

Procedimiento para la entrega de datos personales en caso de que estos sean requeridos por una autoridad competente

Unidad Técnica de Transparencia y Protección de Datos Personales
Versión 1.0

Control de versiones

DESCRIPCIÓN	RESPONSABLE DE LA ACTUALIZACIÓN	FECHA DE ACTUALIZACIÓN
Creación del documento	Ana María Salazar Salazar Auxiliar de Protección de Datos Personales José Manuel Ortiz Martínez Jefe de Departamento de Protección de Datos Personales, Consulta y Vinculación	Enero 2023
Revisión del documento	José Leonel Flores Téllez Subdirector de Protección de Datos Personales	Febrero 2023
Revisión y aprobación del documento	Ivette Alquicira Fontes Directora de Acceso a la Información y Protección de Datos Personales	Marzo 2023

HOJA DE FIRMAS:

FECHA	PUESTO	ÁREA	NOMBRE
Febrero 2023	Directora de Acceso a la Información y Protección de Datos Personales	Unidad Técnica de Transparencia y Protección de Datos Personales	Ivette Alquicira Fontes
	Subdirector de Protección de Datos Personales	DAIPDP	José Leonel Flores Téllez

“Este documento ha sido firmado electrónicamente, de conformidad con el artículo 22 del Reglamento para el Uso y Operación de la Firma Electrónica Avanzada en el Instituto Nacional Electoral.”

CONTENIDO

GLOSARIO.....	4
OBJETIVO.....	5
ALCANCE.....	5
CONTEXTO.....	5
JUSTIFICACIÓN.....	6
PROCEDIMIENTO	7

GLOSARIO

- **Áreas u órganos responsables:** Órganos de dirección, ejecutivos, técnicos, de vigilancia, de transparencia, de control y otros órganos colegiados del INE que tratan datos personales y son responsables de administrar una base de datos personales.
- **Aviso de privacidad:** Documento a disposición de la persona titular de forma física, electrónica o en cualquier formato generado por el área 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.
- **Bitácora:** Registro físico o electrónico de los requerimientos realizados por autoridades competentes, respecto de datos personales tratados por la Subdirección de Protección de Datos Personales.
- **DAIPDP:** Dirección de Acceso a la Información y Protección de Datos Personales.
- **Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.
- **Derechos ARCOP:** Los derechos de acceso, rectificación, cancelación, oposición y portabilidad al tratamiento de datos personales.
- **Expediente:** La unidad documental compuesta por documentos de archivo, ordenados y relacionados por un mismo asunto, actividad o trámite de los sujetos obligados.
- **INE o Instituto:** Instituto Nacional Electoral.
- **INFOMEX-INE:** Sistema electrónico autorizado por el INE para tramitar las solicitudes de acceso a la información y de datos personales al interior del propio Instituto.
- **LGPDPSSO:** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- **Titular:** La persona física a quien corresponden los datos personales.
- **Transferencia:** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.
- **Tratamiento.** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.
- **UT o UTTPDP:** Unidad Técnica de Transparencia y Protección de Datos Personales.

OBJETIVO

Describir el procedimiento que deberá seguir el personal de la DAIPDP, adscrita a la UTTYPDP, respecto del tratamiento de datos personales en la entrega o transferencia que, en su caso, se realice a las autoridades competentes en el ejercicio de sus funciones.

ALCANCE

El procedimiento interno está dirigido al personal de la DAIPDP, responsable del tratamiento de los datos personales, recabados para la gestión de las solicitudes de derechos ARCOP, contenidos en el INFOMEX-INE.

CONTEXTO

Auditoría de control interno en materia de protección de datos personales, señalada en el Plan de Auditoría de Control Interno: INE/PACIPDP/2022-2023/01ARCO01.

El 15 de marzo de 2022, mediante oficio INE/UTTyPDP/0045/2022, la titular de la UTTYPDP, comunicó a la Directora de Acceso a la Información y Protección de Datos Personales, en su carácter de área responsable del proceso de tratamiento de datos personales que, conforme al Programa de auditorías de control interno en materia de protección de datos personales 2022-2023, el 28 de marzo de 2022, iniciaría la ejecución de la auditoría de control interno al procedimiento “Atención de Solicitudes para el ejercicio de los derechos ARCO”.

