INSTITUTO ELECTORAL DEL ESTADO DE MÉXICO

COMITÉ DE TRANSPARENCIA

ACUERDO N°. IEEM/CT/308/2018

DE APROBACIÓN DE LOS FORMATOS PARA LA ELABORACIÓN DE DOCUMENTOS DE SEGURIDAD, ASÍ COMO DE LA BITÁCORA DE VIOLACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

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

GLOSARIO.

Código Electoral. Código Electoral del Estado de México.

Constitución General. Constitución Política de los Estados Unidos Mexicanos.

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

IEEM. Instituto Electoral del Estado de México.

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

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

A N T E C E D E N T E S

1. El 26 de enero de 2017, se publicó en el Diario Oficial de la Federación, la Ley General de Datos, la cual determina que son Sujetos Obligados de la misma 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.

2. El 30 de mayo del 2017, 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 Datos.

3. En cumplimiento a lo preceptuado por el artículo QUINTO TRANSITORIO de la Ley de Protección de Datos del Estado, el Comité de Transparencia de este Órgano Electoral, en su sesión Trigésima Tercera Extraordinaria celebrada el 31 de mayo de 2018, mediante acuerdo **IEEM/CT/191/2018** denominado *POR EL QUE SE ACTUALIZA EL INVENTARIO Y REGISTRO DE SISTEMAS DE DATOS PERSONALES DEL INSTITUTO ELECTORAL DEL ESTADO DE MÉXICO, ASÍ COMO DE ELIMINACIÓN DE REGISTROS*, aprobó los Sistemas de Datos Personales con que cuenta, en los que se seguirán tratando datos personales.

4. Conforme a lo expuesto, la UT solicitó al Comité de Transparencia la aprobación, mediante el presente Acuerdo, de los formatos de elaboración de Documentos de Seguridad, así como de la bitácora de violaciones a la seguridad de los datos personales, del Instituto Electoral del Estado de México.

CONSIDERACIONES:

I. Competencia

Este Comité de Transparencia es competente para aprobar los formatos para la elaboración de documentos de seguridad, de los sistemas y bases de datos personales del IEEM, de conformidad con lo dispuesto en los artículos 48 de la Ley de Protección de Datos del Estado y 86 del Reglamento de Transparencia.

II. Fundamentación

Constitución General.

El artículo 6°, apartado A, base II, establece que la información que se refiere a la vida privada y 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.

Ley General de Datos.

El artículo 3° establece en sus fracciones II, III, IX, XIV, XXVIII y XXXIII, lo siguiente:

- El **Aviso de privacidad** es el documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

- Las **bases de datos** son un 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;

- Los **datos personales**, son 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;

- **Documento de seguridad:** Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

- El **Responsable** es el Sujeto Obligado, que decide sobre el tratamiento de los datos personales.

- El **tratamiento** es cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

El artículo 4° determina que la ley en cita, será aplicable a cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

En su artículo 16 dispone 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 19 señala que el Responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos y, debe privilegiar la protección de los intereses del titular, así como la expectativa razonable de privacidad.

El artículo 35, de manera particular, establece que el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:

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 39 indica que el responsable deberá llevar una bitácora de las vulneraciones a la seguridad en la que se describa ésta, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

Constitución Local.

El artículo 5°, fracción II, refiere 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.

El artículo 11, en sus párrafos primero y décimo tercero, indica que la organización, desarrollo y vigilancia de los procesos electorales para las elecciones de Gobernador, Diputados a la Legislatura del Estado y miembros de Ayuntamientos es una función que se realiza a través del Instituto Nacional Electoral y el Organismo Público Electoral del Estado de México, denominado IEEM, cuyos principios rectores son la certeza, imparcialidad, independencia, legalidad, máxima publicidad y objetividad y, que este 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, entre otras.

Código Electoral.

El artículo 168 define al IEEM como el 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 y objetividad.

Ley de Protección de Datos del Estado.

El artículo 2, fracción IV, instituye que dentro las finalidades de la ley, se encuentra la de proteger los datos personales en posesión de los Sujetos Obligados del Estado de México, con la finalidad de regular su tratamiento.

