DOCUMENTO DE SEGURIDAD

DE TRANSPARENCIA DE LA GESTIÓN

Área Responsable: Órgano Interno de Control

INE-CT-PDP-DOC_SEG-002-2022

Versión: 2.0

Fecha de presentación: 1 de diciembre de 2022

Fecha de última actualización: 29 de junio de 2023

Instituto Nacional Electoral

DOCUMENTO DE SEGURIDAD

Órgano Interno de Control

Unidad de Evaluación, Normatividad y Desarrollo Administrativo

Proceso: Transparencia de la gestión

Base de datos: BD-SIAER

Versión 2.0

Junio 2023

CONTROL DE VERSIONES

VERSIÓN	COMENTARIO / DESCRIPCIÓN	RESPONSABLE DE LA ACTUALIZACIÓN / CREACIÓN / REVISIÓN	FECHA DE ACTUALIZACIÓN / CREACIÓN / REVISIÓN
1.0	Creación del documento	Adolfo Romero Alvario	Septiembre 2022
1.0	Revisión del documento	Samuel Espinosa García	Octubre 2022
1.0	Aprobación del documento	Jesús Mazariegos Aguilar	Noviembre 2022
2.0	Actualización del documento 8. Inventario 10. Análisis de riesgos 11. Análisis de brecha 12. Plan de Trabajo	Adolfo Romero Alvario	Mayo 2023
2.0	Revisión del documento	Samuel Espinosa García	Mayo 2023
2.0	Aprobación del documento	Jairo Orlando Perilla Camelo	Junio 2023

HOJA DE FIRMAS

ELABORÓ:

FECHA	PUESTO	ÁREA	NOMBRE
Mayo 2023	Subdirector de Sistemas	Dirección de Desarrollo Administrativo	Adolfo Romero Alvario

REVISÓ:

FECHA	PUESTO	ÁREA	NOMBRE
Mayo 2023	Director de Desarrollo Administrativo	Unidad de Evaluación, Normatividad y Desarrollo Administrativo	Samuel Espinosa García

APROBÓ:

FECHA	PUESTO	ÁREA	NOMBRE
Al día de la firma del documento el funcionario público no se encontraba en activo	Titular de la Unidad de Evaluación, Normatividad y Desarrollo Administrativo	Órgano Interno de Control	Jairo Orlando Perilla Camelo

AUTORIZÓ:

FECHA	PUESTO	ÁREA	NOMBRE
Junio 2023	Titular del Órgano Interno de Control	Órgano Interno de Control	Jesús George Zamora

"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

1 DEFINICIONES

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 prejuicio de lo previsto en la normatividad aplicable en la materia, se entenderá por:

ADO. NET: Conjunto de componentes del software que pueden ser usados por los programadores para acceder a datos y a servicios de datos.

Entity Framework: Conjunto de tecnologías que permiten el desarrollo de aplicaciones de software orientadas a datos.

Persona servidora pública obligada: Todo servidor público del Instituto Nacional Electoral, a partir del nivel de Jefe de Departamento, homólogos y niveles hasta el de Consejero Presidente, contratado tanto bajo la modalidad de plaza presupuestal de estructura, como en el régimen de honorarios permanentes o eventuales; y/o manejen recursos financieros, obligados a redactar su acta, con independencia de la causa o motivo que origine la separación del empleo, cargo o comisión tales como renuncia, suspensión, inhabilitación, despido, destitución, licencia por tiempo definido o indefinido, cambio de cargo o adscripción, entre otros.[1]

SQL Injection: Tipo de ataque a una base de datos en la cual, por la mala filtración de las variables se puede inyectar un código creado por el atacante al propio código fuente de la base de datos.

2 ACRÓNIMOS

DOF: Diario Oficial de la Federación.

INE o Instituto: Instituto Nacional Electoral.

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

OIC: Órgano Interno de Control.

[1] Conforme al artículo 1 de los *Lineamientos para la realización del acta entrega-recepción, de los asuntos y recursos asignados a las y los servidores públicos del Instituto Nacional Electoral, al separarse de su empleo, cargo o comisión*.

SIAER: Sistema de Información de Actas Entrega-Recepción.

SQL: Server Sistema de gestión de bases de datos relacionales de Microsoft que está diseñado para el entorno empresarial.

UTSI: Unidad Técnica de Servicios de Informática.

3 PRESENTACIÓN

El Órgano Interno de Control 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 las personas servidoras públicas del Instituto Nacional Electoral, el cual es responsabilidad de todos aquellos que en el estricto apego a sus funciones tratan esta información.

Asimismo, este ente fiscalizador tiene el objetivo de garantizar las condiciones para que las personas servidoras públicas del Instituto, den cumplimiento a los postulados establecidos en los "*Lineamientos para realizar la entrega-recepción de los asuntos y recursos asignados a las personas servidoras públicas del Instituto Nacional Electoral, al separarse de su empleo, cargo o comisión y se formalice el acto de entrega-recepción de los asuntos y recursos a su cargo que les fueron asignados para el desempeño de su encargo*", para que, aquellos que los sustituyan, cuenten con los elementos necesarios para cumplir con las actividades respectivas y así continuar en forma regular con las funciones que desempeña el Instituto Nacional Electoral.

En función de ello, este Órgano Interno de Control **presenta el Documento de Seguridad**[2] del proceso denominado **Transparencia de la gestión**, y a nuestro proceso de impulsar la consolidación del comportamiento ético en el ejercicio de la función electoral; de la cultura de la integridad en el desempeño de las funciones de las personas servidoras públicas electorales; y de una efectiva rendición de cuentas, concretamente en cuanto hace a los actos de entrega recepción, que se realizan dentro del Instituto, este sistema tiene como objetivo automatizar los actos de entrega recepción de las personas servidoras públicas que se separan de su cargo, encargo o comisión.

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

El documento está integrado por los apartados:

I. Las funciones y obligaciones de las personas que tratan datos personales;
II. Inventario de datos personales y sus sistemas de tratamiento;
III. Resultados del Análisis de riesgos;
IV. Resultados del Análisis de brecha;
V. Plan de trabajo para atender los hallazgos;
VI. Mecanismos de monitoreo y revisión de las medidas de seguridad; y
VII. Programa general de capacitación.

