Instituto Nacional Electoral

DOCUMENTO DE SEGURIDAD

DEL SERVICIO DE VERIFICACIÓN DE DATOS DE LA CREDENCIAL PARA VOTAR

Área Responsable: Dirección Ejecutiva del Registro Federal de Electores

INE-CT-PDP-DOC_SEG-001-2024

Versión: 1.0

Fecha de presentación: 25 de junio 2024.

Instituto Nacional Electoral

DOCUMENTO DE SEGURIDAD

Dirección Ejecutiva del Registro Federal de Electores

Coordinación de Procesos Tecnológicos

Secretaría Técnica Normativa

Macroproceso: Integración y Actualización del Registro Electoral

Proceso: Orientación, Atención y Servicios Registrales para la Ciudadanía y Actores Externos

Subproceso: Productos y Servicios Registrales a la Ciudadanía

Procedimiento: Servicio de Verificación de Datos de la Credencial para Votar

Base de datos: SVCV

Versión 1.0

Mayo 2024

CONTROL DE VERSIONES

VERSIÓN	COMENTARIO / DESCRIPCIÓN	RESPONSABLE DE LA ACTUALIZACIÓN / CREACIÓN / REVISIÓN	FECHA DE ACTUALIZACIÓN / CREACIÓN / REVISIÓN
1.0	Creación del documento	Alejandro Rodríguez Domínguez Fausto Jesús Cano Hernández	Abril 2024
1.0	Revisión del documento	Miriam Inés García Puebla Raúl Hinojos Moreno	Mayo 2024
1.0	Aprobación del documento	Alejandro Andrade Jaimes	Mayo 2024

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

HOJA DE FIRMAS

ELABORÓ:

FECHA	PUESTO	ÁREA	NOMBRE
Abril 2024	Supervisor de Servicios de Información	Dirección de Infraestructura y Tecnología Aplicada	Alejandro Rodríguez Domínguez
Abril 2024	Coordinador de Verificación de Procesos	Dirección de Infraestructura y Tecnología Aplicada	Fausto Jesús Cano Hernández

REVISÓ:

FECHA	PUESTO	ÁREA	NOMBRE
Mayo 2024	Líder de Proyectos de Investigación de Tecnologías	Dirección de Infraestructura y Tecnología Aplicada	Miriam Inés García Puebla
Mayo 2024	Dirección de Infraestructura y Tecnología Aplicada	Dirección de Infraestructura y Tecnología Aplicada	Raúl Hinojos Moreno

APROBÓ:

FECHA	PUESTO	ÁREA	NOMBRE
Mayo 2024	Coordinador de Procesos Tecnológicos	Coordinación de Procesos Tecnológicos	Alejandro Andrade Jaimes

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

CONTENIDO

DEFINICIONES

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

- **Medio de almacenamiento digital:** Es todo recurso al que se puede acceder mediante el uso de equipo que procese su contenido para examinar, modificar o almacenar los datos personales, por ejemplo, discos duros (tanto los propios del equipo de cómputo como los portátiles), memorias extraíbles como USB o SD, CD, Blu-ray, discos duros extraíbles, entre otros. También podemos contemplar como medio de almacenamiento digital, el uso de servicios de almacenamiento en línea.

- **Padrón Electoral:** Instrumento electoral conformado por registros inscritos en la sección de residentes en México y aquellos inscritos en la sección del extranjero.

- **Riesgo inherente**: Riesgo intrínseco al dato personal derivado del impacto negativo a la privacidad que puede causar en la persona.

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

- **Rol usuario:** El área autorizada para acceder a los datos. Son quienes utilizan la información.

- **Sistema de tratamiento:** Conjunto de elementos mutuamente relacionados o que interactúan para realizar la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, en medios físicos o electrónicos.[1]

- **Sitio de almacenamiento:** Instalaciones donde se resguardan los medios de almacenamiento, en cualquier soporte documental.

[1] Recomendaciones para el manejo de incidentes de seguridad de datos personales. INAI

ABREVIATURAS

- **CNDH:** Comisión Nacional de los Derechos Humanos
- **CECyRD:** Centro de Cómputo y Resguardo Documental
- **DDOS:** Dirección de Desarrollo y Operación de Sistemas
- **DERFE:** Dirección Ejecutiva del Registro Federal de Electores
- **DITA:** Dirección de Infraestructura y Tecnología Aplicada
- **INE o Instituto:** Instituto Nacional Electoral
- **LGPDPPSO:** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- **Lineamientos Generales**. Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- **SiPRODAP:** Sistema de Gestión para la Protección de Datos Personales
- **Servicio:** Servicio de Verificación de datos de la Credencial para Votar
- **UTTyPDP o Unidad de Transparencia:** Unidad Técnica de Transparencia y Protección de Datos Personales

1 PRESENTACIÓN

La Dirección Ejecutiva del Registro Federal de Electores 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 la ciudadanía, el cual, es responsabilidad de todos aquellos que en el estricto apego a sus funciones tratan esta información.

En función de ello, esta Dirección Ejecutiva **presenta el Documento de Seguridad**[2] (en adelante Documento) que atiende al procedimiento del Servicio de Verificación de Datos de la Credencial para Votar.

