Programa para la Protección de Datos Personales del Instituto Nacional Electoral

(Anexo Único del Acuerdo INE-CT-ACG-PDP-004-2018,

Aprobado en sesión extraordinaria del Comité de Transparencia, el 8 de noviembre de 2018)

Programa para la Protección de Datos Personales del Instituto Nacional Electoral

(Anexo Único del Acuerdo INE-CT-ACG-PDP-004-2018,

Aprobado en sesión extraordinaria del Comité de Transparencia, el 8 de noviembre de 2018

CONTENIDO

Programa para la Protección de Datos Personales

del Instituto Nacional Electoral

(Anexo Único del Acuerdo INE-CT-ACG-PDP-004-2018,

Aprobado en sesión extraordinaria del Comité de Transparencia, el 8 de noviembre de 2018

1 GLOSARIO

Áreas: 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.

Base de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Custodio: Área que implementa las medidas de seguridad de la información y asesora a los propietarios sobre los mecanismos de seguridad existentes.

Datos Personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Datos personales sensibles: Aquellos que se refieren a la esfera más íntima del titular, o cuya utilización indebida puede dar origen a discriminación que conlleve un riesgo grave para este. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que pueden relevar aspectos como origen racial o técnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Encargado: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que solo o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable. También tendrá el carácter de encargado quien preste el servicio de cómputo en la nube.

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

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

Propietario: El área dueña de datos personales, que toma decisiones respecto a su tratamiento y es el responsable final de la protección y el uso de los datos.

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

Responsable: Los sujetos obligados a los que hace referencia el artículo 1 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que deciden sobre el tratamiento de los datos personales.

SNT: Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

Titular: La persona física a quien corresponden los datos personales.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionados con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Usuario: El área autorizada para acceder a los datos. Son quienes utilizan la información.

2 PREÁMBULO

Por lo que se refiere a la Ley de Datos, en el Título Segundo establece los Principios y Deberes que el responsable (INE) deberá observar en el tratamiento de los datos personales.

En este sentido, el principio de responsabilidad (artículo 29) indica que el responsable deberá implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidas en la Ley y rendir cuentas –sobre el tratamiento de los datos personales en su posesión– al titular y al INAI.

Con respecto a los mecanismos para cumplir con el principio de responsabilidad, la Ley señala que se deben adoptar, al menos, los siguientes (artículo 30):

- Destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales;
- Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización;
- Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;
- Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;
- Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;
- Establecer procedimientos para recibir y responder dudas y quejas de los titulares;
- Diseñar, desarrollar e implementar políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la Ley y las que resulten aplicables en la materia;
- Finalmente, el responsable debe garantizar que las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la Ley y las que resulten aplicables en la materia.

En el mismo contexto, derivado del Diagnóstico de la situación normativa realizado en 2017, la Unidad de Transparencia realizó a principios de 2017, el Proyecto denominado “Análisis normativo del impacto que la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados tendrá en las disposiciones internas vigentes del Instituto”, con el objetivo de establecer las bases procedimentales, temporales, lógicas, y materiales, para la gestión del proyecto consistente en la implementación del Reglamento del Instituto Nacional Electoral en materia de protección de datos personales.

Como resultado de este análisis se detectaron 48 espacios de riesgo legal, clasificados con prioridad alta, media y baja.

Entre los riesgos clasificados con prioridad alta se encuentran los derivados de los principios y deberes de la protección de datos, que resultan en acciones inmediatas en términos de la Ley de Datos, incluyendo las obligaciones que requieren una actuación del Instituto en el corto plazo.

Aunado a lo anterior, en el cuarto trimestre del 2017, la Unidad de Transparencia realizó otro estudio –a nivel conceptual- enfocado a los Deberes de Seguridad y Confidencialidad con el fin de conocer e identificar las medidas de seguridad implementadas por los responsables del tratamiento de los datos y verificar las áreas de oportunidad que pudieran existir para alinearlas con lo que establece la Ley de Datos.

Con la finalidad de cumplir con el artículo transitorio séptimo, el 22 de noviembre de 2017, el Consejo General aprobó el Reglamento del Instituto Nacional Electoral en materia de protección de datos personales, mismo que fue publicado en el DOF el 15 de diciembre de 2017.

Por todo lo expuesto, la Unidad de Transparencia elaboró el Programa para la Protección de los Datos Personales (en adelante el Programa), que tiene como finalidad alinear los esfuerzos a nivel institucional referente a la protección de datos personales en cumplimiento a lo señalado en la Ley de Datos.