Para atender lo anterior, se llevaron a cabo mesas de trabajo con el área involucrada en el tratamiento de los datos personales del proceso en mención de acuerdo con las siguientes etapas[3]:

- **Etapa Preliminar.** En esta etapa se llevó a cabo la identificación de la base de datos, persona que funge el rol de propietario y proceso de negocio.
- **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, 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:

  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.

[3] 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, aprobado mediante acuerdo INE-CT-ACG-PDP-004-2018.

Fase 2. Análisis de riesgos de datos personales y privacidad. En esta etapa se identificaron los riesgos derivados del tratamiento de datos personales -al que están expuestos en cada etapa de su ciclo de vida- para la posterior implementación o adecuación de las medidas de protección o controles, y comprender los impactos de eventos temidos o no deseados en las personas, los grupos o la sociedad.

- **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*.

  Etapa 4. Mejora continua. La Unidad de Transparencia incorporó el proceso "*Impulsar la consolidación del comportamiento ético en el ejercicio de la función electoral; de la cultura de la integridad en el desempeño de las funciones de las personas servidoras públicas electorales; y de una efectiva rendición de cuentas"* 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 durante todo su ciclo de vida, resultando una mejora periódica de sus controles.

4 MARCO NORMATIVO

- Artículos 6, Base A y 16, párrafo segundo de la Constitución de los Estados Unidos Mexicanos.

- Titulo 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 del Instituto Nacional Electoral en materia de protección de datos personales.

En particular:

- Artículo 41, base V de la Constitución de los Estados Unidos Mexicanos.

- Artículo 487, de la Ley General de Instituciones y Procedimientos Electorales.

- Artículo 490, numeral 1, inciso u) de la Ley General de Instituciones y Procedimientos Electorales.

- Artículo 82, numeral 1, inciso hh) del Reglamento Interior del Instituto Nacional Electoral.

- Artículo 71, fracciones XI y XVI del Estatuto del Servicio Profesional Electoral Nacional y del Personal de la Rama Administrativa.

- Lineamientos para realizar la entrega-recepción de los asuntos y recursos asignados a las y los servidores públicos del Instituto Nacional Electoral, al separarse de su empleo, cargo o comisión.

5 TRANSPARENCIA DE LA GESTIÓN

5.1 DESCRIPCIÓN DEL PROCESO A NIVEL NEGOCIO

El Órgano Interno de Control, es un órgano del Instituto que dentro de sus atribuciones se encuentra la de intervenir en los procesos de entrega-recepción, por conclusión del puesto o encargo de las personas servidoras públicas del Instituto, de mandos medios y superiores, así como de quienes manejen recursos económicos. Asimismo, administra y opera el Sistema de Actas de Entrega-Recepción donde, resguarda la información relacionada con las actas de entrega-recepción y cualquier información que involucre el tratamiento de datos personales en el proceso transparencia de la gestión.

Por lo que, derivado de las atribuciones anteriores y con el propósito de facilitar la presentación de las actas de entrega-recepción de las personas servidoras públicas del INE, el Órgano Interno de Control pone a disposición el SIAER permitiendo que las personas servidoras públicas puedan realizar el proceso de elaboración de su acta de entrega-recepción en una herramienta informática que se encuentra disponible las 24 horas del día, los siete días de la semana y es accesible desde cualquier punto de la República Mexicana a través de la intranet institucional con la VPN configurada.

Las personas servidoras públicas obligadas son quienes realizan la solicitud para la obtención de usuario y contraseña, e ingresan los datos requeridos de conformidad con los Lineamientos que regulan la entrega-recepción de los asuntos y recursos asignados a las y los servidores públicos del INE, al separarse de su empleo, cargo o comisión.

Dichas personas servidoras públicas, son responsables del ingreso de sus datos personales al SIAER una vez que concluye el llenado del acta y se valida la realización con firmas de la misma.

Por otra parte, la Unidad de Evaluación, Normatividad y Desarrollo Administrativo (UENDA) coordina las responsabilidades de la Dirección de Desarrollo Administrativo (DDA) que

genera reportes estadísticos para fines de control dentro del OIC. Por tanto, realiza compulsas y verifica la información proporcionada por la Dirección Ejecutiva de Administración (DEA), para identificar a las personas que no presentaron su acta de entrega-recepción (omisos) y determinar obligados.

Previo a la determinación de las personas servidoras públicas omisas, la DDA establece medidas de seguimiento y apoyo al personal obligado para la presentación de su acta de entrega-recepción, a través de la emisión de requerimientos, así como, mediante la plataforma teams y el correo electrónico institucional, con la finalidad de brindar las asesorías y capacitaciones necesarias, con el propósito de lograr que las personas servidoras públicas cumplan en tiempo y forma con el acto de entrega-recepción. En el caso de no presentar el acta de entrega-recepción solicitada dentro del plazo que se les otorga, de conformidad con los Lineamientos, se dará vista a la Dirección de Investigación de Responsabilidades Administrativas de la Unidad de Asuntos Jurídicos del OIC, para los efectos conducentes.

A continuación, se describen las actividades relacionadas:

1. La persona servidora pública obligada, realiza el proceso de obtención de usuario y contraseña en el sistema SIAER.

2. La persona servidora pública obligada, ingresa al SIAER y captura la “Solicitud de representante del Órgano Interno de Control” en su Acta Entrega-Recepción.

3. La persona servidora pública obligada, envía su solicitud para “visto bueno” de su jefe inmediato.

4. El jefe inmediato de la persona servidora pública obligada, otorga el “visto bueno”.

5. La persona servidora pública obligada procede al llenado de su Acta Entrega-Recepción.

6. El servidor público obligado, envía a la Subdirección de Desarrollo Administrativo, a través del SIAER, su Proyecto de Acta Entrega-Recepción.

7. La Subdirección de Desarrollo Administrativo:

    a. Autoriza la presencia del Representante del Órgano Interno de Control, si el acta fue enviada con tres días de anticipación a la celebración del Acta Entrega-Recepción; o

    b. Niega la presencia del Representante del Órgano Interno de Control, si el acta no fue enviada con tres días de anticipación a la celebración del Acta Entrega-Recepción.

8. La persona servidora pública obligada, recibe la aprobación o la respuesta de no participación del representante del Órgano Interno de Control en su Acta Entrega-Recepción.

9. La persona servidora pública obligada, descarga del SIAER su Proyecto de Acta Entrega-Recepción, agrega los anexos correspondientes y procede a su firma.