El Documento está integrado por los apartados:

- Descripción del macroproceso;
- Inventario de datos personales y sus sistemas de tratamiento;
- Ciclo de vida de los datos personales;
- Las funciones y obligaciones de las personas que tratan datos personales;
- Resultados del Análisis de riesgos;
- Resultados del Análisis de brecha;
- Plan de trabajo para atender los hallazgos;
- Mecanismos de monitoreo y revisión de las medidas de seguridad; y
- Programa general de capacitación.

Para atender lo anterior se realizaron 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. Identificación de la base de datos, persona propietaria y proceso.** Consiste en la identificación del proceso, subproceso, base o bases de datos personales y personas que fungen el rol de propietario.
- **Etapa 1. Identificación del flujo de los datos personales.** Contribuye a la identificación y documentación de:

[2] En cumplimiento al artículo 35 de la LGPDPPSO.

[3] Atendiendo al *Manual de Procesos y Procedimientos de "Protección de Datos Personales"*, específicamente al procedimiento de *Alineación para el Cumplimiento de Deberes de Datos Personales.*

- Los datos personales que componen cada base de datos, su categorización, tipo, personal que tiene acceso, permisos otorgados, funciones y obligaciones.
- El ciclo de vida de los datos personales, conforme al artículo 59 de los Lineamientos Generales.

- **Etapa 2 Evaluación de las medidas de seguridad.** Coadyuva a la gestión del riesgo; si bien no es posible eliminar los riesgos, es necesario identificar e implementar medidas de seguridad adecuadas a la categoría del dato personal y de su tratamiento para prevenir una vulneración.

  La obligación de establecer medidas de seguridad se encuentra contemplada en los artículos 31, 32 y 33 fracciones VI y VII de la LGPDPPSO. Esta etapa se compone de dos fases:

  Fase 1. Análisis de brecha. Su finalidad es identificar las medidas de seguridad físicas, técnicas y administrativas:

  a) existentes,
  b) faltantes, o
  c) el reforzamiento de las actuales.

  Fase 2. Análisis de riesgos de datos personales y privacidad. En esta etapa son identificados 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.** Tiene la finalidad de establecer las medidas a implementar o mejorar, en atención al artículo 33, fracción VI de la LGPDPPSO, y debe contener, al menos, los siguientes elementos:

  - El orden de prioridad de las acciones a realizar para la implementación de las medidas de seguridad faltantes, las que serán sustituidas o reforzadas detectadas en el análisis de brecha y análisis de riesgos.
  - El tiempo de ejecución.
  - La persona responsable de ejecutar las actividades.
  - Los recursos requeridos.

- **Etapa 4. Mejora continua.** La DERFE incorporará en en el tercer trimestre de 2024 el procedimiento *Servicio de Verificación de Datos de la Credencial para Votar* 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.

2 MARCO NORMATIVO

2.1 GENERAL

- Artículos 6, Base A y 16, párrafo segundo de la Constitución de los Estados Unidos Mexicanos.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Reglamento del Instituto Nacional Electoral en materia de protección de datos personales.

2.2 PARTICULAR

- Artículos 54, y 126, numeral 3, de la Ley General de Instituciones y Procedimientos Electorales.
- INE/CG92/2016. Acuerdo del Consejo General del Instituto Nacional Electoral, por el que se Aprueba la implementación del Servicio de Verificación de los datos de la Credencial para Votar, que servirá para garantizar el derecho de protección de datos de los ciudadanos, contenidos en el Padrón Electoral.
- INE/CG91/2020. Acuerdo del Consejo General del Instituto Nacional Electoral por el que se aprueban las adecuaciones para ampliar y fortalecer el Servicio de Verificación de datos de la Credencial para Votar.

3 SERVICIO DE VERIFICACIÓN DE DATOS DE LA CREDENCIAL PARA VOTAR

3.1 DESCRIPCIÓN DEL PROCESO A NIVEL NEGOCIO

El Servicio de Verificación de datos de la Credencial para Votar tiene como objetivo proporcionar un servicio de verificación de los datos de la Credencial para Votar y la comparación biométrica contra la información del Padrón Electoral, para mitigar la usurpación de identidad y prevenir el uso no autorizado de los datos personales[4]. A continuación, se detalla el procedimiento:

A. Antecedentes

Previo a la entrada en operación del Servicio de verificación el INE:

- Solicitó -proactivamente- al INAI una opinión especializada sobre la viabilidad de la aplicación del Servicio. En esta opinión, el órgano garante consideró que el servicio es una política pública socialmente útil, que beneficia tanto a los titulares como a las instituciones, y emitió recomendaciones para el cumplimiento de los principios en la materia.

- Participó en la "Firma de Bases de Colaboración para inhibir la suplantación de Identidad a través del Sistema Financiero en México", junto al INAI, la Procuraduría de la Defensa del Contribuyente, la Asociación Mexicana de Bancos y, como testigo, la Secretaría de Hacienda y Crédito Público.

