



# **Estrategia para el Cumplimiento de los Deberes de Seguridad y Confidencialidad para la Protección de Datos Personales 2021-2023**

Documento integrante del Programa para la Protección de Datos Personales 2018-2023, aprobado en Sesión extraordinaria del Comité de Transparencia del 8 de noviembre de 2018, mediante Acuerdo INE-CT-ACG-PDP-004-2018

(Documento integrante del Programa para la Protección de los Datos Personales 2018-2023, aprobado en sesión extraordinaria del Comité de Transparencia del 8 de noviembre de 2018)

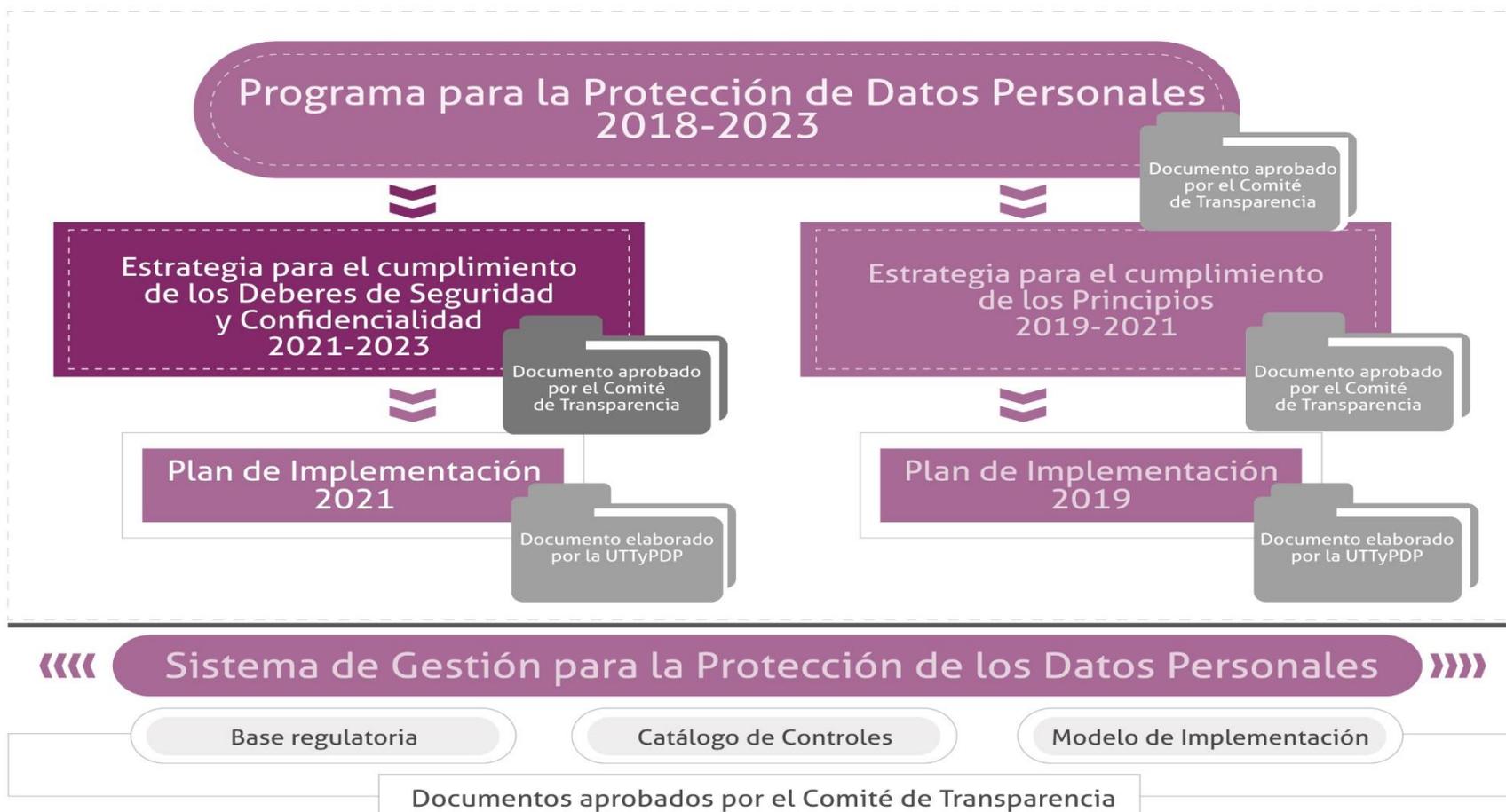


Figura 1. Modelo de Protección de Datos Personales del Instituto Nacional Electoral

## CONTENIDO

---

|        |   |    |
|--------|---|----|
| 1      | Acrónimos.....  | 5  |
| 1.1    | Áreas.....  | 5  |
| 1.2    | Instrumentos.....   | 6  |
| 2      | Definiciones.....   | 6  |
| 3      | Antecedentes.....   | 7  |
| 4      | Metodología para la selección de áreas responsables y bases de datos personales 2021-2023 ..... | 10 |
| 4.1    | Órganos centrales .....   | 12 |
| 4.2    | Órganos desconcentrados.....  | 13 |
| 4.3    | Bases de datos personales de nueva detección .....  | 15 |
| 5      | Metodología de Trabajo.....   | 16 |
| 5.1    | Actividades de la Unidad de Transparencia.....  | 16 |
| 5.2    | Actividades de las Áreas responsables.....  | 17 |
| 6      | Objeto.....   | 18 |
| 7      | Objetivo General.....   | 18 |
| 8      | Objetivos Específicos.....  | 18 |
| 9      | Alcance.....  | 18 |
| 10     | Recursos.....   | 18 |
| 11     | Actores involucrados .....  | 19 |
| 12     | Líneas de acción .....  | 19 |
| 12.1   | Acciones a corto plazo (3 a 6 meses) .....  | 19 |
| 12.2   | Acciones a mediano plazo (6 meses a 2 años).....  | 20 |
| 12.3   | Acciones a largo plazo (2 a 3 años).....  | 21 |
| 13     | Estrategia.....   | 21 |
| 13.1   | Etapa Preliminar. Identificación de la base de datos, persona propietaria y proceso .....       | 23 |
| 13.2   | Etapa 1. Identificación del flujo de los datos personales .....                                 | 24 |
| 13.2.1 | Fase 1. Identificación de datos personales .....  | 25 |
| 13.2.2 | Fase 2. Identificación de mecanismos de obtención de datos personales ..                        | 25 |