El artículo 4 dispone en sus fracciones I, IV, V, VI, XI, XLI, XLIII y L, que se entenderá como:

- **Administrador,** a la servidora pública, el servidor público o la persona física, facultada y nombrada por el Responsable para llevar a cabo el tratamiento de los datos personales y que tienen bajo su responsabilidad, los sistemas y bases de datos personales.

- **Áreas o Unidades Administrativas,** a las instancias que pertenecen los Sujetos Obligados que cuenten o puedan contar, dar tratamiento y ser responsables o encargados, usuarias o usuarios de los sistemas y bases de datos personales previstos en las disposiciones legales aplicables.
-
- **Aviso de Privacidad**, al documento físico, electrónico o en cualquier formato generado por el responsable que es puesto a disposición del Titular con el objeto de informarle los propósitos del tratamiento al que serán sometidos sus datos personales.

- **Base de Datos:** al conjunto de archivos, registros, ficheros, condicionados a criterios determinados con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento, organización y acceso.

- **Datos personales:** a la información concerniente a una persona física o jurídica colectiva identificada o identificable, establecida en cualquier formato o modalidad, que esté almacenada en los sistemas y bases de datos; se considerará que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier documento informativo físico o electrónico.

- **Responsable:** a los Sujetos Obligados a que se refiere la presente Ley que deciden sobre el tratamiento de los datos personales.

- **Sistema de datos personales:** a los datos personales contenidos en los archivos de un Sujeto Obligado que puede comprender el tratamiento de una o diversas bases de datos para el cumplimiento de una o diversas finalidades.

- **Tratamiento:** a las operaciones efectuadas por los procedimientos manuales o automatizados, aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

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.

Y en cuanto a los documentos de seguridad, el artículo 48 establece que los sujetos obligados elaborarán y aprobarán un documento que contenga las medidas de seguridad aplicables a las bases y sistemas de datos personales, tomando en cuenta los estándares internacionales de seguridad, la presente Ley, así como los lineamientos que se expidan.

El documento de seguridad será de observancia obligatoria para los responsables, encargados y demás personas que realizan algún tipo de tratamiento a los datos personales. A elección del sujeto obligado, éste podrá ser único e incluir todos los sistemas y bases de datos personales que posea, por unidad administrativa en que se incluyan los sistemas y bases de datos personales en custodia, individualizado para cada sistema, o mixto.

El artículo 49 determina que el documento de seguridad deberá contener como mínimo lo siguiente:

I. Respecto de los sistemas de datos personales:
   a) El nombre.
   b) El nombre, cargo y adscripción del administrador de cada sistema y base de datos.
   c) Las funciones y obligaciones del responsable, encargado o encargados y todas las personas que traten datos personales.
   d) El folio del registro del sistema y base de datos.
   e) El inventario o la especificación detallada del tipo de datos personales contenidos.

f) La estructura y descripción de los sistemas y bases de datos personales, lo cual consiste en precisar y describir el tipo de soporte, así como las características del lugar donde se resguardan.

II. Respecto de las medidas de seguridad implementadas deberá incluir lo siguiente:

a) Transferencia y remisiones.
b) Resguardo de soportes físicos y electrónicos.
c) Bitácoras para accesos, operación cotidiana y violaciones a la seguridad de los datos personales.
d) El análisis de riesgos.
e) El análisis de brecha.
f) Gestión de incidentes.
g) Acceso a las instalaciones.
h) Identificación y autenticación.
i) Procedimientos de respaldo y recuperación de datos.
j) Plan de contingencia.
k) Auditorías.
l) Supresión y borrado seguro de datos.
m) El plan de trabajo.
n) Los mecanismos de monitoreo y revisión de las medidas de seguridad.
o) El programa general de capacitación.

El artículo 53 establece que el responsable llevará una bitácora de las violaciones a la seguridad, de manera conjunta o separada con la bitácora de incidentes, en la que se describa la violación, la fecha en que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

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 las funciones que le sean conferidas en la normatividad que le resulte aplicable.