2.1 EL PROGRAMA NACIONAL DE PROTECCIÓN DE DATOS PERSONALES (PRONADATOS)

El Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (SNT), desarrolló el Programa Nacional de Protección de Datos Personales (PRONADATOS) -en cumplimiento al artículo 12 de la Ley de Datos- que es el instrumento a través del cual define y coordina las bases de la política pública de protección de datos personales en el país dentro del sector público.

En el Acuerdo CNAIP/SNT/ACUERDO/EXT01-23/01/2018-4 del PRONADATOS, incluye una prospectiva a 20 años del desarrollo de las políticas públicas para garantizar el derecho a la protección de los datos personales, que contiene una línea del tiempo dividida en cuatro etapas: *Dónde estamos (2018-2020), dónde estaremos (2020-2022), hacia dónde vamos (2022-2026) y qué aspiramos (2037),* la cual es importante considerar para poder determinar el avance del Instituto en el cumplimiento de la protección de datos a nivel nacional.

Es importante recordar que el Instituto trabaja, desde hace varios años, en garantizar a los titulares de los datos personales que tiene bajo su resguardo la protección de los mismos. En este sentido, con la aprobación de la Ley de Datos, surgió la necesidad de alinear los procesos a nivel institucional que incluyen el tratamiento de los datos personales a las exigencias de la nueva legislación.

Para conocer en dónde se encuentran las actividades que el Instituto ha definido en materia de protección de datos personales, en la siguiente figura se observa una **comparativa** entre las acciones señaladas en las cuatro etapas mencionadas anteriormente del **PRONADATOS** y las acciones que el Instituto ha implementado y las que está por implementar, permitiendo visualizar en dónde se ubica el Instituto con respecto al PRONADATOS.

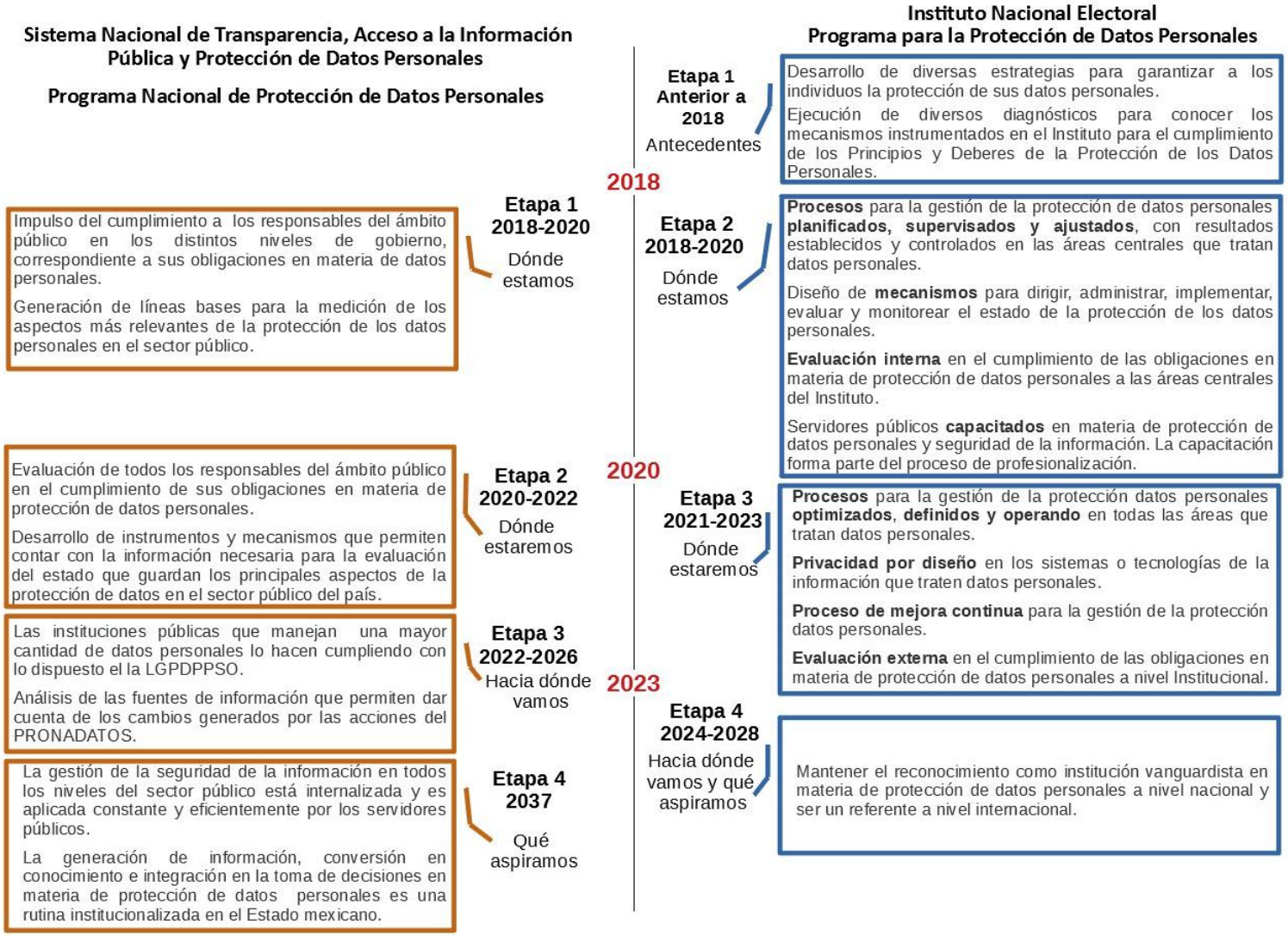
Programa para la Protección de Datos Personales