(Documento integrante del Programa para la Protección de los Datos Personales 2018-2023, aprobado en sesión extraordinaria del Comité de Transparencia del 8 de noviembre de 2018)

|        |  |    |
|--------|--|----|
| 13.2.3 | Fase 3. Identificación de medios de almacenamiento.....                | 25 |
| 13.2.4 | Fase 4. Identificación de permisos y tratamiento .....                 | 25 |
| 13.2.5 | Fase 5. Identificación del ciclo de vida de los datos personales ..... | 26 |
| 13.3   | Etapa 2. Evaluación de las medidas de seguridad.....                   | 26 |
|        | Fase 1. Análisis de brecha.....  | 27 |
| 13.3.1 | Fase 2. Análisis de riesgos de datos personales y privacidad .....     | 27 |
| 13.4   | Etapa 3. Plan de Trabajo .....   | 28 |
| 13.5   | Etapa 4. Mejora Continua .....   | 29 |
| 13.5.1 | Fase 1. Implementación de las medidas de seguridad .....               | 29 |
| 13.5.2 | Fase 2. Modelo de madurez .....  | 29 |
| 13.6   | Capacitación.....  | 30 |

# 1 ACRÓNIMOS

---

## 1.1 ÁREAS

**CAI:** Coordinación de Asuntos Internacionales

**CNCS:** Coordinación Nacional de Comunicación Social

**CT:** Comité de Transparencia del Instituto Nacional Electoral

**DEA:** Dirección Ejecutiva de Administración

**DECEyEC:** Dirección Ejecutiva de Capacitación Electoral y Educación Cívica

**DEOE:** Dirección Ejecutiva de Organización Electoral

**DEPPP:** Dirección Ejecutiva de Prerrogativas y Partidos Políticos

**DERFE:** Dirección Ejecutiva del Registro Federal de Electores

**DESPEN:** Dirección Ejecutiva del Servicio Profesional Electoral Nacional

**DJ:** Dirección Jurídica

**DS:** Dirección del Secretariado

**JDE:** Junta Distrital Ejecutiva

**JLE:** Junta Local Ejecutiva

**OIC:** Órgano Interno de Control

**SE:** Secretaría Ejecutiva

**UTCE:** Unidad Técnica de lo Contencioso Electoral

**UTF:** Unidad Técnica de Fiscalización

**UTIGyND:** Unidad Técnica de Igualdad de Género y No Discriminación

**UTSI:** Unidad Técnica de Servicios de Informática

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

**UTVOPLE:** Unidad Técnica de Vinculación con los Organismos Públicos Locales

## 1.2 INSTRUMENTOS

**Estrategia de Deberes 2018-2020:** Estrategia para el Cumplimiento de los Deberes de Seguridad y Confidencialidad 2018-2020

**Estrategia de Deberes 2021-2023:** Estrategia para el Cumplimiento de los Deberes de Seguridad y Confidencialidad 2021-2023

**LGPDPPO o Ley de Datos:** 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

## 2 DEFINICIONES

---

Para efectos del presente documento, se tomarán las definiciones establecidas en la Ley de Datos, en el Programa para la Protección de Datos Personales del INE y sin perjuicio de lo previsto en la normativa aplicable en la materia, se entenderá por:

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

**Cabeceras electorales:** Capital de la entidad federativa establecida para cada una de las cinco Circunscripciones Plurinominales Electorales en que se divide el país.

**Ciclo de vida de la información:** Las etapas de la información desde su captación hasta su borrado o conservación.

**Circunscripciones Plurinominales:** Espacio geográfico en que se divide el territorio nacional para efectos electorales. En cada circunscripción se eligen diputados y senadores por el principio de representación proporcional (RP). La Constitución establece que para la

elección de diputados federales plurinominales deberán conformarse cinco circunscripciones a nivel nacional.<sup>1</sup>

**Formatos:** Conjunto de documentos elaborados por la Unidad de Transparencia y Protección de Datos Personales, para documentar el resultado de la identificación del flujo de los datos personales.

**Persona propietaria:** La o las personas servidoras públicas de las áreas responsables que deciden sobre el tratamiento de los datos personales.

**Proceso:** Conjunto de fases sucesivas de un fenómeno natural o de una operación artificial.<sup>2</sup> Conjunto de actividades mutuamente relacionadas o que interactúan, que utilizan las entradas para proporcionar un resultado previsto<sup>3</sup>.

### 3 ANTECEDENTES

---

El Instituto Nacional Electoral ha ejecutado diversas acciones encaminadas a la protección de datos personales en su posesión, con el objetivo de garantizar este derecho humano a sus titulares y el cumplimiento de sus obligaciones, es por ello que -en 2018- el Comité de Transparencia aprobó el Programa para la Protección de Datos Personales del INE y la Estrategia de Deberes 2018-2020.

En la Estrategia de Deberes 2018-2020, la Unidad de Transparencia determinó iniciar con las actividades orientadas a la elaboración del Documento de Seguridad con cuatro Direcciones Ejecutivas del Instituto, atendiendo a los resultados las siguientes acciones:

- *Diagnóstico inicial para la adecuación de la normativa interna del Instituto Nacional Electoral a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.* Del resultado, la Unidad de Transparencia determinó la necesidad de verificar -de manera conceptual- el cumplimiento de los Deberes de Seguridad y Confidencialidad de las cuatro áreas.
- *Verificación de medidas de seguridad respecto al tratamiento de los datos personales en posesión de diversas áreas centrales del Instituto Nacional Electoral (INE).* El informe señaló actividades a seguir para el cumplimiento de los Deberes

---

<sup>1</sup> Glosario INE en línea,

[https://portalanterior.ine.mx/archivos2/CDD/Reforma\\_Electoral2014/glosario.html](https://portalanterior.ine.mx/archivos2/CDD/Reforma_Electoral2014/glosario.html)

<sup>2</sup> Diccionario de la Lengua española en línea, URL: <https://dle.rae.es/proceso>

<sup>3</sup> Gestión de Calidad. Universidad Santiago de Cali, URL:

<https://www.usc.edu.co/index.php/gestion-de-calidad/terminos-y-definiciones>

(Documento integrante del Programa para la Protección de los Datos Personales 2018-2023, aprobado en sesión extraordinaria del Comité de Transparencia del 8 de noviembre de 2018)

de Seguridad y Confidencialidad, en específico, para contar con los instrumentos que describan las medidas de seguridad que implementan dichas áreas.

Las áreas y bases de datos seleccionadas fueron:

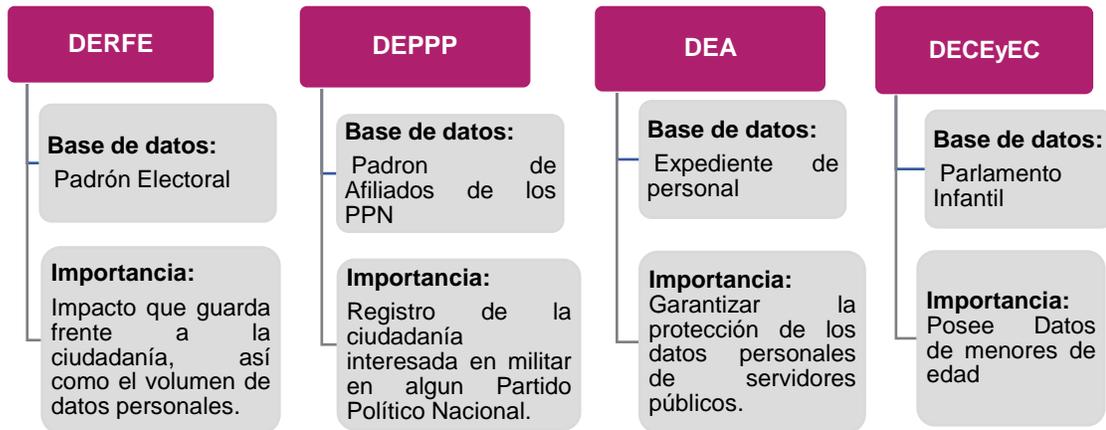


Figura 2. Áreas seleccionadas para la Estrategia de Deberes 2018-2020.

