INSTITUTO ELECTORAL DEL ESTADO DE MÉXICO
COMITÉ DE TRANSPARENCIA

ACUERDO N° IEEM/CT/180/2023

POR EL QUE SE APRUEBA EL PROCEDIMIENTO DE ANÁLISIS DE RIESGOS Y BRECHA

El Comité de Transparencia del Instituto Electoral del Estado de México emite el presente Acuerdo, con base en lo siguiente:

GLOSARIO

Análisis de brecha: Análisis comparativo de las medidas de seguridad existentes contra las faltantes.

Análisis de riesgos: Proceso que permite realizar la evaluación y gestión de riesgos, así como implementar las medidas de seguridad necesarias para proteger los activos.

Comité de Transparencia. Cuerpo colegiado que funge como máxima autoridad en materia de protección de datos personales al interior del Instituto Electoral del Estado de México.

Constitución Federal. Constitución Política de los Estados Unidos Mexicanos.

Constitución Local. Constitución Política del Estado Libre y Soberano de México.

Código Electoral. Código Electoral del Estado de México.

IEEM. Instituto Electoral del Estado de México.

Incidentes. Hechos o eventos inesperados en el que una amenaza explota una vulnerabilidad o conjunto de vulnerabilidades y que compromete o puede comprometer la seguridad de los datos personales contenidos en Sistemas y/o Bases de Datos Personales.

INFOEM. Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios.

Ley de Protección de Datos del Estado. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios.

Ley de Transparencia del Estado. Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios.

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

Manual de Organización. Manual de Organización del Instituto Electoral del Estado de México.

Reglamento de Transparencia: Reglamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Instituto Electoral del Estado de México.

Reglamento Interno. Reglamento Interno del Instituto Electoral del Estado de México.

Responsable. El Instituto Electoral del Estado de México que en el ejercicio de sus atribuciones decide sobre el tratamiento de datos personales.

Sistema de Gestión. Sistema de Gestión de Seguridad de Protección de Datos Personales del Instituto Electoral del Estado de México.

Tratamiento: Obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

UT. Unidad de Transparencia.

Violaciones a la seguridad de los datos personales: Hechos o eventos que en cualquier fase del tratamiento afectan directamente a los datos personales contenidos Sistemas y/o Bases de Datos Personales.

ANTECEDENTES

PRIMERO. En fecha veintiséis de enero de dos mil diecisiete, se publicó en el Diario Oficial de la Federación la Ley General de Protección de Datos, en la cual se establece que son Sujetos Obligados en el Ámbito Federal, Estatal y Municipal, cualquier Autoridad, Entidad, Órgano y Organismo de los Poderes Ejecutivo, Legislativo y Judicial, Órganos Autónomos, Partidos Políticos, Fideicomisos y Fondos Públicos.

SEGUNDO. El treinta de mayo de dos mil diecisiete, se publicó en el Periódico Oficial del Gobierno del Estado Libre y Soberano de México "Gaceta del Gobierno", la Ley de Protección de Datos del Estado, por la que se abrogó la Ley de Protección de Datos del Estado de México, misma que homologa sus disposiciones con la Ley General de Protección de Datos y establece, entre otros aspectos, que los Responsables en el tratamiento de datos como parte de las acciones interrelacionada para establecer y mantener las medidas de seguridad deben realizar análisis de riesgos de los datos personales y de brecha respecto de las medidas de seguridad existentes contra las faltantes.

TERCERO. El catorce de octubre de dos mil veintiuno, en la Vigésimo Tercera Sesión Extraordinaria del Comité de Transparencia fueron aprobadas la Política de Gestión de Datos Personales, la Misión y Visión del Sistema de Gestión de Seguridad de Protección de Datos Personales del Instituto Electoral del Estado de México, las cuales están orientadas al cumplimiento de la normatividad en materia de protección de datos personales.

CONSIDERACIONES

I. COMPETENCIA

Este Comité de Transparencia es competente para coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales, dentro de las que se encuentra la aprobación del presente Procedimiento, de conformidad con lo dispuesto por los artículos 83 y 84, fracción I de la Ley General de Protección de Datos; 94, fracción I de la Ley de Protección de Datos del Estado, así como 11 y 12 del Reglamento de Transparencia.

