

DOCUMENTO DE SEGURIDAD

Unidad Técnica de Transparencia y Protección de Datos Personales

Dirección de Acceso a la Información y Protección de Datos Personales

Procedimientos: Atención de las Solicitudes de Acceso a la Información y Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO).

Versión 3.0

2022

CONTROL DE VERSIONES

VERSIÓN	COMENTARIO / DESCRIPCIÓN	RESPONSABLE DE LA ACTUALIZACIÓN	FECHA DE ACTUALIZACIÓN ¹
1.0	Creación del documento	Israel López Martell Heidi María Luisa Cambero Martínez Gema Celeste Velázquez Díaz	Enero 2022
1.0	Revisión del documento	José Manuel Ortiz Martínez José Leonel Flores Téllez Joaquín Martínez Velázquez Sentry Lucia Murillo Vargas	Enero 2022
1.0	Revisión del documento	Ivette Alquicira Fontes	Marzo 2022
2.0	Actualización del documento en los apartados: 10. Análisis de Riesgos 10.1 Riesgos inherentes de los datos personales 12. Plan de Trabajo	Israel López Martell Heidi María Luisa Cambero Martínez	Junio 2022
2.0	Revisión del documento	José Manuel Ortiz Martínez José Leonel Flores Téllez	Julio 2022
2.0	Revisión del documento	Ivette Alquicira Fontes	Julio 2022
3.0	Actualización del documento en los apartados:	Gema Celeste Velázquez Díaz	Septiembre 2022

¹ Se precisa que las actividades relativas a la creación, revisión y actualización del presente documento iniciaron desde abril de 2019.

VERSIÓN	COMENTARIO / DESCRIPCIÓN	RESPONSABLE DE LA ACTUALIZACIÓN	FECHA DE ACTUALIZACIÓN ¹
	10.2 Análisis de riesgos de privacidad y datos personales 12. Plan de Trabajo		
3.0	Revisión del documento	Joaquín Martínez Velázquez Sendy Lucia Murillo Vargas	Septiembre 2022
3.0	Revisión del documento	Ivette Alquicira Fontes	Septiembre 2022

“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.”

HOJA DE FIRMAS

ELABORÓ:

FECHA	PUESTO	ÁREA	NOMBRE
Septiembre/2022	Especialista en Acceso a la Información y Datos Personales	Unidad Técnica de Transparencia y Protección de Datos Personales	Gema Celeste Velázquez Díaz

REVISÓ:

FECHA	PUESTO	ÁREA	NOMBRE
Septiembre/2022	Jefe de Departamento de Análisis y Seguimiento	Unidad Técnica de Transparencia y Protección de Datos Personales	Joaquín Martínez Velázquez
Septiembre/2022	Subdirectora de Acceso a la Información	Unidad Técnica de Transparencia y Protección de Datos Personales	Sendy Lucia Murillo Vargas

APROBÓ:

FECHA	PUESTO	ÁREA	NOMBRE
Septiembre/2022	Directora de Acceso a la Información y Protección de Datos Personales	Unidad Técnica de Transparencia y Protección de Datos Personales	Ivette Alquicira Fontes

“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

Definiciones para el documento de seguridad.....	7
Acrónimos.....	8
1 Presentación.....	9
2 Marco normativo.....	11
3 Alcance.....	12
4 Administración de Transparencia y Acceso a la Información y Protección de Datos Personales.....	12
4.1 Descripción de los procedimientos a nivel negocio.....	12
4.1.1 Atención de las Solicitudes de Acceso a la Información.....	13
4.1.2 Atención de solicitudes para el ejercicio de los derechos ARCO.....	15
4.2 Diagrama a bloques.....	17
4.2.1 Diagrama de bloques. Procedimiento Atención de las Solicitudes de Acceso a la Información.....	17
4.2.2 Diagrama de bloques. Procedimiento Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO).....	18
5 Persona que funge el rol propietario.....	20
6 Funciones y obligaciones de las personas que tratan datos personales.....	20
7 Inventario.....	23
8 Ciclo de vida de los datos personales.....	26
8.1 Obtención.....	26
8.2 Almacenamiento de los datos personales.....	26
8.3 Uso de los datos personales.....	26
8.4 Divulgación de los datos personales considerando las remisiones y transferencias.....	27
8.5 Bloqueo de los datos personales.....	27
8.6 Cancelación, supresión o destrucción de los datos personales.....	27
9 Diagrama de flujo de los datos personales.....	28
9.1.1 Diagrama de flujo. Procedimiento Atención de las Solicitudes de Acceso a la Información.....	28
9.1.2 Diagrama de flujo. Procedimiento Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO).....	29
10 Análisis de Riesgos.....	31

10.1	Riesgos inherentes de los datos personales.....	31
10.2	Análisis de riesgos de privacidad y datos personales.....	32
11	Análisis de brecha	32
12	Plan de Trabajo	36
13	Mecanismos de monitoreo y revisión de las medidas de seguridad.....	38
14	Programa General de Capacitación.....	38
14.1	Cursos Virtuales	39
14.2	Cursos presenciales.....	39
14.3	Cursos impartidos por el INAI	40
15	Anexos.....	41

DEFINICIONES PARA EL DOCUMENTO DE SEGURIDAD

Para los efectos del presente documento, se tomarán las definiciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el Programa para la Protección de Datos Personales del Instituto Nacional Electoral y, sin perjuicio de lo previsto en la normativa aplicable en la materia, se entenderá por:

Áreas responsables: Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales.

Comité de Transparencia: Comité de Transparencia del Instituto Nacional Electoral a que hace referencia el artículo 3, fracción V, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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

Día hábil: Todos los días, exceptuando los sábados, domingos, los señalados en términos del Estatuto del Servicio Profesional Nacional y del Personal de la Rama Administrativa, los que estipule el Instituto y aquellos que determine el INAI.

IFESAI: Sistema electrónico autorizado por el entonces Instituto Federal Electoral para tramitar las solicitudes de acceso a la información (no vigente).

Medio de almacenamiento físico: Es todo recurso inteligible a simple vista y con el que se puede interactuar sin la necesidad de ningún aparato que procese su contenido para examinar, modificar o almacenar datos personales.²

Medio de almacenamiento digital: Es todo recurso al que se puede acceder mediante el uso de equipo que procese su contenido para examinar, modificar o almacenar los datos personales.³

Persona solicitante: Persona física o moral que solicita información de interés público o información como titular de datos personales.

Rol propietario: Se refiere a las personas servidoras públicas de las áreas responsables que deciden sobre el tratamiento de los datos personales. Es el responsable final de la protección y uso de los datos.

Sistema INFOMEX-INE: Sistema electrónico autorizado por el Instituto Nacional Electoral para tramitar las solicitudes de acceso a la información y para el ejercicio de los derechos ARCO al interior del propio Instituto.

² Almacenados en archiveros y gabinetes de la Dirección de Acceso a la Información y Protección de Datos Personales.

³ Almacenados en equipos de cómputo y servidores del Instituto.

Sitio de almacenamiento: Instalaciones donde se resguarden los medios de almacenamiento, en cualquier soporte documental.

Soporte Documental: Medio en el cual está contenida la información y puede variar según los materiales y la tecnología empleada, por lo que puede ser impreso o digital, por ejemplo: fotografías, filminas, cintas, plástico, metal, discos duros, memorias flash, discos compactos, entre otros⁴.

Sujeto obligado: Cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, de los ámbitos federal, estatal y municipal, que deciden sobre el tratamiento de los datos personales que obtienen y resguardan en ejercicio de sus atribuciones.

ACRÓNIMOS

Fideicomiso MAC: Fondo para el Cumplimiento del Programa de Infraestructura Inmobiliaria y para la Atención Ciudadana y Mejoramiento de Módulos del Instituto Nacional Electoral.

Fideicomiso Banjército: Contrato de Fideicomiso con número 108601 con el Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C. (BANJERCITO) para la Administración del Fondo por concepto de las aportaciones para el cumplimiento del programa del pasivo laboral.

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

INE o Instituto: Instituto Nacional Electoral.

JLE: Juntas Locales Ejecutivas.

JDE: Juntas Distritales Ejecutivas.

LGPDPSSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

PNT: Plataforma Nacional de Transparencia.

Reglamento de Datos Personales: Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales.

Unidad de Transparencia o UTTPDP: Unidad Técnica de Transparencia y Protección de Datos Personales.

⁴ Definiciones tomadas (Aramburu, 2008)

1 PRESENTACIÓN

La Unidad de Transparencia reconoce que la información que recaba, genera, procesa y resguarda, requiere ser tratada en estricto apego al marco legal aplicable durante todo su ciclo de vida y preservando, en todo momento, el derecho de protección de datos personales de todas las personas, incluyendo servidoras y servidores públicos del Instituto, el cual es responsabilidad de todos aquellos que en el estricto apego a sus funciones tratan esta información.

Para lograr lo anterior, la Unidad de Transparencia y las áreas responsables del Instituto participan en los siguientes procedimientos:

- Atención de las solicitudes de Acceso a la Información.
- Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO).

En la siguiente tabla se muestran los macroprocesos, procesos y subprocesos relacionados con ambos procedimientos.