Durante su periodo de ejecución, se integraron a las actividades de acuerdo con el alcance establecido a largo plazo las siguientes áreas:



Figura 3. Áreas integradas durante la ejecución de la Estrategia de Deberes 2018-2020.

En la siguiente imagen se observa el estatus de las acciones establecidas en la Estrategia de Deberes 2018-2020, así como aquellas que se retomarán en el periodo de 2021- 2023.

(Documento integrante del Programa para la Protección de los Datos Personales 2018-2023, aprobado en sesión extraordinaria del Comité de Transparencia del 8 de noviembre de 2018)



Figura 4. Acciones de la Estrategia de Deberes 2018-2020 que se integran a la Estrategia de Deberes 2021-2023

## 4 METODOLOGÍA PARA LA SELECCIÓN DE ÁREAS RESPONSABLES Y BASES DE DATOS PERSONALES 2021-2023

En este apartado se describirá la forma en la que se seleccionarán las áreas responsables y bases de datos personales para esta Estrategia, a través de tres mecanismos:

- Bases de datos personales de los órganos centrales.
- Bases de datos personales de órganos desconcentrados.
- Bases de datos personales de nueva detección.

A continuación, se muestran las áreas que conformarán el alcance de esta Estrategia:

| Tabla 1. Distribución de áreas responsables de acuerdo con cada Estrategia |  |  |   |
|--|--|--|---|
| Áreas responsables   | Seleccionadas en Estrategia de Deberes 2018-2020 | Seleccionadas en Estrategia de Deberes 2021-2023 | Áreas que integrarán la Estrategia de Deberes 2021-2023 |
| DEA  | ✓  |  | ✓   |
| DECEYEC  | ✓  |  | ✓   |
| DEOE   | ✓  |  | ✓   |
| DEPPP  | ✓  |  | ✓   |
| DERFE  | ✓  |  | ✓   |
| DESPEN   | ✓  |  | ✓   |
| OIC  | ✓  |  | ✓   |
| SE   | ✓  |  | ✓   |
| UTF  | ✓  |  | ✓   |
| UTTyPDP  | ✓  |  | ✓   |
| CAI  |  | ✓  | ✓   |
| CNCS   |  | ✓  | ✓   |
| DJ   |  | ✓  | ✓   |
| DS   |  | ✓  | ✓   |
| JDE  |  | ✓  | ✓   |
| JLE  |  | ✓  | ✓   |
| UTCE   |  | ✓  | ✓   |
| UTIGyND  |  | ✓  | ✓   |
| UTSI   |  | ✓  | ✓   |
| UTVOPLE  |  | ✓  | ✓   |

Lo anterior se muestra de manera gráfica en la Figura 5.

(Documento integrante del Programa para la Protección de los Datos Personales 2018-2023, aprobado en sesión extraordinaria del Comité de Transparencia del 8 de noviembre de 2018)

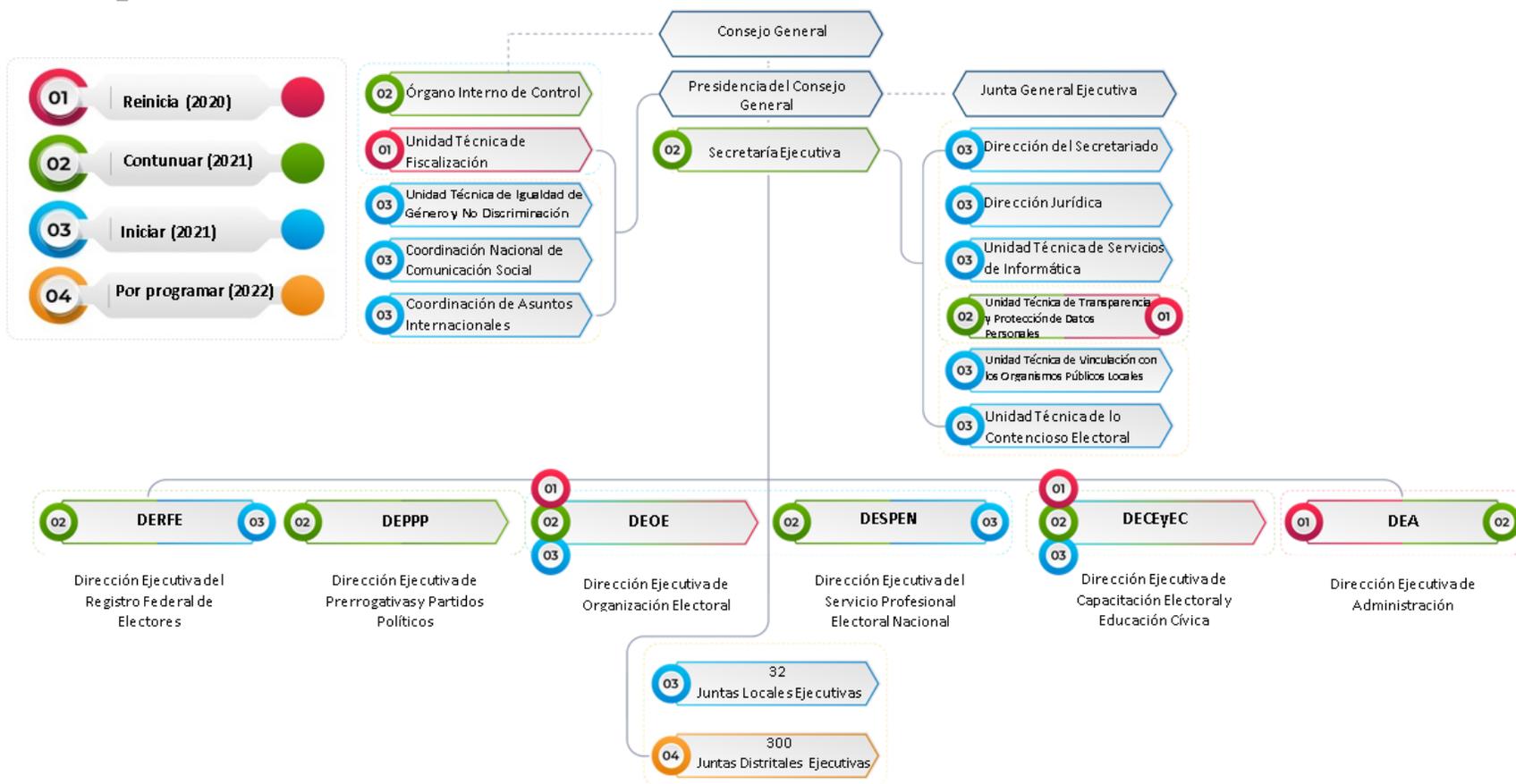


Figura 5. Programación de áreas

## 4.1 ÓRGANOS CENTRALES

Se incorporan ocho áreas del Instituto y sus sistemas de tratamiento<sup>4</sup>, con el objetivo de implementar los Deberes de Seguridad y Confidencialidad a nivel central, las cuales tendrán, al menos, el siguiente alcance<sup>5</sup>:

### a) Dirección Jurídica

- Sistema de Medios de Impugnación

### b) Dirección del Secretariado

- Sistema de la Oficialía Electoral

### c) Unidad Técnica de Igualdad de Género y No Discriminación

- Buzón de Quejas y/o Denuncias para casos de Hostigamiento y Acoso Sexual o Laboral
- Registro de asistencia a eventos organizados por la Unidad Técnica de Igualdad de Género y No Discriminación
- Base de datos plataforma “Red de Mujeres Electas”

### d) Unidad Técnica de lo Contencioso Electoral

- Sistema Integral de Quejas y Denuncias

### e) Unidad Técnica de Vinculación con los Organismos Públicos Locales

- Sistema de Vinculación con los Organismos Públicos Locales Electorales (Que contiene el Sistema de Registro para el proceso de Selección de las y los aspirantes a Consejeros Presidentes y las y los Consejeros Electorales de los Organismos Públicos Locales Electorales)

### f) Unidad Técnica de Servicios de Informática

---

<sup>4</sup> Sistemas de datos personales listados en la página web del Instituto con corte al 22 de febrero de 2021.

<sup>5</sup> Puede variar de acuerdo con los hallazgos detectados al momento de realizar el análisis de los procesos y subprocesos.

- Sistema Campus Virtual v8

**g) Coordinación Nacional de Comunicación Social**

- Directorio de medios impresos y de Internet para la gestión de publicidad y mensajes institucionales
- Directorio de Medios Nacionales y Locales, correspondientes a empresas de Televisión, Radio, Prensa Escrita y Agencias Online
- Sistema de Acreditación para el Proceso Electoral Federal 2014-2015
- Base de datos recabados mediante encuesta realizada para la integración del público participativo del Segundo Debate Presidencial
- Directorio de Proveedores, Invitados y Medios de Comunicación que asistirán al debate entre los candidatos a la gubernatura de Puebla 2019

**h) Coordinación de Asuntos Internacionales**

- Sistema de datos de contactos de Mexicanos Residentes en el Extranjero

## 4.2 ÓRGANOS DESCONCENTRADOS

Atendiendo a la cartografía electoral nacional, la Unidad de Transparencia seleccionó a los órganos delegacionales y subdelegacionales -Juntas Locales Ejecutivas y Juntas Distritales Ejecutivas<sup>6</sup>- de estados de la República donde se ubican las cinco cabeceras electorales<sup>7</sup> para sumarse a las actividades.

Los órganos desconcentrados seleccionados, corresponden a las siguientes entidades federativas:

- **Jalisco**, en Guadalajara se encuentra la cabecera de la Primera Circunscripción Plurinominal Electoral Federal<sup>8</sup>.

---

<sup>6</sup> La Unidad de Transparencia seleccionará una muestra de las Juntas Distritales Ejecutivas para analizar.

<sup>7</sup> El Consejo General del INE aprobó mediante Acuerdo INE/CG329/2017 el ámbito territorial de las cinco circunscripciones plurinominales electorales federales en que se divide el país y la capital de la entidad federativa en la que se ubica la cabecera de cada una de ellas.

<sup>8</sup> Integrada por las entidades federativas de Baja California, Baja California Sur, Chihuahua, Durango, Jalisco, Nayarit, Sinaloa y Sonora.

(Documento integrante del Programa para la Protección de los Datos Personales 2018-2023, aprobado en sesión extraordinaria del Comité de Transparencia del 8 de noviembre de 2018)

- **Nuevo León**, en Monterrey se localiza la cabecera de la Segunda Circunscripción Plurinominal Electoral Federal<sup>9</sup>.
- **Veracruz**, en Xalapa se ubica la cabecera de la Tercera Circunscripción Plurinominal Electoral Federal<sup>10</sup>.
- **Ciudad de México**, se halla la cabecera de la Cuarta Circunscripción Plurinominal Electoral Federal<sup>11</sup>.
- **Estado de México**, en Toluca de Lerdo se encuentra la cabecera de la Quinta Circunscripción Plurinominal Electoral Federal<sup>12</sup>.



**JLE Jalisco**

Guadalajara, cabecera de la primera circunscripción



**JLE Nuevo León**

Monterrey, cabecera de la segunda circunscripción



**JLE Veracruz**

Xalapa, cabecera de la tercera circunscripción



**JLE Ciudad de México**

Cabecera de la cuarta circunscripción



**JLE Estado de México**

Toluca de Lerdo, cabecera de la quinta circunscripción

Figura 6. Cabeceras electorales

La Unidad de Transparencia ha detectado dos supuestos de tratamiento de datos personales en órganos delegacionales:

<sup>9</sup> Integrada por las entidades federativas Aguascalientes, Coahuila, Guanajuato, Nuevo León, Querétaro, San Luis Potosí, Tamaulipas y Zacatecas.

<sup>10</sup> Integrada por las entidades federativas Campeche, Chiapas, Oaxaca, Quintana Roo, Tabasco, Veracruz y Yucatán.

<sup>11</sup> Integrada por las entidades federativas Ciudad de México, Guerrero, Morelos, Puebla y Tlaxcala.

<sup>12</sup> Integrada por las entidades federativas Colima, Hidalgo, México y Michoacán.

**a) Supuesto 1.** Procesos identificados durante el periodo 2018-2020 que tratan datos personales, en órganos desconcentrados:

Acción: Iniciar con los procesos identificados en la Estrategia de Deberes 2018-2020 -en los que intervienen las JLE, así como las JDE y son tratados datos personales- los cuales se listan a continuación:

- Conformación del padrón electoral y credencialización
- Orientación, atención y servicios registrales para ciudadanía y actores externos
- Fortalecimiento de la Educación Cívica y Participación Ciudadana
- Gestión de las mesas receptoras de votación y Capacitación electoral
- Administración de recursos humanos

**b) Supuesto 2.** Identificación de procesos que traten datos personales:

Acción: Celebrar reuniones con los Vocales Ejecutivos de los órganos delegacionales y subdelegaciones con la finalidad de:

- Analizar si sus procesos tratan datos personales,
- Si el área trata datos personales, entonces se identificarán las bases de datos y sistemas de tratamiento.