B. Convenios de apoyo y colaboración

Con la finalidad de contar con servicios de información confiable, el INE celebra convenios de apoyo y colaboración con diversas instituciones, públicas o privadas, con el objeto de que cuenten con los elementos técnicos necesarios para verificar el estatus de los registros de los ciudadanos en el Padrón Electoral y la Lista Nominal

[4] Manual de proceso y procedimientos de orientación, atención y servicios registrales para la ciudadanía y actores externos. Disponible en: https://sidj.ine.mx/restWSsidj-nc/app/doc/1623/20/1

de Electores, a través de los datos contenidos en la Credencial para Votar que la ciudadanía exhibe al momento de requerir algún trámite. Entre las Instituciones que cuentan con el servicio se encuentran:

- Banco Compartamos, S.A., Institución de Banca Múltiple
- Volkswagen Leasing, S.A. de C.V.
- Fundación Dónde Banco S. A.

C. Verificación de datos de la Credencial para Votar

El INE, a través de la DERFE, diseñó el Servicio como un mecanismo para verificar los datos de la Credencial para Votar que la ciudadanía presenta al realizar trámites ante instituciones públicas o privadas con las que se han suscrito Convenios de Colaboración.

Este Servicio permite verificar la información proporcionada por las instituciones con los registros del Padrón Electoral sin que el INE divulgue datos personales de la ciudadanía, es decir, la respuesta se limita a una negativa o aprobación de la información.

La información enviada por la institución es cifrada con la llave pública del Instituto, garantizando que solo el INE pueda leerla para realizar la verificación. Es importante señalar que el Instituto no conserva la información remitida por las instituciones.

La base de datos SVCV obtiene los datos personales del Padrón Electoral, a través de un proceso de sincronización cada 24 horas, a fin de mantener la calidad de la información para las verificaciones. Por lo tanto, este proceso no implica la supresión, eliminación, borrado o destrucción de la información.

A continuación, se señalan las actividades relacionadas con la verificación de la Credencial para Votar:

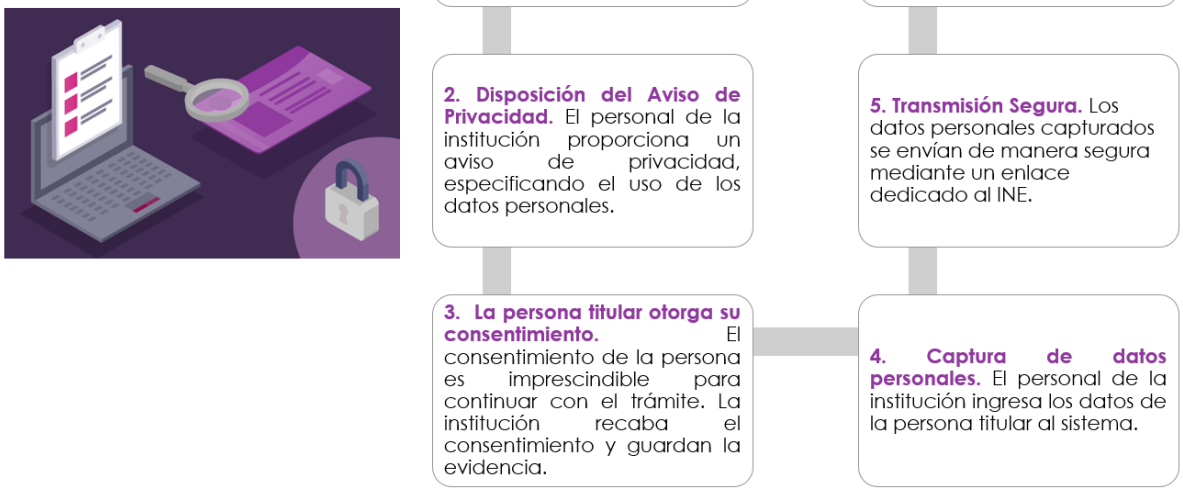


Figura 1. Descripción del procedimiento

D. Beneficios

El Servicio permite:

- Fortalecer los trabajos de depuración del Padrón Electoral y actualización de la Lista Nominal de Electores.
- Prevenir delitos como la usurpación de identidad o algún otro que pueda generar perjuicio a los titulares de los datos personales
- No vulnerar los datos personales resguardados por el INE.
- Apoyar a las instituciones que otorguen créditos, suministren bienes y servicios o realicen trámites.

El INE y las instituciones del sistema financiero trabajan para garantizar el derecho a la identidad, la tranquilidad, la honorabilidad y el patrimonio de la ciudadanía.

E. Innovación

Inicialmente, el Servicio de Verificación se diseñó para comparar datos de la credencial para votar y las huellas dactilares. Debido a la pandemia de COVID-19, se han considerado solicitudes para realizar trámites de verificación de manera remota, sin necesidad de interacción física. Para facilitar este proceso, se están implementando medidas de seguridad robustas que permitan la autenticación biométrica facial.

El INE continúa trabajando para adaptar y mejorar el Servicio de Verificación, ampliando los mecanismos de autenticación biométrica y promoviendo el uso de medios digitales seguros. Esto permitirá a las instituciones ofrecer servicios de autenticación a la ciudadanía, tanto en modalidad presencial como remota, manteniendo siempre la seguridad y confidencialidad de los datos personales.