del Instituto Nacional Electoral

(Anexo Único del Acuerdo INE-CT-ACG-PDP-004-2018,

Aprobado en sesión extraordinaria del Comité de Transparencia, el 8 de noviembre de 2018

Etapas para el cumplimiento de la protección de datos personales



3 OBJETIVO

Establecer una gestión a nivel institucional en materia de protección de datos personales, a través de la implementación de mecanismos que acrediten el cumplimiento de las obligaciones derivadas de los principios, deberes y derechos, conforme a lo establecido en el artículo 29 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

4 ESTRATEGIAS

Para que el Instituto cumpla con lo descrito anteriormente, la Unidad de Transparencia determinó el desarrollo de dos Estrategias de Cumplimiento, ambas a 5 años (2018-2023):

I. **Estrategia para el cumplimiento de los Principios de Protección de Datos Personales**. Objetivo: Determinar las acciones a seguir por parte de la Unidad de Transparencia y de las áreas respecto al tratamiento de los datos en lo referente al Título Segundo, Capítulo I de la Ley.
II. **Estrategia para el cumplimiento de los Deberes de Seguridad y Confidencialidad**. Objetivo: Determinar las acciones concretas a seguir por parte de la Unidad de Transparencia y de las áreas respecto al tratamiento de los datos en lo referente al Título Segundo, Capítulo II de la Ley.

Cada estrategia debe estar integrada por sus respectivos Planes de Implementación y líneas de acción, para llevar una adecuada gestión de seguimiento.

Por lo que respecta al ejercicio de los derechos de los titulares, para su cumplimiento, desde el 2017, los procesos de Acceso, Rectificación, Cancelación y Oposición se encuentran integrados al Proyecto INFOMEX-INE. Cabe señalar que el ejercicio de los derechos ARCO respecto de los datos personales contenidos en el Padrón Electoral, se regirá por lo previsto en la LGIPE y en las disposiciones que emita el Instituto en la materia, tal como lo señalan los artículos 5 y 6 del Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales.

5 ALCANCE

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

Asimismo, en virtud de que uno de los objetivos del Programa es cumplir con las obligaciones establecidas en la Ley de Datos, se cubrirán todos los principios, deberes y obligaciones derivadas de los mismos que establece dicha norma para los responsables del tratamiento y quienes interviene en el mismo.

Quedan exceptuados de la aplicación de este programa, los datos personales que correspondan al cumplimiento de las obligaciones de transparencia a las que refieren la Ley General de Transparencia y Acceso a la Información Pública y la Ley Federal de Transparencia y Acceso a la Información Pública.

Los órganos que deberán observar el Programa, serán los establecidos en el artículo 4 del Reglamento Interior del Instituto Nacional Electoral que traten datos personales.

6 ROLES Y RESPONSABILIDADES

6.1 DEL COMITÉ DE TRANSPARENCIA

Con fundamento en lo dispuesto por los artículos 83 y 84, fracción I de la Ley de Datos y 47, segundo párrafo, y 48 de los Lineamientos Generales, que señalan que el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales, dicho órgano tendrá, además, las siguientes funciones con relación a este Programa:

I. Coordinar y supervisar el Programa en conjunto con las áreas técnicas y administrativas del Instituto que estime necesario involucrar o consultar;
II. Proponer cambios y mejoras al Programa, a partir de la experiencia de su implementación;
III. Dar a conocer el Programa al interior del Instituto;

IV. Presentar un informe anual, en el que se describan las acciones realizadas para cumplir con lo dispuesto por este Programa;
V. Las demás que de manera expresa señale el propio Programa.