La Unidad de Transparencia, junto con los órganos centrales, delegacionales y subdelegaciones del Instituto ejecutarán la presente Estrategia.

### **4.3 BASES DE DATOS PERSONALES DE NUEVA DETECCIÓN**

Si, derivado de la ejecución de la estrategia, la Unidad de Transparencia junto con las áreas responsables detectan bases de datos personales y/o sistemas de tratamiento que la Unidad no tenía conocimiento de su existencia, se incorporarán a las actividades relacionadas con el cumplimiento de los Deberes de Seguridad y Confidencialidad.

## 5 METODOLOGÍA DE TRABAJO

---

### 5.1 ACTIVIDADES DE LA UNIDAD DE TRANSPARENCIA

#### a) Contacto

- I. Comunicar, mediante oficio, a la Direcciones Ejecutivas o Titulares de áreas la presente Estrategia.
- II. Establecer comunicación con el área responsable con el propósito de iniciar y/o dar continuidad a las actividades consideradas en esta Estrategia, involucrando preferentemente a su Enlace de Protección de Datos Personales.
- III. Proporcionar al personal de las áreas responsables que inician las actividades consideradas en la Estrategia, una capacitación de *Introducción a la estrategia para el Cumplimiento de los Deberes de Seguridad y Confidencialidad para la protección de datos personales*, previo al inicio de las reuniones de trabajo.

#### b) Seguimiento

- I. Enviar un resumen de los puntos tratados en las reuniones, los compromisos adquiridos y los plazos para su cumplimiento a la persona propietaria, su superior jerárquico, a los asistentes a las reuniones de trabajo y, en su caso, al Enlace de Protección de Datos Personales, a través del correo electrónico institucional.

#### c) Plazos

- I. En caso de que el área responsable no atienda los compromisos en los tiempos acordados con la Unidad de Transparencia, enviará un correo electrónico a la persona propietaria, a su superior jerárquico y, en su caso, al Enlace de Protección de Datos Personales, para establecer nuevos plazos para el cumplimiento.
- II. Si el área responsable solicita una ampliación de plazo para el cumplimiento de las actividades, la Unidad de Transparencia reprogramará los plazos, considerando los tiempos establecidos con otras áreas responsables.

#### d) Informes

(Documento integrante del Programa para la Protección de los Datos Personales 2018-2023, aprobado en sesión extraordinaria del Comité de Transparencia del 8 de noviembre de 2018)

- I. Presentar al Comité de Transparencia los informes trimestrales y el anual<sup>13</sup>, donde se indique el seguimiento y avance de las áreas.
- II. Enviar los informes trimestrales y anuales a las personas a cargo de las Direcciones Ejecutivas o Titulares de áreas, con los resultados de las actividades contenidas en los Planes anuales de Implementación.

## **5.2 ACTIVIDADES DE LAS ÁREAS RESPONSABLES**

### a) Contacto

- I. Enviar a la Unidad de Transparencia -conforme al calendario establecido por la UTTPPD y el área responsable- los lineamientos, reglamentos, procedimientos, manuales operativos o diagramas donde se documente qué datos personales son tratados o información referente a su tratamiento.
- II. Establecer comunicación con la Unidad de Transparencia para dar seguimiento a las actividades, preferentemente a través de su Enlace de Protección de Datos Personales, o de la persona propietaria.

### b) Organización

- I. Elaborar un plan de trabajo interno, con base en los procesos de negocio seleccionados que traten datos personales, donde se establezcan los plazos para el cumplimiento de las actividades. En caso de no presentarlo, se entenderá que se sujetarán a los tiempos señalados por la UTTPPD, de acuerdo con las actividades contenidas en los Planes anuales de Implementación
- II. Ejecutar las actividades señaladas en el plan de trabajo interno, respetando los plazos establecidos con la Unidad de Transparencia<sup>14</sup>.

### c) Plazos

- I. Podrá acordar con la UTTPPD una ampliación del plazo para el cumplimiento de las actividades antes de que concluya el periodo señalado en su plan de trabajo interno, con una breve justificación.

---

<sup>13</sup> Conforme al ejercicio fiscal.

<sup>14</sup> Conforme la Estrategia de Deberes y al Procedimiento para elaborar el documento de seguridad, disponibles en <https://norma.ine.mx/>.

## 6 OBJETO

---

Desarrollar las líneas de acción a corto, mediano y largo plazo, durante el periodo 2021-2023, para dar atención a los Deberes de Seguridad y Confidencialidad respecto a la protección de datos personales en posesión del INE.

## 7 OBJETIVO GENERAL

---

Establecer la ruta a seguir para que los órganos del INE -como responsables del tratamiento de los datos personales- cumplan con los Deberes de Seguridad y Confidencialidad establecidos en la LGPDPSO y las demás disposiciones aplicables.

## 8 OBJETIVOS ESPECÍFICOS

---

- Guiar a los órganos del Instituto en la elaboración de su Documento de Seguridad, a través de capacitación y entrega de materiales de apoyo.
- Apoyar a los órganos del Instituto a identificar el nivel de protección necesario para la salvaguarda de los datos personales, de acuerdo con el tipo de dato, su riesgo inherente y el tratamiento al que es sometido.
- Proveer de insumos para la implementación del Sistema de Gestión para la Protección de Datos Personales.

## 9 ALCANCE

---

El presente instrumento es aplicable para los órganos ejecutivos, técnicos, de vigilancia, en materia de transparencia, y de control, a nivel central y los órganos ejecutivos a nivel delegacional y subdelegacional que, por sus funciones, traten datos personales en el INE.

### **Excepciones**

Quedan fuera del ámbito de aplicación todos los procesos, sistemas o infraestructura que no se encuentren relacionados con el tratamiento de datos personales.

## 10 RECURSOS

---

Los planes a mediano y largo plazo deberán estar sustentados en programas y/o proyectos que contemplen los recursos materiales, financieros y humanos -de las áreas responsables del tratamiento- y el tiempo de ejecución de estos.

## 11 ACTORES INVOLUCRADOS

---

- Comité de Transparencia del INE.
- Unidad de Transparencia.
- Áreas responsables del tratamiento de los datos personales.
- En su caso, órganos vinculados con seguridad de la información (protección civil, capital humano, entre otros).