10. La persona servidora pública obligada sube el Acta al SIAER.

11. La Subdirección de Desarrollo Administrativo, revisa el Acta Entrega-Recepción.

    a. Si el Acta Entrega-Recepción cumple con todos los requisitos, da por concluido el proceso;

    b. Si no cumple con todos los requisitos, la Subdirección de Desarrollo Administrativo realiza observaciones al Acta Entrega-Recepción y la regresa a la persona servidora pública obligada.

12. En su caso, la persona servidora pública obligada, atiende las observaciones realizadas por la Subdirección de Desarrollo Administrativo (regresa al paso 11).

5.2 DIAGRAMA A BLOQUES

Para su mejor visualización, consultar el Anexo I.

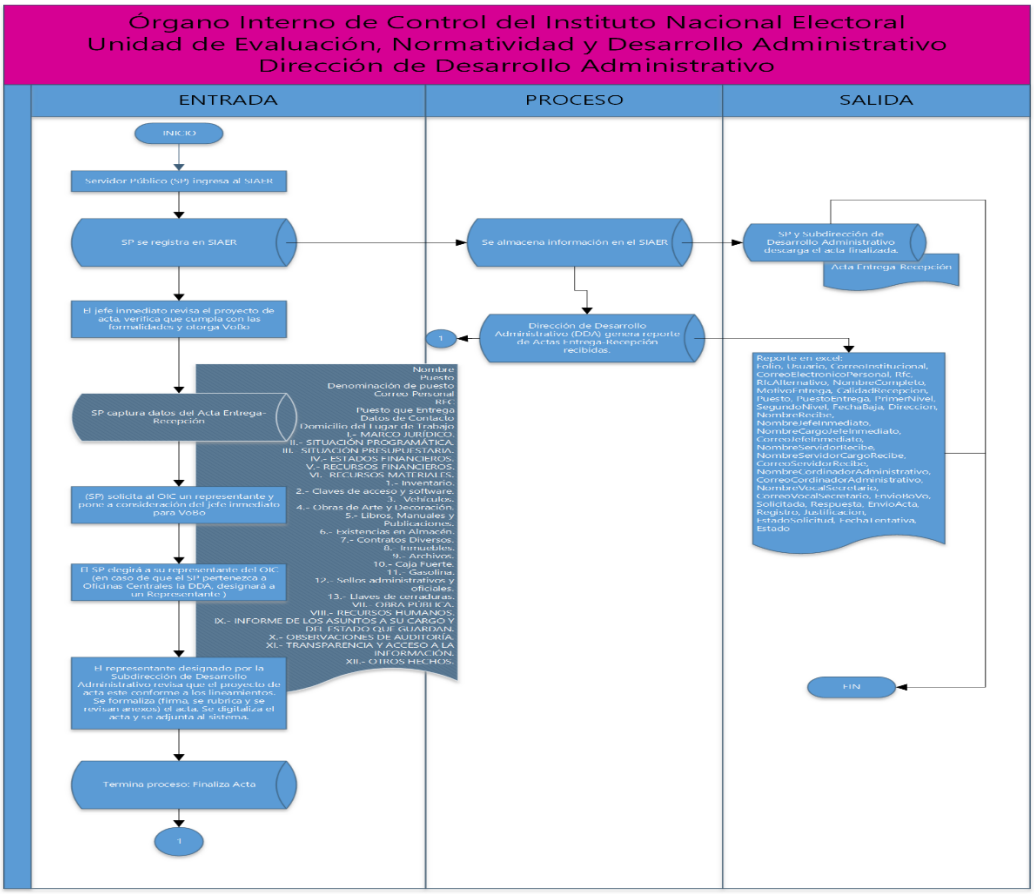


Figura 1. Diagrama a bloques

6 PERSONAS QUE FUNGEN EL ROL PROPIETARIO

Seudónimo de la base de datos	Nombre de la persona propietaria de la base de datos	Cargo que ocupa
BD - SIAER	L.C. Samuel Espinosa García	Director de Desarrollo Administrativo
	Lic. María Dolores López Cortés	Subdirectora de Desarrollo Administrativo

7 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
Administrador (Sistema)	Persona servidora pública que desempeña el puesto de Director o Directora de Desarrollo Administrativo	Consulta de información de las actas de entrega-recepción. Generación de datos estadísticos. Decisión sobre el tratamiento de los datos personales. Resguardar la información contenida en las actas de entrega-recepción. Mantener la confidencialidad de la información. Cumplir con las políticas de seguridad.

Función (Perfil / Rol)	Cargo que ocupa	Obligaciones
		Utilizar los datos personales para la finalidad para la que fueron recabados.
Administrador (Sistema)	Persona servidora pública que desempeña el puesto de Subdirector o Subdirectora de Desarrollo Administrativo	Consulta de información de las actas de entrega-recepción. Generación de datos estadísticos. Decisión sobre el tratamiento de los datos personales. Resguardar la información contenida en las actas de entrega-recepción. Mantener la confidencialidad de la información. Cumplir con las políticas de seguridad. Utilizar los datos personales para la finalidad para la que fueron recabados.
Administrador (Sistema)	Persona servidora pública que desempeña el puesto de Jefe o Jefa de departamento de declaraciones	Consulta de información de las actas de entrega-recepción. Generación de datos estadísticos. Apoyar a servidores en el proceso de realización de actas de entrega-recepción. Mantener la confidencialidad de la información. Cumplir con las políticas de seguridad. Rendir cuentas a la persona que funge el rol propietario. Utilizar los datos personales para la finalidad para la que fueron recabados.

Función (Perfil / Rol)	Cargo que ocupa	Obligaciones
Administrador (BD)	Persona servidora pública que desempeña el puesto de Subdirector o Subdirectora de Sistemas	Provee la administración de la seguridad del sistema de información. Explotación de base de datos, para fines estadísticos. Rendir cuentas a la persona que funge el rol propietario. Administración de servidor de base de datos y aplicativo. Mantener la confidencialidad de la información. Cumplir con las políticas de seguridad. Rendir cuentas a la persona que funge el rol propietario. Utilizar los datos personales para la finalidad para la que fueron recabados.
Administrador (BD)	Persona servidora pública que desempeña el puesto de Jefe o Jefa de Departamento de Sistemas	Provee la administración de la seguridad del sistema de información. Explotación de base de datos, para fines estadísticos. Administración de servidor de base de datos y aplicativo. Programación de funcionalidades del aplicativo. Programación de reportes estadísticos. Mantener la confidencialidad de la información. Cumplir con las políticas de seguridad. Rendir cuentas a la persona que funge el rol propietario.