6.2 De la Unidad de Transparencia

I. Preparar el informe al que refiere la fracción IV anterior en las primeras dos semanas del mes de febrero de cada año y referirá al año inmediato anterior;
II. Ejecutar el Programa en los términos señalados en el presente documento y sus correspondientes estrategias;
III. Asesorar a las Unidades Administrativas en la implementación de este Programa, con el apoyo de las áreas técnicas que estime pertinente;
IV. Definir y desarrollar los indicadores que permitan verificar el avance de implementación de las acciones que componen las estrategias, así como la eficacia de las mismas;
V. Diseñar y ejecutar las auditorías a las Unidades Administrativas en materia de datos personales para conocer el estado de cumplimiento en la protección de los mismos;
VI. Informar al Comité cualquier incumplimiento de las Unidades Administrativas sobre las obligaciones previstas en este Programa;
VII. Coordinar e implementar el Sistema de Gestión para la Protección de los Datos Personales.
VIII. Presentar, de manera trimestral, informes de seguimiento y avance ante el Comité de Transparencia.
IX. Las demás que de manera expresa señale el propio Programa.

6.3 De las Unidades Administrativas

I. Cada área, con apoyo de la Unidad de Transparencia, deberán elaborar su plan de trabajo para el cumplimiento del Programa;
II. Destinar los recursos humanos, financieros y materiales para llevar a cabo la implementación de su plan de trabajo;
III. Cumplir con las observaciones realizadas por la Unidad de Transparencia o cualquier órgano en la materia, como resultado de las auditorías;

IV. Realizar las acciones necesarias para cumplir con las obligaciones que establece este Programa.

6.4 DE LOS SERVIDORES PÚBLICOS, PRESTADORES DE SERVICIOS, ENCARGADOS

I. Todos los servidores públicos, prestadores de servicio y/o encargados que, en el ejercicio de sus funciones, traten datos personales, deberán observar, de manera obligatoria, lo señalado en el Programa, esto con la finalidad de que tenga como resultado el cumplimiento integral de las obligaciones que establece la Ley de Datos y el Reglamento.

7 CAUSAS DE SANCIÓN

La Unidad de Transparencia informará al Comité cualquier incumplimiento de alguna obligación prevista en este Programa, quien realizará un exhorto a la unidad administrativa correspondiente para que lleve a cabo las acciones que resulten pertinentes, con objeto de modificar dicha situación y evitar incumplimientos futuros o situaciones de riesgo que los pudieran ocasionar.

De conformidad con el artículo 163 de la Ley de Datos, serán causas de sanción por incumplimiento de las obligaciones establecidas en dicha ley, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;
II. Incumplir los plazos de atención previstos en la Ley de Datos para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;
III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la Ley de Datos;

V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la Ley de Datos, según sea el caso, y demás disposiciones que resulten aplicables en la materia;
VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;
VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la Ley de Datos;
VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la Ley de Datos;
IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la Ley de Datos;
X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la Ley de Datos;
XI. Obstruir los actos de verificación de la autoridad;
XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la Ley de Datos, y
XIII. No acatar las resoluciones emitidas por el INAI.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, y XII, así como la reincidencia en las conductas previstas en el resto de las fracciones, serán consideradas como graves. Cabe destacar que las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

Las responsabilidades que resulten de los procedimientos administrativos correspondientes, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

El Comité de Transparencia, a través de la Unidad de Transparencia, tomará las medidas necesarias para dar a conocer esta información a los servidores públicos, prestadores de servicio, y quienes intervengan en cualquier tipo de tratamiento de los datos personales al interior del Instituto.

Estrategia para el Cumplimiento de los Deberes de Seguridad y Confidencialidad para la Protección de Datos Personales 2018-2020

El 8 de noviembre de 2018, mediante Acuerdo INE-CT-ACG-PDP-004-2018 el Comité de Transparencia aprobó el Programa para la Protección de Datos Personales del Instituto Nacional Electoral, así como la presente Estrategia cuya finalidad es determinar las acciones concretas a seguir por parte de la Unidad de Transparencia y de las áreas respecto al tratamiento de los datos en lo referente al Título Segundo, Capítulo II de la Ley de Datos; además de contribuir al cumplimiento de la Ley de Datos, también permitirá reforzar la seguridad de la información que contenga datos personales.

Estrategia para el Cumplimiento de los Deberes de Seguridad y Confidencialidad
Para la Protección de Datos Personales 2018-2020.