II. FUNDAMENTACIÓN

Constitución Federal

El artículo 6°, apartado A, fracción II, establece que la información que se refiere a la vida privada y a los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

Asimismo, el artículo 16, párrafo segundo, dispone que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Constitución Local

El artículo 5°, fracciones II y III dispone que la información referente a la intimidad de la vida privada y la imagen de las personas será protegida a través de un marco jurídico rígido de tratamiento y manejo de datos personales, con las excepciones que establezca la ley reglamentaria; además de que toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.

Además, dicho ordenamiento prevé en el artículo 11 que la organización, desarrollo y vigilancia de los procesos electorales para las elecciones de la Gubernatura, Diputaciones Locales y de las y los integrantes, es una función que se realiza a través del Instituto Nacional Electoral y el Organismo Público Electoral del Estado de México, denominado IEEM que tendrá a su cargo, además de las que determine la Ley de la materia, las actividades relativas al desarrollo de la democracia y la cultura política.

Ley General de Protección de Datos

El artículo 1 refiere que son Sujetos Obligados en el ámbito federal, estatal y municipal los órganos autónomos.

Por otra parte, el artículo 16 prevé que el Responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

El artículo 31 establece que con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

El artículo 33, fracciones IV, V, VI y VII, menciona que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

- Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;

- Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;

- Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;

- Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

El artículo 34 refiere que las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.

Asimismo, define al sistema de gestión como el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

El artículo 35, fracciones III, IV, V, VI señala que el Responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:

- El análisis de riesgos;
- El análisis de brecha;
- El plan de trabajo;
- Los mecanismos de monitoreo y revisión de las medidas de seguridad.

El artículo 83 establece que cada Responsable contará con un Comité de Transparencia que será la autoridad máxima en materia de protección de datos personales, el cual se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública, así como demás normativa aplicable.

El artículo 84, fracción I establece que el Comité de Transparencia tendrá como funciones coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales, de conformidad con las disposiciones previstas en la normatividad de la materia, establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de las leyes en la materia y establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales.

Código Electoral

El artículo 168 define al IEEM como un organismo público dotado de personalidad jurídica y patrimonio propio, autónomo en su funcionamiento e independiente en sus decisiones, responsable de la organización, desarrollo y vigilancia de los procesos electorales; autoridad electoral de carácter permanente, y profesional en su desempeño se regirá por los principios de certeza, imparcialidad, independencia, legalidad, máxima publicidad, objetividad y paridad; así como sus actividades se realizarán con perspectiva de género.

Ley de Protección de Datos del Estado

El artículo 3, fracción V contempla dentro de los Sujetos Obligados en materia de protección de datos personales a los Organismos Autónomos.

El artículo 15 señala que los responsables en el tratamiento de datos personales, observarán los principios de calidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad y responsabilidad; los cuales son regulados por la propia ley en sus artículos subsecuentes del 16 al 28.

El artículo 27, primer y último párrafo refiere al principio de responsabilidad que implica que el responsable deberá cumplir con los principios de protección de datos establecidos y adoptar las medidas necesarias para su aplicación, para lo cual se deberán implementar los mecanismos previstos en dicha Ley para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos y rendirá cuentas sobre el tratamiento de datos personales en su posesión a la o el titular y al INFOEM, caso en el cual deberá observar la Constitución Federal y los tratados internacionales en los que el Estado Mexicano sea parte, en lo que no se contraponga con la normativa mexicana podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines.

El artículo 38 establece que el responsable adoptará, establecerá, mantendrá y documentará las medidas de seguridad administrativas, físicas y técnicas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales, a través de controles y acciones que eviten su daño, alteración, pérdida, destrucción, o el uso, transferencia, acceso o cualquier tratamiento no autorizado o ilícito, de conformidad con lo dispuesto en los lineamientos que al efecto se expidan.