Macroproceso	Proceso	Subproceso	Procedimiento
Gestión de Acciones de Transparencia, Acceso a la Información y Protección de Datos Personales	Administración de Transparencia y Acceso a la Información	Atención de las Solicitudes de Acceso a la Información	<i>Atención de las Solicitudes de Acceso a la Información</i>
	Protección de Datos Personales	Protección de Datos Personales	<i>Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO)⁵</i>

En función de ello, esta Unidad de Transparencia **presenta el Documento de Seguridad⁶** (en adelante Documento) que atiende a los procedimientos *Atención de las Solicitudes de Acceso a la Información* y *Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO)*.

El Documento está integrado por los apartados:

- Las funciones y obligaciones de las personas que tratan datos personales
- Inventario de datos personales y sus sistemas de tratamiento
- Resultados del Análisis de riesgos

⁵ Conforme al Manual de Proceso y Procedimientos de Protección de Datos Personales.

⁶ En cumplimiento al artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

- Resultados del Análisis de brecha
- Plan de trabajo para atender los hallazgos
- Mecanismos de monitoreo y revisión de las medidas de seguridad
- Programa general de capacitación

Para atender lo anterior se realizaron mesas de trabajo con las áreas involucradas en el tratamiento de datos personales de los procedimientos en mención de acuerdo con las siguientes etapas⁷:

- **Etapa Preliminar.** En esta etapa se llevó a cabo la identificación de la base de datos, persona propietaria y proceso.
- **Etapa 1.** Identificación del flujo de los datos personales. Esta etapa a su vez, se compone de cinco fases:
 - Fase 1. Identificación de datos personales
 - Fase 2. Identificación de mecanismos de obtención de datos personales
 - Fase 3. Identificación de medios de almacenamiento
 - Fase 4. Identificación de permisos y tratamiento
 - Fase 5. Identificación del ciclo de vida de los datos personales

Su propósito fue identificar los datos personales que componen la base, su clasificación, tipo, el personal que tiene acceso, los permisos otorgados y sus funciones y obligaciones, así como identificar y documentar el ciclo de vida de los datos personales.

- **Etapa 2.** Evaluación de medidas de seguridad. Esta etapa tuvo como finalidad la gestión del riesgo para identificar e implementar medidas de seguridad adecuadas a la categoría del dato personal para proteger los datos personales de una vulneración, a través de dos fases:
 - a. **Fase 1. Análisis de brecha.** Se identificaron medidas de seguridad físicas, técnicas y administrativas existentes, faltantes o, en su caso, el reforzamiento de las actuales.⁸
 - b. **Fase 2. Análisis de riesgos de datos personales y privacidad.** Se identifican los riesgos derivados del tratamiento de datos personales -al que están expuestos los datos personales en cada etapa de su ciclo de vida- para la posterior implementación o adecuación de las medidas de protección

⁷ Con base en lo establecido en la Estrategia para el Cumplimiento de los Deberes de Seguridad y Confidencialidad, del Programa para la Protección de los Datos Personales del Instituto Nacional Electoral.

⁸ Si bien, a la fecha, aún falta información que corresponde proporcionar a la Unidad Técnica de Servicios de Informática (UTSI), por lo que el Análisis de Brecha no se ha concluido, con la información obtenida es factible contar con la primera versión del Documento de seguridad.

o controles, y comprender los impactos de eventos temidos o no deseados en las personas, los grupos o la sociedad.⁹

- **Etapa 3.** Plan de Trabajo. En esta etapa se determinaron las acciones a realizar para la gestión del riesgo, a través de la implementación de las medidas de seguridad faltantes, las que serán sustituidas o reforzadas, con base en los resultados de la *Etapa 2*.¹⁰
- **Etapa 4.** Mejora continua. La Unidad de Transparencia incorporó los procedimientos referidos al Sistema de Gestión para la Protección de Datos Personales del Instituto Nacional Electoral, que permitirá verificar la seguridad en el tratamiento de los datos personales contenidos en los procedimientos *Atención de las Solicitudes de Acceso a la Información y Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO)*, resultando en una mejora periódica de sus controles.

2 MARCO NORMATIVO

- Artículos 6, Base A y 16, párrafo segundo de la Constitución de los Estados Unidos Mexicanos.
- Título Primero. Capítulo II. De la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Título Segundo. Capítulo II. De los Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Título Tercero. Capítulo II. Del Reglamento de Datos Personales.

En particular:

- Títulos Sexto y Séptimo de la Ley General de Transparencia y Acceso a la Información Pública.
- Título Tercero, Capítulo I y II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Título Quinto de la Ley Federal de Transparencia y Acceso a la Información Pública.
- Título Tercero, Capítulo II del Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública.
- Título Cuarto, Capítulos I, II y III del Reglamento de Datos Personales.

⁹ Falta información que la (UTSI) no ha proporcionado, por lo tanto, el Análisis de Riesgos no se ha concluido, sin embargo, con la ya obtenida es factible contar con la primera versión del documento de seguridad

¹⁰ Falta información que la (UTSI) no ha proporcionado, por lo tanto, el Plan de Trabajo no se ha concluido, sin embargo, con la ya obtenida es factible contar con la primera versión del documento de seguridad e iniciar la elaboración del plan de trabajo.

3 ALCANCE

El Documento de Seguridad contempla los procedimientos *Atención de las Solicitudes de Acceso a la Información y Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO)*.

4 ADMINISTRACIÓN DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

4.1 DESCRIPCIÓN DE LOS PROCEDIMIENTOS A NIVEL NEGOCIO

La Unidad de Transparencia es un área del Instituto entre cuyas atribuciones se encuentra la de gestionar las solicitudes de acceso a la Información y solicitudes para el ejercicio de los derechos ARCO, gestión que involucra el tratamiento de datos personales en la base de datos del sistema de gestión interno.

A partir del 2006 el otrora Instituto Federal Electoral (IFE), ahora Instituto Nacional Electoral (INE) contaba con un sistema para la recepción y trámite de solicitudes de acceso a la información y datos personales denominado “IFESAI”.

Con el fin de homologar su plataforma de gestión y así facilitar el ejercicio del derecho a la información, en 2008 el IFE, mediante un convenio de colaboración celebrado con el otrora Instituto Federal de Acceso a la Información Pública (IFAI), ahora Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), implementó el denominado INFOMEX-IFE¹¹; posteriormente, en 2014 se denominó al Sistema como “INFOMEX”, cuyo inicio data del 1 de abril de ese año.

Después, con la versión 6.0 y, a partir de ese momento, cambia la denominación a INFOMEX-INE y de aquí en adelante se ha reconocido como el sistema de gestión interna de solicitudes de información y de datos personales.¹²

En materia de acceso a la información, a partir del 6 de mayo de 2016, el INE se sumó al uso de los sistemas que conforman la PNT y el 1° de abril de 2018, la Unidad de Transparencia dejó de recibir solicitudes para el ejercicio de los derechos ARCO, a través del INFOMEX-INE, mismas que se comenzaron a atender a través de la PNT.

También es importante decir que, con el reconocimiento de nuevos sujetos obligados, el INE se hace cargo de dos fideicomisos sin estructura (Fideicomiso MAC y Fideicomiso Banjército). Las solicitudes que ingresan, mediante la PNT, a cualquiera de las cuentas de estos sujetos obligados, son almacenados en el sistema INFOMEX-INE.

¹¹ Información proporcionada por la Unidad Técnica de Servicios de Informática (UTSI) mediante oficio INE/UNICOM/4370/2021, en el que remite archivo denominado “01.información general”.

¹² Idem.

En este sentido, para la atención de las solicitudes de acceso a la información y para el ejercicio de los derechos ARCO, la UTTPDP realiza las siguientes actividades:

4.1.1 Atención de las Solicitudes de Acceso a la Información

Actividad	Responsable de la actividad
<p>Presentación de solicitud</p> <p>La persona solicitante puede realizar sus solicitudes de acceso a la información, a través de los siguientes medios:</p> <ul style="list-style-type: none"> • PNT • Correo electrónico • Oficialía de partes (por escrito libre) 	<p>La persona solicitante hasta el momento en que presenta la solicitud.</p>
<p>Migración y captura de solicitudes</p> <p>En caso de que la solicitud se realice en la PNT se migran al sistema INFOMEX-INE.</p> <p>Las solicitudes que ingresan por correo electrónico y oficialía de partes se registran de forma manual en el sistema INFOMEX-INE y posteriormente en la PNT.</p>	<p>UTTPDP</p>
<p>Procedencia de la solicitud</p> <ul style="list-style-type: none"> • En caso de que las áreas responsables consideren que falta información para atender la solicitud, por única ocasión se realiza un requerimiento (parcial o total) la persona solicitante, mismo que se notifica mediante número de control, ya sea a través de la PNT, correo electrónico, notificación personal y/o correo por electrónico y éste se deberá desahogar en el plazo de diez días hábiles posterior a la notificación. <p>El requerimiento total se registra en la PNT y el sistema INFOMEX-INE. En caso de no desahogar dicho requerimiento, la solicitud se tiene por no presentada (se desecha).</p> <p>Por lo que hace el requerimiento parcial si no es desahogado por la persona solicitante, el área o las áreas responsables del Instituto se tendrán que pronunciar por los puntos que no fueron requeridos.</p> <ul style="list-style-type: none"> • De haberse desahogado el requerimiento (total) se turna de nueva cuenta la solicitud al o las áreas responsables del Instituto que se estime tienen atribución para emitir respuesta. 	<p>Áreas responsables y la UTTPDP</p>
<p>Atención de solicitud</p> <p>Las áreas responsables analizan la solicitud, emiten la respuesta a través del sistema de gestión de solicitudes, actualmente INFOMEX INE</p>	<p>Áreas responsables, UTTPDP y Comité de Transparencia</p>