Reglamento de Transparencia.

El artículo 84 que todo sistema de datos personales en posesión del Instituto, deberá contar con medidas de seguridad administrativas, físicas y técnicas que permitan garantizar la integridad, confidencialidad y disponibilidad de los datos personales.

Será responsabilidad de las áreas responsables garantizar la protección de los datos personales bajo su resguardo, evitando su daño, alteración, pérdida, destrucción, uso, transferencia, acceso, o cualquier tratamiento no autorizado o

ilícito, así como definir los tipos y niveles de seguridad que serán aplicados a los sistemas de datos personales atendiendo a la naturaleza de los datos.

El artículo 85 prevé que para definir los tipos y niveles de seguridad que serán implementados se tomará en consideración lo establecido en la Ley General de Datos, la Ley de Protección de Datos Personales del Estado, la Ley de Gobierno Digital y demás disposiciones emitidas por los Organismos Garantes, contando en su caso con el apoyo de las áreas técnicas del Instituto.

El artículo 86 determina que las medidas de seguridad serán documentadas a través del formato que para tal efecto apruebe el Comité a propuesta de la Unidad de Transparencia y serán consideradas información confidencial.

El formato de documento de seguridad deberá contener los requisitos establecidos en la Ley General de Datos Personales y en la Ley de Protección de Datos Personales del Estado, sin perjuicio de que atendiendo a los fines institucionales y al tratamiento de datos en el ámbito político electoral se adopten medidas de seguridad adicionales.

III. Motivación

De acuerdo con el artículo 35 de la Ley de Protección de Datos del Estado, corresponde a cada sujeto obligado determinar, a través del Comité de Transparencia, la creación, modificación o supresión de sistemas y bases de datos personales.

Ahora bien, siendo que la Ley de Protección de Datos del Estado exige a los sujetos obligados que los datos personales que recaben para su tratamiento sean incorporados a un sistema o base de datos personales, de acuerdo con su finalidad, funciones y atribuciones que tiene conferidas, también contar con medidas de seguridad administrativas, físicas y técnicas que permitan garantizar la integridad, confidencialidad y disponibilidad en su tratamiento, así como de llevar una bitácora de violaciones a la seguridad de los datos personales, resulta necesario someter a consideración del Comité de Transparencia de este Órgano Electoral los formatos que se adjuntan, dada la íntima relación que guardan.

Con motivo de la publicación el 30 de mayo del 2017, en el Periódico Oficial del Gobierno del Estado Libre y Soberano de México, "Gaceta del Gobierno", de la Ley de Protección de Datos del Estado, que abrogó la anterior, resulta necesario que todos los documentos de seguridad contengan los requisitos previstos en el artículo 49 del mismo ordenamiento, y que conforme al artículo 53, se cuente con una bitácora para violaciones a la seguridad de los datos personales.

Lo anterior es así, derivado que la Ley de Protección de Datos Personales del Estado de México, que fue abrogada, contemplaba requisitos legales diversos a los de la Ley vigente, aunado a que no establecía la obligación de elaborar una bitácora de violaciones a la seguridad de los datos personales y no preveía la modalidad del nombre y cargo del encargado, del procedimiento para el caso de violación de la seguridad de los datos personales, tal y como se muestra a continuación:

TEXTO VIGENTE	TEXTO ABROGADO
Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios.	Ley de Protección de Datos Personales del Estado de México.
Obligatoriedad del Documento de Seguridad Artículo 48. Los sujetos obligados elaborarán y aprobarán un documento que contenga las medidas de seguridad aplicables a las bases y sistemas de datos personales, tomando en cuenta los estándares internacionales de seguridad, la presente Ley así como los lineamientos que se expidan. El documento de seguridad será de observancia obligatoria para los responsables, encargados y demás personas que realizan algún tipo de tratamiento a los datos personales. A elección del sujeto obligado, éste podrá ser único e incluir todos los sistemas y bases de datos personales que posea, por unidad administrativa en que se incluyan los sistemas y bases de datos personales en custodia, individualizado para cada sistema, o mixto. Contenido del Documento de Seguridad Artículo 49. El documento de seguridad deberá contener como mínimo lo siguiente: I. Respecto de los sistemas de datos personales: a) El nombre. b) El nombre, cargo y adscripción del administrador de cada sistema y base de datos. c) Las funciones y obligaciones del responsable, encargado o encargados y todas las personas que traten datos personales. d) El folio del registro del sistema y base de datos. e) El inventario o la especificación detallada del tipo de datos personales contenidos. f) La estructura y descripción de los sistemas y bases de datos personales, lo cual consiste en precisar y describir el tipo de soporte, así como las características del lugar donde se resguardan. II. Respecto de las medidas de seguridad implementadas deberá incluir lo siguiente: a) Transferencia y remisiones. b) Resguardo de soportes físicos y electrónicos. c) Bitácoras para accesos, operación cotidiana y violaciones a la seguridad de los datos personales. d) **El análisis de riesgos.** e) **El análisis de brecha.** f) Gestión de incidentes. g) Acceso a las instalaciones. h) Identificación y autenticación. i) Procedimientos de respaldo y recuperación de datos. j) Plan de contingencia. k) Auditorías. l) Supresión y borrado seguro de datos. m) **El plan de trabajo.**	Obligatoriedad del documento de seguridad Artículo 62. Los sujetos obligados elaborarán y aprobarán un documento que contenga las medidas de seguridad administrativas, tecnológicas, físicas y técnicas aplicables a los sistemas de datos personales, tomando en cuenta los estándares internacionales de seguridad, la presente Ley así como los lineamientos que se expidan. El documento de seguridad será de observancia obligatoria para los responsables, encargados y demás personas que realizan algún tipo de tratamiento a los sistemas de datos personales. A elección del sujeto obligado, éste podrá ser único e incluir todos los Sistemas de datos personales que posea; o bien, por unidad administrativa en que se incluyan los sistemas de datos personales en custodia; o individualizado para cada sistema. Contenido del Documento de Seguridad Artículo 63.- El documento de seguridad deberá contener como mínimo lo siguiente: I. Respecto de los sistemas de datos personales: a) El nombre; b) El nombre, cargo y adscripción del responsable y los encargados de cada base de datos señalando, en su caso, quiénes son externos; c) Las funciones y obligaciones del Responsable y Encargados; d) El folio de registro de la solicitud; e) La especificación detallada del tipo de datos personales contenidos; y f) La estructura y descripción de los sistemas de datos personales, lo cual consiste en precisar y describir el tipo de soporte, así como las características del lugar donde se resguardan. II. Respecto de las medidas de seguridad implementadas deberá incluir lo siguiente: a) Transmisiones; b) Resguardo de soportes físicos y/o de soportes electrónicos; c) Bitácoras para accesos y operación cotidiana; d) Gestión de incidentes; e) Acceso a las instalaciones; f) Identificación y autenticación; g) Procedimientos de respaldo y recuperación de datos; h) Plan de contingencia; i) Auditorías; y j) Cancelación de datos.

Elaboró. Luis Enrique Fuentes Tavira

n) **Los mecanismos de monitoreo y revisión de las medidas de seguridad.** o) **El programa general de capacitación.** **De la Bitácora de Violaciones a la Seguridad de los Datos Personales** Artículo 53. El responsable llevará una bitácora de las violaciones a la seguridad, de manera conjunta o separada con la bitácora de incidentes, en la que se describa la violación, la fecha en que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.	

En este sentido, el Comité de Transparencia advierte que los formatos para la elaboración de los Documentos de Seguridad relativos a los sistemas y bases de datos personales y la bitácora de violaciones a la seguridad de los datos personales constituyen documentos obligatorios por medio de los cuales el IEEM, como responsable del tratamiento a través de sus diferentes áreas administradoras de datos personales, llevará en forma ordenada un registro de los datos personales que recabe, así como las medidas de seguridad que se contemplen para su protección y resguardo, sea de manera electrónica o física.