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

En cuanto a las cuestiones administrativas, las cuotas de recuperación aportadas por las instituciones en el marco de los Convenios de Apoyo y Colaboración se destinan a la subcuenta del Fondo para la Atención Ciudadana y Mejoramiento de Módulos del Instituto Nacional Electoral. Este fondo forma parte del Fideicomiso de Administración e Inversión denominado "Fondo para el Cumplimiento del Programa de Infraestructura Inmobiliaria y para la Atención Ciudadana y Mejoramiento de Módulos del Instituto Nacional Electoral".

Cabe señalar que, este fideicomiso no trata datos personales.

3.2 DIAGRAMA A BLOQUES

Para la consulta del diagrama dar clic en este enlace.

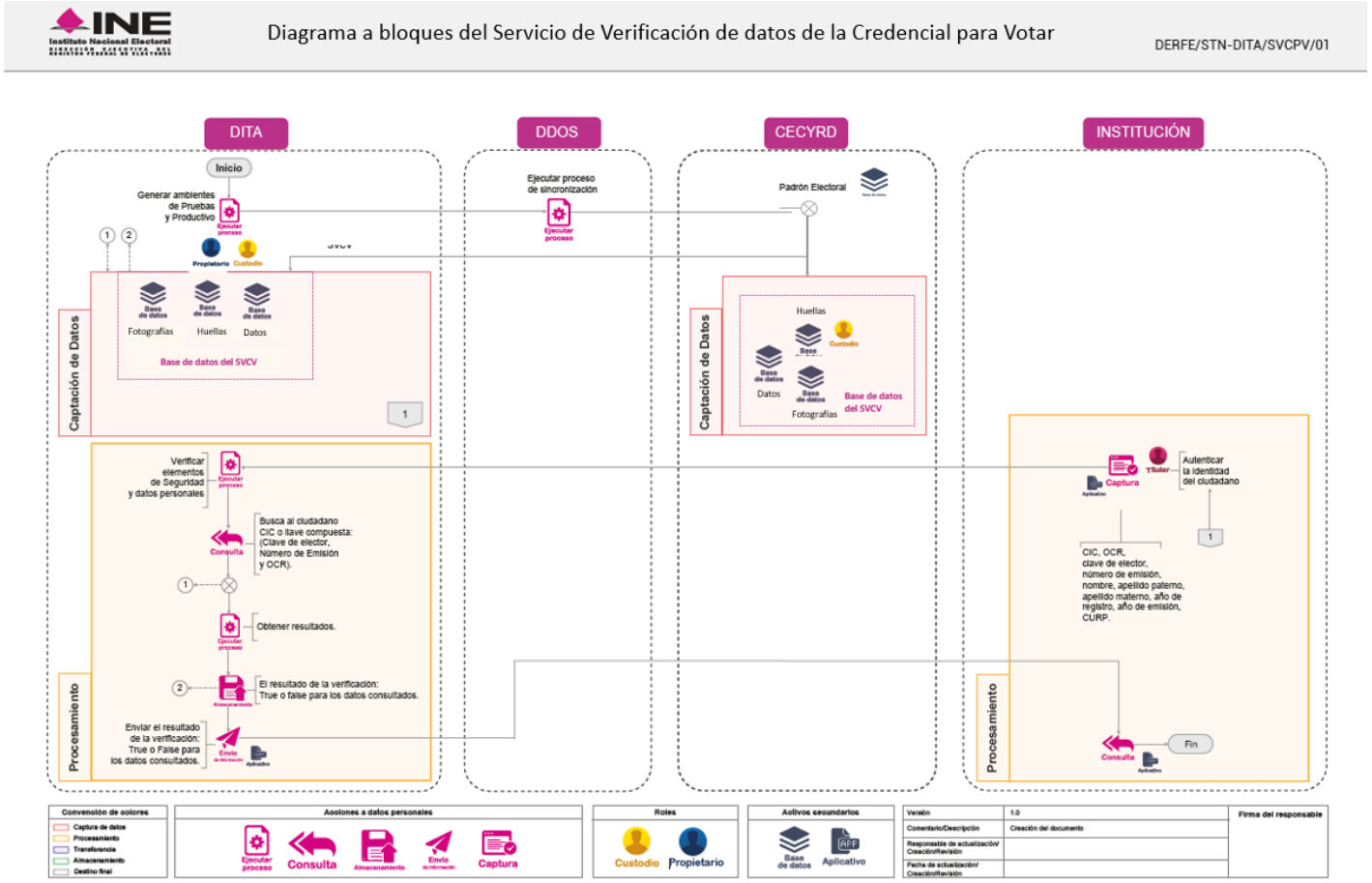


Figura 2. Diagrama a bloques del Servicio de Verificación de datos de la Credencial para Votar

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

Seudónimo de la Base de datos	Nombres de las personas propietarias de la base de datos	Cargos que ocupan
SVCV	Alejandro Andrade Jaimes	Coordinador de Procesos Tecnológicos de la Dirección Ejecutiva del Registro Federal de Electores

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 que ocupa	Obligaciones
Usuario	Técnico en Procesos Operativos	• Actualizar inventario de infraestructura y servicios de información de los centros de datos que involucren los procesos operativos a su cargo. • Implementar las políticas de seguridad de la información en los procesos operativos a su cargo. • Cumplir con las políticas de seguridad. • Mantener la confidencialidad de la información.
Usuario	Técnico en Servicios Operativos	• Apoyar en la elaboración de oficios, revisión de documentos y registro de información relacionada con las actividades del área. • Llevar a cabo la clasificación de la documentación para integrar los expedientes al archivo digital. • Mantener la confidencialidad de la información. • Mantener actualizado el inventario (Hardware y Software) de la infraestructura de servicios de información. • Revisar la documentación y dar seguimiento a las actividades relacionadas a los Convenios de Apoyo y Colaboración que establece el Instituto con instituciones públicas y privadas. • Cumplir con las políticas de seguridad.