## 12 LÍNEAS DE ACCIÓN

---

La Unidad de Transparencia llevará a cabo las siguientes acciones:

### 12.1 ACCIONES A CORTO PLAZO (3 A 6 MESES)

- a) Establecer contacto con las áreas responsables que se listan para **continuar** con la implementación de los Deberes de Seguridad y Confidencialidad:

- DERFE
- DEA
- DEPPP
- DECEyEC
- DEOE
- DESPEN
- OIC
- SE
- UTF
- UTTyPDP

- b) Establecer contacto con las áreas responsables que se listan para **iniciar** con la ejecución de actividades para implementar los Deberes de Seguridad y Confidencialidad:

- CAI
- CNCS
- DJ
- SE
- UTCE
- UTIGyND
- UTSI

(Documento integrante del Programa para la Protección de los Datos Personales 2018-2023, aprobado en sesión extraordinaria del Comité de Transparencia del 8 de noviembre de 2018)

- UTVOPLE
  - JLE<sup>15</sup>
- c) Elaborar un Plan específico de capacitación y concientización para que el personal -responsable del tratamiento de los datos personales del Instituto- cuente con los conocimientos respecto del cumplimiento en las obligaciones derivadas de la protección de datos personales.<sup>16</sup>
- d) Generar un procedimiento para que los órganos del Instituto presenten su Documento de Seguridad al Comité de Transparencia.
- e) Presentar el Documento de Seguridad Institucional al CT, el cual será actualizado de manera semestral por la Unidad de Transparencia, integrando la información de los documentos generados por las áreas responsables.

## **12.2 ACCIONES A MEDIANO PLAZO (6 MESES A 2 AÑOS)**

La Unidad de Transparencia llevará a cabo las siguientes acciones:

- a) Establecer contacto con las áreas responsables que se listan para **iniciar** con la ejecución de actividades para implementar los Deberes de Seguridad y Confidencialidad:
- JDE de Jalisco
  - JDE de Nuevo León
  - JDE de Veracruz
  - JDE de Ciudad de México
  - JDE de Estado de México
- a) Efectuar auditorías internas en la materia para la verificación del cumplimiento de los Deberes de Seguridad y Confidencialidad a través del Sistema de Gestión para la Protección de Datos Personales del Instituto.
- b) Seleccionar, y en su caso diseñar, una metodología que contenga elementos (indicadores y métricas) que permitan evaluar de manera cuantitativa, el cumplimiento de las acciones para la protección de los datos.

---

<sup>15</sup> Las Juntas Locales Ejecutivas de Jalisco, Nuevo León, Veracruz, Ciudad de México y Estado de México.

<sup>16</sup> El Plan se alinearé a lo señalado en los Programas de capacitación del Instituto Nacional Electoral anuales, en materia de transparencia, acceso a la información pública, protección de datos personales y gestión documental.

- c) Efectuar auditorías externas en los **órganos centrales** del Instituto para la verificación del cumplimiento de la Ley de Datos.

## 12.3 ACCIONES A LARGO PLAZO (2 A 3 AÑOS)

Las siguientes acciones representan compromisos que la Unidad de Transparencia llevará a cabo a la conclusión de esta Estrategia:

- a) Dar seguimiento al cumplimiento de las actividades contenidas en los Planes de trabajo de las áreas responsables -establecido en el Documento de Seguridad- para la implementación de medidas de seguridad físicas, técnicas y administrativas.
- b) Efectuar auditorías externas en los **órganos delegacionales** para la verificación del cumplimiento de la Ley de Datos.

El presente documento representa la **Estrategia de cumplimiento a los Deberes de Seguridad y Confidencialidad 2021-2023**, que contiene las **líneas de acción a corto, mediano y largo plazo para cumplir con los Deberes de Seguridad y Confidencialidad en el Instituto Nacional Electoral en un ámbito técnico-normativo.**

## 13 ESTRATEGIA

---

La Estrategia de Deberes está compuesta por cinco etapas secuenciales y una transversal:

- **Secuenciales:**
  - Preliminar. Identificación de la base de datos, persona propietaria y proceso
  - Etapa 1. Identificación del flujo de los datos personales
  - Etapa 2. Evaluación de las medidas de seguridad
  - Etapa 3. Plan de trabajo
  - Etapa 4. Mejora continua
- **Transversal:**
  - Capacitación

(Documento integrante del Programa para la Protección de los Datos Personales 2018-2023, aprobado en sesión extraordinaria del Comité de Transparencia del 8 de noviembre de 2018)



Figura 7. Etapas de la Estrategia

Cada una de ellas genera un entregable y cuenta con material de apoyo para su ejecución, como se muestra a continuación:

| Etapa   | Entregable   | Material de apoyo proporcionado por la UTTYDP   |
|---|--|---|
| Preliminar. Identificación de la base de datos, persona propietaria y proceso | Directorio responsables y bases de datos.  | <ul style="list-style-type: none"> <li>Manual en materia de Seguridad de Datos Personales.</li> <li>Procedimiento para elaborar el Documento de Seguridad.</li> <li>Guía para solicitar el Dictamen de procedencia para la baja de un sistema y/o base de datos del Listado de bases de datos personales del INE</li> </ul> |
| Etapa 1. Identificación del flujo de los datos personales                     | <ul style="list-style-type: none"> <li>✓ Formato 1. Datos mínimos</li> <li>✓ Formato 2. Mecanismos de obtención</li> <li>✓ Formato 3. Sitios y medios de almacenamiento.</li> <li>✓ Formato 4. Sistema de tratamiento</li> <li>✓ Formato 5. Inventario</li> <li>✓ Formato 6. Tratamiento</li> <li>✓ Diagrama de flujo del ciclo de vida de los datos personales</li> </ul> | <ul style="list-style-type: none"> <li>Formatos del 1 al 6.</li> <li>Modelo de ciclo de vida de la información.</li> <li>Criterios para elaborar el Diagrama de flujo de los datos personales.</li> </ul>   |
| Etapa 2. Evaluación de las medidas de seguridad                               | <ul style="list-style-type: none"> <li>✓ Análisis de brecha</li> <li>✓ Informe Ejecutivo de Análisis de Brecha</li> <li>✓ Identificador de escenarios de riesgos</li> <li>✓ Análisis de riesgos</li> </ul>   | <ul style="list-style-type: none"> <li>Metodología de Análisis de brecha.</li> <li>Analizador de brecha.</li> <li>Metodología de Análisis de Riesgos en materia de Datos Personales y Privacidad.</li> <li>Identificador de escenarios de riesgos</li> </ul>  |

(Documento integrante del Programa para la Protección de los Datos Personales 2018-2023, aprobado en sesión extraordinaria del Comité de Transparencia del 8 de noviembre de 2018)

| Etapa   | Entregable                                    | Material de apoyo proporcionado por la UTTYPDP |
|---|---|--|
|   | ✓ Informe Ejecutivo de Analisis de Riesgos    | • Analizador de Riesgos.                       |
| Etapa 3. Plan de trabajo  | Plan de trabajo                               | Plantilla de Plan de trabajo                   |
| Etapa 4. Mejora continua  | Informe de verificaciones internas o externas | No aplica                                      |
| Capacitación  | Constancias                                   | Disponible en cada curso o taller.             |
| <p>El entregable general es el <b>Documento de Seguridad de las áreas responsables</b> quienes deberán presentarlo ante el Comité de Transparencia<sup>17</sup> conforme al Procedimiento<sup>18</sup> establecido por la Unidad de Transparencia para tal fin.</p> <p>Estos documentos abonarán para la actualización del Documento de Seguridad Institucional<sup>19</sup>- de conformidad con lo establecido en el artículo 35 de la LGPDPPSO.</p> |   |  |

Las áreas responsables elaborarán un calendario de trabajo para la entrega de la información, revisión de material y reuniones para la aclaración de dudas, en cada una de las etapas, atendiendo a los periodos establecidos en los Planes de implementación anuales.