Actividad	Responsable de la actividad
<p>y, en su caso, envían archivos o ponen a disposición información realizando la cuantificación para el previo pago.</p> <p>Según el sentido de respuesta procede lo siguiente:</p> <p>No conoce el Comité de Transparencia:</p> <ul style="list-style-type: none"> • Pública: Se emite respuesta que contempla de manera íntegra todos los puntos de la solicitud. <p>Sí conoce el Comité de Transparencia:</p> <ul style="list-style-type: none"> • Incompetencia: Corresponde atender la solicitud a un sujeto obligado diverso al INE. • Inexistencia: El área responsable indica motivo de la inexistencia, así como circunstancias de modo tiempo y lugar de la búsqueda, ya que no localizó la información solicitada y funda y motiva la respuesta. • Clasificada como confidencial: Se protegen datos personales y el área responsable funda y motiva su respuesta • Clasificada por reserva: El área responsable emite la prueba de daño y el plazo de reserva, funda y motiva la reserva. 	
<p>Elaboración de la respuesta o resolución</p> <p>Se elabora la respuesta o resolución para la persona solicitante, de conformidad con la información proporcionada por el o las áreas responsables.</p>	<p>UTTyPDP</p>
<p>Notificación</p> <p>Se notifica la persona solicitante por el medio seleccionado, el cual puede ser:</p> <ul style="list-style-type: none"> • Correo electrónico • PNT • Estrados • Notificación personal en el domicilio otorgado por la persona solicitante. 	<p>UTTyPDP y en caso de notificaciones personales en domicilios fuera de la Ciudad de México se solicita apoyo al personal adscrito a las JLE de cada entidad federativa</p>
<p>Se concluye la solicitud</p> <ul style="list-style-type: none"> • Se notifica la respuesta a la persona solicitante por el medio seleccionado, a través de la PNT, y de permitir la capacidad de esta herramienta se adjuntan los archivos que remiten las áreas que atendieron la solicitud. • Se procede a dar de baja la solicitud en el Sistema INFOMEX-INE, adjuntando los archivos que remiten las áreas que atendieron. 	<p>UTTyPDP</p>
<p>Se concluye la solicitud</p>	<p>UTTyPDP</p>

Actividad	Responsable de la actividad
El expediente queda en el archivo de trámite de la UTTPDP y transcurrido el plazo para su guarda se traslada al Archivo Institucional.	

4.1.2 Atención de solicitudes para el ejercicio de los derechos ARCO

Actividad	Responsable de la actividad
<p>Presentación de solicitud</p> <p>El persona solicitante o titular de los datos personales puede realizar su solicitud de ejercicio de derechos ARCO, a través de los siguientes medios:</p> <ul style="list-style-type: none"> • PNT • Correo electrónico • Oficialía de partes (por escrito libre) 	<p>La persona solicitante hasta el momento en que presenta la solicitud.</p>
<p>Migración y captura de solicitudes</p> <p>Si la solicitud ingresa en la Plataforma Nacional de Transparencia (PNT), se migra al sistema de gestión interno actualmente INFOMEX-INE.</p> <p>Si la solicitud ingresa por correo electrónico y oficialía de partes se registra manualmente en el sistema de gestión interno actualmente INFOMEX-INE y en la PNT.</p>	<p>UTTPDP</p>
<p>Procedencia de la solicitud</p> <ul style="list-style-type: none"> • Se analiza la solicitud, se determina si alguna de las áreas del Instituto es competente para atenderla y se turna a las mismas. • De no ser el caso, se declara la notoria incompetencia, se concluye la solicitud y se integra el expediente. • En caso de considerar que falta información para poder atender la solicitud, por única ocasión y a petición del área que le fue turnada la solicitud, la UTTPDP previene a la persona solicitante para que proporcione elementos que permitan atender de manera óptima su solicitud. • La prevención se notifica vía correo electrónico y a través de la PNT, la persona solicitante deberá desahogar en el plazo de diez días hábiles posterior a su notificación. • En caso de no desahogar dicho requerimiento se concluye la solicitud (se desecha). • De ser el caso, el área a la que fue turnada la solicitud puede informar al ciudadano, a través de la UTTPDP, la existencia de un trámite específico a través del cual también se puede atender la solicitud. 	<p>UTTPDP y Áreas Responsables</p>

Actividad	Responsable de la actividad
<ul style="list-style-type: none"> La persona solicitante tendrá un plazo de cinco días hábiles posteriores a su notificación, para elegir por cual vía desea tramitar su solicitud. 	
<p>Atención de solicitud</p> <ul style="list-style-type: none"> Las áreas responsables analizan la solicitud y remiten la información con que cuentan a la UTyPDP. Los sentidos de respuesta pueden ser: <ul style="list-style-type: none"> - Procedencia - No procedencia - Incompetencia 	Áreas responsables
<p>Análisis de la respuesta</p> <ul style="list-style-type: none"> La UTyPDP analiza la respuesta proporcionada por el área responsable del Instituto. En su caso, formula un Requerimiento Intermedio de Información (RII) o Requerimiento de Aclaración (RA) al área responsable. 	UTyPDP
<p>Elaboración de la respuesta</p> <ul style="list-style-type: none"> La UTyPDP elabora la respuesta para la persona solicitante, de conformidad con la información proporcionada por el o las áreas responsables. 	UTyPDP
<p>Notificación</p> <ul style="list-style-type: none"> Si el titular tiene domicilio en la CDMX, la respuesta es entregada por personal de la UTyPDP, previa acreditación de la identidad del titular de los datos personales. Si el titular de los datos personales vive fuera de la CDMX, personal de las JLE y JDE acredite la personalidad del titular y hace entrega de la respuesta. La JLE y JDE, envían a la UTyPDP la cédula de notificación y los acuses correspondientes. En el caso de solicitudes de acceso a datos personales, la acreditación de la personalidad debe llevarse a cabo previo a la entrega de la información. En el caso de solicitudes de rectificación, cancelación y oposición la acreditación de la identidad es previo a ejecutar el ejercicio del derecho solicitado; sin embargo, para la entrega de la respuesta y los documentos que integran la misma, también debe acreditarse su identidad. 	UTyPDP, JLE y JDE de cada entidad federativa
<p>Se concluye la solicitud</p> <ul style="list-style-type: none"> La UTyPDP recibe las cédulas de notificación y procede a integrar el expediente. La UTyPDP concluye la solicitud en el INFOMEX-INE y en la PNT. 	UTyPDP

4.2 DIAGRAMA A BLOQUES

4.2.1 Diagrama de bloques. Procedimiento Atención de las Solicitudes de Acceso a la Información

La figura 1 muestra el diagrama a bloques del procedimiento, para su mejor visualización consultar el Anexo I.

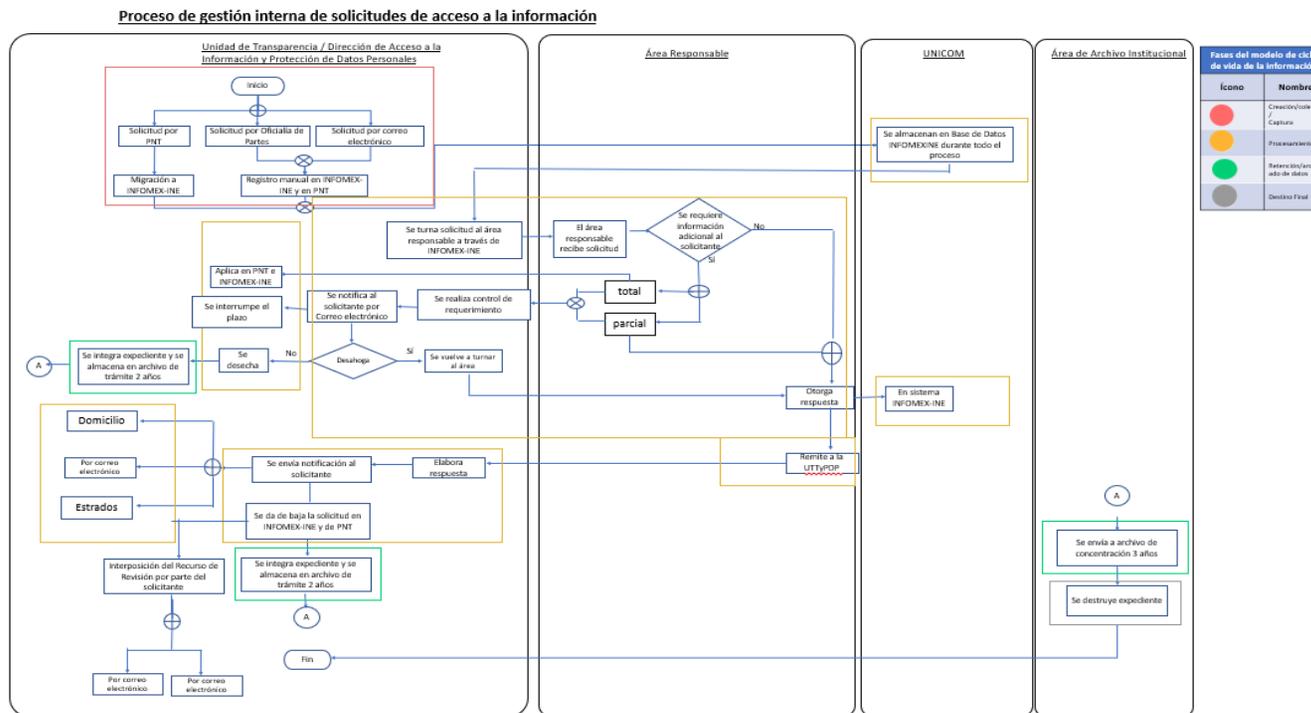


Figura 1. Diagrama a bloques Atención de las Solicitudes de Acceso a la Información

4.2.2 Diagrama de bloques. Procedimiento Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO)

Las figuras 2 y 3 muestran el diagrama a bloques del procedimiento, para su mejor visualización consultar el Anexo II.