Función (Perfil / Rol)	Cargo que ocupa	Obligaciones
Usuario	Supervisor de Servicios de Información	• Vigilar la operación de la infraestructura tecnológica y los servicios de información mediante el establecimiento de políticas preventivas y correctivas para mantener la disponibilidad de éstos. • Implementar las políticas de seguridad en la instalación de sistemas operativos y aplicaciones a cargo del área, para el cumplimiento de la normatividad establecida. • Coordinar los programas de mantenimiento preventivo y correctivo de la infraestructura tecnología que soporta los servicios, para mantener la disponibilidad continua de los mismos. • Cumplir con las políticas de seguridad. • Mantener la confidencialidad de la información.
Usuario	Técnico en Análisis de Datos	• Integrar el inventario de datos que se derivan de la operación de la infraestructura y servicios de información de los centros de datos que involucren los procesos operativos del Padrón Electoral. • Consultar la información contenida en la base de datos. • Mantener la confidencialidad de la información. • Vigilar el cumplimiento de las políticas de seguridad de la información en los procesos operativos de análisis de datos. • Cumplir con las políticas de seguridad.
Usuario	Analista de Información D	• Analizar e interpreta información estadística de los datos relacionados con el servicio de verificación • Cumplir con las políticas de seguridad. • Consultar la información contenida en la base de datos. • Mantener la confidencialidad de la información.
Usuario	Especialista en Infraestructura de Servicios	• Documentar cada una de las funcionalidades asignadas para la debida identificación de procesos operativos necesarios para el mantenimiento de la plataforma tecnológica. • Cumplir con las políticas de seguridad.
Usuario	Supervisor de Arquitectura Tecnológica	• Supervisar que la infraestructura tecnológica se instale y configure correctamente en cumplimiento con las líneas base de configuración establecidas. • Vigilar la operación de la infraestructura tecnológica y los servicios de información mediante el establecimiento de

Función (Perfil / Rol)	Cargo que ocupa	Obligaciones
		políticas preventivas y correctivas para mantener la disponibilidad de los mismos. • Implementa las políticas de seguridad en la instalación de sistemas y aplicaciones a cargo del área, para el cumplimiento de la información establecida.
Usuario	Coordinador de Verificación de Procesos Informáticos	• Cumplir con las políticas de seguridad. • Consultar la información contenida en la base de datos. • Mantener la confidencialidad de la información. • Coordinar el desarrollo de procedimientos para la aplicación de controles de seguridad y de acceso a los servicios y portales Web del Instituto. • Supervisar que la infraestructura tecnológica se instale y configure correctamente en cumplimiento con las líneas base de configuración establecidas. • Monitoreo de la operación del Servicio de Verificación.

6 INVENTARIO

Este apartado presenta el inventario de los datos personales que trata el Servicio, 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 de SVCV almacena 15 datos personales de **100,040,440**[5] personas titulares, de acuerdo con lo siguiente:

Medios de obtención	Finalidad o finalidades del tratamiento	Formatos de almacenamiento y ubicación de los datos personales	Personal que tiene acceso a los sistemas de tratamiento (cargos)	Encargados del tratamiento de datos personales	Destinatarios o terceros receptos de transferencia	¿Se realiza la difusión de datos personales?
Los datos personales, se obtienen de los titulares de forma electrónica mediante la base de datos del Padrón Electoral.	Verificar que los datos contenidos en la Credencial para Votar que presenta la ciudadanía para trámites o servicios -previo consentimiento de sus titulares- ante las instituciones públicas y/o privadas, sea auténtica, a fin de proteger su identidad y evitar usurpación o robo de dicha identidad y con ello, la posible comisión de un ilícito por parte de terceros.	**A. Sitios de almacenamiento** • Oficinas de Quantum • Oficinas CECyRD **B. Medios de almacenamiento digitales** • Servidores Virtuales • Servidores físicos	La información se encuentra contenida en el apartado *5 Funciones y obligaciones de las personas que tratan datos personales* del presente documento.	No cuenta con encargados para el tratamiento de datos personales.	No se realizan transferencias de datos personales.	No se realiza difusión de datos personales

[5] La información tiene fecha de corte a 21 de marzo de 2024.

Datos Personales por categoría
12 Datos personales estándar: ▪ **Identificación y contacto:** Apellido paterno, apellido materno, nombre (s), CIC, clave de elector, CURP, distrito, entidad, municipio, OCR, residente en el extranjero y sección. **2 Datos personales sensibles:** ▪ **De autenticación:** Huella dactilar del dedo índice derecho, huella dactilar del dedo índice izquierdo y fotografía.
Sistema de tratamiento
El sistema que trata la base de datos SVCV es el Servicio de verificación de los datos de la Credencial para Votar.

