



Procedimiento para presentar el Documento de Seguridad ante el Comité de Transparencia

(segunda edición)

(Anexo Único del Acuerdo INE-CT-ACG-PDP-007-2024, aprobado en sesión extraordinaria del Comité de Transparencia el 26 de noviembre de 2024)

Primera edición: Marzo, 2021.

Segunda edición: Noviembre, 2024.

CONTENIDO

Abreviaturas.....	3
Definiciones.....	3
Introducción	4
Objetivo.....	4
Marco legal.....	5
1 Procedimiento.....	5
1.1 Actividades preliminares.....	5
1.2 Presentación del Documento de Seguridad ante el Comité de Transparencia	5
1.2.1 Actividades del órgano responsable.....	5
1.2.2 Actividades de la Subdirección de Gobierno de Datos Personales.....	6
1.2.3 Sesión del Comité de Transparencia	6
1.2.4 Envío de documentos al órgano responsable.....	6
1.2.5 Publicación del Documento de Seguridad	7
1.3 Actualización del Documento de Seguridad	7
1.4 Valoración de las modificaciones	10

ABREVIATURAS

Apartado incorporado en la versión 2.0

Comité de Transparencia o CT: Comité de Transparencia del Instituto Nacional Electoral.

DAIPDP: Dirección de Acceso a la Información y Protección de Datos Personales.

Documento: Documento de Seguridad.

Instituto o INE: Instituto Nacional Electoral.

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

Reglamento: Reglamento del Instituto Nacional Electoral en materia de protección de datos personales.

SAI: Subdirección de Acceso a la Información.

Subdirección de Gobierno o SGDP: Subdirección de Gobierno de Datos Personales.

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

DEFINICIONES

Apartado incorporado en la versión 2.0

Para los efectos de este procedimiento se tomarán las definiciones establecidas en el artículo 3º de la LGPDPSO y, sin perjuicio de lo previsto en la normativa aplicable, se entenderá por:

Órgano responsable: Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar con datos personales, así como dar tratamiento, y ser responsables o encargadas de estos.

INTRODUCCIÓN

Apartado actualizado en la versión 2.0

El Documento de Seguridad constituye un pilar fundamental en la salvaguarda de los datos personales tratados por los órganos del Instituto, que da cuenta de las medidas, procedimientos y controles establecidos por cada uno de ellos para su protección, así como la preservación de su confidencialidad, integridad y disponibilidad.

El Documento debe contener, al menos, lo siguiente¹:

- i. El inventario de datos personales y de los sistemas de tratamiento;
- ii. Las funciones y obligaciones de las personas que traten datos personales;
- iii. El análisis de riesgos;
- iv. El análisis de brecha;
- v. El plan de trabajo;
- vi. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
- vii. El programa general de capacitación.

El artículo 31 del Reglamento del Instituto en materia de Datos establece que los órganos del Instituto “remitirán al Comité, para fines de supervisión y conforme al procedimiento y plazos que dicho órgano colegiado apruebe, el documento de seguridad a que se refiere el artículo 35 de la Ley General, mismo que deberá ser actualizado cuando ocurran las hipótesis previstas en dicho ordenamiento”.

En función de lo anterior el Comité de Transparencia, previa propuesta de la Unidad de Transparencia, elaboró el procedimiento descrito en este documento.

OBJETIVO

Proveer a los órganos del Instituto los pasos a seguir para la presentación de su Documento ante el Comité de Transparencia.

¹ Artículo 35 de la LGPDPPSO

MARCO LEGAL

Apartado actualizado en la versión 2.0

- Constitución de los Estados Unidos Mexicanos (Artículos 6, Base A y 16, párrafo segundo).
- 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 (artículo 31).