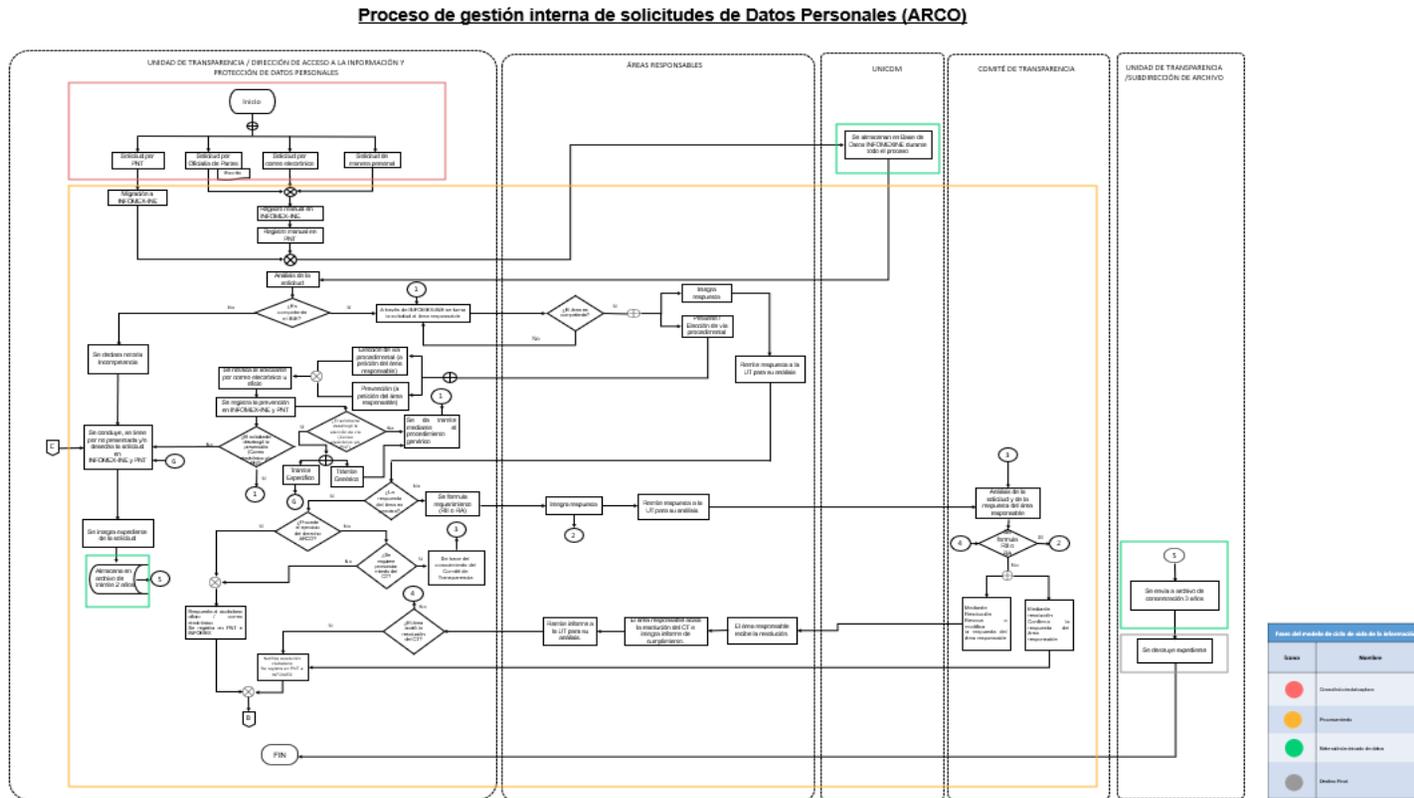


Figura 2. Diagrama a bloques Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO)

5 PERSONA QUE FUNGE EL ROL PROPIETARIO

Seudónimo de la Base de datos	Nombre de la persona propietaria de la base de datos	Cargo que ocupa
INFOMEX-INE	Ivette Alquicira Fontes	Directora de Acceso a la Información y Protección de Datos Personales

6 FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES

Las funciones y obligaciones de quienes intervienen en cualquier parte del tratamiento de los datos personales durante su ciclo de vida se muestran en la siguiente tabla:

Función (Perfil / Rol)	Cargo que ocupa	Obligaciones
Usuarios (UT-Gestión- Comité de Transparencia)	Analista de Protección de Datos Personales	<ul style="list-style-type: none"> Utilizar los datos personales para la finalidad para la que fueron recabados. Cumplir con las políticas de seguridad. Mantener la confidencialidad de la información. Rendir cuentas a la persona que funge el rol propietario.¹³ Gestionar las solicitudes de acceso a la información y para el ejercicio de los derechos ARCO. Implementar mecanismos que propicien y faciliten el desahogo del procedimiento de acceso a la información y de recursos de revisión, así como la atención de solicitudes de protección de datos personales, para el cumplimiento de la normativa aplicable.¹⁴ Orientar a las áreas del Instituto, para la mejora continua de los mecanismos que se implementan en el ejercicio del derecho
	Auxiliar de Protección de Datos Personales	
	Asistente Proyectista Jurídico	
	Especialista de Acceso a la Información y Protección de Datos Personales	
	Asistente jurídico	
	Auxiliar de Gestión de Solicitudes	
	Asistente Proyectista de Acceso a la Información	
	Asistente Proyectista de Acceso a la Información "A"	
	Analista Jurídico de Proyectos de Órganos de Transparencia	
	Jefe de Departamento de Protección de Datos Personales, Consulta y Vinculación	

¹³ No aplica para solicitudes de Acceso a la Información.

¹⁴ No aplica para solicitudes de Acceso a la Información

Función (Perfil / Rol)	Cargo que ocupa	Obligaciones
	Jefe de Departamento de Análisis y Seguimiento Jefe de Departamento de Apoyo Jurídico y Auxiliar del Comité de Transparencia Subdirector de Protección de Datos Personales Subdirectora de Acceso a la Información Integrantes del Comité de Transparencia Directora de Acceso a la Información y Protección de Datos Personales	de acceso a la información y protección de datos personales. <ul style="list-style-type: none"> Orientar a las personas, en relación con las solicitudes de acceso a la información y protección de datos personales para garantizar el ejercicio efectivo de sus derechos Efectuar la habilitación de las y los servidores públicos del Instituto en el sistema interno para la gestión de solicitudes de acceso a la información y de protección de datos personales, para el desahogo del procedimiento correspondiente. Asesorar a las personas interesadas, al personal y a quienes presten sus servicios al Instituto en el uso de las herramientas informáticas para el trámite de solicitudes de acceso a la información y protección de datos personales, a fin de otorgar los mecanismos que faciliten el ejercicio de ese derecho. Brindar capacitación en materia de acceso a la información y protección de datos personales a las áreas del Instituto, para transmitir el conocimiento que les permita cumplir con la normativa. Verificar la integración, consulta y resguardo de los expedientes que se generen, con motivo de la presentación de solicitudes de acceso a la información y protección de datos personales, para mantener el orden en las constancias generadas.
Administrador	Especialista en Acceso a la Información y Datos Personales Jefe de Departamento de Protección de Datos Personales, Consulta y Vinculación Jefe de Departamento de Análisis y Seguimiento Subdirector de Protección de Datos Personales Subdirección de Acceso a la Información Directora de Acceso a la Información y Protección de Datos Personales	<ul style="list-style-type: none"> Utilizar los datos personales para la finalidad para la que fueron recabados. Cumplir con las políticas de seguridad. Mantener la confidencialidad de la información. Actualizar información Retira turnos Realiza turnos al registrar una solicitud de información Realiza altas y bajas de los usuarios del sistema

Función (Perfil / Rol)	Cargo que ocupa	Obligaciones
Área responsable	Enlaces Propietarios Enlaces Suplentes	<ul style="list-style-type: none"> • Utilizar los datos personales para la finalidad para la que fueron recabados. • Cumplir con las políticas de seguridad. • Mantener la confidencialidad de la información. • Rendir cuentas a la persona que funge el rol propietario. • Otorgar respuesta a las solicitudes de acceso a la información y/o protección de datos personales que le son turnadas.

7 INVENTARIO

Este apartado presenta el inventario de los datos personales que se tratan en los procedimientos señalados en el alcance, relacionándolos con información básica de su tratamiento, como su tipo y categorización -estándar, sensible o especial-, los sitios, medios, soportes documentales y formatos que se utilizan para su almacenamiento y resguardo. Además, identifica al personal involucrado durante el tratamiento -incluyendo a los encargados, personas destinatarias o terceras personas-.