Función (Perfil / Rol)	Cargo que ocupa	Obligaciones
		Utilizar los datos personales para la finalidad para la que fueron recabados.
Usuario	Personas servidoras públicas que desempeñan los puestos de: Profesional Dictaminador de Servicios Especializados Profesional de Servicios Especializados	Utiliza las funciones de la aplicación para realizar el proceso de gestión de presentación de las actas de entrega-recepción. Mantener la confidencialidad de la información. Cumplir con las políticas de seguridad. Rendir cuentas a la persona que funge el rol propietario.
Personas Servidoras Públicas Obligadas	Personas servidoras públicas del Instituto Nacional Electoral, que cambiaron, o concluyeron una encargaduría o un puesto de mando medio o superior	Presentar su Acta de Entrega-Recepción, por el término de su encargo, puesto o la entrega de bienes e información. Mantener la confidencialidad de la información. Cumplir con las políticas de seguridad. Rendir cuentas a la persona que funge el rol propietario.

8 INVENTARIO

Este apartado presenta el inventario de los datos personales que trata el proceso señalado 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, destinatarios o terceros-.

La base de datos **BD- SIAER** almacena 80 datos personales de 4,319 titulares[4] conforme a 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?
Los datos personales tratados, son obtenidos por los siguientes medios: **Físico:** Acta entrega-recepción **Digital:** Correo electrónico[5] SIAER: Formulario	Los datos son recabados para las siguientes finalidades: recibir, registrar, almacenar, automatizar los actos de entrega recepción de las personas servidoras públicas obligadas a realizar un acto de entrega-recepción al separarse de su empleo, cargo o	**Sitios de almacenamiento:** • Oficinas del Órgano Interno de Control • Oficinas de la Unidad Técnica de Servicio de Informática. • Archivo Institucional **Medio de almacenamiento físico:** • Estantes, en bodega. • Cajas **Medio de almacenamiento digitales:**	• Persona servidora pública que desempeña el puesto de Director o Directora de Desarrollo Administrativo • Persona servidora pública que desempeña el puesto de Subdirectora o Subdirector de Desarrollo Administrativo. • Persona servidora pública que desempeña el puesto de Jefe o Jefa de departamento de declaraciones patrimoniales y otros servicios • Persona servidora pública que desempeña el puesto de Subdirector o Subdirectora de Sistemas	No cuenta con encargados para el tratamiento de datos personales.	No se realiza transferencia de datos personales.	No se realiza difusión de datos personales.

[4] Con corte al 4 de abril de 2023.

[5] El medio se utilizó de 2019-2021 para obtener datos personales.

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?
	comisión.	• Disco duro externo • Estantes • Computadoras de escritorio • Think Pad Core i5 • Unidad SAN (Sistemas, Bases de Datos y las Unidades de Respaldo) • Controladora HP DL380 G5 • Unidad SAN • Net App FAS 2750	• Persona servidora pública que desempeña el puesto de Jefe o Jefa de Departamento de Sistemas. • Profesional Dictaminador de Servicios Especializados • Profesional de Servicios Especializados			

Datos Personales por categoría

75 datos personales estándar. A continuación, se listan los datos personales:

- **39 identificación y contacto:** Nombre, RFC, Usuario (correo electrónico institucional), Nombre del jefe inmediato, Nombre del coordinador administrativo, Nombre del vocal secretario de la junta local, Nombre Completo del servidor público propuesto para representar al OIC, Nombre del servidor público que entrega, RFC del servidor público que entrega, Número de identificación del servidor público que entrega, Nombre de la calle del domicilio particular de quien entrega, Número exterior del domicilio particular de quien entrega, Número interior del domicilio particular de quien entrega, Colonia del domicilio particular de quien entrega, Alcaldía o municipio del domicilio particular de quien entrega, Código postal del servidor público que entrega, Correo electrónico personal del servidor público que entrega, Nombre del servidor público que recibe, RFC del servidor público que recibe, Nombre del servidor público que expide el nombramiento o designación, Nombre del comisionado por el Órgano Interno de Control, Nombre completo del primer testigo, Número de la identificación del primer testigo, Calle, Número exterior e interior del domicilio particular del primer testigo, Colonia del domicilio particular del primer testigo, Alcaldía o Municipio del domicilio particular del primer testigo, Código postal del domicilio particular del primer testigo, Nombre completo del segundo testigo, Número de la identificación del segundo testigo, Calle del domicilio particular del segundo testigo, Colonia del domicilio particular del segundo testigo, Alcaldía o municipio del domicilio particular del segundo testigo, Código postal del domicilio particular del segundo testigo, Nombre del servidor público autorizado para realizar transferencias bancarias o expedir cheques, Nombre del servidor público del que se solicitó su registro para realizar transferencias bancarias o expedir cheques, Nombre del beneficiario del último cheque expedido y/o transferencia bancaria, Nombre del servidor público que tiene bajo su resguardo cheques sin entregar al beneficiario, Nombre del servidor público que actúa como pagador habilitado, Justificación (podría contener datos personales).
- **29 laborales:** Puesto que entrega, Cargo que entrega, Unidad administrativa, Área de Adscripción, Fecha de la baja, Correo electrónico institucional del servidor público que entrega, En calidad de que recibe el cargo, Cargo del servidor público que recibe (en caso de que aplique), Correo electrónico del servidor público que recibe, Correo electrónico del jefe inmediato, Correo electrónico institucional del coordinador administrativo, Correo electrónico del vocal secretario de la junta local, Cargo del servidor público propuesto para representar al OIC, Área de adscripción del servidor público propuesto para representar al OIC, Correo electrónico del servidor público propuesto para representar al OIC, Unidad administrativa del servidor público, Cargo del servidor público que recibe, Área de adscripción del primer testigo, Cargo del primer testigo, Área de adscripción del segundo testigo, Cargo del segundo testigo, Cargo del servidor público que tiene bajo su resguardo cheques sin entregar al beneficiario, Puesto que entrega, Correo electrónico institucional del coordinador administrativa, Área de adscripción del segundo testigo, Cargo del segundo testigo, Cargo del servidor público autorizado para realizar transferencias bancarias o expedir cheques, Cargo del servidor público que tiene bajo su resguardo cheques sin entregar al beneficiario.
- **7 académicos:** Título académico del servidor público que entrega, Título académico del servidor público que recibe, Título académico del servidor público que expide el nombramiento o designación, Título académico del primer testigo, Título académico del segundo testigo, Último nivel de estudios, Título académico del servidor público autorizado para realizar transferencias bancarias o expedir cheques.