Informe de la Auditoría de Control Interno en Materia de Protección de Datos Personales, señalada en el Plan de Auditoría de Control Interno INE/PACIPDP/2022-2023/01-ARCO01.

El 10 de junio de 2022, la titular de la UTTYPDP de este Instituto, mediante el Sistema de Archivos Institucional (SAI), a través del oficio INE/UTTyPDP/0104/2022, notificó el Informe final del resultado de la Auditoría de Control Interno en Materia de Protección de Datos Personales, señalada en el Plan de Auditoría de Control Interno INE/PACIPDP/2022-2023/01-ARCO01, practicada a la DAIPDP, en relación con el procedimiento “Atención de Solicitudes para el ejercicio de los derechos ARCO”.

En el Informe final de la auditoría, se comunicó la siguiente no conformidad menor:

Resumen de resultados			
Dominio	Control	Descripción	Recomendación
D4. Protección de datos personales en la operación	C12. Protección de datos personales para la revelación de información a las	El área responsable manifiesta no contar con evidencia que respalde la aplicabilidad y cumplimiento del	Se recomienda al área responsable, como acción preventiva, contar con un instrumento que incluya información acerca de la entrega de datos personales en caso de que éstos sean requeridos por una autoridad

	autoridades	control.	competente y en el ejercicio de sus funciones.
--	-------------	----------	--

JUSTIFICACIÓN

La Unidad de Transparencia es un área del Instituto que trata datos personales, mediante la gestión de las solicitudes para el ejercicio de los derechos ARCOP, a través del sistema INFOMEX-INE.

- A. Para el tratamiento de datos, el INE debe contar con el consentimiento de sus titulares, salvo en los casos previstos en el artículo 22 de la LGPDPPSO, como podría actualizarse en el presente procedimiento.
- B. Toda transferencia de datos personales -nacional o internacional- que realice el INE, se encuentra sujeta al consentimiento de sus titulares **excepto** en los supuestos previstos en el artículo 70 de la LGPDPPSO:
- (i) cuando la transferencia esté prevista en la Ley General u otras leyes, convenios o tratados internacionales suscritos y ratificados por México,
 - (ii) cuando la transferencia se realice entre el INE y otra instancia responsable, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales,
 - (iii) cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia,
 - (iv) cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última,
 - (v) cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados,
 - (vi) cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el INE y de la persona titular de los datos personales,
 - (vii) cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés de la persona titular, por el INE y una tercera o tercero,
 - (viii) cuando se trate de los casos en los que el INE no está obligado a recabar el consentimiento de la persona titular para el tratamiento y transmisión de sus datos personales, conforme a lo dispuesto en el artículo 22 de la LGPDPPSO, o
 - (ix) cuando la transferencia sea necesaria por razones de seguridad nacional.
- C. Toda transferencia debe encontrarse formalizada mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normativa aplicable al INE, con excepción de los supuestos previstos en el artículo 66 de la LGPDPPSO.

En toda transferencia de datos personales, el INE debe comunicar al receptor de los datos personales el aviso de privacidad conforme al cual tratan los datos personales que recaba y resguarda en ejercicio de sus atribuciones.

En este contexto, la DAIPDP, como responsable del tratamiento de datos personales, respecto al procedimiento "Atención de Solicitudes para el ejercicio de los derechos ARCO", considera necesario contar con un instrumento interno que, en términos de lo previsto en la LGPDPSO, le permita, en su caso, transferir los datos personales que sean requeridos por una autoridad competente, en el ejercicio de sus funciones, los cuales deriven de la gestión de dichas solicitudes y estos se encuentren alojados en el sistema INFOMEX-INE.

PROCEDIMIENTO

Para efectos de atender un requerimiento de alguna autoridad competente, conforme a los principios rectores del tratamiento de datos personales y con el objetivo de adoptar las medidas de seguridad físicas, administrativas y técnicas para proteger los datos personales en la entrega de la información, el personal de la DAIPDP deberá atender el siguiente procedimiento:

1. Recibir por escrito o por medios electrónicos la orden judicial, resolución o mandato fundado y motivado de autoridad competente.