7 CICLO DE VIDA DE LOS DATOS PERSONALES

7.1 OBTENCIÓN

Los datos personales, se obtienen de los titulares de forma electrónica mediante la base de datos de Padrón Electoral, mediante un proceso de sincronización de datos que se realiza cada 24 horas.

7.2 ALMACENAMIENTO DE LOS DATOS PERSONALES

Los datos personales se almacenan en servidores propios (físicos y virtuales) en las oficinas de DERFE, en particular en el edificio de Quantum y en el Centro de Cómputo y Resguardo Documental (CECyRD).

La información que llega de las instituciones no es almacenada, solo funciona para la verificación y se arroja un resultado de coincidencias.

Los datos estándares y sensibles que se reciben en la petición de la institución, se descifran de manera segura para realizar la comparación, el servicio que realiza dicha comparación la efectúa en memoria y una vez finalizado el proceso de verificación, el contenedor de la aplicación elimina dicha memoria.

7.3 USO DE LOS DATOS PERSONALES

Verificar que los datos contenidos en la Credencial para Votar que se presenta la ciudadanía para trámites o servicios -previo consentimiento de sus titulares- ante las instituciones públicas y/o privadas, sea auténtica, a fin de proteger su identidad y evitar usurpación o robo de dicha identidad y con ello, la posible comisión de un ilícito por parte de terceros.

7.4 DIVULGACIÓN DE LOS DATOS PERSONALES CONSIDERANDO LAS REMISIONES Y TRANSFERENCIAS

No se realizarán transferencias, remisiones o divulgación de datos personales.

7.5 BLOQUEO DE LOS DATOS PERSONALES

No aplica el bloque de datos personales, ya que la información es conservada de manera permanente.

7.6 CANCELACIÓN, SUPRESIÓN O DESTRUCCIÓN DE LOS DATOS PERSONALES.

No aplica la supresión, ya que la información contenida en la base de datos se actualiza diariamente, a través de un proceso de sincronización.