(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)


Protección de Datos Personales
1990-2014
Ejecución de diversas acciones para salvaguardar los datos personales en posesión del Instituto Federal Electoral
IFE
INSTITUTO FEDERAL ELECTORAL
2014
Transformación del Instituto Federal Electoral al Instituto Nacional Electoral
INE
Instituto Nacional Electoral
2015
Creación de la Subdirección de Protección de Datos Personales
2016
Creación del Comité de Transparencia.
Ejecución del Proyecto para verificar el cumplimiento de los principios de la protección de los datos personales.
2017
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
Creación de la Subdirección de Seguimiento a Políticas de Datos Personales.
Ejecución del Proyecto para verificar de manera conceptual las medidas de seguridad en el tratamiento de los datos personales.
2018
Procedimientos y plazos de conservación para el bloqueo en su caso y supresión de los datos personales.
Manual para la atención de consultas, emisión de opiniones y elaboración de dictámenes a proyectos normativos en materia de protección de datos personales

(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)

CONTENIDO

1 ANTECEDENTES

La Unidad Técnica de Transparencia y Protección de Datos Personales (Unidad de Transparencia), ha ejecutado diversas iniciativas traducidas en proyectos, con el objetivo de cumplir con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en adelante, Ley de Datos).

En marzo de 2017, se llevó a cabo el *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*, con la finalidad de establecer las líneas de acción y ruta de trabajo que derivaron en la emisión del Reglamento del INE en materia de Protección de Datos Personales.

Como resultado del diagnóstico, la Unidad de Transparencia determinó que era necesario verificar –de manera conceptual- el cumplimiento que cuatro áreas centrales del Instituto realizan a los Deberes de Seguridad y Confidencialidad -por ser las más representativas- a efecto de identificar las medidas de carácter administrativo, físico y técnico que se implementan en el tratamiento de los datos personales, por lo que, en el cuarto trimestre del 2017, la Unidad de Transparencia, a través de una consultora, llevó a cabo el proyecto denominado "*Verificación de medidas de seguridad respecto al tratamiento de los datos personales en posesión de diversas áreas centrales del Instituto Nacional Electoral (INE)*", enfocado a los Deberes de Seguridad y Confidencialidad.

En el informe entregado a la Unidad de Transparencia fueron señaladas diversas actividades a seguir para cumplir con los Deberes de Seguridad y Confidencialidad en materia de protección de datos personales y, en específico, para contar con los instrumentos que describan las medidas de seguridad que implementan las áreas seleccionadas en el análisis.

Las áreas y bases de datos seleccionadas fueron:

- **Dirección Ejecutiva del Registro Federal de Electores (DERFE). Base de Datos "Registro Federal de Electores (Padrón Electoral)**".
    - Fue seleccionada, tomando en consideración el impacto que guarda frente a la ciudadanía, así como el volumen de datos personales que se tratan en las bases que conforman el Padrón.

- **Dirección Ejecutiva de Prerrogativas y Partidos Políticos (DEPPP). Base de datos "Sistema de verificación del Padrón de Afiliados de los PPN**".
    - Fue seleccionada, en virtud de también se lleva a cabo el registro de la ciudadanía interesada en militar en alguno de los partidos políticos nacionales, sumado a que existe interrelación de dos sujetos obligados (INE y partidos políticos).
- **Dirección Ejecutiva de Administración (DEA). Base de datos "Expediente de Personal"**.
    - Fue seleccionada, ya que también el INE garantiza la protección de los datos personales de servidores públicos, de forma que cubre los aspectos de impacto interno.
- **Dirección Ejecutiva de Capacitación Electoral y Educación Cívica (DECEYEC). Base de datos "Registro de Representantes Escolares del Parlamento de las Niñas y los Niños de México 2017".**
    - Fue seleccionada, considerando que, si bien el INE, mayormente brinda servicios a mayores de edad, también posee datos de menores, con lo que asegura que ante cualquier tratamiento –con independencia de la calidad de la persona titular de los datos- es seguro y apegado a las normas aplicables.

El orden de análisis de las áreas se priorizó atendiendo a lo anterior. Además, se sumarán a este análisis las bases de datos personales identificadas en el listado de bases de datos personales del Instituto, así como las que se generen.

En ese sentido, este documento representa la **Estrategia de cumplimiento a los Deberes de Seguridad y Confidencialidad**, que contiene las **Líneas de Acción -a Corto, Mediano y Largo Plazo- para cumplir con los Deberes de Seguridad y Confidencialidad en un ámbito técnico-normativo**.

2 OBJETO

La presente Estrategia tiene por objeto desarrollar las líneas de acción a corto, mediano y largo plazo, durante el periodo 2018-2020, para dar atención a los Deberes de Seguridad y Confidencialidad respecto de la protección de datos personales en posesión del INE.

3 Objetivo General

Proveer las bases a los órganos del INE, para que los responsables del tratamiento de los datos personales cumplan con los Deberes de Seguridad y Confidencialidad establecidos en la Ley de Datos y las demás disposiciones aplicables.

4 Objetivos Específicos

- Generar el Documento de Seguridad para demostrar el cumplimiento respecto de la protección de los datos personales.
- Coadyuvar en la implementación del Sistema de Gestión para la Protección de los Datos Personales.