1.1. Identificar y registrar en la bitácora los siguientes elementos:

1.1.2. El área a la que se encuentra dirigido.

1.1.3. La fecha de recepción del requerimiento de datos personales en el INE.

1.1.4. El plazo de atención (en su caso).

1.1.5. La fecha de recepción del requerimiento de datos personales en la DAIPDP y su asignación a la Subdirección de Protección de Datos Personales.

1.1.6. Las facultades de la DAIPDP para la atención del requerimiento.

NOTA. Las atribuciones del área están definidas en los artículos 80 del Reglamento Interior del Instituto Nacional Electoral y 14 del Reglamento del Instituto Nacional Electoral en materia de Protección de Datos Personales, así como en los puntos 1.2 y 1.2.2 del Manual de Organización Específico de la UTTYPDP.

1.1.7. El fundamento de la autoridad requirente.

La obligación de la autoridad que lo emite, para citar los preceptos legales,

sustantivos y adjetivos, en que se apoye el requerimiento¹.

1.1.8. La motivación de la autoridad requirente.

Es el razonamiento, contenido en el requerimiento, conforme al cual, la autoridad que lo emite llega a la conclusión de que el caso concreto se ajusta a las disposiciones legales que sirven de fundamento². Asimismo, son “los razonamientos inherentes a las circunstancias de hecho, contenidas en su texto, formuladas por la autoridad para establecer la adecuación de caso a la hipótesis legal”³.

1.1.9. Los datos personales requeridos.

1.1.9.1 Identificar si en el inventario de datos personales del Sistema INFOMEX-INE están contenidos los requeridos por la autoridad.

NOTA. Los datos personales tratados en el procedimiento para la atención de solicitudes para el ejercicio de derechos ARCOP, son 21, que corresponden a 16 datos personales estándar y 5 datos personales sensibles.⁴

Si el resultado de la búsqueda es negativo (datos no localizados), ir al paso 2 de este procedimiento.

Si el resultado de la búsqueda es positivo (datos sí localizados), continuar con las siguientes acciones:

1.1.9.2 Identificar la categoría del dato personal, de conformidad con el punto anterior.

1.1.9.3 Identificar el riesgo inherente atendiendo a la categoría de dato personal de conformidad con Metodología de Análisis de Riesgos de Privacidad de Datos Personales que se conforma con los siguiente:

A. Nivel bajo: Considera información general como datos de identificación y contacto o información académica o laboral, en este caso los datos personales categorizados como estándar.

¹ FUNDAMENTACION Y MOTIVACION, CONCEPTO DE. [...]. Octava Época, Tribunales Colegiados de Circuito, *Seminario Judicial de la Federación*, Tomo XIV, noviembre de 1994, P.450, tesis I. 4º. P.56 aislada, Penal IUS 209986.

² MOTIVACION, CONCEPTO DE. [...] Octava Época, Tribunales Colegiados de Circuito, *Seminario Judicial de la Federación*, Tomo XIII, febrero de 1994, P.357, aislada, común IUS 213531.

³ MOTIVACION, CONCEPTO DE. [...]. Octava Época, Tribunales Colegiados de Circuito, *Seminario Judicial de la Federación*, Tomo XII, octubre de 1993, P.449, aislada, común IUS 214714.

⁴ Ver el **Anexo I**: Inventario de datos personales tratados en el procedimiento para la Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación, oposición y portabilidad de datos personales (ARCOP).

B. Nivel alto: Datos personales que puedan dar origen a discriminación o conlleven un riesgo grave a la integridad del titular, para este proceso se consideran los datos personales categorizados como sensibles.