5 datos personales sensibles. A continuación, se listan los datos personales:

- **1 patrimonial:** Importe de los cheques pendientes de entregar en poder del pagador habilitado.
- **4 de autenticación:** Identificación escaneada de la persona que realiza la entrega (credencial de empleado, Credencial de elector, Cédula profesional, Pasaporte, Licencia de conducir), Identificación escaneada de la persona que recibe la entrega (Credencial de empleado, Credencial de elector, Cédula profesional, Pasaporte, Licencia de conducir), Identificación escaneada de la persona servidora pública que funge como primer testigo (Credencial de empleado, Credencial de elector, Cédula profesional, Pasaporte, Licencia de conducir),

Identificación escaneada de la persona servidora pública que funge como segundo testigo (Credencial de empleado, Credencial de elector, Cédula profesional, Pasaporte, Licencia de conducir).
Sistema de tratamiento
El sistema que trata la base de datos SIAER es el Sistema de Actas de Entrega-Recepción versión 2.0.

9 CICLO DE VIDA DE LOS DATOS PERSONALES

9.1 OBTENCIÓN

Los datos personales se obtienen directamente de las personas titulares a través de:

- Formatos de acta entrega-recepción,
- Correo electrónico, y
- SIAER.

9.2 ALMACENAMIENTO DE LOS DATOS PERSONALES

Los datos personales son almacenados:

- **Físico:** Instalaciones del Órgano Interno de Control y del Archivo Institucional, y

- **Digital:** En los servidores alojados en las instalaciones de la Unidad Técnica de Servicios de Informática.

9.3 USO DE LOS DATOS PERSONALES

Los datos personales obtenidos son utilizados para las siguientes finalidades: recibir, registrar, almacenar, automatizar los actos de entrega-recepción de las personas servidoras públicas obligadas a realizar un acto de entrega-recepción al separarse de su empleo, cargo o comisión.

Lo anterior permite garantizar el cumplimiento de que establecen los Lineamientos para realizar la entrega-recepción de los asuntos y recursos asignados a las y los servidores públicos del Instituto Nacional Electoral, al separarse de su empleo, cargo o comisión.

9.4 DIVULGACIÓN DE LOS DATOS PERSONALES CONSIDERANDO LAS REMISIONES Y TRANSFERENCIAS

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

9.5 BLOQUEO DE LOS DATOS PERSONALES

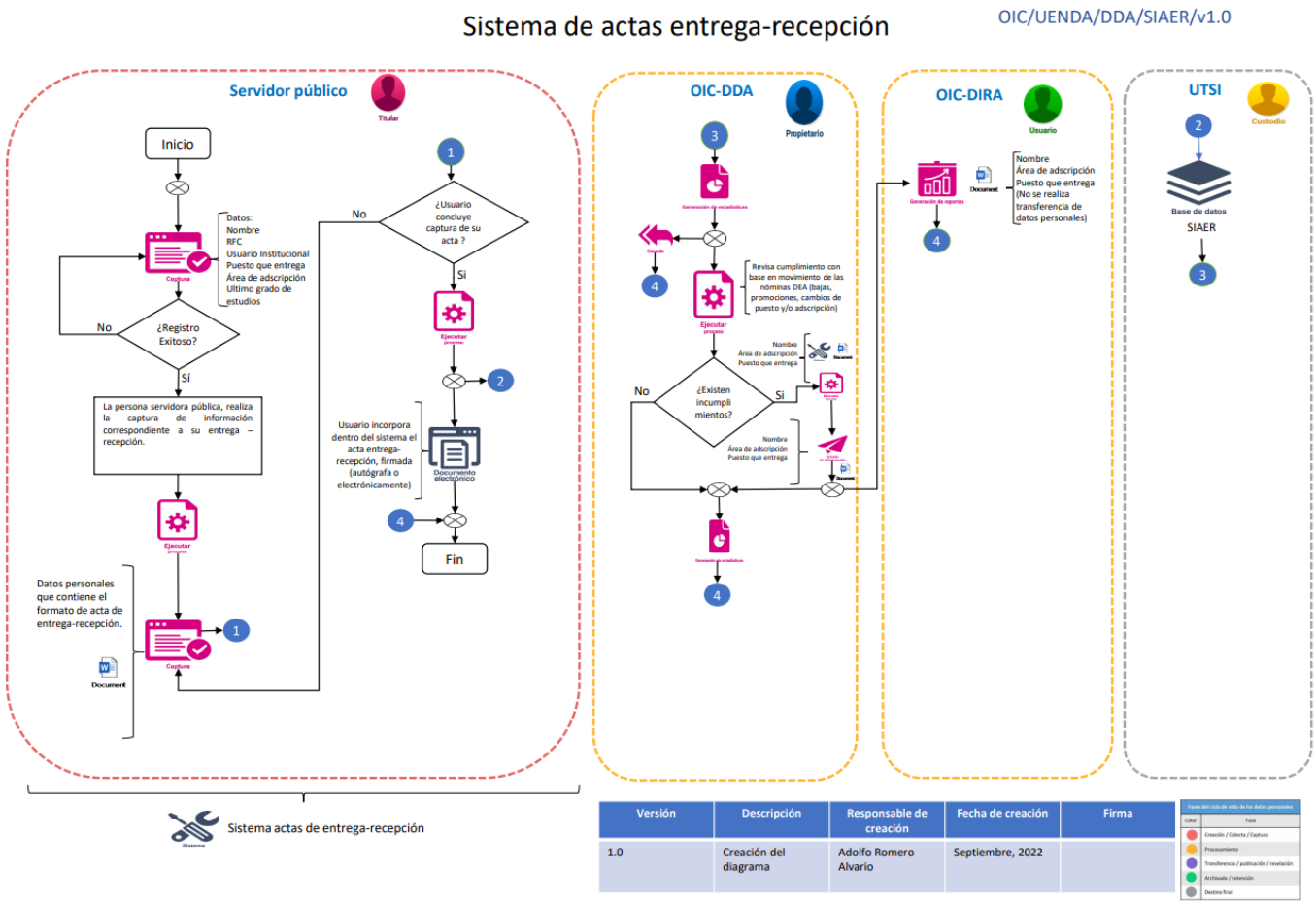
El área responsable no cuenta, a la fecha, con reglas de bloqueo de los datos personales, por lo que no se ha ejecutado la acción. Sin embargo, es una actividad que se tiene contemplada como una prioridad.

