabo, en los términos establecidos por la Ley General, los Lineamientos Generales, así como en la presente Política, para un debido cumplimiento.

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

II.6.1. Actividades vinculadas al principio de información

Artículo 17. Para dar atención al principio de información, las unidades de transparencia que traten datos personales deben:

I. Redactar las modalidades de avisos de privacidad, integral y simplificado que se requieran, conforme a los tratamientos que se lleven a cabo.

II. Considerar la elaboración de los avisos de privacidad con todos los elementos informativos y normativos que resulten aplicables, de manera clara, comprensible, así como con una estructura y con un diseño que facilite su entendimiento, considerando en todo momento su accesibilidad para personas con algún tipo de discapacidad.

III. Difundir el aviso de privacidad por medios electrónicos y físicos, en la medida de lo posible.

IV. 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. Promover que los avisos de privacidad sean redactados de conformidad con lo establecido por la Ley General y los Lineamientos Generales.

VII. Comunicar el aviso de privacidad a quienes se transfieran datos personales.

VIII. Considerar y dar continuidad a la implementación de medidas compensatorias, en términos de lo dispuesto en la Ley General y demás disposiciones aplicables, para dar a conocer los avisos de privacidad a través de medios masivos de difusión (periódico oficial, *página de Internet*, carteles u otro similar), cuando resulte imposible hacerlo de manera directa al/a la titular o, ello exija esfuerzos desproporcionados.

II.6.2. Mecanismos para acreditar el cumplimiento del principio de información

Artículo 18. En aras de acreditar el cumplimiento del principio de información, las unidades administrativas deben realizar las acciones siguientes:

I. Contar con los avisos de privacidad integral y simplificado por cada proceso de tratamiento de datos personales que lleven a cabo.

II. Implementar un procedimiento gratuito para la puesta de disposición del aviso de privacidad.

III. Realizar las gestiones para que los avisos de privacidad, en sus modalidades simplificada e integral, sean publicados en la página de Internet, en la sección que se destine para ello, a fin de que se difunda por medios electrónicos.

IV. Documentar los lugares y medios en los que se difunden y colocan los avisos de privacidad para un mejor control y evidencia.

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

II.7. PRINCIPIO DE PROPORCIONALIDAD

Artículo 19. Las unidades administrativas deben recabar 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 al IMPI.

II.7.1. Actividades vinculadas al principio de proporcionalidad

Artículo 20. Para el cumplimiento del principio de proporcionalidad, las unidades administrativas responsables del tratamiento de datos personales deben:

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

II. Realizar esfuerzos razonables para actualizar la normativa y formatos internos, con el fin de limitar los datos personales tratados al mínimo necesario, considerando las finalidades que motivan su tratamiento.

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 21. En aras de acreditar el cumplimiento del principio de proporcionalidad, las unidades administrativas deben llevar a cabo, al menos, las acciones siguientes:

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

II. Promover que en su área se requiera el mínimo posible 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, así como señalarlas en el Documento de Seguridad.

II.8. PRINCIPIO DE CALIDAD

Artículo 22. Las unidades administrativas deben adoptar las medidas necesarias para mantener los datos personales exactos, correctos, completos y actualizados**,** a fin de que no se altere la veracidad de éstos.

Se entiende que los datos personales son:

I. **Exactos y correctos**: Cuando los datos personales 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 del responsable.

III. **Actualizados**: Cuando los datos personales responden fielmente a la situación actual del/de la titular.

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

Cuando los datos personales se hayan obtenido indirectamente de la persona titular de los datos personales, las unidades administrativas deben garantizar que éstos respondan al principio de calidad, de acuerdo con la categoría de datos personales, así como las condiciones y medios del tratamiento.

Ante la identificación de datos personales que hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones aplicables, deben ser suprimidos, previo bloqueo una vez que concluya el plazo de conservación de éstos.