2. Verificar los elementos enlistados en el punto anterior.

- 2.1. El área facultada** para atender el requerimiento y entregar los datos personales que solicite la autoridad competente es la DAIPDP, a través de la Subdirección de Protección de Datos Personales, de conformidad con lo establecido en los artículos 80 del Reglamento Interior del Instituto Nacional Electoral y 114 del Reglamento del Instituto Nacional Electoral en materia de Protección de Datos Personales, así como en los puntos 1.2 y 1.2.2 del Manual de Organización Específico de la UTTYPDP.
- 2.2.** Revisar que **el fundamento** citado sea adecuado y pertinente.
- 2.3.** Revisar que **la motivación** sea suficiente, precisa y clara.
- 2.4.** Identificar los datos personales que, en su caso se hubieren localizado dentro del inventario y el nivel de riesgo.

3. Elaborar el oficio de respuesta al requerimiento de la autoridad que deberá contener, como mínimo, lo siguiente:

- 3.1.** Informar a la autoridad receptora de los datos personales que **adquirirá el carácter de responsable y se obligará en términos de la LGPDPPSO**, en consecuencia, deberá:
 - 3.1.1. Observar los principios** de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales y cumplir con lo establecido en la normativa aplicable.
 - 3.1.2. Garantizar su confidencialidad.**
 - 3.1.3. Utilizar** los datos personales para **los fines que fueron transferidos** y
 - 3.1.4. Atender** a lo convenido en el aviso de privacidad.
 - 3.1.5. Establecer y mantener las medidas de seguridad** de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado.

3.2. El resultado de la búsqueda dentro del Sistema INFOMEX-INE.

4. Comunicar el aviso de privacidad respectivo al tercero receptor.

- 4.1. El DAIPDP, área facultada para atender el requerimiento y entregar los datos personales, deberá comunicar a la autoridad requirente, en el oficio de respuesta al requerimiento, el **aviso de privacidad** conforme al cual trata los datos de las personas titulares.
- 4.2. De acuerdo con el tipo de transferencia de datos, la DAIPD o la autoridad receptora deberán:
 - 4.2.1. **Transferencias nacionales.** La autoridad receptora de los datos personales deberá:
 - 4.1.1.1 Tratar los datos personales, comprometiéndose a garantizar su confidencialidad.
 - 4.1.1.2 Utilizar los datos personales únicamente para los fines que fueron transferidos, atendiendo lo establecido en el aviso de privacidad que le será comunicado por el INE.
 - 4.2.2. **Transferencias internacionales.** Previo a que éstas ocurran, la DAIPDP, deberá solicitar a la autoridad receptora **que manifieste por escrito** que se obliga a proteger los datos personales conforme a los principios y deberes que establece la LGPDPSO y a las demás disposiciones que resulten aplicables en la materia.

5. Definir las medidas de seguridad para la protección de datos personales en la entrega del oficio a las autoridades competentes y facultadas.

Con el objetivo de proteger los datos personales y salvaguardarlos de una posible vulneración, así como garantizar su confidencialidad, integridad y disponibilidad, se establecen las siguientes medidas de seguridad atendiendo a los riesgos de nivel bajo y alto:

5.1. Medidas Físicas:

- 5.1.1. Monitoreo de la ruta del envío de información que contenga datos personales.
 - a) Entrega en la Ciudad de México: a través de comunicación directa con el personal de la UTTPDP desde la salida de la información y hasta su entrega.
 - b) Mensajería externa (ubicaciones distintas a la Ciudad de México): a través de números guía de identificación del paquete que el servicio de mensajería proporcione.

5.1.2. Remitir la documentación en sobre sellado.

Enviar la documentación que contiene datos personales en sobre sellado, considerando lo siguiente:

a) Si dispone de cinta adhesiva de seguridad:

- Identificar todas las uniones de apertura del sobre.
- La persona responsable o propietaria debe colocar su firma autógrafa o rúbrica entre la pestaña de apertura principal del sobre y el cuerpo de este.
- Colocar la cinta adhesiva de seguridad sobre las uniones de apertura del sobre.
- Adherir una etiqueta en la parte frontal del sobre que contenga nombre del destinatario, dirección de destino y la leyenda “Esta información contiene datos personales considerados confidenciales”.

b) Si dispone de una cinta de enmascarar o *masking tape*.