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

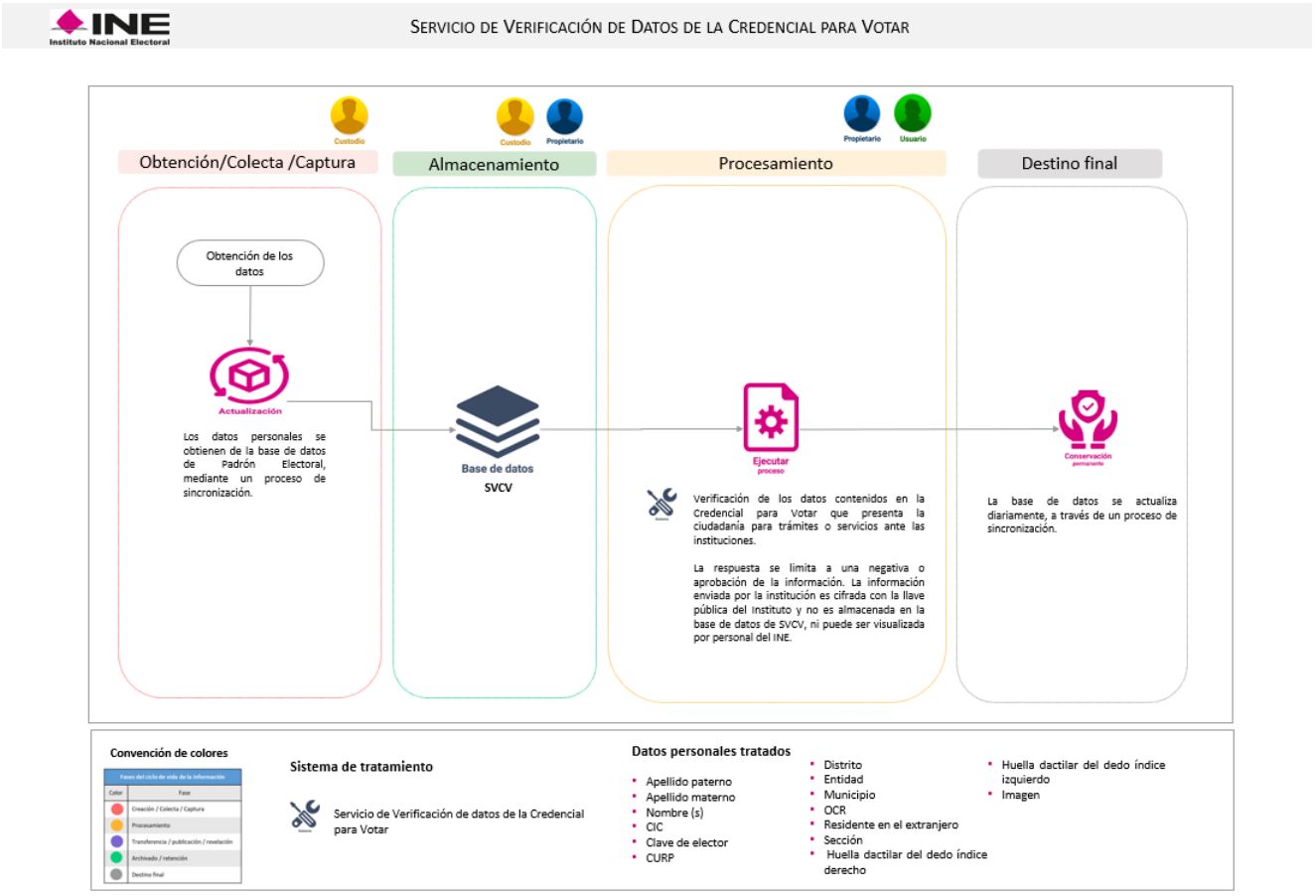


Figura 3. Diagrama de flujo

Para la consulta del diagrama dar clic en este enlace.

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*[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,
   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: 12	**Nivel medio: 2**	**Nivel alto: 0**	**Nivel reforzado: 0**
1. Apellido paterno 2. Apellido materno 3. Nombre (s) 4. CIC 5. Clave de elector 6. CURP 7. Distrito 8. Entidad 9. Municipio 10. OCR 11. Residente en el extranjero 12. Sección	1. Huellas dactilares 2. Fotografía		

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

8.2 ANÁLISIS DE RIESGOS DE PRIVACIDAD Y DATOS PERSONALES

El análisis de riesgos abarcó los activos relacionados con el procedimiento de Servicio de Verificación de Datos de la Credencial para Votar.

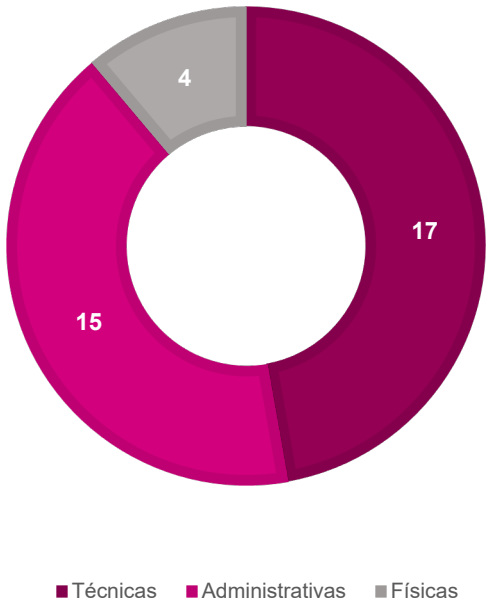
Resultado del análisis de riesgos, el área responsable detectó que debe reforzar las medidas de seguridad relacionadas con los controles de código malicioso durante la obtención de los datos personales para gestionar los riesgos identificados en el tratamiento al que están expuestos los mismos.

9 ANÁLISIS DE BRECHA

El análisis de brecha fue aplicado a los activos secundarios que intervienen en el tratamiento de los datos personales. Dicho análisis se ejecutó atendiendo a la *Metodología Análisis de Brecha para la Seguridad Aplicada a los Datos Personales,*[7] , basada en el estándar internacional *ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls*[8].

Actualmente se cuenta con **36** medidas de seguridad implementadas que se listan a continuación

Gráfica 1. Medidas de seguridad



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

[8] La Unidad de Transparencia actualizó la *Metodología Análisis de Brecha para la Seguridad Aplicada a los Datos Personales*, atendiendo al estándar internacional *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*, que aplicará a partir de junio de 2024.

A. *17 medidas de seguridad técnicas*

1. Aplicación de baseline de seguridad a la infraestructura y a nivel comunicaciones existe un aislamiento entre redes.
2. Uso de contraseñas robustas:
    - Longitud mínima de la contraseña.
    - Evitar la reutilización de un número específico de contraseñas.
    - Reglas de complejidad (mayúsculas, minúsculas, números, símbolos, etc.).
    - Cambio forzado de contraseñas en el primer inicio de sesión.
    - Encubrimiento de la contraseña mediante caracteres durante el ingreso.
3. Implementación de la herramienta Kleopatra para cifrado asimétrico en documentos que contengan datos personales.
4. Monitoreo de los puntos de acceso mediante cámaras de vigilancia.
5. Acceso al Site a través de biométricos.
6. Respaldo en dos centros de datos.
7. Implementación de Firewalls.
8. Uso del Sistema de Gestión de Vulnerabilidades definido por la Subdirección de Seguridad Informática.
9. Uso de la herramienta de Red Hat Identity Management.
10. Implementación de la herramienta de administración de sites NETBOX.
11. Creación de conexiones por medio de VPN.
12. Implementación del Protocolo SSH.
13. Autenticación MAC para conexiones a redes WiFi.
14. Programación de reglas en FIREWALL para aislar las redes productivas.
15. Realización de pruebas de seguridad para cada actualización del sistema.
16. Uso de Protocolos de comunicación HTTPS.
17. Uso de Red interna del INE.

B. *15 medidas de seguridad administrativas*

1. Directriz de Seguridad de la información de la DERFE.
2. Comunicación de las políticas de seguridad mediante correo electrónico.
3. Infografías compartidas mediante correo electrónico desde las cuentas SomosINE y Entérate.
4. Lista de contactos de correos de grupos especiales en materia de seguridad de la información.