II.8.1. Actividades vinculadas al principio de calidad

Artículo 23. Para el cumplimiento del principio de calidad, las unidades administrativas que traten datos personales deben:

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

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

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

II.8.2. Mecanismos para acreditar el cumplimiento del principio de calidad

Artículo 24. Para acreditar el cumplimiento del principio de calidad, las unidades administrativas deben realizar lo siguiente:

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

II. Documentar las actualizaciones y supresiones realizadas.

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

II.9. PRINCIPIO DE RESPONSABILIDAD

Artículo 25. Conforme al principio de responsabilidad, las unidades administrativas deben velar por el cumplimiento todos los principios señalados con antelación, promover la adopción de medidas necesarias para su aplicación y, demostrar ante las personas titulares de los datos personales, del organismo garante 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 26. Para dar cumplimiento al principio de responsabilidad, las unidades administrativas deben realizar lo siguiente:

I. Establecer entre el personal de las unidades administrativas la obligatoriedad y exigibilidad del programa de protección de datos personales que apruebe el Comité de Transparencia.

II. Prever recursos para la instrumentación de la presente Política y del programa de protección de datos, en su caso.

III. Incentivar la capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.

IV. Revisar periódicamente el programa de protección de datos personales y el Documento de Seguridad para determinar las modificaciones que se requieran.

V. Establecer procedimientos para recibir y responder dudas y quejas de los/las titulares.

II.9.2. Mecanismos para acreditar el cumplimiento del principio de responsabilidad

Artículo 27. Para acreditar el cumplimiento al principio de responsabilidad, las unidades administrativas deben:

I. Contar con las constancias de capacitación de su personal en temas relacionados con la materia de protección de datos personales.

II. Llevar un registro de las dudas y quejas de los/las titulares.

III. Documentar la comunicación hacia su personal de la presente Política y del programa de protección de datos que al efecto sea aprobado.

IV. Guardar evidencia del cumplimiento de la presente Política.

CAPÍTULO III. DE LOS DEBERES

Periférico Sur 3106, Jardines del Pedregal, Álvaro Obregón, 01900
Ciudad de México, Teléfono: 55 5624 0400 www.gob.mx/impi

III.1. DEBERES PARA PROTECCIÓN DE DATOS PERSONALES EN EL IMPI

Artículo 28. Además de los principios señalados en el Capítulo anterior, las unidades administrativas deben dar cumplimiento al:

I. Deber de confidencialidad, y

II. Deber de seguridad.

III.2. DEBER DE CONFIDENCIALIDAD

Artículo 29. Las unidades administrativas deben establecer controles o mecanismos de observancia obligatoria para las personas servidoras públicas que intervengan en cualquier fase del tratamiento, con la finalidad de que éstos guarden confidencialidad de los datos personales, obligación que subsistirá aún después de finalizar su relación laboral con el IMPI.

III.2.1. Actividades vinculadas al deber de confidencialidad

Artículo 30. Para el cumplimiento del deber de confidencialidad, las unidades administrativas deben efectuar lo siguiente:

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 al tratamiento para la finalidad que fueron compartidos estos, durante y posterior a la vigencia del instrumento jurídico.

III. Implementar campañas de sensibilización para el personal, sobre la importancia de la confidencialidad y tratamiento que recae a los datos personales que se obtengan en el ejercicio de funciones.

IV. Proponer la implementación de mejores prácticas al interior del IMPI para garantizar la secrecía de los datos personales, cuando así proceda.

III.2.2. Mecanismos para acreditar el cumplimiento del deber de confidencialidad

Artículo 31. Para acreditar el cumplimiento del deber de confidencialidad, las unidades administrativas realizaran, al menos, lo siguiente:

I. Incluir en el Documento de Seguridad, los controles y medidas de seguridad implementadas para garantizar la secrecía de los datos personales.

II. Generar la evidencia de los controles implementados para garantizar la confidencialidad de los datos.

III. Prever cláusulas de confidencialidad de datos personales en los contratos, cuando esto proceda, respecto de transferencias o remisiones.

IV. Tener la evidencia documental de los cursos, talleres, seminarios o similar en los que haya participado el personal de las unidades responsables conforme a los roles y tramos de control en los que se involucren, y que se encuentren relacionados con el tratamiento de datos personales.

V. Documentar la implementación de mejores prácticas que garanticen la confidencialidad de los datos tratados.

III.3. DEBER DE SEGURIDAD

Artículo 32. Las unidades administrativas del IMPI adoptarán e instrumentarán las medidas de seguridad físicas, técnicas y administrativas para garantizar la protección de los datos personales tratados, a fin de evitar cualquier afectación a éstos y a su titular.

