DOCUMENTO DE SEGURIDAD

DE FIRMA ELECTRÓNICA AVANZADA INSTITUCIONAL

Área Responsable: Dirección Ejecutiva de Administración

INE-CT-PDP-DOC_SEG-004-2023

Versión: 1.0

Fecha de presentación: 6 de diciembre de 2023.

Instituto Nacional Electoral

DOCUMENTO DE SEGURIDAD

Dirección Ejecutiva de Administración

Dirección de Personal

Subproceso: Firma Electrónica Avanzada Institucional

Bases de datos: FEA

Versión 1.0

Noviembre 2023

CONTROL DE VERSIONES

VERSIÓN	COMENTARIO / DESCRIPCIÓN	RESPONSABLE DE LA ACTUALIZACIÓN / CREACIÓN / REVISIÓN	FECHA DE ACTUALIZACIÓN / CREACIÓN / REVISIÓN
1.0	Creación del documento	Ing. Teresa Guevara Morales	Octubre 2023
1.0	Revisión del Documento	Mtro. Antonio Lara Rodríguez	Noviembre 2023
1.0	Aprobación del Documento	Mtro. Raúl Rosas Barriga	Noviembre 2023

HOJA DE FIRMAS

ELABORÓ:

FECHA	PUESTO	ÁREA	NOMBRE
Octubre 2023	Técnico Operador de Portal de Firma Electrónica	Dirección de Personal	Ing. Teresa Guevara Morales

REVISÓ:

FECHA	PUESTO	ÁREA	NOMBRE
Noviembre 2023	Subdirector de Firma Electrónica Avanzada	Dirección de Personal	Mtro. Antonio Lara Rodríguez

APROBÓ:

FECHA	PUESTO	ÁREA	NOMBRE
Noviembre 2023	Director de Personal	Dirección Ejecutiva de Administración	Mtro. Raúl Rosas Barriga

CONTENIDO

ABREVIATURAS

CURP: Clave Única de Registro de Población.

DEA: Dirección Ejecutiva de Administración.

FEA: Firma Electrónica Avanzada.

FirmaINE: Firma Electrónica Avanzada del Instituto Nacional Electoral.

INE o Instituto: Instituto Nacional Electoral.

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

PortalFirmaINE: Herramienta web para el firmado electrónico de documentos.

RFC: Registro Federal de Contribuyentes.

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

UTSI: Unidad Técnica de Servicios de Informática.

DEFINICIONES

Para los efectos del presente documento, se consideran las definiciones establecidas en la Ley General de Protección de Datos Personales y el Programa para la Protección de Datos Personales del Instituto Nacional Electoral.

Actos: las comunicaciones, trámites, servicios, actos jurídicos y administrativos, así como procedimientos de naturaleza administrativa o jurisdiccional en los cuales se utilice la Firma Electrónica Avanzada;

Acuse de recibo electrónico: la constancia que se emite o genera el INE para acreditar de manera fehaciente la fecha y hora de la recepción o registro de las actuaciones electrónicas, actos, mensajes de datos o documentos;

Agente Certificador: persona designada por el Titular de la DEA, a propuesta de los Titulares de las Unidades Responsables de Oficinas Centrales y Juntas Ejecutivas, para llevar a cabo el proceso de enrolamiento y certificación de los usuarios;

Autoridad Certificadora: la DEA, a través de sus agentes certificadores, una vez que validan la documentación, se encarga de expedir el certificado digital a los solicitantes, asimismo lleva a cabo la revocación de los certificados digitales cuando el solicitante lo

requiera;

Autoridad Electoral: órgano encargado de cumplir algunas de las funciones del Estado relacionadas con la organización y vigilancia de los procedimientos democráticos de acceso al poder público[1].

Las autoridades electorales en México son: Instituto Nacional Electoral, Organismos Públicos Locales, Tribunal Electoral del Poder Judicial de la Federación y la Fiscalía Especializada en Delitos Electorales. En cada entidad federativa deben existir instituciones encargadas de impartir justicia y de proteger el voto[2];

Certificado(s) digital(es): es el mensaje de datos o registro que confirma el vínculo entre un firmante, la llave privada y su contraseña;

Contraseña: serie secreta de caracteres que solo el usuario conoce y que confirma el vínculo entre la llave privada y el certificado digital;

Correo electrónico: medio por el cual los usuarios recibirán notificaciones respecto a la Firma Electrónica Avanzada del INE. En el caso de los usuarios internos se deberá utilizar el correo electrónico institucional;

Destinatario: toda persona a quien van dirigidas las actuaciones electrónicas, actos, mensajes de datos o documentos;

Documento: archivo o conjunto de datos en formato digital que es generado, consultado, modificado o procesado por medios electrónicos;

Firma Electrónica Avanzada: es el conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa; los certificados digitales utilizados en la misma, podrán ser emitidos por el INE o por alguna Autoridad Certificadora externa con la que el INE haya firmado algún convenio;

Firmante: usuarios internos y/o externos que utilizan la Firma Electrónica Avanzada para suscribir actuaciones electrónicas, actos, mensajes de datos o documentos dentro de los procesos y procedimientos que se habiliten en el INE para tal fin;

Infraestructura: componentes tecnológicos que conforman la infraestructura de Llave Pública y que da soporte a la Firma Electrónica Avanzada del INE;

---

[1] Tribunal del Poder Judicial de la Federación. Autoridades Electorales en México. Manual del participante. Disponible en: https://www.te.gob.mx/ccje/Archivos/manual_autoridades.pdf

[2] https://www.ine.mx/wp-content/uploads/2018/01/DECEyEC_Autoridades_Electorales.pdf

Llave privada: corresponde a los datos que el firmante genera de manera personal y secreta para crear su Firma Electrónica Avanzada, a fin de lograr el vínculo entre dicha firma, el firmante y su contraseña;

Llave pública: corresponde a los datos contenidos en un certificado digital que permiten verificar la autenticidad de la Firma Electrónica Avanzada, del firmante y su contraseña;

Medios electrónicos: los componentes necesarios para el envío, recepción, registro y conservación de documentos electrónicos;

Mensaje de datos: la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o a través de cualquier otra tecnología que puede contener y manejar documentos electrónicos;

Reglamento: reglamento para el uso y operación de la Firma Electrónica Avanzada en el Instituto Nacional Electoral;

Requerimiento de certificado digital: archivo electrónico que el usuario crea y que es necesario para llevar a cabo la expedición del certificado digital de la Firma Electrónica Avanzada;

Revocación: procedimiento por el cual, se cancela e inhabilita el uso del certificado digital;