5. Cláusulas contractuales para prestadores de servicios en contratos.
6. Declaratoria de confidencialidad.
7. Capacitaciones en materia de Protección de Datos Personales impartidos por la Unidad Técnica de Transparencia y Protección de Datos Personales y la Subdirección de Seguridad Informática.
8. Procedimiento Laboral Disciplinario.
9. Estándar de seguridad para la construcción de contraseñas.
10. Política de criptografía.
11. Pre-registros de personas visitantes a instalaciones mediante PowerApps.
12. Notificaciones sobre asistencias a actividades relacionadas con seguridad de la información.
13. Guía para la gestión y notificación de vulneraciones a la seguridad de los datos personales.
14. Revisión de lecciones aprendidas derivadas de los incidentes de seguridad que involucran datos personales, mejorando los conocimientos de riesgo y los controles de seguridad.
15. Documento relacionado con Especificaciones técnicas que incluyen características y procedimientos definidos para la seguridad de la información.

C. *4 medidas de seguridad físicas*

1. Personal de seguridad 24 horas en las instalaciones donde reside la información que contiene datos personales.
2. Acompañamiento a personas externas que ingresan al Instituto por parte del personal de Servicio de Verificación.
3. Control de acceso y vigilancia por medio de personal de seguridad del INE al área de servidores, comunicaciones y bases de datos.
4. Gestión de usuarios y privilegios de usuarios para las instalaciones.

10 PLAN DE TRABAJO

El plan de trabajo para el proceso 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	Actualizar los roles y responsabilidades en seguridad de la información.
2	Robustecer la segregación de tareas.
3	Afianzar el contacto con las autoridades.
4	Reforzar la clasificación de la información.
5	Incrementar el uso de la información secreta de autenticación.
6	Mantener la identificación de la legislación aplicable y de los requisitos contractuales.

Las actividades serán atendidas por esta Dirección en el periodo de 2024-2025.

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 de un programa de seguridad**. El Servicio de Verificación de datos de la Credencial para votar elaboró su programa, el cual tiene como objetivo monitorear y revisar de manera periódica las medidas de seguridad de los datos personales tratados por la DERFE referente al procedimiento para garantizar su confidencialidad, integridad y disponibilidad en el periodo 2024 – 2025.

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)**[9]. El procedimiento se integrará al SiPRODAP en el tercer trimestre de 2024.

3. Auditorias de Control Interno en Materia de Protección de Datos Personales, de conformidad con el Programa de Auditorías que establezca la Unidad de Transparencia.

[9] La 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.

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 se detallan en los siguientes apartados[10].

12.1CURSOS VIRTUALES

A continuación, se muestran las estadísticas de capacitación -en función del Diseño curricular- a través del Centro Virtual del INE.

Nombre del curso	Número de personas que acreditaron el módulo
Introducción a la Protección de Datos Personales	10
Principios y Deberes	1
Implementación de Deberes (Taller)	1
Implementación de Principios (Taller)	2
Comunicaciones de Datos Personales	2
Lenguaje claro	3

12.2 CURSOS PRESENCIALES Y PRESENCIALES A DISTANCIA

De manera adicional, el Instituto ofrece una capacitación especializada, a través de la Unidad de Transparencia, referente a los Deberes de Seguridad y Confidencialidad y, en particular para la conformación del Documento de Seguridad

Nombre del curso	Número de personas que acreditaron el módulo
Taller de diseño de diagramas	1
Riesgos en la Privacidad y la Protección de Datos Personales	13
Plan de Trabajo	5

[10] Con corte a marzo de 2024.

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	4
Fundamentos del Documento de Seguridad en materia de protección de datos personales	1

FIRMADO POR: RODRIGUEZ DOMINGUEZ ALEJANDRO
AC: Autoridad Certificadora del Instituto Nacional Electoral
ID: 3577138
HASH:
C82A74149CA4EB4382232C4182ADAFB739797DDBD5B1B1
30000C8005D8842092

FIRMADO POR: CANO HERNANDEZ FAUSTO JESUS
AC: Autoridad Certificadora del Instituto Nacional Electoral
ID: 3577138
HASH:
C82A74149CA4EB4382232C4182ADAFB739797DDBD5B1B1
30000C8005D8842092

FIRMADO POR: GARCIA PUEBLA MIRIAM INES
AC: Autoridad Certificadora del Instituto Nacional Electoral
ID: 3577138
HASH:
C82A74149CA4EB4382232C4182ADAFB739797DDBD5B1B1
30000C8005D8842092

FIRMADO POR: HINOJOS MORENO RAUL
AC: Autoridad Certificadora del Instituto Nacional Electoral
ID: 3577138
HASH:
C82A74149CA4EB4382232C4182ADAFB739797DDBD5B1B1
30000C8005D8842092

FIRMADO POR: ANDRADE JAIMES ALEJANDRO
AC: Autoridad Certificadora del Instituto Nacional Electoral
ID: 3577138
HASH:
C82A74149CA4EB4382232C4182ADAFB739797DDBD5B1B1
30000C8005D8842092