III.3.1. Actividades vinculadas al deber de seguridad

Artículo 33. Para el cumplimiento del deber de seguridad, las unidades administrativas deben llevar a cabo, al menos, lo siguiente:

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

II. Determinar a las personas servidoras públicas en cada unidad administrativa del IMPI, que pueden intervenir en el tratamiento de los datos personales, así como definir las funciones y obligaciones que les correspondan en sus respectivos tramos de control.

III. Realizar labores de cooperación institucional encaminadas a realizar un análisis de riesgo de los datos personales tratados en el IMPI, así como de los sistemas físicos y/o electrónicos en el cual se desarrolle dicho tratamiento.

IV. Desarrollar acciones de cooperación institucional para la prevención y mitigación de amenazas o vulneraciones los datos personales en posesión.

V. Monitorear y revisar las medidas de seguridad adoptadas para garantizar la protección de datos personales que se tienen bajo resguardo.

VI. Incentivar la capacitación del personal involucrado en el tratamiento de datos personales, conforme al nivel de responsabilidad que éstos tengan asignado

III.3.2. Mecanismos para acreditar el cumplimiento del deber de seguridad

Artículo 34. Para acreditar el cumplimiento del deber de seguridad, las unidades administrativas deben realizar, al menos, lo siguiente:

I. Elaborar un inventario de datos y de los sistemas de tratamiento de los datos personales.

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

III. Elaborar 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 y documentar las medidas de seguridad físicas, técnicas y administrativas adoptadas para garantizar el tratamiento de los datos recabados, así como las acciones de monitoreo, análisis y revisión a implementar, a fin de mantenerlas actualizadas y, en su caso, detectar áreas de oportunidad para su desarrollo y ejecución.

V. Contar con la evidencia documental de los cursos, talleres, seminarios o similar en los que haya participado el personal de las unidades administrativas y que se encuentre relacionado con la materia de protección de datos personales.

CAPÍTULO IV. PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES

IV.1. OBJETO Y ALCANCES DEL PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES

Artículo 35. Contar con un programa de protección de datos personales, puesto a consideración y aprobación en su caso, por el Comité de Transparencia, cuyo objetivo es determinar las pautas generales bajo las cuales se llevarán a cabo las actividades institucionales orientadas a mantener la observancia en el cumplimiento de los principios y deberes, así como a garantizar el derecho a la protección de datos personales al interior de este sujeto obligado.

IV.2. VIGENCIA Y ACTUALIZACIÓN DEL PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES

Artículo 36. El programa prevé una vigencia trianual, a fin de garantizar el desarrollo ininterrumpido de actividades, sin demérito de que pueda ser sometido a ajustes o actualizaciones por parte del Comité de Transparencia del IMPI, de conformidad con las facultades y atribuciones que le establece la normativa aplicable, en caso de estimarse necesario, para lograr una mejora continua.

Artículo 37. La Unidad de Transparencia del IMPI consolidará la propuesta de ajustes o actualizaciones al programa de protección de datos personales del sujeto obligado, la cual será presentada al Comité de Transparencia para su revisión y, en su caso, aprobación**.**

Cualquier modificación y actualización se sujeta a los términos señalados en el párrafo anterior.

IV.3. CONTENIDO MÍNIMO DEL PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES

Artículo 38. El Programa de Protección de Datos Personales del IMPI deberá prever al menos:

I. La vigencia del programa.

II. Un diagnóstico sobre los problemas, necesidades o áreas de oportunidad detectadas para el cumplimiento de los principios y deberes en materia de protección de datos personales dentro del IMPI.

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 los problemas, necesidades o áreas de oportunidad que hayan sido detectadas.

IV. Una propuesta de medición, a través de la cual se pueda cuantificar el desarrollo y cumplimiento de las actividades propuestas.

IV.4. SUPERVISIÓN DEL PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES

Artículo 39. Corresponde a la Unidad de Transparencia del IMPI coordinar el seguimiento a la ejecución de las actividades previstas en el programa de protección de datos personales e informar al Comité de Transparencia de este Instituto acerca de su cumplimiento.