Portal de registro y certificación: sitio web, a través del cual, los usuarios internos crean su requerimiento de certificado digital y su acuse correspondiente;

Sistemas de servicios informáticos: las herramientas informáticas del INE para el envío, recepción de comunicaciones, así como para la consulta de información o en donde se haga uso de la Firma Electrónica Avanzada;

Solicitante: es la persona que solicite a la Autoridad Certificadora del INE la expedición o revocación del certificado digital de la Firma Electrónica Avanzada;

Sujetos obligados en FirmaINE: usuarios internos y externos previstos;

Tablero electrónico: el medio electrónico a través del cual se ponen a disposición de los sujetos obligados que utilicen la Firma Electrónica Avanzada en términos de este Reglamento, las actuaciones electrónicas, actos, mensajes de datos o documentos que fueron suscritos con Firma Electrónica Avanzada, y que muestra un acuse de recibo electrónico;

Titular: usuario interno o externo al que, una vez cumplidos los requisitos, se le expide el certificado digital;

Usuarios internos: el personal del INE de la Rama Administrativa y del Servicio Profesional Electoral Nacional, así como los prestadores de servicios que sean contratados por honorarios asimilados y/o eventuales;

Usuarios externos: personas físicas nacionales y/o extranjeras ajenas al INE, así como aquellos que formen parte de los procesos en donde se hayan implementado los sistemas de servicios informáticos; asimismo, las personas morales nacionales y/o extranjeras y Partidos Políticos Nacionales, Candidaturas Independientes y/o Consejeros del Poder Legislativo, a través de su representante legal o personas autorizadas por los mismos en términos del artículo 19 de la Ley Federal de Procedimiento Administrativo, así como los casos en los que deban ser acreditados por el INE; que soliciten y les sea autorizada por la Autoridad Certificadora, el otorgamiento del certificado digital, previo cumplimiento de los requisitos que se establecen en el Reglamento; y

Unidad(es) Responsable(s): son los órganos centrales, delegacionales y subdelegacionales, que rinden cuentas sobre el manejo de los recursos humanos, materiales, obra pública y financieros asignados para contribuir al cumplimiento de los programas comprendidos en la estructura programática autorizada al INE.

1 PRESENTACIÓN

La información que recaba, procesa y resguarda la Dirección Ejecutiva de Administración, requiere ser tratada con 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 usuarias de la Firma Electrónica Avanzada, lo cual es responsabilidad de todos aquellos que en el estricto apego a sus funciones tratan esta información.

En función de ello, esta Dirección presenta el Documento de Seguridad[3] (en adelante Documento) que atiende al subproceso de Firma Electrónica Avanzada Institucional.

El Documento está integrado por los apartados:

I. 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 la DEA celebró mesas de trabajo con la UTTyPDP para atender las actividades de las siguientes etapas[4]:

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

[4] 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.

- **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:

    a. Fase 1. Identificación de datos personales.

    b. Fase 2. Identificación de mecanismos de obtención de datos personales.

    c. Fase 3. Identificación de medios de almacenamiento.

    d. Fase 4. Identificación de permisos y tratamiento.

    e. 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.

    b. **Fase 2.** Análisis de riesgos de datos personales y privacidad. Se identificaron 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 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 DEA incorporó el subproceso de Firma Electrónica Avanzada al Sistema de Gestión para la Protección de Datos Personales del Instituto, que permitirá verificar la seguridad en el tratamiento de los datos personales durante todo su ciclo de vida, resultando en una mejora periódica de sus controles.

2 MARCO NORMATIVO

- Título I. Capítulo II. De la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley de Datos)
- Título II. Capítulo II. De los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos)
- Título III. Capítulo II. Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales (Reglamento)

En particular:

- Artículo 50, párrafo 1, incisos e) y o) del Reglamento Interior del Instituto Nacional Electoral;
- Artículos 25, 26, 27, 28 y 29 del Reglamento para el Uso y Operación de la Firma Electrónica Avanzada en el Instituto Nacional Electoral.

3 FIRMA ELECTRÓNICA AVANZADA INSTITUCIONAL

3.1 DESCRIPCIÓN DEL PROCESO A NIVEL NEGOCIO

En 2013 el Consejo General del entonces Instituto Federal Electoral aprobó el Reglamento para el uso y operación de la Firma Electrónica Avanzada en el Instituto Federal Electoral[5], que tuvo por objeto regular la emisión, uso y revocación de la Firma Electrónica Avanzada por parte de órganos centrales, delegacionales y subdelegacionales del Instituto, para el personal[6] y prestadores de servicios -que en el ejercicio de sus atribuciones conferidas en las normas legales y reglamentarias tengan la facultad de suscribir documentos-, así como para personas jurídicamente colectivas, públicas y privadas, nacionales o extranjeras, de los partidos políticos y particulares[7].

En 2019, el Consejo del Instituto Nacional Electoral aprobó la modificación del Reglamento para el uso y operación de la Firma Electrónica Avanzada en el Instituto Nacional Electoral, cuyo objeto es establecer las bases que regulan la Firma Electrónica Avanzada en los actos, actuaciones electrónicas, mensajes de datos o documentos dentro de los procesos y procedimientos que consideren su uso conforme a las disposiciones aplicables, así como los servicios relacionados con la Firma Electrónica Avanzada, lo anterior, a fin de promover la innovación, modernización y eficiencia institucional, que permita racionalizar el gasto público y transitar hacia una cultura de ahorro de papel, sin dejar de cumplir con las atribuciones institucionales y dar continuidad a las operaciones frente a contingencias[8].

[5] Mediante acuerdo CG314/2013. Disponible: https://portalanterior.ine.mx/archivos3/portal/historico/recursos/IFE-v2/DS/DS-CG/DS-SesionesCG/CG-acuerdos/2013/Octubre/CGext201310-28-1a/CGex201310-28_ap_8.pdf

[6] Personal de la Rama Administrativa y Miembros del Servicio Profesional Electoral Nacional.

[7] Para usuarios externos que hagan uso de los sistemas y servicios informáticos, sujetos al uso de la Firma Electrónica Avanzada, atendiendo al Acuerdo INE/CG314/2013.