9.6 CANCELACIÓN, SUPRESIÓN O DESTRUCCIÓN DE LOS DATOS PERSONALES.

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

Sección Catálogo Disposición Documental 2018 - 2021	Sección Catálogo Disposición Documental 2022
10.10 Proceso de entrega-recepción Tiempo de conservación: 7 años. Destino final: baja. -supresión de los registros en base de datos y destrucción de la información en papel-	10C-9 Participar en actos de entrega recepción. Tiempo de conservación: 7 años. Destino final: baja. -supresión de los registros en base de datos y destrucción de la información en papel-.

El flujo que siguen los datos personales durante todo su ciclo de vida se muestra a continuación:



Versión	Descripción	Responsable de creación	Fecha de creación	Firma
1.0	Creación del diagrama	Adolfo Romero Alvario	Septiembre, 2022	

Figura 2. Diagrama de flujo

Para su mejor visualización, consultar el Anexo II.

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*[6] 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, y
   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.

En la siguiente tabla se incorporan los datos personales tratados y se relacionan con su riesgo inherente, atiendo a lo señalado líneas arriba.

Riesgo inherente			
Nivel bajo: 75	**Nivel medio: 5**	**Nivel alto: 0**	**Nivel reforzado: 0**
1. Nombre 2. RFC 3. Usuario (correo electrónico institucional) 4. Nombre del jefe inmediato 5. Nombre del coordinador administrativo 6. Nombre del vocal secretario de la junta local 7. Nombre Completo del servidor público propuesto para representar al OIC 8. Nombre del servidor público que entrega 9. RFC del servidor público que entrega	1. Identificación escaneada de la persona que realiza la entrega (Credencial de empleado, Credencial de elector, Cédula profesional, Pasaporte, Licencia de conducir) 2. Identificación escaneada de la persona que recibe la entrega (Credencial de empleado, Credencial de elector, Cédula profesional, Pasaporte, Licencia de conducir) 3. Importe de los cheques pendientes de entregar en poder del pagador habilitado		

[6] Desarrollada por la Unidad Técnica de Transparencia y Protección de Datos Personales del INE.

Riesgo inherente			
Nivel bajo: 75	**Nivel medio: 5**	**Nivel alto: 0**	**Nivel reforzado: 0**
10. Número de identificación del servidor público que entrega 11. Nombre de la calle del domicilio particular de quien entrega 12. Número exterior del domicilio particular de quien entrega 13. Número interior del domicilio particular de quien entrega 14. Colonia del domicilio particular de quien entrega 15. Alcaldía o municipio del domicilio particular de quien entrega 16. Código postal del servidor público que entrega 17. Correo electrónico personal del servidor público que entrega 18. Nombre del servidor público que recibe 19. RFC del servidor público que recibe 20. Nombre del servidor público que expide el nombramiento o designación 21. Nombre del comisionado por el Órgano Interno de Control 22. Nombre completo del primer testigo 23. Número de la identificación del primer testigo 24. Calle 25. Número exterior e interior del domicilio particular del primer testigo 26. Colonia del domicilio particular del primer testigo 27. Alcaldía o Municipio del domicilio particular del primer testigo 28. Código postal del domicilio particular del primer testigo 29. Nombre completo del segundo testigo 30. Número de la identificación del segundo testigo 31. Calle del domicilio particular del segundo testigo	4. Identificación escaneada de la persona que recibe la entrega (Credencial de empleado, Credencial de elector, Cédula profesional, Pasaporte, Licencia de conducir) 5. Identificación escaneada de la persona servidora pública que funge como primer testigo (Credencial de empleado, Credencial de elector, Cédula profesional, Pasaporte, Licencia de conducir)		

Riesgo inherente			
Nivel bajo: 75	**Nivel medio: 5**	**Nivel alto: 0**	**Nivel reforzado: 0**
32. Colonia del domicilio particular del segundo testigo 33. Alcaldía o municipio del domicilio particular del segundo testigo 34. Código postal del domicilio particular del segundo testigo 35. Nombre del servidor público autorizado para realizar transferencias bancarias o expedir cheques 36. Nombre del servidor público del que se solicitó su registro para realizar transferencias bancarias o expedir cheques 37. Nombre del beneficiario del último cheque expedido y/o transferencia bancaria 38. Nombre del servidor público que tiene bajo su resguardo cheques sin entregar al beneficiario 39. Nombre del servidor público que actúa como pagador habilitado 40. Puesto que entrega 41. Cargo que entrega 42. Unidad administrativa 43. Área de Adscripción 44. Fecha de la baja 45. Correo electrónico institucional del servidor público que entrega 46. En calidad de que recibe el cargo 47. Cargo del servidor público que recibe (en caso de que aplique) 48. Correo electrónico del servidor público que recibe 49. Correo electrónico del jefe inmediato 50. Correo electrónico institucional del coordinador administrativo 51. Correo electrónico del vocal secretario de la junta local 52. Cargo del servidor público propuesto para representar al OIC 53. Área de adscripción del servidor público propuesto para representar al OIC			

Riesgo inherente			
Nivel bajo: 75	**Nivel medio: 5**	**Nivel alto: 0**	**Nivel reforzado: 0**
54. Correo electrónico del servidor público propuesto para representar al OIC 55. Título académico del servidor público que entrega 56. Unidad administrativa del servidor público 57. Área de adscripción del servidor público 58. Título académico del servidor público que recibe 59. Cargo del servidor público que recibe 60. Título académico del servidor público que expide el nombramiento o designación 61. Título académico del primer testigo 62. Área de adscripción del primer testigo 63. Cargo del primer testigo 64. Título académico del segundo testigo 65. Área de adscripción del segundo testigo 66. Cargo del segundo testigo 67. Cargo del servidor público que tiene bajo su resguardo cheques sin entregar al beneficiario 68. Correo electrónico institucional del coordinador administrativo 69. Área de adscripción del segundo testigo 70. Cargo del segundo testigo 71. Cargo del servidor público autorizado para realizar transferencias bancarias o expedir cheques 72. Cargo del servidor público que tiene bajo su resguardo cheques sin entregar al beneficiario 73. Último nivel de estudios 74. Título académico del servidor público autorizado para realizar transferencias bancarias o expedir cheques 75. Justificación (podría contener datos personales)			