CAPÍTULO V. DOCUMENTO DE SEGURIDAD

V.1. OBJETOY ALCANCES DEL DOCUMENTO DE SEGURIDAD

Artículo 40. El IMPI cuenta con un Documento de Seguridad como parte de los mecanismos implementados para asegurar el cumplimiento al deber de seguridad, en materia de datos personales, 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 41. El Documento de Seguridad debe contener como mínimo, lo siguiente:

I. El inventario de datos personales y de los sistemas 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

V.2. ACTUALIZACIONES AL DOCUMENTO DE SEGURIDAD

Artículo 42. En las actualizaciones que se realicen al Documento de Seguridad deben participar todas las unidades administrativas conforme a competencia, por medio de las personas servidoras públicas de nivel mando y técnico operativo (apoyo) a que se hace referencia el artículo 1 de la presente Política, quiénes en todo momento deberán observar los principios y deberes a que se refiere la Ley General, los Lineamientos Generales y demás disposiciones legales aplicables. Para la formulación de propuestas de actualización del Documento de Seguridad.

La Unidad de Transparencia del IMPI coadyuvará en la elaboración de formatos, formularios, cuestionarios o cualquier otro instrumento de apoyo, que resulte útil para el cumplimiento de esta Política y demás disposiciones aplicables en la materia.

Acorde con lo dispuesto en la Ley General, el Documento de Seguridad se actualizará en los siguientes casos:

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

II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión con que se cuente o para mitigar el impacto de una vulneración a la seguridad.

III. 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 puede ser actualizado cuando menos cada tres años.

Artículo 43. Cuando alguna de las unidades administrativas se encuentre en los supuestos referidos, la persona designada como enlace responsable debe solicitar por escrito al Comité de Transparencia del IMPI las actualizaciones necesarias, el cual resolverá lo conducente.

Las personas designadas como enlaces responsables y el enlace de operativo técnico de apoyo pueden solicitar orientación a la Unidad de Transparencia de este Instituto, para la integración o cualquier acto relacionado con los alcances del Documento de Seguridad.

V.3. SUPERVISIÓN DEL DOCUMENTO DE SEGURIDAD

Artículo 44. Corresponderá a la persona titular del IMPI, al responsable de la unidad administrativa y al Comité de Transparencia en el ámbito de competencia, supervisar o solicitar la supervisión externa de las políticas internas para la gestión y tratamiento de datos personales, derivado de lo cual se generarán los informes correspondientes, conteniendo los hallazgos identificados durante la revisión.

V.4. VULNERACIONES A LA SEGURIDAD DE LOS DATOS

Periférico Sur 3106, Jardines del Pedregal, Álvaro Obregón, 01900
Ciudad de México, Teléfono: 55 5624 0400 www.gob.mx/impi

Artículo 45. En términos de lo previsto en la Ley General, se consideran vulneraciones a la seguridad de los datos personales, las siguientes:

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.

Artículo 46. Cuando las vulneraciones afecten de forma significativa los derechos patrimoniales o morales de las personas titulares de los datos personales, las unidades administrativas involucradas deben generar un informe detallado que contenga al menos lo siguiente:

I. La naturaleza del incidente.

II. Los datos personales comprometidos.

III. Las recomendaciones a la persona titular de los datos afectada, respecto a las medidas que puede adoptar para proteger sus intereses.

IV. Las acciones correctivas implementadas para mitigar la vulneración.

V. Los datos de contacto de quien funge como enlace responsable y técnico operativo de apoyo de la unidad administrativa involucrada al cual puede acudir la persona titular de los datos personales afectada para obtener más información al respecto.

El referido informe también deberá ser remitido a la Unidad de Transparencia en un plazo no mayor a dos días hábiles posteriores a que se haya confirmado la vulneración, para que ésta lo haga del conocimiento de las personas titulares de datos personales involucrados y del Comité de Transparencia del IMPI.

Adicionalmente, las unidades administrativas deben prever en el informe a notificarse al INAI a través de la Unidad de Transparencia, lo siguiente:

1) La hora y fecha de la identificación de la vulneración.

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

3) La naturaleza del incidente o vulneración ocurrida.

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

5) Las categorías y número aproximado de los/las titulares afectados/as.

Periférico Sur 3106, Jardines del Pedregal, Álvaro Obregón, 01900
Ciudad de México, Teléfono: 55 5624 0400 www.gob.mx/impi

6) Los sistemas de tratamiento y datos personales comprometidos.

7) La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida.

8) Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.