El artículo 45, prevé dentro de los elementos a considerar para la adopción de medidas de seguridad y su naturaleza a cargo del Responsable las siguientes:

I. El riesgo inherente a los datos personales tratados.

II. La sensibilidad de los datos personales tratados.

III. El desarrollo tecnológico.

IV. Las posibles consecuencias de una vulneración para las y los titulares.

V. Las transferencias de datos personales que se realicen.

VI. El número de titulares.

VII. Las violaciones a la seguridad previas ocurridas en los sistemas de tratamiento.

VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

El artículo 46 en sus fracciones IV, V, VI y VII menciona que para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable realizará, al menos, las actividades interrelacionadas siguientes:

- Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.
- Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.
- Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.
- Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulnerabilidades a las que están sujetos los datos personales.

El artículo 47 dispone que las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales serán documentadas y contenidas en un sistema de gestión.

Asimismo, define al sistema de gestión como el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

Los artículos 48 y 49 señalan que los Sujetos Obligados elaborarán y aprobarán un documento que contenga las medidas de seguridad aplicables a las bases y sistemas de datos personales, así como el análisis de riesgo, análisis de brecha y plan de trabajo.

El artículo 94 dispone, en sus párrafos primero y tercero, que cada Sujeto Obligado contará con un Comité de Transparencia, el cual se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y la Ley de Transparencia del Estado y tendrá entre sus funciones coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la Ley y en aquellas disposiciones que resulten aplicables en la materia.

Reglamento Interno

El artículo 46 prevé que la UT es la encargada de coordinar las acciones, políticas y estrategias en materia de transparencia, acceso a la información pública y protección de datos personales; así como garantizar el cumplimiento de principio de máxima publicidad y de las disposiciones aplicables locales y nacionales que regulen la materia de transparencia, el ejercicio del derecho de acceso a la información pública y de protección a los datos personales.

Reglamento de Transparencia

El artículo 7 prevé que la UT es la encargada de coordinar acciones, políticas y estrategias en materia de transparencia, acceso a la información pública y protección de datos personales; garantizar el cumplimiento del principio de máxima publicidad y de las disposiciones aplicables locales y nacionales que regulen estas materias, para lo cual se regirá por los principios rectores del IEEM.

Los artículos 11 y 12 disponen que el Comité de Transparencia es el cuerpo colegiado y autoridad máxima al interior del IEEM, en materia de transparencia, del derecho de acceso a la información y protección de datos personales, conformado para resolver, en su caso, sobre la clasificación de la información, así como para atender y resolver los requerimientos de la UT y las áreas que conforman este Instituto, conforme a las atribuciones establecidas en la Ley General de Transparencia, la Ley General de Datos, la Ley de Transparencia del Estado, la Ley de Protección de Datos del Estado, y la normatividad que resulte aplicable.

Además, los artículos 74 y 75 señalan que el IEEM será el responsable de los sistemas y bases de datos personales que obren en su poder, por lo que quienes sean titulares de las áreas responsables serán los administradores de los sistemas de datos personales que competan conforme a sus atribuciones y estarán facultados para llevar a cabo el tratamiento de los mismos, debiendo observar los

principios de calidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad, responsabilidad, y los deberes de confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad.

Manual de Organización

En su numeral 10 en el apartado "Objetivo" establece que corresponde a la UT coordinar las acciones, políticas y estrategias en materia de transparencia, acceso a la información pública y protección de datos personales; así como garantizar el cumplimiento del principio de máxima publicidad y de las disposiciones aplicables locales y nacionales que regulen el ejercicio del derecho de acceso a la información pública y protección de datos personales.

Correlativo a ello, el citado numeral en la viñeta vigésimo tercera dispone como función a cargo de la UT la siguiente:

- Establecer los mecanismos y buenas prácticas para fortalecer la cultura institucional de transparencia, rendición de cuentas y protección de datos personales.

III. MOTIVACIÓN

Como se ha señalado anteriormente, la Constitución Federal y Local señalan que toda persona tiene derecho a la protección de sus datos personales.

De esta manera, el IEEM debe realizar diversas acciones para proteger los datos personales a los que en ejercicio de sus atribuciones da tratamiento y se encuentran contenidos en Sistemas y/o Bases de Datos Personales.

Derivado de ello, se deben establecer y mantener medidas de seguridad las cuales estarán contenidas en un Sistema de Gestión y en los documentos de seguridad de los Sistemas y/o Bases de Datos Personales de los Responsables, como lo es este Instituto

Lo anterior, con el objeto de proteger los datos personales a los que se da tratamiento, así como para garantizar su confidencialidad, integridad y disponibilidad.