10.2 ANÁLISIS DE RIESGOS DE PRIVACIDAD Y DATOS PERSONALES

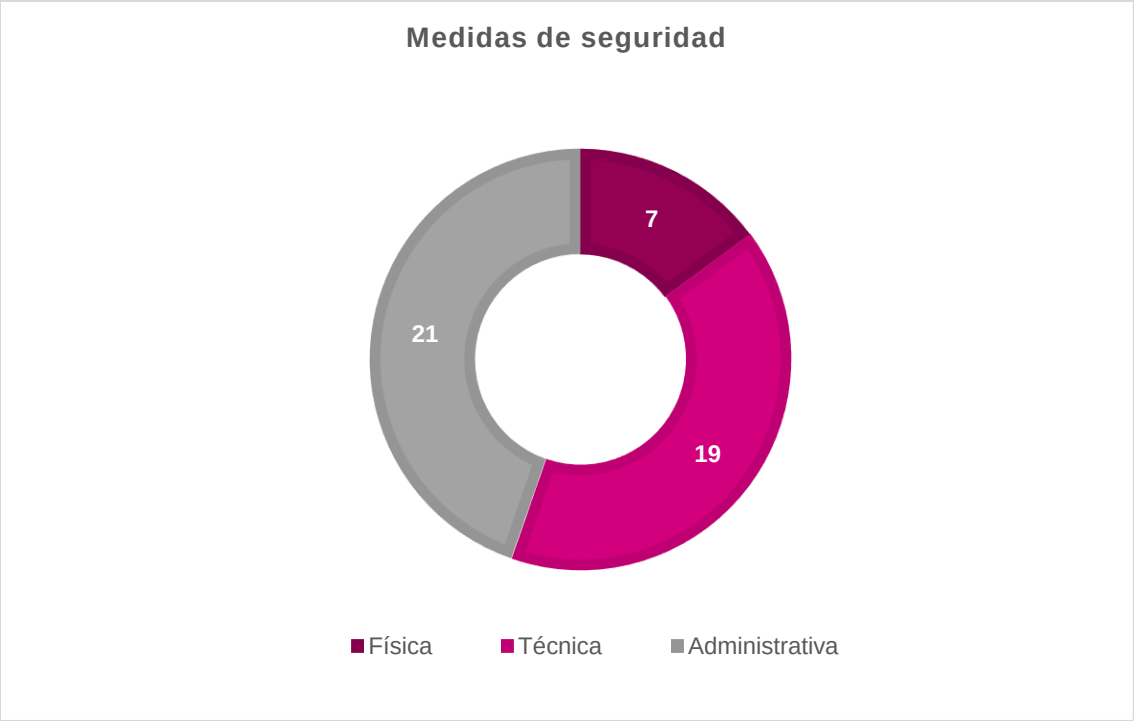
El análisis de riesgos abarcó los activos relacionados con el proceso de Transparencia de la Gestión.

Resultado del análisis de riesgos, el área responsable detectó que deben reforzar las acciones relacionadas con el trámite de solicitudes de derechos ARCO y la puesta a disposición del aviso de privacidad, para gestionar 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 27002:2013[7].

Actualmente se cuenta con **47** medidas de seguridad implementadas.



A continuación, se listan los **36** controles[8] a los que corresponden dichas medidas.

- Trabajo a distancia
- Términos y condiciones del empleo
- Propiedad de los activos
- Uso aceptable de los activos

[7] 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.

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

- Devolución de activos
- Etiquetado de la información
- Acceso a las redes y a los servicios de red
- Registro y baja de usuario
- Gestión de acceso de usuario
- Eliminación o reasignación de los derechos de acceso
- Restricción de acceso a la información
- Sistema de gestión de contraseñas
- Uso de herramientas y administración de sistemas
- Control de acceso al código fuente de los programas
- Seguridad de oficinas, salas y recursos
- Emplazamiento y protección de equipo
- Instalaciones de suministro (Centros de cómputo)
- Seguridad del cableado (Centros de cómputo)
- Seguridad de los equipos fuera de las instalaciones
- Equipo de usuario desatendido
- Separación de los ambientes de desarrollo, prueba y operación
- Protección de la información del registro de accesos
- Sincronización del reloj
- Restricción de la instalación de software
- Controles de red
- Seguridad de los servicios de red
- Acuerdos de confidencialidad o no revelación
- Protección de las transacciones de servicios de aplicaciones
- Procedimiento de control de cambios en sistemas
- Revisión técnica de las aplicaciones después de efectuar cambios en el sistema operativo
- Pruebas funcionales de seguridad de sistemas
- Pruebas de aceptación de sistemas
- Respuesta a incidentes de seguridad de la información
- Aprendizaje de los incidentes de seguridad de la información
- Recopilación de evidencias
- Protección y privacidad de la información personal

12 PLAN DE TRABAJO

A continuación, se listan las acciones que integran el plan de trabajo, de acuerdo con los resultados del análisis de riesgos y análisis de brecha.

No.	Acciones
1	Robustecer roles y responsabilidades en seguridad de la información
2	Mejorar la segregación de tareas
3	Actualizar los contactos con las autoridades y grupos de interés especial
4	Fortalecer la seguridad de la información en la gestión de proyectos
5	Actualizar las responsabilidades de gestión
6	Completar el inventario de activos
7	Fortalecer la clasificación, etiquetado, y manejo de la información
8	Regularizar la gestión y eliminación de medios extraíbles
9	Robustecer el control de acceso
10	Mejorar la gestión de acceso de usuarios con privilegios especiales
11	Complementar la revisión de los derechos de acceso de usuario
12	Regularizar el uso de la información secreta de autenticación
13	Consolidar las políticas y procedimientos de intercambio de información
14	Regularizar la notificación de eventos y puntos débiles de seguridad de la información
15	Mejorar la evaluación y decisión sobre los eventos de seguridad de información
16	Mejorar la continuidad de la seguridad de la información
17	Fortalecer la identificación de la legislación aplicable y de los requisitos contractuales
18	Revisar la seguridad de la información que contenga datos personales
19	Consolidar el cumplimiento de las políticas y normas de seguridad
20	Fortalecer el propósito de la reclamación de los datos personales
21	Reforzar los datos de contacto del área responsable para atender quejas

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 revisión[9] del cumplimiento se realiza a través del Sistema de Gestión para la Protección de los Datos Personales del Instituto Nacional Electoral[10] (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 Controles[11] del SIPRODAP, de manera documentada, sistematizada, estructurada, repetible, eficiente y adaptada al entorno institucional, conforme a lo establecido en la LGPDPPSO.