Artículo 47. Conforme a lo previsto en los Lineamientos Generales, se entiende que se afectan los derechos patrimoniales de la persona titular de los datos personales, cuando la vulneración esté 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 entienden como aquellos relacionados, de manera enunciativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, aspecto físico o menoscabe ilegalmente la libertad, integridad física o psíquica del/de la titular de los datos.

Artículo 48. En aquellos casos en los cuales no sea posible notificar directamente a las personas titulares de los datos personales, el informe a que hace referencia la presente Política o ello implique esfuerzos desproporcionados, las unidades administrativas deben instrumentar las medidas compensatorias de comunicación para tal efecto, como son: la publicación en medio oficial, página de Internet, carteles u otro similar.

Artículo 49. El Comité de Transparencia del IMPI puede determinar la implementación de acciones adicionales a las realizadas por las unidades administrativas para evitar futuras vulneraciones y reforzar las medidas de seguridad aplicables.

Para tal efecto, el Comité de Transparencia puede auxiliarse de la asesoría, orientación o apoyo de otras unidades administrativas, así como de la suscripción de convenios de colaboración o de la contratación de especialistas en la materia, siempre y cuando exista la suficiencia presupuestal para ello.

CAPÍTULO VI. AVISOS DE PRIVACIDAD

VI.1. AVISOS DE PRIVACIDAD PARA CADA PROCESO DE TRATAMIENTO DE DATOS PERSONALES

Artículo 50. 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 de los datos personales para el tratamiento, en el IMPI se debe contar con un aviso de privacidad integral y su correlativo aviso de privacidad simplificado, por cada proceso en los 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, y las unidades administrativas que se involucran, de ser el caso de tal suerte que no dé lugar a incertidumbre o ambigüedad a sus titulares.

VI.2. FORMATOS PARA LA ELABORACIÓN O ACTUALIZACIÓN DE AVISOS DE PRIVACIDAD

Artículo 51. Los formatos para la elaboración de los avisos de privacidad integral y simplificado deben ser acordes con los elementos que establece la Ley General, los Lineamientos Generales y demás normatividad que resulte aplicable.

Artículo 52. En la integración y elaboración de los avisos de privacidad, las unidades administrativas deben prever una estructura que facilite su entendimiento por parte de las personas titulares de los datos personales. De ser el caso, la Unidad de Transparencia puede orientar al respecto a fin de facilitar la integración o actualización, para mantener la homogeneidad de los elementos de forma.

VI.3. REDACCIÓN DE LOS AVISOS DE PRIVACIDAD

Artículo 53. Las unidades administrativas se asegurarán de que la información asentada en los avisos de privacidad se encuentre redactada en un lenguaje sencillo, claro y comprensible, considerando en todo momento el perfil de la persona titular de los datos personales al cual vaya dirigido, por lo que se abstendrán de:

I. Usar frases inexactas, ambiguas o vagas.

II. Incluir textos que induzcan a los/las titulares a elegir una opción en específico.

III. Marcar previamente las casillas, en caso de que estas se incluyan, para que las personas titulares de los datos personales otorguen su consentimiento, o bien, incluir declaraciones orientadas a afirmar que la persona titular de los datos personales ha consentido el tratamiento de estos sin manifestación alguna de su parte.

IV. Remitir a textos o documentos que no estén disponibles para las personas titulares de los datos personales

Artículo 54. Para la elaboración o actualización de los avisos de privacidad, quienes funjan como enlaces responsables o de apoyo técnico operativo pueden en todo momento, solicitar orientación técnica a la Unidad de Transparencia del IMPI.

VI.4. CASOS EN LOS QUE SE REQUIERE UN NUEVO AVISO DE PRIVACIDAD

Artículo 55. En sustitución de los avisos de privacidad ya existentes, las unidades administrativas deben considerar la elaboración de un nuevo aviso de privacidad, en sus dos modalidades, cuando:

I. El proceso de tratamiento de datos personales se traslade a una nueva área o esta cambie su denominación.

II. Se requieran recabar datos sensibles a aquéllos informados en el aviso de privacidad original, los cuales no se obtengan de manera directa de la persona titular de los datos personales y se requiera de su consentimiento para el tratamiento de éstos.