[8] Mediante acuerdo INE/C345/2019. Disponible en: https://repositoriodocumental.ine.mx/xmlui/bitstream/handle/123456789/111353/CGex201907-08-ap-13.pdf

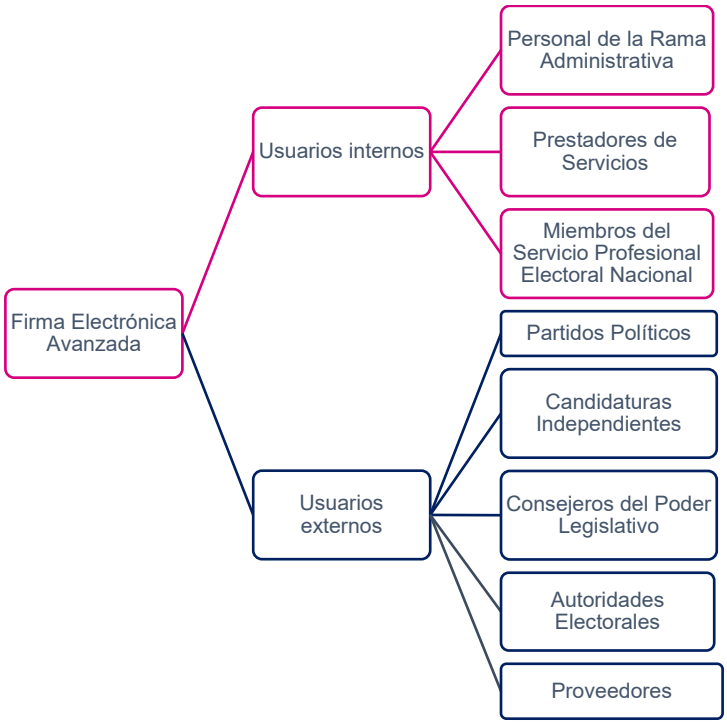


Figura 1. Usuarios de FirmaINE

La Dirección Ejecutiva de Administración tiene entre sus atribuciones el proveer lo necesario para el adecuado funcionamiento de la Rama Administrativa del personal al servicio del Instituto, así como administrar, operar y mantener los sistemas informáticos relacionados con la administración de recursos humanos[9], materiales y financieros en coordinación con la Unidad Técnica de Servicios de Informática y conforme a la normatividad aplicable en la materia.

El subproceso se apoya del Sistema de Firma Electrónica Avanzada del Instituto, el cual se compone por el Portal de Registro y Certificación, a través del cual, los usuarios internos generan el requerimiento de certificado digital (.req), la llave privada (.key) y el acuse de requerimiento, la herramienta denominada requerimiento de certificación 7.34, mediante la cual los usuarios externos generan la llave privada (.key) y el requerimiento de certificación (.req), el aplicativo Agente Certificador 7.34 que es utilizado por los Agentes Certificadores -para la expedición y revocación de los certificados digitales-, -el Portal de Agente, en el que se enrola a los usuarios y PortalFirmaINE dirigido a los usuarios internos y externos -para la firma electrónica de documentos-.

[9] Artículo 50, párrafo 1, incisos e) y o) del Reglamento Interior del Instituto Nacional Electoral.

El uso de la Firma Electrónica Avanzada Institucional[10] implica:

- La vinculación indubitable entre el firmante y las actuaciones electrónicas, actos, mensajes de datos o documentos, en que se asocia con los datos que se encuentran bajo el control exclusivo del firmante;
- Dar certeza jurídica de que los documentos, mensajes de datos, actos y actuaciones fueron emitidos y/o remitidos por el usuario interno y/o externo que firma;
- La responsabilidad de prevenir cualquier modificación o alteración en el contenido de las actuaciones electrónicas, actos, mensajes de datos o documentos electrónicos que se presentan en los procesos y procedimientos de servicios informáticos, al existir un control exclusivo de los medios electrónicos mediante la utilización de la Firma Electrónica Avanzada;
- Garantizar la integridad y autenticidad del documento contenido en las actuaciones electrónicas, actos, mensajes de datos o documentos electrónicos que sean firmados con la Firma Electrónica Avanzada, y
- La correspondencia exclusiva entre la Firma Electrónica Avanzada y el firmante, por lo que todos los documentos o mensajes de datos presentados con la misma serán responsabilidad de su titular y no serán susceptibles de repudio, con lo que se garantiza la autoría e integridad del documento.

La DEA como Autoridad Certificadora del Instituto, se encarga de llevar a cabo el enrolamiento y certificación de usuarios internos y externos, así como la revocación de los certificados digitales[11], mismas que involucra el tratamiento de datos personales. A continuación, se describen las actividades atendiendo al tipo de usuario.

A. Usuarios internos[12]

i. El usuario interno remite la Solicitud de Expedición de Certificado Digital, archivo de Alta de usuarios y su identificación oficial a la cuenta de correo electrónico autoridad.certificadora@ine.mx
ii. Los agentes certificadores verifican que los documentos sean completos y correctos, en caso de hacer falta algún documento, se le solicita al usuario interno la información faltante.
iii. La DEA solicita a la UTSI la actualización de la información en el directorio institucional.
iv. La UTSI informa a la DEA la actualización de la información.
v. El agente certificador notifica al usuario interno a través de correo electrónico la fecha y hora de su cita, con el objetivo de llevar a cabo el enrolamiento y

[10] Artículo 12 del Reglamento para el uso y operación de la Firma Electrónica Avanzada del Instituto Nacional Electoral.
[11] Atendiendo a lo señalado en el artículo 34 del Reglamento para el uso y operación de la Firma Electrónica Avanzada del Instituto Nacional Electoral.
[12] En el caso de prestadores de servicios contratados por honorarios permanentes o eventuales, se asignará su certificado con una vigencia que corresponda al periodo de su contratación.

certificación, adjuntando la guía de operación y la documentación necesaria para realizar el trámite[13].

vi. El usuario interno genera la llave privada (.key), el requerimiento (.req) y el Acuse de requerimiento de Certificado Digital en el Portal de Registro y Certificación.

vii. El agente certificador determina la vigencia y expide el certificado digital en la aplicación denominada "Agente 7.34", realiza el alta del usuario interno y enrola al usuario en el Portal Agente.

viii. El usuario interno ingresa al PortalFirmaINE, para firmar la Carta de Términos y Condiciones, así como el Acuse de requerimiento de certificado digital y los envía por correo electrónico al agente certificador asignado.

ix. El agente certificador recibe firmados electrónicamente la Carta de Términos y Condiciones, así como el Acuse de Requerimiento de certificado Digital.

x. La autoridad certificadora almacena y resguarda la información del usuario interno y certificado digital en la base de datos de Firma electrónica Avanzada.