La base de datos de INFOMEX almacena¹⁵ **21¹⁶ datos personales** de 34,893 titulares, siendo 29,834 de Solicitudes de Acceso a la Información y 5,059 de Solicitudes ARCO,¹⁷ de acuerdo con lo siguiente:

Medios de obtención	Finalidad o finalidades del tratamiento	Formatos de almacenamiento y ubicación de los datos personales	Personal que tiene acceso a los sistemas de tratamiento (cargos)	Encargados del tratamiento de datos personales	Destinatarios o terceros receptos de transferencia	¿Se realiza la difusión de datos personales?
<p>Los datos personales tratados, son obtenidos por los siguientes medios</p> <p>Digitales</p> <ul style="list-style-type: none"> • PNT • Correo electrónico <p>Físicos</p>	<p>Los datos son recabados para las siguientes finalidades:</p> <ul style="list-style-type: none"> • Registrar y gestionar internamente las solicitudes de acceso a la información, de ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (derechos ARCO), recursos de revisión y realizar notificaciones y seguimiento a las personas persona solicitantes. • Generar información estadística para la integrar los informes en materia de transparencia, acceso a la información pública y protección de 	<p>Los sitios y medios de almacenamiento de los datos personales son los siguientes:</p> <p>Sitios de resguardo</p> <ul style="list-style-type: none"> • Oficina de la Dirección de Acceso a la Información y Protección de Datos Personales • Centros de Cómputo y Operaciones (CCO) Tlalpan • Sistema de Archivos Institucional • Archivo Institucional <p>Medios de almacenamiento físico</p> <ul style="list-style-type: none"> • Escritorio/Cajones • Archiveros 	<ul style="list-style-type: none"> • Integrantes del Comité de Transparencia • Enlaces Propietarios y Suplentes de Transparencia y de Protección de Datos Personales • Directora de Acceso a la Información y Protección de Datos Personales • Subdirector de Protección de Datos Personales • Subdirectora de Acceso a la Información • Jefe de Departamento de Análisis y Seguimiento 	<p>No cuenta con encargados para el tratamiento de datos personales</p>	<p>No realizan transferencias de datos personales, salvo aquellas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados</p>	<p>No hacen difusión de datos personales.</p>

¹⁵ Información que obra en el Diccionario de datos proporcionado por la Unidad Técnica de Servicios de Informática (UTSI) y en términos del Archivo de solicitudes txt denominado Layout, remitido por el INAI.

¹⁶ De los 21 datos personales almacenados en INFOMEX, para la atención de solicitudes de acceso a la información se utilizan solo 20 y para la atención de solicitudes para el ejercicio de derechos ARCO se utilizan 21, siendo la CURP el dato que hace la diferencia.

¹⁷ El total de titulares es información proporcionada por la Unidad Técnica de Servicios de Informática (UTSI) mediante archivo adjunto al oficio INE/UTSI/02838/2022 fechado el 12 de septiembre de 2022.

Medios de obtención	Finalidad o finalidades del tratamiento	Formatos de almacenamiento y ubicación de los datos personales	Personal que tiene acceso a los sistemas de tratamiento (cargos)	Encargados del tratamiento de datos personales	Destinatarios o terceros receptos de transferencia	¿Se realiza la difusión de datos personales?
<ul style="list-style-type: none"> Oficialía de partes (escrito libre) 	<p>datos personales, que presenta la Unidad Técnica de Transparencia y Protección de Datos Personales ante diversos órganos colegiados del INE y ante el organismo garante en materia de transparencia, acceso a la información y protección de datos personales.</p>	<ul style="list-style-type: none"> Carpetas/Organizadores Cajas <p>Medios de almacenamiento digital</p> <ul style="list-style-type: none"> Computadoras de escritorio Servidores del Instituto Sistema de Archivo Institucional 	<ul style="list-style-type: none"> Jefe de Departamento de Apoyo Jurídico y Auxiliar del Comité de Transparencia Jefe de Departamento de Protección de Datos Personales, Consulta y Vinculación Especialista de Acceso a la Información y Protección de Datos Personales Auxiliar de Gestión de Solicitudes Asistente Proyectista de Acceso a la Información Analista Jurídico de Proyectos de Órganos de Transparencia Asistente Proyectista Jurídico Auxiliar de Protección de Datos Personales Analista de Protección de Datos Personales 			

La base de datos INFOMEX almacena 20 datos personales de las Solicitudes de Acceso a la información y 21 de Solicitudes para el ejercicio de derechos ARCO. A continuación, se listan los datos que son tratados por cada procedimiento.

Atención de las Solicitudes de Acceso a la Información	Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO)
<p>15 datos personales estándar:</p> <ul style="list-style-type: none"> ▪ 12 identificación y contacto: nombre/s, apellidos (paterno y materno), correo electrónico, nacionalidad, domicilio particular (calle, numero exterior, numero interior, colonia, país, estado, delegación/municipio, código postal), teléfono fijo o móvil con clave lada, fecha de nacimiento (año), nombre del representante, apellido paterno del representante, apellido materno del representante, edad. ▪ 2 laborales: Ámbito de ocupación, ocupación. ▪ 1 Académicos: Nivel educativo. <p>5 datos personales sensibles:</p> <ul style="list-style-type: none"> ▪ 2 Origen étnico: Lengua Indígena. ▪ 1Salud: Manifestación de alguna discapacidad y/o especificaciones de las preferencias de accesibilidad. ▪ 1 Económicos: Estatus socioeconómico. ▪ 1 Afecta a la esfera íntima del titular: Género 	<p>16 datos personales estándar:</p> <ul style="list-style-type: none"> ▪ 13 Identificación y contacto: nombre/s, apellidos (paterno y materno), correo electrónico, año de nacimiento, nacionalidad, CURP, domicilio particular (calle, numero exterior, numero interior, colonia, país, estado, delegación/municipio, código postal), teléfono fijo o móvil con clave lada, fecha de nacimiento, nombre del representante, apellido paterno del representante, apellido materno del representante, edad. ▪ 2 Laborales: Ámbito de ocupación, ocupación. ▪ 1 Académicos: Nivel de estudios. <p>5 datos personales sensibles:</p> <ul style="list-style-type: none"> ▪ 2 Origen étnico: Lengua Indígena, Comunidad indígena. ▪ 1Salud: Manifestación de alguna discapacidad y/o especificaciones de las preferencias de accesibilidad. ▪ 1 Económicos: Estatus socioeconómico. ▪ 1 Afecta a la esfera íntima del titular: Género
Sistema de tratamiento	
El sistema que trata la base de datos INFOMEX es INFOMEX-INE, versión 12.0.	

8 CICLO DE VIDA DE LOS DATOS PERSONALES

8.1 OBTENCIÓN

Los datos personales se obtienen directamente de la persona titular, o bien, a través de su representante:

- **PNT:** La persona solicitante o titular ingresa su solicitud, a través de la PNT, por lo que personal autorizado de la Dirección de Acceso a la Información y Protección de Datos Personales, ingresa a la PNT realiza la descarga de un archivo .txt y los documentos que se hayan adjuntado en la solicitud, los archivos son guardados en el equipo del personal y posteriormente realizan la carga de los mismos al sistema INFOMEX-INE.

Conviene señalar que la PNT es una herramienta que administra otra autoridad y al INE, como sujeto obligado, le asignan cuentas para su uso. Por ello, cuando las solicitudes ingresan a través de dicho medio, el INE no capta de origen los datos personales, sino que los recibe de forma indirecta.

- **Correo electrónico:** La persona solicitante o titular ingresa su solicitud, mediante correo electrónico a cuentas oficiales del Instituto, por lo que el área que recibió la solicitud debe remitirla a la Unidad de Transparencia, con la finalidad de que sea atendida. Se ingresa la solicitud al sistema INFOMEX-INE y de manera posterior se captura en la PNT, sin embargo, los datos personales que pudiese traer la misma no quedan en el equipo de cómputo del personal autorizado para ingresar la solicitud.
- **Oficialía de partes:** La persona solicitante o titular ingresa un escrito en el que consta su solicitud a la oficialía de partes de cualquier área del INE, el escrito es remitido a la UTTPDP para su atención. Y dicha solicitud se escanea por el personal autorizado para ingresar la solicitud quien la captura en el sistema INFOMEX-INE y de manera posterior en la PNT.

8.2 ALMACENAMIENTO DE LOS DATOS PERSONALES

- Los datos personales son almacenados de la siguiente forma:

Espacio	Física	Digital
instalaciones de la Unidad de Transparencia	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Servidor ubicado en el Centros de Cómputo y Operaciones (CCO) Tlalpan	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Sistema de Archivos Institucional	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Archivo Institucional	<input checked="" type="checkbox"/>	<input type="checkbox"/>

8.3 USO DE LOS DATOS PERSONALES

Los datos son recabados o recibidos para las siguientes finalidades:

- Registrar y gestionar internamente las solicitudes de acceso a la información, de ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (derechos ARCO) y realizar notificaciones y seguimiento a las personas persona solicitantes.

- Generar información estadística para integrar los informes en materia de transparencia, acceso a la información y protección de datos personales, que presenta la Unidad Técnica de Transparencia y Protección de Datos Personales ante diversos órganos colegiados del INE y ante el organismo garante en materia de transparencia, acceso a la información y protección de datos personales.

8.4 DIVULGACIÓN DE LOS DATOS PERSONALES CONSIDERANDO LAS REMISIONES Y TRANSFERENCIAS

No realizan transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.