III. Cambien las finalidades señaladas en el aviso de privacidad original, o

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

CAPÍTULO VII. PROGRAMA DE CAPACITACIÓN Y ACTUALIZACIÓN

Artículo 56. El IMPI cuenta con un Programa de Capacitación y Actualización en materia de protección de datos personales, como uno de los mecanismos para dar cumplimiento al principio de responsabilidad, el cual considera los niveles de capacitación atendiendo a los roles y responsabilidades de las personas servidoras públicas que tratan la información personal.

VII.1. ELABORACIÓN Y APROBACIÓN DEL PROGRAMA DE CAPACITACIÓN Y ACTUALIZACIÓN

Artículo 57. El Comité de Transparencia del IMPI es el órgano encargado de aprobar el Programa de Capacitación y Actualización en la materia, con base en la propuesta que sea presentada por la Unidad de Transparencia, en la cual se consideren las necesidades de capacitación de las unidades administrativas y la oferta en relación con la oferta que ofrece el INAI.

CAPÍTULO VIII. EJERCICIO DE LOS DERECHOS ARCO

VIII.1. CONCEPTOS DE LOS DERECHOS ARCO

Artículo 59. Para efectos de este procedimiento, se considera que los derechos ARCO comprenden:

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

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

III. **Cancelación**: Derecho de la persona la titular para solicitar al IMPI 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 al IMPI 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.

Periférico Sur 3106, Jardines del Pedregal, Álvaro Obregón, 01900
Ciudad de México, Teléfono: 55 5624 0400 www.gob.mx/impi

VIII.2. MEDIOS DISPONIBLES PARA LA RECEPCIÓN DE SOLICITUDES DE EJERCICIO DE LOS DERECHOS ARCO

Artículo 60. La presentación de solicitudes de derechos ARCO puede realizarse a través de los medios de recepción siguientes:

I. Unidad de Transparencia, ubicada en Periférico Sur 3106, colonia Jardines del Pedregal, demarcación territorial Álvaro Obregón, C.P. 14110, Ciudad de México;

II. A través del correo electrónico: uenlace@impi.gob.mx;

III. Servicio postal y mensajería, con envío al domicilio antes señalado;

IV Mediante la Plataforma Nacional de Transparencia (PNT) en el hipervínculo: http://www.plataformadetransparencia.org.mx/ y

V. Teléfono INAI 800 835 4324.

Artículo 61. La Unidad de Transparencia es la responsable de turnar las solicitudes del ejercicio de derechos ARCO que sean presentadas a aquellas unidades administrativas que conforme a sus atribuciones, competencias o funciones puedan o deban poseer los datos personales, a fin de atenderlas en los plazos y términos establecidos en la Ley General, los Lineamientos Generales y demás disposiciones aplicables en la materia.

Artículo 62. Las unidades administrativas deben llevar a cabo las acciones pertinentes para garantizar el efectivo ejercicio de los derechos ARCO de las personas titulares, acorde con los principios, deberes y obligaciones en materia de protección de datos personales.

Artículo 63. Las unidades administrativas atenderán las solicitudes y podrán orientarse con la Unidad de Transparencia en los casos que se requiera formular alegatos, derivados de los recursos de revisión interpuestos en términos de la Ley General, con motivo de las respuestas otorgadas.

VIII.3. ACATAMIENTO DE LA RESOLUCIÓN EMITIDA POR EL INSTITUTO

Artículo 64. La resolución que emita el INAI es vinculante para el IMPI y, una vez recibida, la Unidad de Transparencia llevará a cabo las gestiones que resulten necesarias ante las unidades administrativas competentes para dar cumplimiento a lo instruido.

CAPÍTULO IX. DE LAS REMISIONES Y TRANSFERENCIAS DE LOS DATOS PERSONALES EN POSESIÓN DEL IMPI

IX.1. RELACIÓN ENTRE EL IMPI Y EL/LA ENCARGADO/A

Artículo 65. La remisión es toda aquella comunicación de datos personales realizada entre responsables (IMPI) y encargados/as, dentro o fuera del territorio mexicano.

Artículo 66. El IMPI 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 las personas servidoras públicas facultadas para ello.

IX.2. OBLIGACIÓN GENERAL DEL/DE LA ENCARGADO/A

Artículo 67. El/la encargado/a debe tratar los datos personales a nombre y por cuenta del IMPI dentro del ámbito de actuación de la prestación del servicio debidamente formalizado y sin ostentar poder alguno de decisión sobre el alcance y contenido del tratamiento, limitando en ese sentido, sus actuaciones a los términos fijados por el IMPI.