B. **Usuarios externos**

i. El usuario externo remite los siguientes requisitos a la cuenta autoridad.certificadora@ine.mx, dependiendo el tipo de persona:

a. **Personas físicas con nacionalidad mexicana:** Solicitud de Expedición del Certificado Digital, con la firma autógrafa del solicitante, identificación oficial, Cédula de Identificación Fiscal, Clave Única de Registro de Población (CURP), justificación expresa para obtener la Firma Electrónica Avanzada.

b. **Personas morales nacionales, Partidos Políticos, Candidaturas Independientes y sus Representaciones, y/o Consejeros del Poder Legislativo**. Solicitud de Expedición del Certificado Digital, con la firma autógrafa del solicitante, identificación oficial con fotografía, Cédula de Identificación Fiscal, Clave Única de Registro de Población (CURP), documento que acredite la facultad de representación, justificación expresa para obtener la Firma Electrónica Avanzada.

ii. Los agentes certificadores verifican que los documentos sean completos y correctos, en caso de hacer falta algún documento, le solicita al usuario externo la información faltante.

iii. En caso de que la documentación sea correcta y completa, el agente certificador envía al usuario externo a través de correo electrónico, el archivo de instalación de la herramienta denominada "Requerimiento de

[13] Carta de términos y condiciones, así como la Guía para crear la llave privada (.key), Acuse y Requerimiento de Certificado Digital Usuarios Internos

Certificación 7.34", mediante la cual, se genera la llave privada (.key), y el requerimiento de certificado digital (.req), en el mismo correo se adjuntan las guías de instalación y operación de dicha herramienta.

iv. El usuario externo envía únicamente el archivo de requerimiento de certificado digital (.req) al agente certificador.

v. El agente certificador notifica al usuario externo a través de correo electrónico la fecha y hora de su cita, con el objetivo de llevar a cabo la certificación. El agente certificador determina la vigencia y expide el certificado digital del usuario externo en la aplicación denominada "Agente Certificador 7.34".

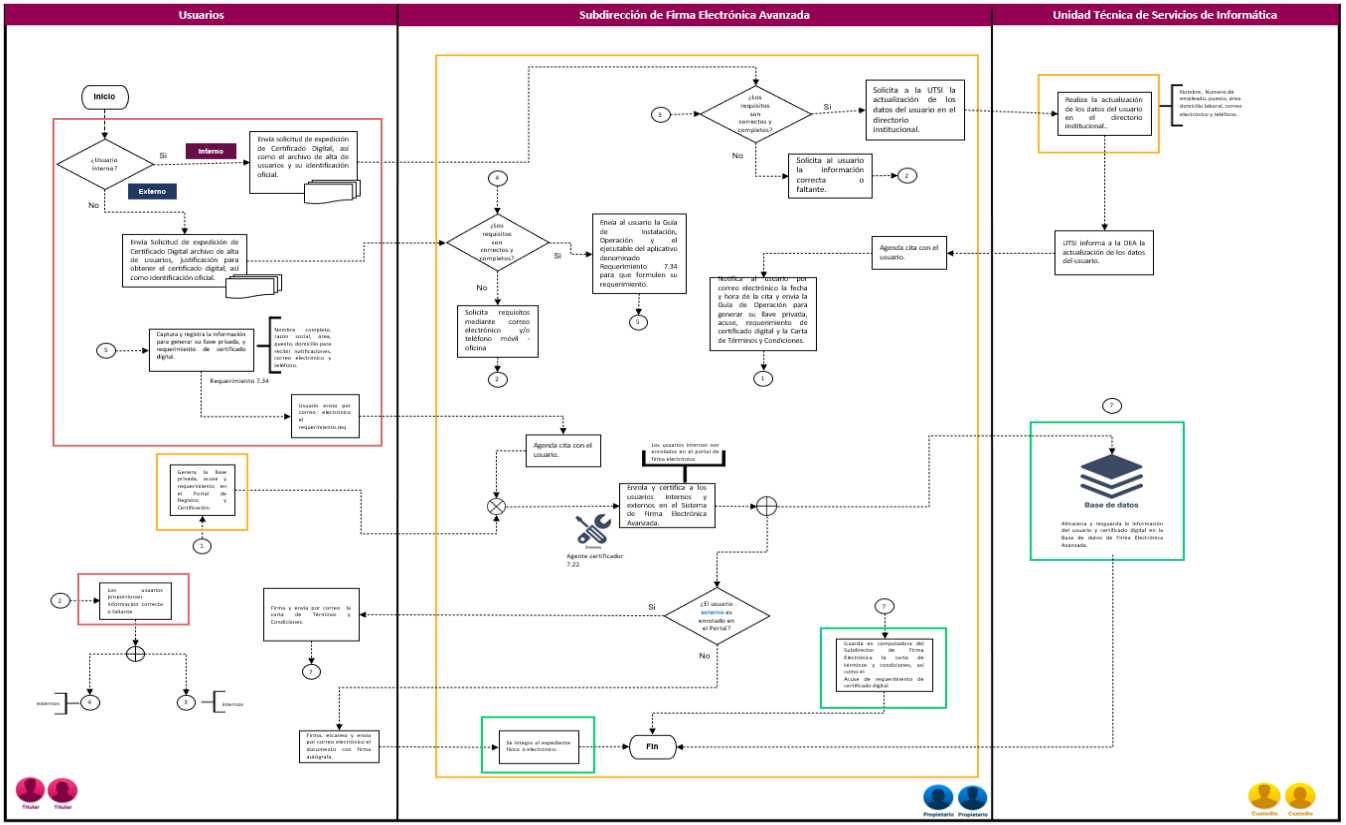
vi. En su caso, realiza el alta del usuario externo y lo enrola en el Portal de Agente.

vii. El usuario externo ingresa al PortalFirmaINE, para firmar la Carta de Términos y Condiciones la envía por correo electrónico al agente certificador asignado.

viii. La autoridad certificadora almacena y resguarda la información del usuario externo y certificado digital en la base de datos de Firma Electrónica Avanzada.

3.2 DIAGRAMA A BLOQUES

Diagrama a bloques del proceso de Firma Electrónica Avanzada Institucional



Versión	Comentarios/Descripción	Responsable de Actualización/Creación/Revisión	Fecha de Actualización/Creación /Revisión	Firma del responsable
1.0	Creación del diagrama			

Fases del ciclo de vida de los datos personales	
Color	Fase
	Creación / Colecta / Captura
	Procesamiento
	Transferencia / publicación / revelación
	Archivado / retención
	Destino final

NOTA:

En caso de que, el usuario solicite la anulación o revocación de su certificado digital –mediante correo electrónico-. La Subdirección de Firma Electrónica Avanzada le envía una constancia con su clave de anulación.