8.5 BLOQUEO DE LOS DATOS PERSONALES

El área responsable no cuenta, a la fecha, con reglas de bloqueo de los datos personales, por lo que no se ha ejecutado la acción. Sin embargo, es una actividad que se tiene contemplada como una prioridad.

8.6 CANCELACIÓN, SUPRESIÓN O DESTRUCCIÓN DE LOS DATOS PERSONALES

Atendiendo a lo establecido en el Catálogo de Disposición Documental, las secciones relacionadas con los procedimientos son las siguientes:

Procedimiento	Sección Catálogo Disposición Documental 2018 - 2021	Sección Catálogo Disposición Documental 2022
Atención de las Solicitudes de Acceso a la Información	12.5 Solicitudes de Acceso a la Información y de Datos Personales. Tiempo de conservación: 5 años. Destino final: baja. -supresión de los registros en base de datos y destrucción de la información en papel-	8C-3 Atender Solicitudes de Acceso a la Información. Tiempo de conservación: 5 años. Destino final: baja. -supresión de los registros en base de datos y destrucción de la información en papel-
Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO)	12.5 Solicitudes de Acceso a la Información y de Datos Personales. Tiempo de conservación: 5 años. Destino final: baja. -supresión de los registros en base de datos y destrucción de la información en papel-	8C-4 Atender solicitudes de Derechos ARCO. Tiempo de conservación: 5 años. Destino final: baja. -supresión de los registros en base de datos y destrucción de la información en papel-

9 DIAGRAMA DE FLUJO DE LOS DATOS PERSONALES

9.1.1 Diagrama de flujo. Procedimiento Atención de las Solicitudes de Acceso a la Información

La figura 4 muestra el diagrama de flujo del procedimiento, para su mejor visualización consultar el Anexo III.

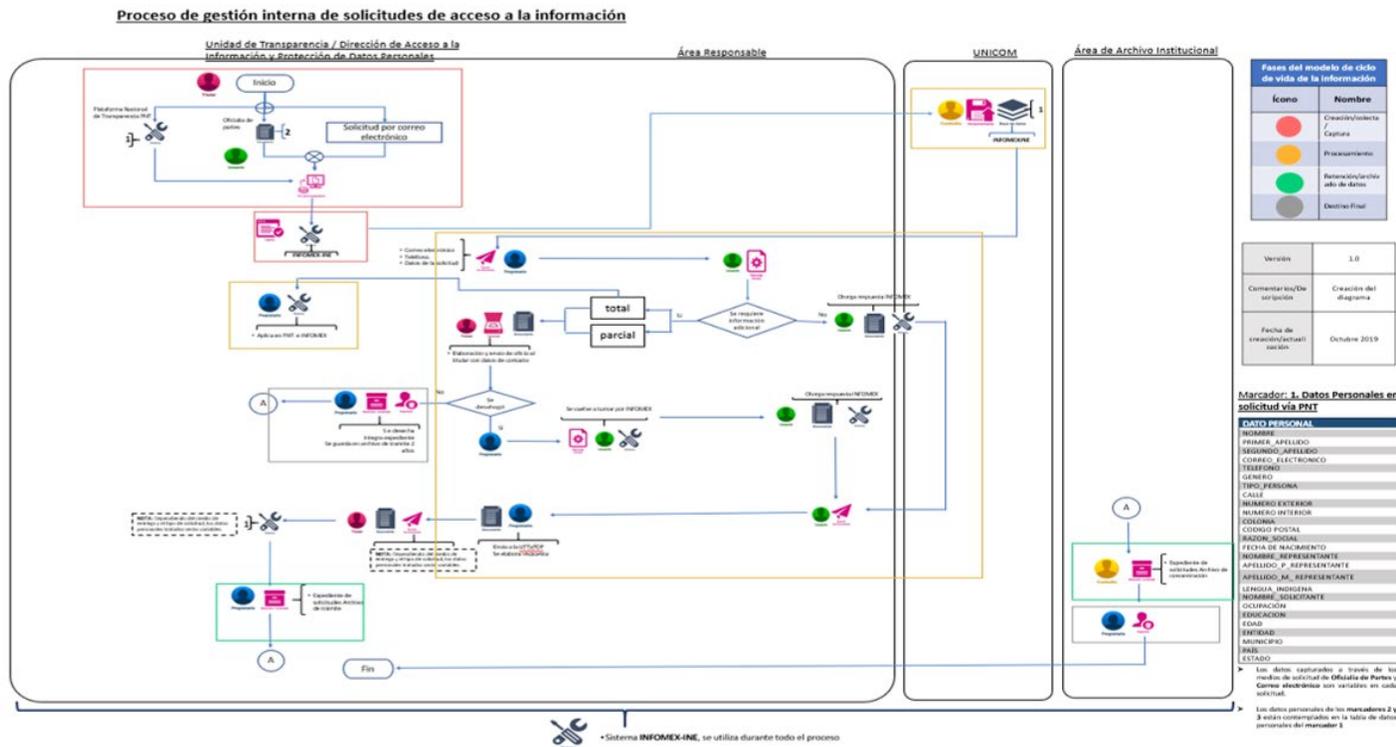


Figura 4. Diagrama de flujo. Atención de las Solicitudes de Acceso a la Información

9.1.2 Diagrama de flujo. Procedimiento Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO)

Las figuras 5 y 6 muestran el diagrama de flujo del procedimiento, para su mejor visualización consultar el Anexo IV.

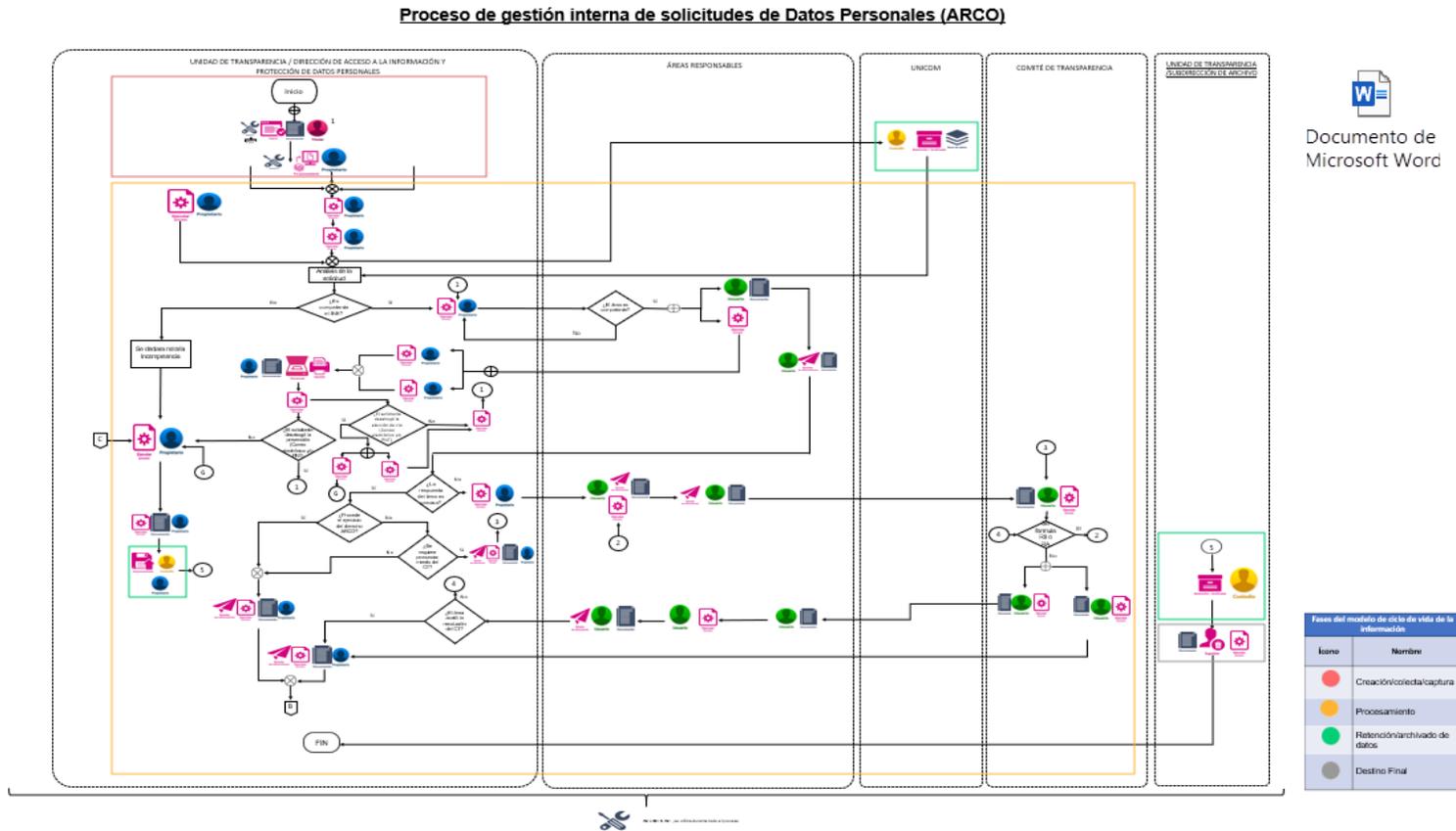


Figura 5. Diagrama de flujo. Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO)

Proceso de gestión interna de solicitudes de Datos Personales (ARCO)