IX.3. INSTRUMENTO JURÍDICO ACORDE CON LAS FINALIDADES INFORMADAS EN EL AVISO DE PRIVACIDAD

Artículo 68. Cualquier acuerdo alcanzado y debidamente formalizado entre el IMPI y el/la encargado/a se efectúa con base en lo previsto por la Ley General, los Lineamientos Generales, la presente Política y el aviso de privacidad puesto a disposición de los/las titulares de los datos personales en el cual quedaron definidas previamente las condiciones de su tratamiento.

IX.4. OBLIGACIONES ESPECÍFICAS DEL/DE LA ENCARGADO/A CONTENIDAS EN EL INSTRUMENTO JURÍDICO

Artículo 69. Acorde con lo dispuesto en la Ley General y los Lineamientos Generales, el instrumento jurídico por el cual se formalice la relación jurídica entre el IMPI y el/la encargado/a debe incluir al menos las siguientes obligaciones para este:

I. Realizar el tratamiento de los datos personales conforme a las instrucciones del IMPI.

II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el IMPI.

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

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

V. Guardar confidencialidad respecto de los datos personales tratados, conforme al caso concreto.

VI. Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el IMPI.

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

VIII. Permitir al INAI o al IMPI realizar verificaciones en el lugar o establecimiento donde se lleva a cabo el tratamiento de los datos personales, de ser viable.

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

IX.5. SUBCONTRATACIÓN DE SERVICIOS QUE IMPLIQUEN EL TRATAMIENTO DE DATOS PERSONALES

Artículo 70. La subcontratación de servicios que impliquen el tratamiento de los datos personales previamente remitidos por el IMPI sólo puede llevarse a cabo cuando en el instrumento jurídico suscrito por el IMPI y el/la encargado/a se contemple dicha situación, debiendo este formalizar, a su vez, la relación jurídica con el/la subcontratado/a por medio de cualquier instrumento jurídico que permita acreditar su existencia, alcance y contenido, en términos de las disposiciones legales aplicables.

En 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 el/la encargado/a.

IX.6. PROVEEDORES/AS DE SERVICIOS DE CÓMPUTO EN LA NUBE Y OTRAS MATERIAS

Artículo 71. El IMPI puede contratar o adherirse a servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el/la proveedor/a externo/a garantice las condiciones y cuente con los mecanismos establecidos en la Ley General.

Para dichos efectos, la unidad administrativa contratante debe solicitar dictamen técnico a la Dirección competente del IMPI, de conformidad con sus atribuciones y la normativa interna en materia de tecnología de la información, comunicación y seguridad informática en el IMPI y suscribir el contrato o instrumento jurídico en el que se prevean las cláusulas generales que se refieren en este capítulo.

CAPÍTULO X. DE LAS TRANSFERENCIAS DE DATOS PERSONALES

X.1. TRANSFERENCIAS A TERCEROS

Artículo 72. El IMPI puede llevar a cabo transferencias nacionales o internacionales a terceros, de los datos personales en su posesión, en los términos y bajo las condiciones que determina la Ley General.

X.2. CONDICIONES GENERALES DE LAS TRANSFERENCIAS

Periférico Sur 3106, Jardines del Pedregal, Álvaro Obregón, 01900
Ciudad de México, Teléfono: 55 5624 0400 www.gob.mx/impi

Artículo 73. Toda transferencia de datos personales que lleve a cabo el IMPI se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en la Ley General. Para tal efecto, las unidades administrativas por medio del aviso de privacidad correspondiente deben informar a la persona titular de los datos personales, las finalidades de la transferencia, así como su destinatario/a

Cuando la transferencia requiera del consentimiento expreso de la persona titular, se deben habilitar los mecanismos para que éste/ésta manifieste su voluntad.

La actualización de alguna de las excepciones previstas en las disposiciones previamente citadas no exime a las unidades administrativas de cumplir con las obligaciones previstas en la Ley General y la presente Política.

X.3. COMUNICACIÓN DE AVISOS DE PRIVACIDAD A TERCEROS RECEPTORES

Artículo 74. En toda transferencia de datos personales, las unidades responsables comunicarán el aviso de privacidad respectivo, al tercero receptor de las transferencias, debiendo documentar detalladamente dicha comunicación.