Para la consulta del diagrama en alta calidad dar clic en Diagrama de Flujo_Bloques FIRMA.pptx

4 PERSONAS QUE FUNGEN EL ROL PROPIETARIO DE LA BASE DE DATOS

Seudónimo de la Base de datos	Nombre de la persona propietaria de la base de datos	Cargo que ocupa
FEA	Mtro. Antonio Lara Rodríguez	Subdirector de Firma Electrónica Avanzada

5 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	Obligaciones
Autoridad Certificadora	Dirección Ejecutiva de Administración	• Cumplir con las políticas de seguridad. • Mantener la confidencialidad de la información. • Expedir los certificados digitales, una vez validada la documentación. • Revocar los certificados de la Firma Electrónica Avanzada. • Llevar el control y administración de los usuarios de la Firma Electrónica Avanzada. • Adoptar las medidas necesarias para difundir el uso correcto de los certificados digitales. • Autentificar que la información que se incorpora a la solicitud de certificado digital corresponda efectivamente a la identidad del solicitante. • Informar a los solicitantes, las razones por las cuales, en su caso, no fue posible emitir un certificado digital.

Función – Perfil / Rol	Cargo	Obligaciones
		• Proporcionar los medios electrónicos necesarios con el propósito de que los solicitantes estén en condiciones de generar su certificado digital. • Habilitar el uso de la Firma Electrónica Avanzada, con todas sus características, emitiendo los certificados digitales correspondientes. • Asesorar a los usuarios internos del INE para el uso del sistema de registro y certificación; así como, a los usuarios externos para el uso de la herramienta que permita generar el requerimiento de certificado digital, que el INE determine. • Fomentar y difundir el uso de la Firma Electrónica Avanzada, y otros medios electrónicos, para agilizar el desarrollo de las actividades sustantivas de los sujetos obligados de acuerdo con sus facultades o atribuciones; así como propiciar la eliminación del uso del papel de manera paulatina en las comunicaciones e intercambio de información que se lleve a cabo entre las unidades responsables. • Atender los requerimientos relacionados con las solicitudes de emisión de certificados digitales en sus respectivos ámbitos de competencia. • Adoptar e implementar las medidas necesarias, para disuadir el uso indebido de certificados digitales. • Preservar la confidencialidad, integridad y seguridad de los datos personales de los titulares de los certificados digitales observando las disposiciones aplicables en materia de

Función – Perfil / Rol	Cargo	Obligaciones
		protección de datos personales y/o datos sensibles; así como aquellas en materia de transparencia y acceso a la información pública. • Establecer los procedimientos en materia de seguridad de la información que garanticen que la generación de llaves, la expedición y revocación de certificados, los procesos de respaldo y resguardo de información, así como los demás procesos operativos relacionados con la infraestructura que soporta el sistema de registro y certificación se lleven a cabo de manera segura y enmarcados en las mejores prácticas en la materia. • Presupuestar los recursos necesarios para el uso y operación de la Firma Electrónica Avanzada de acuerdo con el ámbito de su competencia.
Agente Certificador	• Subdirector de Firma Electrónica Avanzada • Líder de Proyecto de Autoridad Certificadora • Profesional Ejecutivo de Firma Electrónica Avanzada • Informático especialista en Seguridad • Técnico Operador del Portal de Firma Electrónica • Agente Registrador y Certificador	• Recibir y revisar que las solicitudes y documentación que presenten los sujetos obligados de manera física o electrónica para la emisión de certificados digitales. • Registrar a los sujetos obligados que se les haya expedido el certificado para la utilización de la Firma Electrónica Avanzada. • Adoptar las medidas necesarias para difundir el uso correcto de los certificados digitales. • Realizar las altas, bajas, revocaciones o modificaciones de los titulares que repercutan en los certificados digitales. • Llevar registro de los certificados digitales que se emitan y de los que se revoquen.

Función – Perfil / Rol	Cargo	Obligaciones
	• Especialista en procesos de Firma Electrónica Avanzada • Asistente Operativo de Firma Electrónica Avanzada	• Notificar al solicitante respecto de inconsistencias o duplicidades en la documentación física o electrónica que presente. • Utilizar los datos personales con la finalidad para la que fueron recabados. • Cumplir con las políticas de seguridad. • Mantener la confidencialidad de la información.
Administración de la infraestructura de Firma Electrónica Avanzada	Personal de UTSI	• Coordinar la administración de la infraestructura tecnológica necesaria para la operación de la Firma Electrónica Avanzada. • Brindar la asesoría técnica que requiera la DEA para operar el sistema de registro y certificación. • Habilitar el tablero electrónico para consulta de los sujetos obligados. • Habilitar los mecanismos de consulta en línea de los certificados digitales y las listas de revocación, para obtener el estado de los certificados expedidos por el INE. • Diseñar las medidas de seguridad físicas, técnicas y administrativas para la gestión de las llaves criptográficas asociadas a la Autoridad Certificadora. • Establecer y operar los esquemas de monitoreo para garantizar la disponibilidad de la infraestructura que soporta los procesos operativos asociados a la Firma Electrónica Avanzada. • Podrá establecer y llevar a cabo auditorías internas y externas en materia de seguridad informática; en el caso de las externas, estas deberán ser coordinadas por la Secretaría Ejecutiva, conforme a la disponibilidad presupuestal del ejercicio que corresponda, que permitan identificar riesgos y vulnerabilidades potenciales en la

Función – Perfil / Rol	Cargo	Obligaciones
		infraestructura que soporta los procesos operativos asociados al sistema de registro y certificación (internos), así como ejecutar los procesos de remediación que se consideren adecuados. • Proporcionar los medios electrónicos necesarios con el propósito de que los solicitantes estén en condiciones de generar su certificado digital. • Habilitar el uso de la Firma Electrónica Avanzada, con todas sus características, emitiendo los certificados digitales correspondientes. • Fomentar y difundir el uso de la Firma Electrónica Avanzada, y otros medios electrónicos, para agilizar el desarrollo de las actividades sustantivas de los sujetos obligados de acuerdo con sus facultades o atribuciones; así como propiciar la eliminación del uso del papel de manera paulatina en las comunicaciones e intercambio de información que se lleve a cabo entre las unidades responsables. • Preservar la confidencialidad, integridad y seguridad de los datos personales de los titulares de los certificados digitales observando las disposiciones aplicables en materia de protección de datos personales y/o datos sensibles; así como aquellas en materia de transparencia y acceso a la información pública. • Establecer los procedimientos en materia de seguridad de la información que garanticen que la generación de llaves, la expedición y revocación de certificados, los procesos de respaldo y resguardo de información, así como los demás procesos operativos