En razón de ello, se deben realizar análisis de riesgos de los datos personales, así como de aquellos elementos valiosos y necesarios que contribuyan para que este Instituto proteja y cumpla con los principios, deberes y obligaciones en la materia, a efecto de evitar que se materialicen amenazas que provoquen incidentes o violaciones a la seguridad de los datos personales que en ejercicio de sus atribuciones da tratamiento.

Por otra parte, se deben efectuar análisis de brecha para identificar las medidas de seguridad existentes y aquellas que falten por implementarse, para dar una máxima protección a los datos personales a los que se les da tratamiento.

Asimismo, se debe elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como de aquellas indispensables para dar cumplimiento cotidiano a las políticas de gestión y tratamiento de datos personales.

De igual manera, se deben monitorear y revisar de manera periódica las medidas de seguridad que se implementen, así como las a las que están sujetos los datos personales y aquellos elementos necesarios para su protección.

De este modo, resulta importante contar un "procedimiento de análisis de riesgos y brecha" que contribuya a garantizar el derecho a la protección de los datos personales.

Ello, a través del establecimiento de acciones concretas que auxilien y orienten en el cumplimiento de las obligaciones previstas en la normatividad aplicable en la materia, a quienes dan tratamiento a datos personales contenidos en Sistemas y/o Bases de Datos Personales, siendo la UT la encargada de su implementación y las áreas que administran Sistemas y/o Bases de Datos Personales de su debida observancia.

En este sentido, la UT en ejercicio de sus funciones podrá modificar y actualizar los referentes y los anexos del presente Procedimiento, como parte de la mejora continua, las veces que sean necesarias, lo cual se hará del conocimiento del Comité de Transparencia y de las áreas que administran Sistemas y/o Bases de Datos Personales.

Por lo anteriormente fundado y motivado, este Comité de Transparencia:

A C U E R D A

PRIMERO. Se aprueba el "Procedimiento de Análisis de Riesgos y Brecha", el cual es de observancia obligatoria para todas las áreas y unidades administrativas del IEEM que dan tratamiento a datos personales y se encuentran contenidos en Sistemas y/o Bases de Datos Personales.

SEGUNDO. Se instruye a la UT notificar el presente Acuerdo, así como el "Procedimiento de Análisis de Riesgos y Brecha" que se aprueba.

TERCERO. La UT deberá realizar las gestiones necesarias a fin de hacer del conocimiento a las y los servidores públicos electorales el Procedimiento de Análisis de Riesgos y Brecha", aprobado por este Comité de Transparencia.

CUARTO. La UT como parte de la mejora continua podrá modificar y actualizar los referentes y anexos del presente Procedimiento, lo cual se hará del conocimiento del Comité de Transparencia y de las áreas y unidades administrativas del IEEM que dan tratamiento a datos personales y se encuentran contenidos en Sistemas y/o Bases de Datos Personales.

Así lo determinaron por unanimidad de votos los Integrantes del Comité de Transparencia del Instituto Electoral del Estado de México, con la participación de la Oficial de Protección de Datos Personales, de conformidad con las Leyes de Transparencia y Protección de Datos Personales del Estado, en su Décimo Octava Sesión Extraordinaria. del día veintitrés de agosto de dos mil veintitrés y cierran su actuación firmando al calce para constancia legal.

Dra. Paula Melgarejo Salgado
Consejera Electoral y Presidenta
del Comité de Transparencia

Elaboró. Mtra. Cinthya Aboytes Ibarra
Lic. Georgette Ruiz Rodríguez
ACUERDO N° IEEM/CT/180/2023

Lic. Juan José Hernández López
Subdirector de Administración de Documentos e integrante del Comité de Transparencia

Lic. Ismael León Hernández
Suplente de la Contraloría General e integrante del Comité de Transparencia

Mtra. Lilibeth Álvarez Rodríguez
Jefa de la Unidad de Transparencia e integrante del Comité de Transparencia

Dr. Guillermo Cortés Bustos
Suplente de la Directora Jurídico Consultiva e integrante del Comité de Transparencia

Lic. Georgette Ruiz Rodríguez
Oficial de Protección de Datos Personales