Las etapas antes listadas se describen a continuación.

### **13.1 ETAPA PRELIMINAR. IDENTIFICACIÓN DE LA BASE DE DATOS, PERSONA PROPIETARIA Y PROCESO**

Para iniciar la implementación, adecuación o mejora de las medidas de seguridad aplicadas a los datos personales -y de esta manera cumplir con los Deberes de Seguridad y Confidencialidad- es indispensable que las áreas **identifiquen el proceso/subproceso** -de acuerdo con las actividades realizadas con la DEA- y **la base o las bases de datos personales** y la persona o personas propietarias.

<sup>17</sup> Artículo 31 del Reglamento del Instituto Nacional Electoral en materia de Protección de Datos Personales.

<sup>18</sup> Procedimiento para presentar el Documento de Seguridad ante el Comité de Transparencia, aprobado mediante acuerdo INE-CT-ACG-PDP-001-2021.

<sup>19</sup> Integrado por la Unidad de Transparencia.

Para tal efecto, la Unidad de Transparencia:

- a) **Conciliará** la información que previamente hubiere obtenido con motivo de la observación de Principios.
- b) **Establecerá contacto** con los responsables de los sistemas que tratan datos personales -conforme a las cédulas descriptivas de cada uno<sup>20</sup>-, para corroborar quien es la persona propietaria del tratamiento, así como para para identificar los procesos y bases de datos relacionadas.
- c) **Celebrarán mesas de trabajo** con las personas propietarias de las bases de datos para iniciar las siguientes actividades:
  - i. integrar la información del Documento de Seguridad, mediante la ejecución de las Etapas 1 a 4 de la presente Estrategia; o, en su caso,
  - ii. si se identifica que ya no existe tratamiento de datos personales, las personas propietarias deberán iniciar el proceso de baja de los datos personales conforme a la normativa archivística aplicable.

**Entregable de la Etapa Preliminar. Identificación de la base de datos, persona propietaria y proceso**

- Directorio responsables y bases de datos.

*Figura 8. Entregables de la Etapa Preliminar*

## 13.2 ETAPA 1. IDENTIFICACIÓN DEL FLUJO DE LOS DATOS PERSONALES

Esta etapa tiene las siguientes finalidades:

- a) **Identificar los datos personales** que componen cada base, su clasificación, tipo, el personal que tiene acceso, los permisos otorgados, funciones y obligaciones;
- b) **Identificar y documentar el ciclo de vida** de los datos personales, conforme al artículo 59 de los Lineamientos Generales;

El área responsable identificará el flujo de los datos personales -con apoyo de la Unidad de Transparencia y, en su caso, los órganos vinculados con tecnologías de la información -

<sup>20</sup> Es importante señalar que, en el Listado de Bases de Datos Personales, misma que se encuentra en la página oficial del INE, no se contemplan algunos sistemas, por lo que uno de los objetivos de la identificación de la persona propietaria del sistema es actualizar dicho listado. Disponible en [http://portalanterior.ine.mx/archivos3/portal/historico/contenido/XXXII\\_Listado\\_de\\_sistemas\\_de\\_datos\\_personales/](http://portalanterior.ine.mx/archivos3/portal/historico/contenido/XXXII_Listado_de_sistemas_de_datos_personales/)

mediante el llenado de los formatos que se describen en el Anexo I y la elaboración del diagrama de flujo-

Se compone de cuatro fases:

### **13.2.1 Fase 1. Identificación de datos personales**

El área responsable, con apoyo de las áreas custodias y de la Unidad de Transparencia, deberá identificar los datos personales, tipo y categorización -estándar, sensible o especial- que están siendo tratados en el proceso que esté a su cargo.

En caso de no ser así, el área responsable deberá prescindir de los mismos y no incluirlos en nuevos procesos de recolección.

### **13.2.2 Fase 2. Identificación de mecanismos de obtención de datos personales**

El área responsable deberá identificar la forma a través de la cual se recaban los datos personales, proporcionando elementos para verificar si los datos se obtienen de una manera libre, específica e informada.

### **13.2.3 Fase 3. Identificación de medios de almacenamiento**

El área responsable deberá identificar:

- a) Los sitios, medios, soportes documentales y formatos utilizados para almacenar los datos personales,
- b) Si se resguardan en un sitio específico o en un área común, y
- c) Si son resguardados en medios de almacenamiento físicos o digitales.

Incluye a encargados, destinatarios o terceros receptores de las transferencias que se efectúen.

### **13.2.4 Fase 4. Identificación de permisos y tratamiento**

El área responsable procederá a identificar al personal y, en su caso, prestadores de servicios, incluyendo a los encargados, destinatarios o terceros que intervengan en el tratamiento de los datos personales.

La identificación contempla el puesto, rol, los permisos que son asignados al personal para llevar a cabo el tratamiento, así como las obligaciones.

Esta fase se relaciona con el periodo de retención de la información.<sup>21</sup>

Referente al sistema de tratamiento, la persona propietaria identificará:

- a) El nombre, objetivo, fecha de creación y última actualización;
- b) El área dueña del sistema -en caso de diferir de la persona propietaria-;
- c) El área responsable de su desarrollo y mantenimiento;
- d) Si el sistema de tratamiento es manual, automatizado o mixto.

### 13.2.5 Fase 5. Identificación del ciclo de vida de los datos personales

Con base en la información recabada en las fases anteriores, el área responsable identificará los datos personales que son tratados en el proceso y en cada fase del ciclo de vida de los datos personales considerando los activos secundarios utilizados y los roles involucrados en el tratamiento a través de la elaboración un diagrama de flujo.

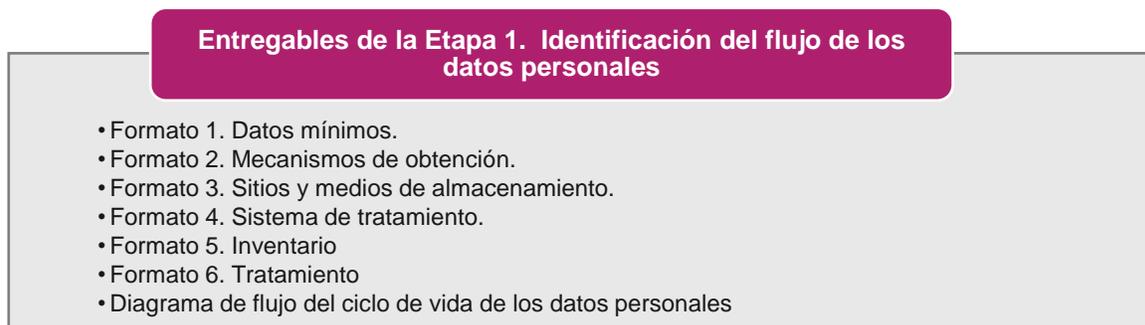


Figura 9. Entregables de la Etapa 1

## 13.3 ETAPA 2. EVALUACIÓN DE LAS MEDIDAS DE SEGURIDAD

Esta etapa tiene como finalidad 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 con la finalidad de proteger los datos personales de 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 LGPDPSO.