Función – Perfil / Rol	Cargo	Obligaciones
		relacionados con la infraestructura que soporta el sistema de registro y certificación se lleven a cabo de manera segura y enmarcados en las mejores prácticas en la materia. • Presupuestar los recursos necesarios para el uso y operación de la Firma Electrónica Avanzada de acuerdo con el ámbito de su competencia.
Sujetos obligados para FirmaINE	Usuarios internos y externos	• Usar bajo su única y exclusiva responsabilidad la Firma Electrónica Avanzada. • Proporcionar a la Autoridad Certificadora información, datos y documentación veraces, completos y exactos al momento de solicitar su certificado. • Custodiar adecuadamente sus datos de creación de firma, la contraseña y la llave privada vinculada con ellos, a fin de mantenerlos en secreto. • Actualizar los datos proporcionados para la tramitación del certificado digital. • Solicitar a la Autoridad Certificadora la revocación de su certificado digital en caso de que la integridad o confidencialidad de sus datos de creación de firma o contraseña hayan sido comprometidos y presuma que su llave privada pudiera ser utilizada indebidamente. • Dar aviso al Agente Certificador cuando requiera realizar cualquier modificación a sus datos de identificación personal, a fin de que éste incorpore las modificaciones en los registros correspondientes y emita un nuevo certificado digital. • Hacer uso de los certificados digitales sólo para los fines autorizados, en términos de los

Función – Perfil / Rol	Cargo	Obligaciones
		procesos que para tal efecto sean implementados por el INE. • Realizar el requerimiento del certificado digital a través del sistema de registro y certificación. • Requisitar debidamente la solicitud correspondiente y firmar el acuse y la Carta de Términos y Condiciones.

6 INVENTARIO DE DATOS PERSONALES Y CATEGORIZACIÓN

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

La base de datos FEA almacena **15** datos personales de **10, 864** titulares[14], 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	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: **Físicos** • Solicitud de expedición del certificado digital • Solicitud de Revocación • Copia de documento de identificación **Digitales** • Solicitud de expedición del certificado digital	Los datos son recabados para las siguientes finalidades: • Contar con un registro actualizado de los Certificados Digitales expedidos y revocados de los usuarios internos y externos por la Autoridad Certificadora (AC) del Instituto. • Otorgar y revocar certificados digitales a los usuarios internos y externos por la autoridad certificadora del Instituto. • Llevar el control y administración de los usuarios de la Firma Electrónica Avanzada. • Expedir los certificados digitales, una vez validada la	**Sitios de almacenamiento** • Oficinas de la DEA • Oficinas de la UTSI **Medios de almacenamiento físico** • Estantes • Archiveros • Carpetas • Organizadores **Medios de almacenamiento digital** • Servidores propios • Equipos de cómputo	• Subdirector de Firma Electrónica Avanzada • Personal de la UTSI • Agentes Certificadores	No cuenta con encargados para el tratamiento de datos personales.	Solo realizaremos transferencias cuando sean necesarios para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados para las cuales no requerimos consentimiento, de conformidad con lo previsto en los artículos 22, fracción III y 70, fracción VIII de la LGPDPPSO.	No se realiza difusión de datos personales.

[14]Con corte a junio de 2023

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	Encargados del tratamiento de datos personales	Destinatarios o terceros receptos de transferencia	¿Se realiza la difusión de datos personales?
• Solicitud de Revocación • Escaneo de documento de identificación • Hoja de cálculo	documentación por parte de los Agentes Certificadores. • Revocar los certificados de la Firma Electrónica Avanzada, cuando se actualice alguno de los supuestos de revocación especificados en el capítulo VI del Reglamento para el Uso y Operación de la Firma Electrónica Avanzada en el Instituto Nacional Electoral. • Autentificar que la información que se incorpora a la solicitud de certificado digital corresponda efectivamente a la identidad del solicitante. • Informar a los solicitantes, las razones por las cuales, en su caso, no fue posible emitir un certificado digital. • Recibir y revisar que las solicitudes y documentación que presenten los sujetos obligados de manera física o electrónica para la emisión de certificados digitales cumplan con los requisitos que al efecto establezca este Reglamento de la Firma. • Realizar las altas, bajas, revocaciones o modificaciones de los titulares que repercutan en los certificados digitales.	• Laptop				

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	Encargados del tratamiento de datos personales	Destinatarios o terceros receptos de transferencia	¿Se realiza la difusión de datos personales?
	• Llevar un registro de los certificados digitales que se emitan y de los que se revoquen.					

Datos Personales recabados por categoría

13 datos personales estándar. A continuación, se listan los tipos de datos personales:

- **10 datos identificación:** Nombre completo, RFC, CURP, correo electrónico, domicilio laboral[15] o domicilio para recibir notificaciones[16] respecto a la Firma Electrónica Avanzada, código postal, país, entidad federativa, municipio y número telefónico laboral o número telefónico para recibir notificaciones respecto a la Firma Electrónica Avanzada.
- **3 datos laborales:** Organización, área, puesto.

1 dato personal sensible

- **1 documento en copia y digitalizado:** Documento de identificación -por ejemplo, Credencial para Votar-.

Datos Personales generados por categoría

1 dato personal sensible

- **1 llave pública.**

Sistema de tratamiento

Sistema de Firma Electrónica Avanzada Institucional

[15] Para usuarios internos
[16] Para usuarios externos

7 CICLO DE VIDA DE LOS DATOS PERSONALES

7.1 OBTENCIÓN

Los datos personales tratados, son obtenidos de manera directa, al momento de solicitar la expedición de la Firma Electrónica Avanzada, a través de los siguientes medios:

A. Físicos

- Solicitud de expedición del certificado digital
- Solicitud de Revocación
- Copia de documento de identificación

B. Digitales

- Solicitud de expedición del certificado digital
- Solicitud de Revocación
- Escaneo de documento de identificación
- Hoja de cálculo

7.2 ALMACENAMIENTO DE LOS DATOS PERSONALES

Los datos personales son almacenados en las instalaciones de la Dirección Ejecutiva de Administración y de la Unidad Técnica de Servicios de Informática.

7.3 USO DE LOS DATOS PERSONALES

El uso de los datos personales proporcionados por los titulares se utiliza para:

- Contar con un registro actualizado de los Certificados Digitales expedidos y revocados de los usuarios internos y externos por la Autoridad Certificadora (AC) del Instituto.
- Otorgar y revocar certificados digitales a los usuarios internos y externos por la Autoridad Certificadora del Instituto.
- Llevar el control y administración de los usuarios de la Firma Electrónica Avanzada.
- Expedir los certificados digitales, una vez validada la documentación por parte de los Agentes Certificadores.
- Revocar los certificados de la Firma Electrónica Avanzada, cuando se actualice alguno de los supuestos de revocación especificados en el capítulo VI, artículo 34 del Reglamento para el Uso y Operación de la Firma Electrónica Avanzada en el Instituto Nacional Electoral.