El proceso fue integrado al SiPRODAP el 14 de octubre de 2022, la solicitud de registro al SiPRODAP está disponible en el Anexo III.

[9] En cumplimiento a los artículos 35, fracción VI de la LGPDPPSO y 63 de los LGPDPSP.
[10] Aprobado por el Comité de Transparencia, mediante acuerdo INE-CT-ACG-PDP-001-2019.
[11] Apartado del SiPRODAP conformado por controles para la protección de datos personales.

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.

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

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.

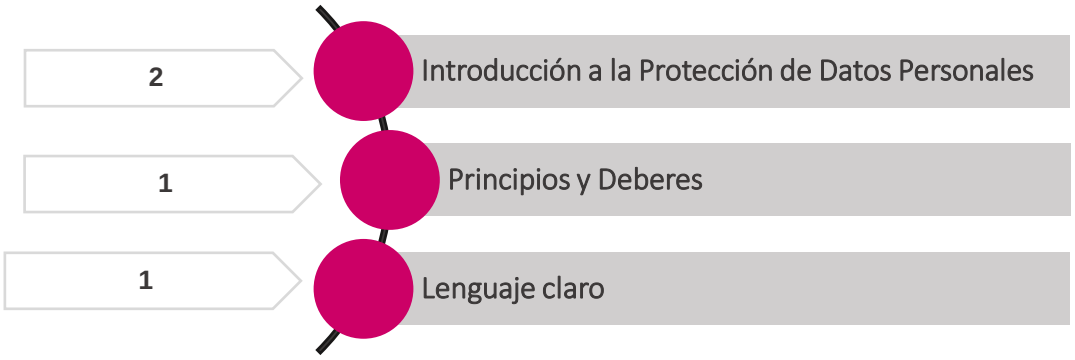


Figura 3. Personal acreditado en cursos virtuales

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 4. 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:

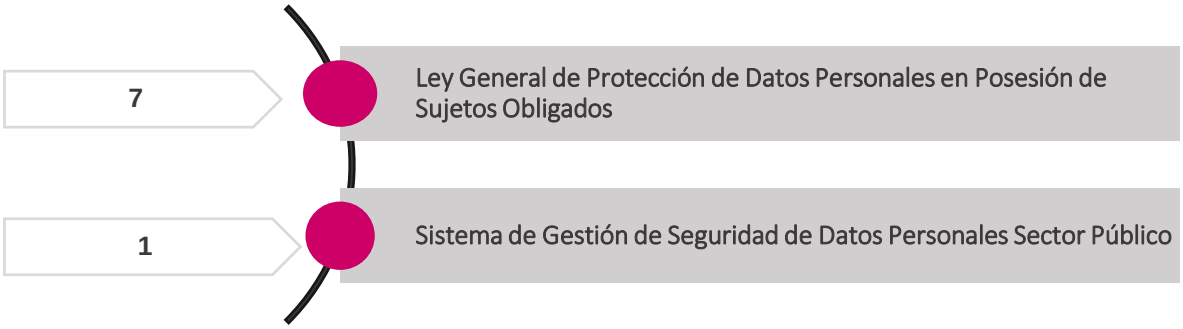


Figura 5. Personal acreditado en cursos impartidos por el INAI

14.4 OTROS CURSOS

De igual manera, el personal acreditó los siguientes cursos, impartidos por la Secretaría de la Función Pública y a la Asociación Iberoamericana de Datos de Ciberseguridad.

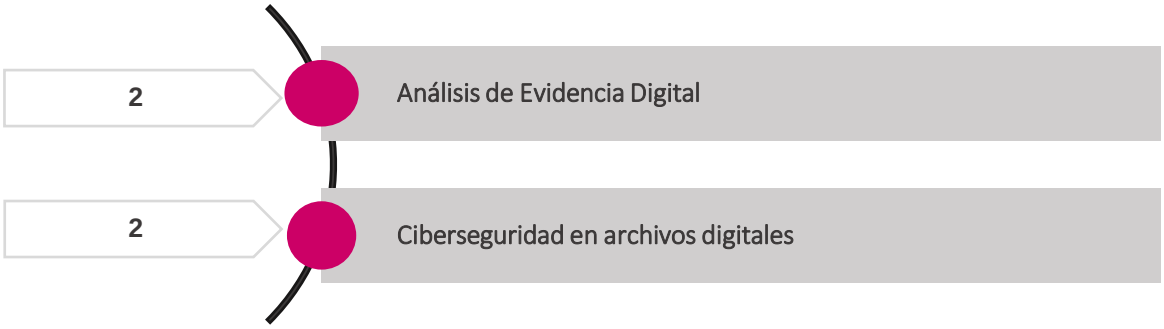


Figura 6. Otros cursos

15 ANEXOS

Anexo	Descripción	Archivo
Anexo I	Diagrama a bloques	Anexo I.pdf
Anexo II	Diagrama de flujo	Anexo II.pdf
Anexo III	Solicitud de registro al SiPRODAP	Anexo III.pdf

FIRMADO POR: ROMERO ALVARIO ADOLFO
AC: Autoridad Certificadora del Instituto Nacional Electoral
ID: 2143148
HASH:
F7914250DFF3AA0A558C10FC91B6323145CF4401928F22F09BE89D840211B745

FIRMADO POR: ESPINOSA GARCIA SAMUEL
AC: Autoridad Certificadora del Instituto Nacional Electoral
ID: 2143148
HASH:
F7914250DFF3AA0A558C10FC91B6323145CF4401928F22F09BE89D840211B745

FIRMADO POR: JESUS GEORGE ZAMORA
AC: AUTORIDAD CERTIFICADORA
ID: 2143148
HASH:
F7914250DFF3AA0A558C10FC91B6323145CF4401928F22F09BE89D840211B745