5 Alcance

El presente instrumento es aplicable para los órganos ejecutivos, técnicos, de vigilancia, en materia de transparencia, y de control, a nivel central 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.

6 Recursos

Lo 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 los mismos.

7 ACTORES INVOLUCRADOS

- Comité de Transparencia del INE.
- Unidad de Transparencia.
- En su caso, órganos vinculados con seguridad de la información

8 LÍNEAS DE ACCIÓN

La Unidad de Transparencia, llevará a cabo las siguientes acciones:

8.1 ACCIONES A CORTO PLAZO (3 A 6 MESES)

- Establecer mesas de trabajo con las áreas responsables del Instituto que tratan datos personales para conocer el estado de cumplimiento de los Deberes de Seguridad y Confidencialidad, y acordar el Plan de Implementación para dar atención a las áreas de oportunidad detectadas.
- Establecer mesas de trabajo con el Archivo Institucional del INE, con la finalidad de tratar temas relacionados con el tratamiento de la información, en particular sobre los tiempos de conservación de los datos personales.
- Establecer mesas de trabajo con los órganos vinculados con seguridad de la información, para determinar la estrategia a seguir con respecto a la implementación de la seguridad en el tratamiento de los datos personales.

8.2 ACCIONES A MEDIANO PLAZO (6 MESES A 2 AÑOS)

La Unidad de Transparencia, llevará a cabo las siguientes acciones:

- Implementar los Deberes de Seguridad y Confidencialidad en las siguientes áreas del Instituto: Dirección Ejecutiva del Registro Federal de Electores, Dirección Ejecutiva de Administración, Dirección Ejecutiva de Prerrogativas y Partidos Políticos, Dirección Ejecutiva de Capacitación Electoral y Educación Cívica.
- Impulsar programas a distancia, de concientización, educación y formación del personal al interior del Instituto, con el objetivo de crear y fomentar la cultura de protección de los datos personales, a través del uso de plataformas digitales.

- Establecer contacto con las áreas de capacitación para determinar la estrategia de capacitación y concientización con relación a la protección de datos personales a nivel institucional.
- Efectuar auditorías internas en materia de datos personales para la verificación del cumplimiento de los Deberes de Seguridad y Confidencialidad.
- Elaborar documentos de apoyo para las áreas sobre seguridad aplicada a los datos personales para la identificación las brechas, los riesgos y el impacto en los datos personales.

8.3 Acciones a largo plazo (2 a 3 años)

La Unidad de Transparencia, llevará a cabo las siguientes acciones:

- Implementar los Deberes de Seguridad y Confidencialidad en las áreas del Instituto que no fueron seleccionadas en las acciones a mediano plazo.
- En su caso, realizar los ajustes necesarios a los sistemas o tecnologías de la información destinados al tratamiento de los datos personales para el cumplimiento de la Ley.
- Seleccionar 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.
- Efectuar auditorías externas para la verificación del cumplimiento de la Ley.

9 Plan de Implementación 2018-2020

El plan de implementación está compuesto por cinco etapas:

- **Etapa Preliminar. Identificación del propietario del sistema y necesidades del área.**
- **Etapa 1. Identificación del flujo de los datos personales.**
- **Etapa 2. Evaluación de medidas de seguridad básicas.**
- **Etapa 3. Plan de trabajo.**
- **Etapa 4. Mejora continua.**

El entregable general –conformado por el resultado de la ejecución de todas las etapas- **es el Documento de Seguridad Institucional, que será integrado por la Unidad de**

Transparencia mismo que acreditará las acciones que el Instituto, como sujeto obligado, implementa para el cumplimiento de los Deberes de Seguridad y Confidencialidad, de conformidad con lo establecido en el **artículo 35** de la Ley de Datos.

Además, **cada base de datos poseerá su propio Documento de Seguridad,** elaborado por los propietarios de las bases de datos personales, con apoyo de la Unidad de Transparencia.

La Unidad de Transparencia presentará a las áreas, 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 fases, lo que facilitará el seguimiento del avance o posibles desfases en el Plan y remitirá a las áreas el *Manual en Materia de Seguridad de Datos Personales para las Áreas del Instituto Nacional Electoral* (en adelante el Manual de Seguridad)[1] *y el Manual de Análisis de Riesgos*, que serán provistos –por la Unidad de Transparencia- a las áreas, con la finalidad de que cuenten con guías para realizar las acciones que permitan cumplir con los Deberes de Seguridad y Confidencialidad, así como materiales diversos en materia de seguridad aplicada a los datos personales que se consideren necesarios.

Las etapas antes listadas se describen a continuación.

9.1 Etapa Preliminar. Identificación del propietario de las base de datos

Para dar inicio a 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 con claridad **la base o las bases de datos personales** de las que son propietarios.