Con base en lo anterior, es dable concluir que los formatos para la elaboración de documentos de seguridad y la bitácora de violaciones a la seguridad de los datos personales cumplen con los requisitos legales previstos en los artículos 49 y 53 de la Ley de Protección de Datos del Estado, por lo que cada área estará en aptitud de contar con un documento de seguridad en el que se incluyan los sistemas y bases de datos personales en custodia.

En consecuencia, las áreas administradoras de sistemas y bases de datos personales deberán actualizar o elaborar a la brevedad los documentos de seguridad con los que cuenten y la bitácora de violaciones a la seguridad de los datos personales en caso de que ocurra una violación, conforme a los presentes formatos; asimismo, en caso de que se solicite la creación o actualización de sistemas o bases de datos personales distintos a los que se aprobaron por parte del Comité de Transparencia mediante Acuerdo N° IEEM/CT/191/2018, las áreas deberán elaborarlos conforme a los presentes formatos.

Del mismo modo, una vez elaborados deberán remitirlos a la Unidad de Transparencia para su revisión y aprobación en su caso, por el Comité de Transparencia.

Por lo antes expuesto, se:

Elaboró. Luis Enrique Fuentes Tavira

A C U E R D A

PRIMERO. Se aprueban los formatos para la elaboración de los Documentos de Seguridad, así como de la bitácora de violaciones a la seguridad de los datos personales.

SEGUNDO. Se instruye a la Unidad de Transparencia notifique el presente Acuerdo a las áreas del IEEM.

TERCERO. Las áreas del IEEM que administran sistemas y bases de datos personales deberán actualizar o elaborar, a la brevedad, sus documentos de seguridad por unidad administrativa en el que se incluyan todos los sistemas y bases de datos personales en custodia, conforme a los formatos aprobados mediante este Acuerdo, así como a la Ley de Protección de Datos del Estado.

CUARTO. Una vez que las áreas del IEEM administradoras de sistemas y bases de datos personales actualicen sus documentos de seguridad conforme a los formatos aprobados por el presente Acuerdo, deberán remitirlos a la Unidad de Transparencia para su revisión y, en su caso, para que se sometan a la aprobación del Comité de Transparencia.

QUINTO. Se instruye a la Unidad de Transparencia notifique el presente Acuerdo a la Junta General así como al Comité de Tecnologías de la Información y Comunicaciones de este Órgano Electoral, para que en el ámbito de su competencia, con fundamento en el artículo 47 de la Ley de Protección de Datos del Estado, se pronuncien respecto a la instrumentación operativa de un Sistema de Gestión, en materia de Seguridad de Protección de Datos Personales y su tratamiento.

Así lo determinaron por unanimidad de votos los Integrantes del Comité de Transparencia del Instituto Electoral del Estado de México, con la participación del oficial de protección de datos personales, en su Cuadragésima Séptima Sesión Extraordinaria del veinte de septiembre de dos mil dieciocho y cierran su actuación, firmando al calce para constancia legal.

Elaboró. Luis Enrique Fuentes Tavira

Dra. María Guadalupe González Jordan

Consejera Electoral y Presidenta
del Comité de Transparencia

C. Juan José Hernández López

Subdirector de Administración de Documentos e Integrante del Comité de Transparencia

Mtro. Jesús Antonio Tobías Cruz

Contralor General e Integrante del Comité de Transparencia

Mtra. Lilibeth Álvarez Rodríguez

Jefa de la Unidad de Transparencia e Integrante del Comité de Transparencia

Luis Enrique Fuentes Tavira

Oficial de Protección de Datos Personales

Elaboró. Luis Enrique Fuentes Tavira

IEEM
Instituto Electoral del Estado de México

TRANSPARENCIA Y ACCESO A LA INFORMACIÓN

DOCUMENTO DE SEGURIDAD DE SISTEMAS Y BASES DE DATOS PERSONALES

Área Responsable: _____

(Se deberá agregar el área administradora de Sistemas y/o Bases de Datos Personales)