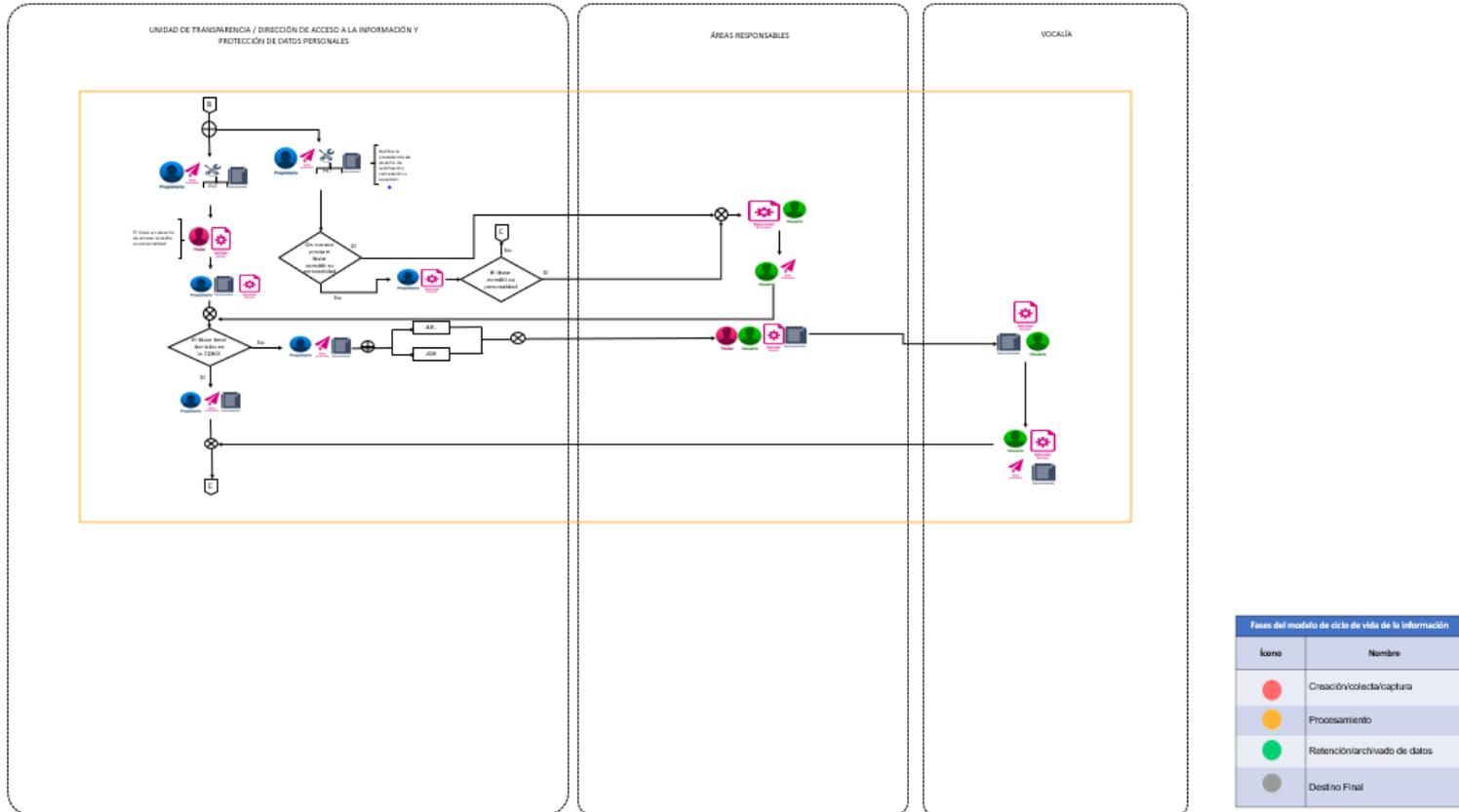


Figura 6. Diagrama de flujo. Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO)

10 ANÁLISIS DE RIESGOS

10.1 RIESGOS INHERENTES DE LOS DATOS PERSONALES

Atendiendo a la *Metodología de Análisis de Riesgos de Privacidad y Datos Personales*¹⁸ se identifica el riesgo inherente de los datos personales de acuerdo con su criticidad.

- I. **Bajo.** Considera información general como datos de identificación y contacto o información académica o laboral.
- II. **Medio.** Contempla los datos:
 - a. De ubicación física,
 - b. De patrimonio,
 - c. De autenticación,
 - d. Jurídicos.
- III. **Alto.** Datos personales que puedan dar origen a discriminación o conlleven un riesgo grave a la integridad del titular.
- IV. **Reforzado.** Son todos los considerados datos especiales.

Dato personal	Riesgo inherente
1. Nombre/s	Bajo
2. Apellidos (paterno y materno)	Bajo
3. Correo electrónico	Bajo
4. Año de nacimiento	Bajo
5. Nacionalidad	Bajo
6. Género	Alto
7. CURP*	Bajo
8. Domicilio particular (calle, número exterior, número interior, colonia, país, estado, delegación/municipio, código postal)	Bajo
9. Teléfono fijo o móvil con clave lada	Bajo
10. Fecha de nacimiento	Bajo
11. Nombre del representante	Bajo
12. Apellido paterno del representante	Bajo
13. Apellido materno del representante	Bajo
14. Edad	Bajo
15. Ámbito de ocupación	Bajo

¹⁸ Desarrollada por la Unidad Técnica de Transparencia y Protección de Datos Personales del INE.

Dato personal	Riesgo inherente
16. Ocupación	Bajo
17. Nivel educativo	Bajo
18. Lengua indígena	Alto
19. Comunidad indígena	Alto
20. Manifestación de alguna discapacidad y/o especificaciones de las preferencias de accesibilidad	Alto
21. Estatus socioeconómico.	Alto

*Nota: Solo aplica para solicitudes de derechos ARCO.

10.2 ANÁLISIS DE RIESGOS DE PRIVACIDAD Y DATOS PERSONALES

El análisis de riesgos abarcó los activos relacionados con los procedimientos de *Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO) y Atención de las Solicitudes de Acceso a la Información.*

Resultado del análisis de riesgos se detectó que el área responsable debe reforzar las acciones relacionadas con la puesta a disposición del aviso de privacidad¹⁹ y el destino final de los datos personales para tratar los riesgos identificados en el tratamiento al que están expuestos los datos personales.

11 ANÁLISIS DE BRECHA

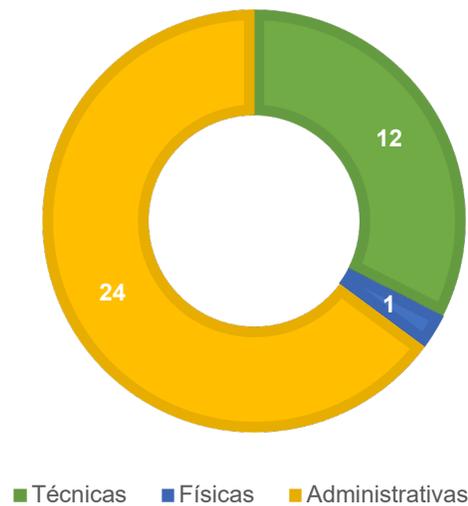
El análisis de brecha fue aplicado a los activos secundarios que intervienen en el tratamiento de los datos personales con base en los controles de seguridad establecidos en el estándar internacional ISO/IEC 27002:2013²⁰.

Actualmente se cuenta con **37** medidas de seguridad implementadas

¹⁹ Acción realizada por la Subdirección de Acceso a la Información.

²⁰ El análisis de brecha se ejecuta con base en la metodología del Análisis de Brecha desarrollada por la Unidad de Transparencia y Protección de Datos Personales.

Gráfica 1. Medidas de seguridad implementadas



A continuación, se listan los 46 controles²¹ a los que corresponden dichas medidas.

- Roles y responsabilidades en seguridad de la información (*)
- Segregación de tareas
- Contacto con las autoridades
- Contacto con grupos de interés especial
- Seguridad de la información en la gestión de proyectos
- Trabajo a distancia (*)
- Investigación de antecedentes
- Términos y condiciones del empleo
- Responsabilidades de gestión
- Proceso disciplinario (*)
- Responsabilidades ante la finalización o cambio
- Acceso a las redes y a los servicios de red
- Revisión de los derechos de acceso de usuario
- Eliminación o reasignación de los derechos de acceso
- Sistema de gestión de contraseñas
- Control de acceso al código fuente de los programas
- Instalaciones de suministro (Centros de cómputo)
- Seguridad del cableado (Centros de cómputo)

²¹ Categorías a través de las cuales se seleccionan las medidas de seguridad para el aseguramiento de los datos personales.

(*) Corresponde a la UTSI en conjunto con la UTyPDP.