Se compone de dos fases:

<sup>21</sup> Las áreas deberán atender lo establecido en el Catálogo de Disposición Documental, el Cuadro General de Clasificación Archivística del INE y demás normas de Archivo.

## **Fase 1. Análisis de brecha**

El área responsable identificará las medidas de seguridad físicas, técnicas y administrativas:

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

De acuerdo con el **artículo 33 fracción V** de la LGPDPPSO y el **artículo 61 de los Lineamientos Generales**.

El análisis lo realizará la persona propietaria -con apoyo de la Unidad de Transparencia y, en su caso, los órganos vinculados con seguridad de la información, protección civil o capital humano, entre otros- mediante la **ejecución de la herramienta Analizador de brecha** (Anexo II), mediante la cual:

1. **Identificarán** -a través de un cuestionario- los controles de seguridad implementados en el proceso de tratamiento para posteriormente determinar los controles faltantes o el reforzamiento de los existentes.
2. **Clasificarán** las medidas de seguridad por cada control identificado.

### **13.3.1 Fase 2. Análisis de riesgos de datos personales y privacidad**

La persona propietaria identificará 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.

Lo anterior en atención al **artículo 33 fracción IV** de la LGPDPPSO y el **artículo 60 de los Lineamientos Generales**.

El análisis lo realizará la persona propietaria -con apoyo de la Unidad de Transparencia y, en su caso, los órganos vinculados con seguridad de la información - mediante la **ejecución de las herramientas Identificador de escenarios de riesgos** (Anexo III) y **Analizador de Riesgos** (Anexo IV), mediante las cuales:

1. **Identificarán** -a través de un cuestionario- los escenarios de riesgo existentes en cada una de las fases del ciclo de vida de los datos personales y de acuerdo con el tipo de dato personal.
2. **Analizarán** – a través de formatos- los eventos temidos, amenazas y sus fuentes por cada uno de los escenarios de riesgos previamente identificados.
3. **Identificarán** los riesgos y su posibilidad de ocurrencia.

**Entregables de la Etapa 2. Evaluación de las medidas de Seguridad**

- Análisis de brecha
- Informe Ejecutivo de Análisis de Brecha
- Identificador de escenarios de riesgos
- Análisis de riesgos
- Informe Ejecutivo de Análisis de Riesgos

*Figura 10. Entregables de la Etapa 2*

### 13.4 ETAPA 3. PLAN DE TRABAJO

La persona propietaria de la base de datos identificará, al menos, los siguientes elementos para elaborar el Plan de Trabajo –en atención al **artículo 33 fracción VI** de la LGPDPSO:

- 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, y
- Los recursos requeridos

Con base a la identificación, la persona propietaria:

1. **Elaborará** y dará a conocer a la Unidad de Transparencia el Plan de trabajo para la implementación o adecuación de las medidas de seguridad –de acuerdo con sus actividades generales y con relación a la prioridad de las acciones-
2. **Determinará** los recursos necesarios para cumplir con las acciones en el periodo establecido.

**Entregable de la Etapa 3. Plan de Trabajo**

- Plan de trabajo

*Figura 11. Entregable de la Etapa 3*

## **13.5 ETAPA 4. MEJORA CONTINUA**

La persona propietaria iniciará un proceso de mejora continua, que permitirá verificar la seguridad en el tratamiento de los datos personales, lo que generará una mejora periódica de sus controles.

El monitoreo y revisión del cumplimiento de la protección de los datos personales se llevará a cabo mediante del Sistema de Gestión para la Protección de los Datos Personales del Instituto Nacional Electoral<sup>22</sup> (SiPRODAP), con apoyo de la Plataforma para la Medición, Evaluación y Monitoreo del Cumplimiento en Protección de Datos Personales (PEC).

Esta etapa se integra por las fases que a continuación se describen:

### **13.5.1 Fase 1. Implementación de las medidas de seguridad**

Con base en el Plan de trabajo se realizará lo siguiente:

- a) El área responsable deberá **implementar las medidas** de seguridad que son necesarias para proteger los datos personales.
- b) La Unidad de Transparencia **verificará que la implementación** se realice conforme a lo establecido en el Plan de trabajo.
- c) En caso de detectar desfases, la Unidad de Transparencia **identificará el nivel de riesgo** al que se expondrán los datos personales derivado de la falta de los controles y determinará las acciones correspondientes, mismas que deberán comunicar a los titulares de las áreas y al CT.

### **13.5.2 Fase 2. Modelo de madurez**

La Unidad de Transparencia podrá realizar **auditorías internas en la materia** - de conformidad con lo establecido en el SiPRODAP-con la siguiente temporalidad:

- **Totales**<sup>23</sup>: al menos cada dos años para determinar el nivel de madurez de las áreas con respecto al cumplimiento de los Deberes de Seguridad y Confidencialidad.
- **Parciales**<sup>24</sup>: de manera periódica, atendiendo al Programa de Auditorías Internas<sup>25</sup>.

---

<sup>22</sup> Aprobado por el Comité de Transparencia, mediante acuerdo INE-CT-ACG-PDP-001-2019

<sup>23</sup> Se refiere a auditorías internas ejecutadas todo el proceso y abarcando todos principios, deberes, derechos y demás obligaciones establecidas en la LGPDPPSO.

<sup>24</sup> Se refiere a auditorías internas ejecutadas a una parte del proceso y seleccionando principios, deberes, derechos o demás obligaciones establecidas en la LGPDPPSO.

<sup>25</sup> Documento que se presentará al Comité de Transparencia en el mes de mayo del 2021.

Lo anterior, atendiendo al **artículo 33, fracción VII** de la LGPDPPSO, relacionado con el monitoreo y revisiones periódicas de las medidas de seguridad implementadas.

La Unidad de Transparencia, de estimar necesario, podrá solicitar una evaluación por parte de un tercero.

### **13.6 CAPACITACIÓN**

La Unidad de Transparencia llevará a cabo dos acciones de capacitación con las áreas responsables:

- a) **Modalidad presencial en línea** para que las personas responsables del tratamiento identifiquen claramente las actividades a realizar en cada una de las etapas, previo a la ejecución de cada una.
- b) **Modalidad virtual**, que se lleva a cabo de manera permanente a través de la Plataforma de Capacitación Institucional.

Las personas propietarias deberán integrar las constancias generadas en cualquiera de las dos modalidades en su Documento de Seguridad para acreditar la capacitación constante.