- Autentificar que la información que se incorpora a la solicitud de certificado digital corresponda efectivamente a la identidad del solicitante.
- Informar a los solicitantes, las razones por las cuales, en su caso, no fue posible emitir un certificado digital.
- Recibir y revisar que las solicitudes y documentación que presenten los sujetos obligados de manera física o electrónica para la emisión de certificados digitales cumplan con los requisitos que al efecto establezca el Reglamento.
- Realizar las altas, bajas, revocaciones o modificaciones de los titulares que repercutan en los certificados digitales.
- Llevar un registro de los certificados digitales que se emitan y de los que se revoquen.

7.4 DIVULGACIÓN DE LOS DATOS PERSONALES CONSIDERANDO LAS REMISIONES Y TRANSFERENCIAS

Solo realizaremos transferencias cuando sean necesarios para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados para las cuales no requerimos consentimiento, de conformidad con lo previsto en los artículos 22, fracción III y 70, fracción VIII de la LGPDPPSO.

7.5 BLOQUEO DE LOS DATOS PERSONALES

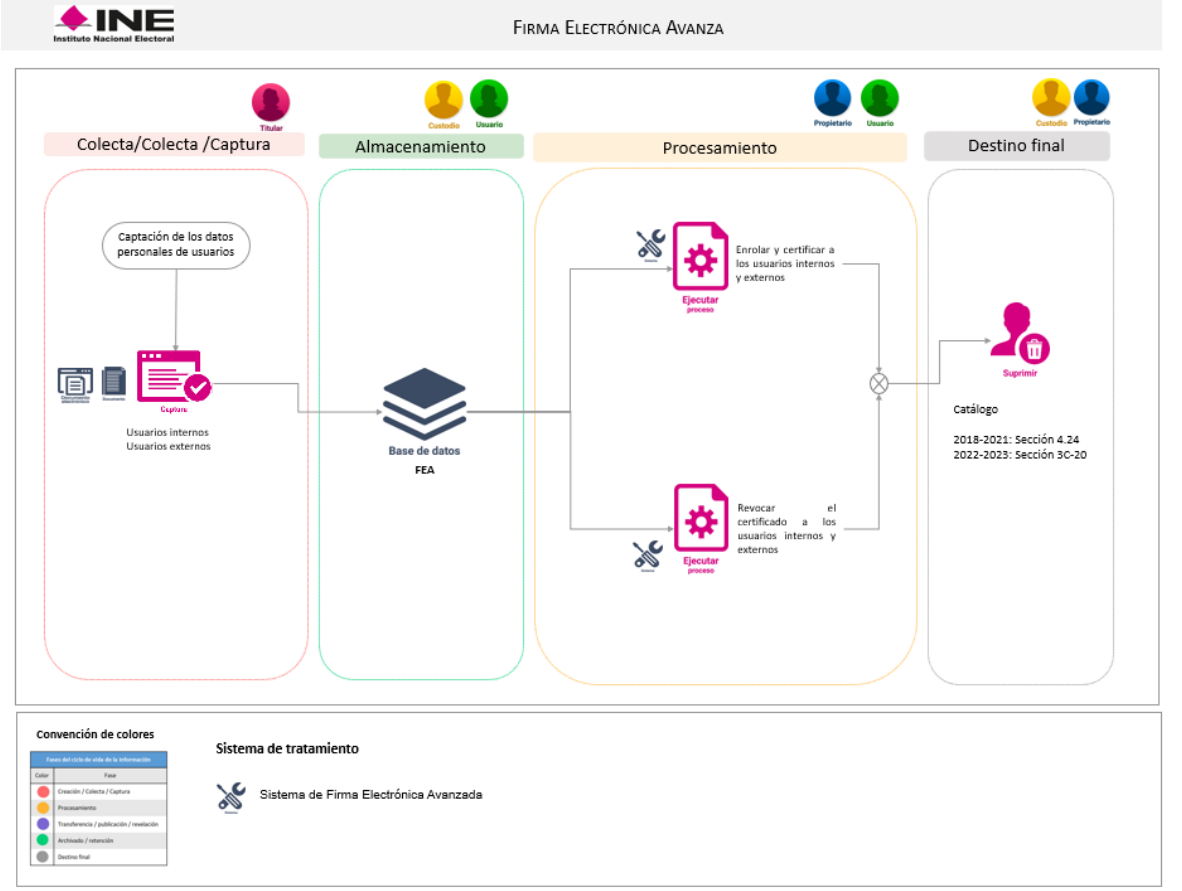
El área responsable no cuenta, a la fecha, con reglas de bloqueo de los datos personales, por lo que no se ha ejecutado la acción.

7.6 CANCELACIÓN, SUPRESIÓN O DESTRUCCIÓN DE LOS DATOS PERSONALES

Atendiendo a lo establecido por el Catálogo de disposición documental (catálogo), el tiempo de conservación es el siguiente:

Firma Electrónica Avanzada			
Vigencia del catálogo	Sección	Tiempo de conservación	Destino final
2018 -2021	4.24 Gestión administrativa de usuarios de la Firma Electrónica Avanzada.	5 años De los cuales 2 años permanecerán en el archivo de trámite y 3 años en el archivo de concentración.	Baja
2022	3C-20 – Gestión de la expedición, renovación y uso de la Firma Electrónica Avanzada Institucional	8 años De los cuales 3 años permanecerán en el archivo de trámite y 5 años en el archivo de concentración.	
2023			

7.7 DIAGRAMA DE FLUJO DE LOS DATOS PERSONALES



Para la consulta del diagrama en alta calidad dar clic en Diagrama de Flujo v0.5 firma.pptx

8 ANÁLISIS DE RIESGOS

8.1 RIESGOS INHERENTES DE LOS DATOS PERSONALES

Atendiendo a la *Metodología de Análisis de Riesgos de Privacidad y Datos Personales*[17] 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.

Riesgo inherente			
Nivel bajo: 14	**Nivel medio: 2**	**Nivel alto: 0**	**Nivel reforzado: 0**
1. Nombre completo 2. RFC 3. CURP 4. Correo electrónico 5. Domicilio laboral [18] o domicilio para recibir notificaciones [19] 6. Organización[20] 7. Área[21] 8. Puesto 9. Código Postal 10. País 11. Entidad Federativa 12. Municipio 13. Teléfono	1. Copia y escaneo de identificación 2. Llave pública		

[17] Desarrollada por la Unidad Técnica de Transparencia y Protección de Datos Personales del INE.
[18] Para usuarios internos
[19] Par usuarios externo
[20] INE para usuarios internos o la Institución a la que pertenece el usuario externo
[21] Área del INE o área de la Institución a la que pertenece el usuario externo.