- Mantenimiento de equipo
- Política de lugar de trabajo/escritorio limpio
- Documentación de procedimientos operacionales
- Gestión de capacidades
- Separación de los ambientes de desarrollo, prueba y operación
- Sincronización del reloj
- Controles de auditoría de sistemas de información
- Controles de red
- Seguridad de los servicios de red
- Segregación en redes
- Mensajería electrónica
- Análisis y especificaciones de requisitos de seguridad de la información
- Aseguramiento de los servicios de aplicaciones en redes públicas
- Revisión técnica de las aplicaciones después de efectuar cambios en el sistema operativo
- Pruebas funcionales de seguridad de sistemas
- Pruebas de aceptación de sistemas
- Política de seguridad de la información en las relaciones con los proveedores
- Responsabilidades y procedimientos
- Notificación de eventos de seguridad de la información
- Notificación de puntos débiles de la seguridad
- Evaluación y decisión sobre los eventos de seguridad de información
- Respuesta a incidentes de seguridad de la información
- Aprendizaje de los incidentes de seguridad de la información
- Recopilación de evidencias
- Disponibilidad de los recursos
- Identificación de la legislación aplicable y de los requisitos contractuales
- Derechos de Propiedad Intelectual (DPI)
- Cumplimiento de las políticas y normas de seguridad

Además, el área responsable programará la mejora en conjunto con la UTSI o, en su caso, la implementación de medidas de seguridad asociadas con 58 controles de acuerdo con los planes de trabajo de las áreas responsables, mismas que se listan a continuación:

- Políticas para la seguridad de la información *
- Revisión de las políticas para la seguridad de la información *
- Política de uso de dispositivos para movilidad *
- Concienciación, educación y capacitación en seguridad de la información *
- Inventario de activos
- Propiedad de los activos
- Uso aceptable de los activos
- Devolución de activos

- Clasificación de la información
- Etiquetado de la información
- Manejo de la información
- Eliminación de medios
- Medios físicos en tránsito
- Política de control de acceso
- Registro y baja de usuario *
- Gestión de acceso de usuario
- Gestión de acceso de usuarios con privilegios especiales
- Gestión de la información secreta de autenticación de los usuarios
- Uso de la información secreta de autenticación
- Restricción de acceso a la información
- Procedimientos seguros de inicio de sesión
- Uso de herramientas y administración de sistemas *
- Perímetro de seguridad física
- Controles físicos de entrada
- Seguridad de oficinas, salas y recursos
- Protección contra las amenazas externas y ambientales
- El trabajo en áreas seguras
- Áreas de carga y entrega
- Emplazamiento y protección de equipo
- Retirada de activos secundarios propiedad del Instituto
- Seguridad de los equipos fuera de las instalaciones
- Reutilización o eliminación segura de equipos
- Equipo de usuario desatendido
- Gestión de cambios *
- Controles contra el código malicioso *
- Copias de seguridad de la información *
- Registro de eventos *
- Protección de la información del registro de accesos *
- Registros de administración y operación *
- Instalación del software en ambientes de producción *
- Gestión de las vulnerabilidades técnicas *
- Restricción de la instalación de software *
- Políticas y procedimientos de intercambio de información
- Acuerdos de intercambio de información
- Acuerdos de confidencialidad o no revelación
- Protección de las transacciones de servicios de aplicaciones *
- Política de desarrollo seguro *
- Procedimiento de control de cambios en sistemas *
- Principios de ingeniería de sistemas seguros *

- Entorno de desarrollo seguro
- Protección de los datos de prueba
- Planificación de la continuidad de la seguridad de la información
- Implementar la continuidad de la seguridad de la información
- Verificación, revisión y evaluación de la continuidad de la seguridad de la información
- Protección de los registros de la organización
- Protección y privacidad de la información personal
- Revisión independiente de la seguridad de la información
- Comprobación del cumplimiento técnico ^{*22}

12 PLAN DE TRABAJO

A continuación, se integra el plan de trabajo que contiene las acciones a implementar de acuerdo con los resultados del análisis de brecha y riesgos.²³

No.	Actividad
1	Complementar el inventario de activos.
2	Reforzar la propiedad y devolución de los activos.
3	Robustecer la clasificación de la información.
4	Fortalecer el etiquetado y manejo de información.
5	Regularizar la eliminación de medios.
6	Reforzar los medios físicos en tránsito.
7	Robustecer el control de acceso.
8	Mejorar la gestión de acceso de usuarios con privilegios especiales.
9	Fortalecer la gestión y uso de la información secreta de autenticación.
10	Consolidar las políticas y procedimientos de intercambio de información.
11	Actualizar los acuerdos de confidencialidad.
12	Robustecer la protección de los datos de prueba.
13	Mejorar la continuidad de la seguridad de la información y la disponibilidad de los recursos.

²² *. La implementación de los controles corresponde a la UTSI.

²³ Lo cual no es determinante, debido a que el análisis de brecha no está concluido.

No.	Actividad
14	Afianzar la protección de los registros.
15	Revisar la seguridad de la información que contenga datos personales.
16	Fortalecer la protección y privacidad de la información personal
17	Reforzar las acciones relacionadas con el destino final de los datos personales.
18	Fortalecer la puesta a disposición del aviso de privacidad.

13 MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

El Instituto lleva a cabo un proceso de mejora continua que permite verificar la seguridad y confidencialidad en el tratamiento de los datos personales, en aras de una mejora periódica de sus controles.

El monitoreo y revisión²⁴ del cumplimiento se realiza a través del Sistema de Gestión para la Protección de los Datos Personales del Instituto Nacional Electoral²⁵ (SiPRODAP), con apoyo de la Plataforma para la Medición, Evaluación y Monitoreo del Cumplimiento en Protección de Datos Personales (PEC).

El PEC es una herramienta informática a través de la cual la Unidad de Transparencia da seguimiento a la implementación del Catálogo de Controles²⁶ del SiPRODAP, de manera documentada, sistematizada, estructurada, repetible, eficiente y adaptada al entorno institucional, conforme a lo establecido en la LGPDPPSO.

Ambos procedimientos forman parte del SiPRODAP desde el 27 de septiembre de 2021. En el Anexo V y VI contiene las Solicitudes de registro al SiPRODAP de ambos procedimientos.

14 PROGRAMA GENERAL DE CAPACITACIÓN

De conformidad con lo establecido en el *Programa de Capacitación y Sensibilización del Instituto Nacional Electoral, en Materia de Transparencia, Acceso a la Información, Protección de Datos Personales y Gestión Documental* emitido anualmente, la Unidad de Transparencia elaboró el Curso de protección de Datos Personales.

Este curso tiene por objetivo especializar a las personas servidoras públicas en materia de protección de datos personales -de acuerdo con sus roles y funciones- en cumplimiento al artículo 30, fracción III de la LGPDPPSO.

Para tal fin la Unidad de Transparencia elaboró el “*Diseño curricular para la capacitación en materia de Protección de Datos Personales del Instituto*” (en adelante Diseño curricular) compuesto por 12 módulos que, en su conjunto, tienen una duración de 82 horas.

Los resultados de las capacitaciones se detallan en los siguientes apartados.

²⁴ En cumplimiento a los artículos 35, fracción VI de la LGPDPPSO y 63 de los LGPDSP.

²⁵ Aprobado por el Comité de Transparencia, mediante acuerdo INE-CT-ACG-PDP-001-2019

²⁶ Apartado del SiPRODAP conformado por controles para la protección de datos personales.

14.1 CURSOS VIRTUALES

De acuerdo con el Diseño curricular, la Unidad de Transparencia invitó a su personal a cursar -a través del Centro Virtual INE- los módulos relacionados con capacitación especializada en materia de datos personales.

A continuación, se muestra el total del personal que acreditó los módulos.



Figura 7. Personal acreditado en cursos virtuales

14.2 CURSOS PRESENCIALES

De manera adicional, para que las áreas u órganos del Instituto responsables cuenten con la capacitación especializada referente a los Deberes de Seguridad y Confidencialidad y en particular para la conformación del Documento de Seguridad, el personal involucrado acreditó los siguientes cursos presenciales impartidos por la Unidad de Transparencia:

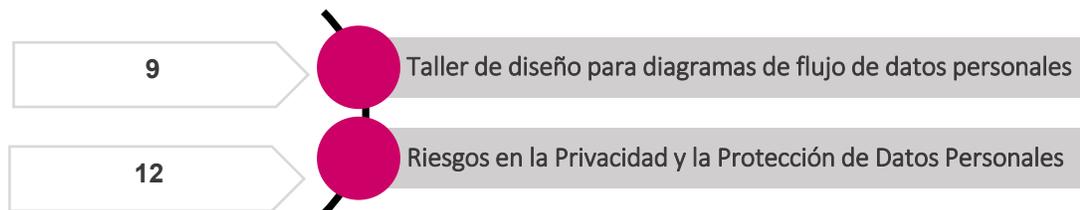


Figura 8. Personal acreditado en cursos presenciales

14.3 CURSOS IMPARTIDOS POR EL INAI

Como parte de las actividades implementadas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en materia de Protección de Datos Personales, el personal involucrado acreditó los cursos siguientes:



Figura 9. Personal acreditado en cursos impartidos por el INAI

15 ANEXOS

Anexo Número	Descripción	Archivo
Anexo I	Diagrama a bloques Atención de las Solicitudes de Acceso a la Información	 Anexo 1.pptx
Anexo II	Diagrama a bloques Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO)	 Anexo%20II.pptx
Anexo III	Diagrama de flujo Atención de las Solicitudes de Acceso a la Información	 Anexo%20III.pptx
Anexo IV	Diagrama de flujo Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO)	 Anexo%20IV.pptx
Anexo V	Solicitud de registro al SIPRODAP del procedimiento de Atención de las Solicitudes de Acceso a la Información	 Registro_SiPRODAP SAI.pdf
Anexo VI	Solicitud de registro al SIPRODAP del procedimiento de Atención de solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO).	 Registro_SiPRODAP.pdf