1 PROCEDIMIENTO

1.1 ACTIVIDADES PRELIMINARES

Apartado actualizado en la versión 2.0

El órgano del Instituto debe integrar el Documento de Seguridad conforme a lo establecido en el [Manual de Procesos y Procedimientos de "Protección de Datos Personales"](#), específicamente atendiendo al procedimiento de *Alineación para el Cumplimiento de Deberes de Datos Personales*.

Cuando disponga del Documento, el órgano responsable debe comunicar a la Subdirección de Gobierno de Datos Personales, mediante correo electrónico, la fecha en que lo presentará ante el Comité de Transparencia.

1.2 PRESENTACIÓN DEL DOCUMENTO DE SEGURIDAD ANTE EL COMITÉ DE TRANSPARENCIA

Apartado actualizado en la versión 2.0

1.2.1 Actividades del órgano responsable

El órgano del Instituto, a través de su Enlace de Transparencia y Protección de Datos Personales solicitará la integración del punto en el orden del día de la sesión a la

Secretaría Técnica del Comité de Transparencia, de acuerdo con el calendario de sesiones ordinarias y extraordinarias².

Para listar el punto, debe considerar los plazos que establezca el Comité de Transparencia, así como anexar a la solicitud el Documento de Seguridad -en formato Word- para estar en posibilidad de circularlo a los miembros del CT.

1.2.2 Actividades de la Subdirección de Gobierno de Datos Personales

Una vez que el órgano responsable comunique a la Subdirección de Gobierno la fecha en que presentará su Documento ante el Comité de Transparencia, dicha Subdirección elaborará:

- El proyecto de Acuerdo de Presentación del Documento de Seguridad, y
- Síntesis del punto.

La Subdirección de Gobierno remitirá los documentos mediante correo electrónico a la Secretaría Técnica del Comité de Transparencia, con la finalidad de que sean integrados al punto previamente solicitado por el órgano del Instituto.

Los documentos y la información serán enviados atendiendo a los plazos establecidos por el Comité de Transparencia.

1.2.3 Sesión del Comité de Transparencia

Durante la celebración de la sesión del Comité de Transparencia, una persona adscrita al órgano del Instituto podrá presentar ante los miembros del Comité el Documento, exponiendo las consideraciones que estime pertinentes.

1.2.4 Envío de documentos al órgano responsable

En un plazo no mayor a diez días hábiles posteriores a la sesión del CT en la que se presentó el Documento, o bien, una vez que el órgano responsable cuente con los ajustes o, en su caso, engroses que resulten de la revisión por parte de los integrantes del Comité y demás órganos del Instituto convocados a la sesión, la DAIPDP remitirá al órgano responsable -mediante correo electrónico- lo siguiente:

- Acuerdo de Presentación del Documento de Seguridad, firmado por los integrantes del órgano colegiado, en formato PDF.

² El órgano responsable debe solicitar a la Secretaría Técnica del Comité de Transparencia el calendario vigente.

- Anexo único del acuerdo, consistente en el Documento de Seguridad con el certificado emitido por la SGDP, en formato Word y PDF.

Los documentos serán remitidos con un *código de integridad* con el fin de preservar su estado original.

1.2.5 Publicación del Documento de Seguridad

Para la publicación del Documento, el órgano responsable debe llevar a cabo lo siguiente:

- a) Gestionar la firma de las personas señaladas en la *Hoja de firmas* dentro del Documento.
- b) Compartir el Documento firmado a la Subdirección de Gobierno.

La Subdirección de Gobierno solicitará a la Secretaría Técnica la carga del Documento en el repositorio del Comité de Transparencia y remitirá al órgano responsable la liga electrónica donde se encuentre.

- c) Solicitar, a través de su Enlace Web, la publicación del Documento en el apartado especializado de Protección de Datos Personales de la página web del Instituto, en específico en el subapartado *Avisos de Privacidad y Documentos de Seguridad*, para lo cual debe proporcionar la liga previamente compartida por la Subdirección de Gobierno³.