8.2 ANÁLISIS DE RIESGOS DE PRIVACIDAD Y DATOS PERSONALES

El análisis de riesgos abarcó los activos relacionados con el subproceso Firma Electrónica Avanzada.

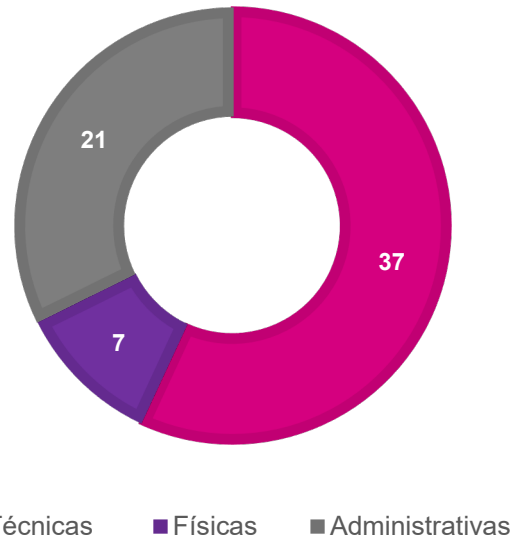
Resultado del análisis de riesgos, se detectó para el subproceso que debe **reforzar las acciones relacionadas con el archivado/retención de los datos personales** para tratar los riesgos identificados en el tratamiento al que están expuestos los mismos.

9 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[22].

Actualmente cuenta con **65** medidas de seguridad implementadas.

Gráfica 1. Medidas de seguridad implementadas



A continuación, se enlistan los **37** controles actualmente implementados a los que corresponden dichas medidas.

1. Seguridad de la información en la gestión de proyectos
2. Trabajo a distancia

[22] 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.

3. Concienciación, educación y capacitación en seguridad de la información
4. Responsabilidades ante la finalización o cambio
5. Devolución de activos
6. Manejo de la información
7. Acceso a las redes y a los servicios de red
8. Registro y baja de usuario
9. Revisión de los derechos de acceso de usuario
10. Eliminación o reasignación de los derechos de acceso
11. Uso de la información secreta de autenticación
12. Procedimientos seguros de inicio de sesión
13. Sistema de gestión de contraseñas
14. Uso de herramientas y administración de sistemas
15. El trabajo en áreas seguras
16. Áreas de carga y entrega
17. Emplazamiento y protección de equipo
18. Seguridad del cableado (Centros de cómputo)
19. Mantenimiento de equipo
20. Equipo de usuario desatendido
21. Gestión de capacidades
22. Registro de eventos
23. Sincronización del reloj
24. Restricción de la instalación de software
25. Seguridad de los servicios de red
26. Políticas y procedimientos de intercambio de información
27. Restricciones a los cambios en los paquetes de software
28. Pruebas de aceptación de sistemas
29. Respuesta a incidentes de seguridad de la información
30. Aprendizaje de los incidentes de seguridad de la información
31. Recopilación de evidencias
32. Disponibilidad de los recursos
33. Derechos de Propiedad Intelectual (DPI)
34. Protección de los registros de la organización
35. Protección y privacidad de la información personal
36. Revisión independiente de la seguridad de la información
37. Cumplimiento de las políticas y normas de seguridad

10 PLAN DE TRABAJO

El plan de trabajo para el subproceso contiene las acciones a implementar de acuerdo con los resultados del análisis de brecha y análisis de riesgos, puede observarse en la tabla siguiente:

No.	Actividad
1	Mejorar la segregación de tareas
2	Actualizar la lista de contacto con autoridades y grupos de interés especial
3	Actualizar las responsabilidades de gestión
4	Fortalecer la clasificación, etiquetado, y manejo de la información
5	Actualizar los acuerdos de confidencialidad
6	Protección de los registros de la organización

Las actividades serán atendidas por esta Dirección en el periodo de 2023 a 2024.

11 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 del cumplimiento se realiza a través de tres acciones:

1. Elaboración del programa de seguridad[23].

2. Integración al Sistema de Gestión para la Protección de los Datos Personales del Instituto Nacional Electoral (SiPRODAP), mediante la Plataforma para la Medición, Evaluación y Monitoreo del Cumplimiento en Protección de Datos Personales (PEC)[24].

3. Auditorias de Control Interno en Materia de Protección de Datos Personales, de conformidad con el Programa de Auditorías[25] vigente, establecido por la Unidad de Transparencia.

El subproceso fue integrado al SiPRODAP el 29 de agosto de 2022. Para consulta la solicitud de registro al SiPRODAP da clic **Aquí**

[23] Actividad programada en 2024.

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

[25] Aprobado por el Comité de Transparencia, mediante acuerdo INE-CT-ACG-PDP-0003-2022.

12 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[26] se detallan en los siguientes apartados.

12.1 CURSOS VIRTUALES

De acuerdo con el *Diseño curricular*, la UTTyPDP invitó al personal de la DEA 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.

Nombre del curso	Número de personas que acreditaron el módulo
Introducción a la Protección de Datos Personales	2
Principios y Deberes	1
Implementación de Deberes (Taller)	2
Comunicaciones de Datos Personales	1

12.2 CURSOS PRESENCIALES

De manera adicional, para que las áreas 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:

Nombre del curso	Número de personas que acreditaron el módulo
Análisis de brecha	2
Riesgos en la Privacidad y la Protección de Datos Personales	3
Taller de Análisis de Riesgos de Privacidad y Datos Personales	2
Plan de Trabajo	2

[26] Con corte a octubre de 2023.

12.3 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:

Nombre del curso	Número de personas que acreditaron el módulo
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	3

FIRMADO POR: GUEVARA MORALES TERESA
AC: Autoridad Certificadora del Instituto Nacional Electoral
ID: 2591442
HASH:
5692776BB609E4AB801A21B274BB68E88C8C76798E3348
7C14944C24A5BD6968

FIRMADO POR: LARA RODRIGUEZ ANTONIO
AC: Autoridad Certificadora del Instituto Nacional Electoral
ID: 2591442
HASH:
5692776BB609E4AB801A21B274BB68E88C8C76798E3348
7C14944C24A5BD6968

FIRMADO POR: ROSAS BARRIGA RAUL
AC: Autoridad Certificadora del Instituto Nacional Electoral
ID: 2591442
HASH:
5692776BB609E4AB801A21B274BB68E88C8C76798E3348
7C14944C24A5BD6968