Para cumplir con lo anterior, la Unidad de Transparencia celebrará reuniones con los propietarios de los sistemas informáticos que tratan datos personales -conforme a las cédulas descriptivas de cada uno[2]-, para identificar a qué bases de datos tienen acceso los

[1] Este manual es una adaptación realizada del Manual en materia de Seguridad de Datos Personales para MYPYMES y organizaciones Pequeñas, publicado por el INAI, junio 2015. Disponible en http://inicio.ifai.org.mx/nuevo/Manual%20seguridad%20MIPYMES.pdf

[2] 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 del propietario del sistema es actualizar dichas cedulas. Cédulas Descriptivas disponibles en

sistemas. La información obtenida de estas reuniones permitirá a la Unidad de Transparencia diseñar mesas de trabajo con los propietarios de las bases de datos con la finalidad de cubrir las necesidades detectadas.

9.2 ETAPA 1. IDENTIFICACIÓN DEL FLUJO DE LOS DATOS PERSONALES

La presente etapa busca **identificar** los **datos personales** que componen cada sistema de información, su clasificación, el personal que tiene acceso a los sistemas de tratamiento y los permisos otorgados, para poder identificar las bases de datos utilizadas.

El entregable de la etapa es el **inventario de datos personales y el tratamiento** al que son sometidos los datos, para dar cumplimiento al **artículo 33**, **fracciones II y III** de la Ley de Datos.

Esta etapa permitirá identificar y documentar el ciclo de vida de los datos personales, en los términos establecidos en el **artículo 59 de los Principios de Protección** (Lineamientos Generales) y **verificar el cumplimiento de los ocho principios** para la protección de los datos personales.

Asimismo, será la base para determinar el nivel de protección necesario para la salvaguarda de los datos personales, en razón del tipo de dato –y su riesgo inherente- y del tratamiento al que es sometido.

Se compone de cuatro fases:

9.2.1 Fase 1. Identificación de datos personales

El propietario, con apoyo de las áreas custodias y de la Unidad de Transparencia, deberá identificar los datos personales que están siendo tratados en el sistema de datos personales que esté a su cargo y su categorización, es decir, si los datos personales son estándar, sensibles o especiales[3].

http://portalanterior.ine.mx/archivos3/portal/historico/contenido/XXXII_Listado_de_sistemas_de_datos_personales/

[3] El área de transparencia compartirá con las áreas la categorización de los datos personales definidas por el INAI.

Lo anterior permitirá determinar si los datos personales recabados cumplen con los principios de *licitud*, *finalidad, proporcionalidad*, y en caso de no ser así, el propietario deberá prescindir de los mismos y no incluirlos en nuevos procesos de recolección.

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

El propietario deberá identificar el flujo y la forma a través de la cual se recaban los datos personales, proporcionando elementos para verificar, posteriormente, el aviso de privacidad; si los datos se obtienen de una manera libre, especifica e informada, lo cual permitirá acreditar la observancia al *principio de información, lealtad, consentimiento*, que establece la Ley de Datos.

Cabe señalar que la Unidad de Transparencia analizará las particularidades de los datos personales que son recabados, como es el caso de los datos de menores.

9.2.3 Fase 3. Identificación de medios de almacenamiento

El propietario deberá identificar los sitios, medios y formatos utilizados para almacenar los datos, si se resguardan en un sitio específico o en un área común, y si son resguardados en medios de almacenamiento físicos o digitales.

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

9.2.4 Fase 4. Identificación de permisos y tratamiento

El propietario 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.

La identificación contempla el rol y los permisos que son asignados al personal para llevar a cabo el tratamiento; esto, a través de un formato integrado al Manual de Seguridad en el cual deberán señalar el tipo de permisos que tiene cada una de las personas/roles en la base o bases de datos correspondientes.

Esta fase guarda relación con el tiempo de almacenamiento de los datos, que deberá corresponder al tiempo necesario para el cumplimiento de las finalidades que justifican su tratamiento, así como del principio de *calidad* (incluyendo la *supresión* de los datos personales).

En este sentido, es importante señalar que las áreas deberán atender lo establecido en el Cuadro General de Clasificación Archivística del INE y demás normas de Archivo.

9.3 ETAPA 2. EVALUACIÓN DE LAS MEDIDAS DE SEGURIDAD

La presente etapa tiene como finalidad la gestión del riesgo. Si bien, no es posible eliminar los riesgos, es necesario identificar e implementar medidas de seguridad con la finalidad de minimizar las vulneraciones a la seguridad de las bases de datos personales.

La obligación de establecer medidas de seguridad se encuentra contemplada en **los artículos 31, 32 y 33 fracciones VI y VII** de la Ley de Datos.