1.3 ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

Apartado actualizado en la versión 2.0

El órgano del Instituto es responsable de actualizar el Documento de Seguridad por modificaciones menores o mayores. A continuación, se describe cada una:

- **Modificaciones de forma (ajustes menores):** Comprende los siguientes:
 - a. Ajustes de forma, como redacción, ortografía, justificación del texto, paginado, entre otros.
 - b. Actualización del personal señalado en el Documento.

³ De conformidad con lo establecido en el primer párrafo del artículo 11 del Reglamento de Transparencia y Acceso a la Información Pública.

El órgano responsable debe:

1. Impactar las modificaciones menores en el Documento.
2. Modificar el versionado en la parte decimal. Ejemplo: De la versión 1.0 pasa a ser la versión 1.1.
3. Remitir a la Subdirección de Gobierno mediante correo electrónico la nueva versión del Documento señalando las modificaciones realizadas, considerando lo siguiente:
 - Número de la página que se modificó;
 - Dice, Debe decir; y
 - Justificación del cambio.

La Subdirección de Gobierno:

1. Revisará el Documento conforme a lo establecido en el [Manual de Procesos y Procedimientos de "Protección de Datos Personales"](#), específicamente al procedimiento de *Alineación para el Cumplimiento de Deberes de Datos Personales*.
2. Emitirá un nuevo certificado que será incorporado a la nueva versión del Documento.
3. Enviará el Documento al órgano responsable en formato Word y PDF.

Los documentos son remitidos con un código de integridad con el fin de preservar su estado original.

4. Informará a la Secretaría Técnica del Comité de Transparencia la modificación al Documento, para que esta, a su vez, lo haga del conocimiento de los integrantes del Comité de Transparencia.

Dicha comunicación no implica que el órgano responsable deba presentar nuevamente el Documento en sesión del Comité, salvo que este último así lo determine.

Una vez que el órgano responsable cuente con la versión actualizada del Documento de Seguridad, el órgano responsable debe realizar las actividades descritas en el apartado 1.1.1 *Publicación del Documento de Seguridad*.

- **Modificaciones de fondo (ajustes mayores):** Los supuestos previstos en el artículo 36 de la LGPDPSO, así como aquellos ajustes que impactan al fondo o contenido del Documento.

De manera enunciativa, son consideradas modificaciones mayores⁴:

- a. Modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo.
- b. Proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión.
- c. Proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida.
- d. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.
- e. Ajustes al Plan de Trabajo que aumenten el riesgo de los datos personales.

El órgano responsable debe:

1. Aplicar las modificaciones mayores al Documento.
2. Modificar el versionado en la parte entera. Ejemplo: De la versión 1.0 pasa a ser la versión 2.0.
3. Remitir a la Subdirección de Gobierno lo siguiente:
 - La sección modificada, y
 - Justificación del cambio.

⁴ Los incisos a), b), c) y d) corresponden a lo señalado en el artículo 36 de la LGPDPSO.

La Subdirección de Gobierno, revisará el Documento conforme a lo establecido en el [Manual de Procesos y Procedimientos de "Protección de Datos Personales"](#), específicamente atendiendo al procedimiento de *Alineación para el Cumplimiento de Deberes de Datos Personales*.

Derivado de las modificaciones mayores el órgano del Instituto debe realizar las actividades descritas en el apartado *1.2 Presentación del Documento de Seguridad ante el Comité de Transparencia*.

1.4 VALORACIÓN DE LAS MODIFICACIONES

Apartado incorporado en la versión 2.0

El órgano responsable podrá consultar a la Subdirección de Gobierno de Datos Personales para confirmar si se tratan de modificaciones de forma o de fondo.

La Unidad de Transparencia, a través de la Subdirección de Gobierno, cuenta con cinco días hábiles posteriores a la recepción del Documento para el análisis de la o las actualizaciones, a fin de identificar si se trata de modificaciones mayores o menores y comunicará al órgano responsable las acciones a seguir, de acuerdo con este procedimiento.