- Identificar todas las uniones de apertura del sobre.
- Colocar cinta de enmascarar (*masking tape*) sobre las uniones de apertura.
- La persona responsable o propietaria debe colocar su firma autógrafa o rúbrica sobre la cinta de enmascarar asegurándose que el trazo alcance la pestaña de apertura principal y el cuerpo del sobre.
- Adherir una etiqueta en la parte frontal del sobre que contenga los siguientes datos: nombre de la persona destinataria, dirección de destino, y la leyenda “Esta información contiene datos personales considerados confidenciales”.

5.2. Medidas Administrativas:

5.2.1. Designar a una persona responsable de coordinar el traslado y la recepción de la información, conforme al punto 5.1.1 de este procedimiento.

Designar a una persona que dé seguimiento al traslado de información que contenga datos personales y registrar: la fecha y hora de salida, la persona o compañía de transporte utilizado, la fecha y hora de llegada al destino y el acuse con sello y firma de la persona que recibe.

5.2.2. El personal que intervenga en el procedimiento deberá guardar confidencialidad, secrecía y discreción sobre la información a la que tendrá acceso o conocimiento, durante su relación laboral y una vez que esta haya finalizado, acorde con el estatuto aplicable o el clausulado del contrato de prestación de servicio.

El personal que intervenga en el procedimiento está impedido a difundir, reproducir, publicar, ceder, vender o usar para fines personales, lucrativos, comerciales o en beneficio de terceros.

- La información podrá ser clasificada como reservada o confidencial, de conformidad con la Ley General de Transparencia y Acceso a la Información Pública.

En caso de que la DAIPDP estime necesario que el personal que interviene en el procedimiento firme algún documento de confidencialidad, procederá a formalizarlo.

5.3. Medidas Técnicas:

5.3.1. Generación de código de integridad.

En el envío de información digital generar un código de integridad, a fin de corroborar que la información remitida no haya sido alterada, editada o modificada durante su envío.

Se recomienda utilizar el algoritmo SHA-256 bites, para ello puede emplear la herramienta nativa de *Windows* llamada *POWERSHELL*. A continuación, se detallan los pasos a seguir:

1. Pulse sobre la tecla *Windows*, escriba *PowerShell* y pulse la tecla *Enter* para iniciarla.
2. Agregar el comando *get-filehash* e incorporar en la misma línea la ruta donde está alojado el documento.
3. Dar click en la tecla *Enter*.
4. Obtendrá el código SHA-256, compuesto de una cadena de 64 caracteres alfanuméricos

5.3.2. Uso de la Firma Electrónica Avanzada.

Se sugiere el uso de la Firma Electrónica Avanzada del Instituto para comprobar la autenticidad de la procedencia y la integridad de la información.

5.3.3. Entrega de información en diferentes soportes documentales.

Si por el tamaño de la documentación requiere que se respalde en un medio de almacenamiento conocido como *USB* o *CD* (por sus siglas en ingles).

Previo a su envío se recomienda el uso de cifrado, a través de las herramientas de *Office 365* y *7 ZIP* realizar lo siguiente:

- a) Generar una contraseña que permita el acceso al documento

- b) Enviar el documento protegido
 - c) Compartir la contraseña al emisor por un medio diferente al que fue compartida la información
 - d) El receptor deberá descifrar con la contraseña compartida.
- 6. Para la entrega de la información por oficio a la autoridad competente se deberán observar las medidas de seguridad señaladas en el punto 5 de este procedimiento.**
- 7. Generar un “acuse de recepción” posterior a la entrega del oficio que contenga, como mínimo, los siguientes elementos:**
- 7.1. Fecha y hora de la entrega.
 - 7.2. Sello y firma de la oficina de la autoridad receptora.
 - 7.3. Identificación de los archivos adjuntos al escrito.
- 8. Resguardar el “acuse de recepción” en el expediente correspondiente.**
- 9. Conservar el expediente conforme a lo establecido por la norma aplicable en materia de archivos.**

Fin del procedimiento.



Hoja de firmas de la Guía interna para la entrega de datos personales en caso de que estos sean requeridos por una autoridad competente en el ejercicio de sus funciones.

Lic. Ivette Alquicira Fontes	Directora de Acceso a la Información y Protección de Datos Personales
Mtro. José Leonel Flores Téllez	Subdirector de Protección de Datos Personales