X.4. FORMALIZACIÓN DE LA TRANSFERENCIA

Artículo 75. Acorde con lo previsto en la Ley General, toda transferencia de datos personales que realicen las unidades administrativas debe formalizarse 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; se realice derivado de una petición de la autoridad extranjera u organismo internacional competente en su carácter de receptor; cuando las facultades entre el IMPI y el responsable receptor sean homólogas; o cuando las finalidades que motivan la transferencia sean análogas.

X.5. TRANSFERENCIAS INTERNACIONALES

Artículo 76. Cuando la comunicación de datos personales se realice fuera del territorio nacional, previo a su transferencia, el IMPI se debe asegurar que el tercero 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 normatividad mexicana aplicable en la materia, así como a los términos previstos en el aviso de privacidad que le es comunicado por el IMPI.

En todo caso, el IMPI puede solicitar al INAI la opinión respecto de las transferencias internacionales que se le susciten, en términos de lo dispuesto en los Lineamientos Generales.

GLOSARIO

SIGLAS Y ACRÓNIMOS	DENOMINACIONES
AVISO DE PRIVACIDAD	Documento a disposición del/de la titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.
COMITÉ DE TRANSPARENCIA	Autoridad máxima en materia de protección de datos personales al interior del IMPI.
DERECHOS ARCO	Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales
DOCUMENTO DE SEGURIDAD	Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.
ENCARGADO/A	La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable
ENLACE RESPONSABLE	Persona servidora pública de mando superior con nivel de dirección general u homóloga designada por cada unidad administrativa para fungir como enlace en materia de datos personales ante la Unidad de Transparencia y el Comité de Transparencia.
ENLACE APOYO	Persona servidora pública de nivel de mando director de área subdirector coordinador designado en cada unidad administrativa para fungir como apoyo al enlace responsable en materia de datos personales ante la Unidad de Transparencia y el Comité de Transparencia del IMPI
IMPI	Instituto Mexicano de la Propiedad Industrial
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
INVENTARIO	Inventario de datos personales del IMPI al que se refieren los artículos 33, fracción III de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 58 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.
LEY GENERAL	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
LINEAMIENTOS GENERALES	Lineamientos Generales de Protección de Datos Personales para el Sector Público

Periférico Sur 3106, Jardines del Pedregal, Álvaro Obregón, 01900
Ciudad de México, Teléfono: 55 5624 0400 www.gob.mx/impi

SIGLAS Y ACRÓNIMOS	DENOMINACIONES
MEDIDAS COMPENSATORIAS	Mecanismos alternos para dar a conocer a los/las titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance.
MEDIDAS DE SEGURIDAD	Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales
POLÍTICA	Política de Protección de Datos Personales del IMPI
REMISIÓN	Toda comunicación de datos personales realizada exclusivamente entre el responsable y el/la encargado/a, dentro o fuera del territorio mexicano.
RESPONSABLE	Los sujetos obligados a que se refiere el artículo 1 de la Ley General que deciden sobre el tratamiento de datos personales (Instituto Mexicano de la Propiedad Industrial).
TITULAR	La persona física a quien corresponden los datos personales.
TRANSFERENCIA	Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del/de la titular, del responsable o del/de la encargado/a
TRATAMIENTO	Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.
UNIDAD ADMINISTRATIVA	Todas las áreas que, de acuerdo con el Reglamento del Instituto Mexicano de la Propiedad Industrial, Estatuto Orgánico del Instituto Mexicano de la Propiedad Industrial y los acuerdos delegatorios vigentes, lleve a cabo el tratamiento de datos personales a nombre del IMPI.

APROBACIÓN

Esta Política fue aprobada por unanimidad de votos de los integrantes del Comité de Transparencia del Instituto Mexicano de la Propiedad Industrial, en su Cuarta sesión Ordinaria de fecha 15 de diciembre 2023, mediante acuerdo CT/04/2023/4ªO.

La Unidad de Transparencia realizará las gestiones necesarias para que la Política sea publicada en el Apartado de Protección de Datos de la página de Internet del IMPI.

El presente documento entrará en vigor al día siguiente de su aprobación.

FIN DEL DOCUMENTO.

Periférico Sur 3106, Jardines del Pedregal, Álvaro Obregón, 01900
Ciudad de México, Teléfono: 55 5624 0400 www.gob.mx/impi