Las medidas de seguridad se analizarán en el siguiente orden:

1. De la cultura del personal: medidas administrativas.
2. Del entorno físico: medidas de seguridad físicas.
3. Del entorno de trabajo digital: medidas de seguridad técnicas.

Lo anterior se llevará a cabo mediante la elaboración de un **Análisis de brecha** para conocer las medidas de seguridad existentes e identificarán las medidas faltantes, o el reforzamiento de las actuales.

El **artículo 33 fracción V** de la Ley de Datos, señala la obligación de realizarlo, conforme a lo establecido en el **artículo 61 de los Lineamientos Generales**.

El análisis lo realizará el propietario, con apoyo de la Unidad de Transparencia y, en su caso, los órganos vinculados con seguridad de la información.

El entregable generado en esta etapa es el Análisis de Brecha.

9.3.1 Fase 1. Medidas de seguridad administrativas

El propietario de la base o bases de datos personales, con apoyo de la Unidad de Transparencia y, en su caso, de los órganos vinculados con seguridad de la información, identificará las medidas de seguridad administrativas implementadas, con el objetivo de detectar prácticas inadecuadas en el tratamiento de los datos a su interior, mismas que podrían suscitar una vulneración.

La verificación de las medidas de seguridad se realizará con base en los estándares y buenas prácticas en la materia.

9.3.2 Fase 2. Medidas de seguridad medidas físicas

La seguridad del entorno de trabajo físico es un elemento básico para mitigar las vulneraciones a la seguridad de los datos personales, por lo que en la presente fase se identificarán las medidas de seguridad implementadas, así como las áreas involucradas para su implementación.

La verificación de las medidas de seguridad se realizará con base en los estándares y buenas prácticas en la materia.

9.3.3 Fase 3. Medidas de seguridad medidas técnicas

En la presente fase se evaluarán las medidas utilizadas en el entorno digital que busquen proteger los equipos de cómputo y dispositivos de almacenamiento, contra el acceso lógico no autorizado y contra amenazas informáticas.

La verificación de las medidas de seguridad se realizará con base en los estándares y buenas prácticas en la materia.

9.4 Etapa 3. Plan de Trabajo

El propietario de la base de datos, previo a elaborar el Plan de trabajo, deberá ejecutar un análisis de riesgos, con la finalidad de identificar el orden de prioridad de las acciones a realizar para la implementación de las medidas de seguridad faltantes –detectadas en el análisis de brecha- o la mejora de las ya existentes. Lo anterior atendiendo al **artículo 33 fracción VI** de la Ley de Datos.

Los entregables de esta etapa son el Plan de Trabajo y el Análisis de Riesgos.

Fases que componen esta etapa son:

9.4.1 Fase 1. Selección de acciones prioritarias

Una vez realizada la identificación de los datos personales y su valor, el propietario –con apoyo de la Unidad de Transparencia y, en su caso, de los órganos vinculados con seguridad de la información- realizará un **Análisis de riesgos**, de conformidad con lo establecido en **artículo 33, fracción IV** de la Ley de Datos.

9.4.2 Fase 2. Periodo de cumplimiento de acciones

El propietario –de acuerdo a sus actividades generales y con relación a la prioridad de las acciones- elaborará y dará a conocer a la Unidad de Transparencia el Plan de trabajo para la implementación o adecuación de las medidas de seguridad.

La Unidad de Transparencia reportará lo conducente ante el Comité de Transparencia.

9.4.3 Fase 3. Recursos humanos y materiales

El propietario determinará los recursos necesarios para cumplir con las acciones en el periodo establecido, con la finalidad de solicitarlo al área correspondiente del Instituto.

9.5 Etapa 4. Mejora Continua

El propietario, con apoyo de la Unidad de Transparencia y, en su caso, de los órganos vinculados con seguridad de la información, iniciarán 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, para lo cual se empleará el modelo de madurez que, previo análisis, estime pertinente la Unidad de Transparencia.

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

9.5.1 Fase 1. Implementación de las medidas de seguridad

Con base en el Plan de trabajo, el área responsable deberá implementar las medidas de seguridad que son necesarias para lograr el cumplimiento de los Deberes de Seguridad y Confidencialidad.

La Unidad de Transparencia verificará que la implementación se realice conforme a lo establecido en el Plan de trabajo.

En caso de detectar desfases, la Unidad de Transparencia verificará 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.

9.5.2 Fase 2. Modelo de madurez

La Unidad de Transparencia, realizará **auditorías 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, de conformidad con lo establecido en el Sistema de Gestión para la Protección de Datos Personales.

Lo anterior, atendiendo al **artículo 33, fracción VII** de la Ley General de Datos, relacionado al 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.