Sistemas y/o Bases de Datos Personales administrados por el área: *(En este apartado deberán enlistarse todos los sistemas y/o bases de datos que están en poder del área)* *1.*_____ *2.*_____	
Sujeto Obligado.	Instituto Electoral del Estado de México
Nombre del Administrador. Cargo. Área de adscripción.	*(En este apartado deberá anotarse el nombre del titular del área).* *(En este apartado deberá anotarse el cargo del titular del área).* *(En este apartado deberá anotarse la adscripción del área).*
Funciones y Obligaciones del Responsable (administrador), encargado o encargados y todas las personas que traten datos personales.	*(En este apartado se precisarán, conforme al Código Electoral del Estado de México, el Manual de Organización, el Reglamento Interno del Instituto Electoral del Estado de México y en su caso, la legislación específica aplicable, las funciones y obligaciones que corresponden al administrador, a los encargados, así como a todas las personas que traten datos personales contenidos en los Sistemas y/o Bases de Datos, con un nivel de básico a alto de protección del área o unidad administrativa que corresponda).*
Folio del registro del sistema y base de datos.	*(En este apartado se precisarán el número o números de registro de cédula en el INTRANET del INFOEM por sistema y/o bases de datos en poder del área).*
El inventario o la especificación detallada del tipo de datos personales contenidos.	*(En este apartado deberán precisarse o enlistarse los datos personales que se encuentran en tratamiento por sistema y/o base de datos).*
La estructura y descripción de los sistemas y bases de datos personales, las cuales consisten en	*(En este apartado deberá precisarse por cada sistema y/o base de datos personales en poder del área si el soporte es en forma física, electrónica o ambas).*

precisar y describir el tipo de soporte, así como las características del lugar donde se resguardan.	*(Se describirá el soporte en el que se encuentran los datos, por ejemplo, para soportes físicos podrían ser entre otros, documentos o expedientes y para soportes electrónicos, hojas de cálculo).*
	(Se deberán precisar por cada uno de los sistemas y/o bases de datos personales las características del lugar donde se resguardan los datos personales dependiendo si se trata de un soporte físico o electrónico).
MEDIDAS DE SEGURIDAD IMPLEMENTADAS	
Transferencia y remisiones.	*(Se deberán precisar por cada uno de los sistemas y/o bases de datos personales las transferencias que en su caso se realicen de los datos personales, así como los destinatarios de los mismos).*
Resguardo de soportes físicos y electrónicos.	*(Se deberán señalar las medidas de seguridad para el resguardo de los soportes físicos y electrónicos de los sistemas y/o bases de datos personales para evitar la alteración, pérdida o accesos no autorizados a los mismos).*
Bitácoras para accesos, operación cotidiana y violaciones a la seguridad de los datos personales.	*(Se deberán especificar todos los elementos que se encuentran contenidos en las bitácoras de acceso, operación cotidiana y violaciones a la seguridad de los datos personales, elaboradas por las áreas. De igual manera se deberá señalar quien es el servidor público(a) responsable de llevar el control de acceso por sistemas y/o bases de datos personales en poder del área).*
El análisis de riesgos.	*(En este apartado el área deberá agregar de manera sintetizada por cada sistema y/o bases de datos personales que obran en su poder, los riesgos detectados respecto a la seguridad de los datos personales y los recursos involucrados en su tratamiento a partir de las medidas de seguridad implementadas).*
El análisis de brecha.	*(En este apartado se deberán anotar de manera sintetizada los resultados del análisis de la comparación realizada por el área de las medidas de seguridad existentes contra las faltantes, de acuerdo con el tipo y nivel de seguridad aplicable a los sistemas y/o bases de datos personales de conformidad con lo establecido en el artículo 44 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios).*
Gestión de incidentes.	*(En este apartado se deberán describir los mecanismos, políticas y controles de seguridad que se deberán tomar en caso de que ocurra un incidente de seguridad. Dicho apartado aplica a los sistemas y/o bases de datos personales con un nivel de básico a alto de protección).*

Acceso a las instalaciones.	*(Se deberá especificar quiénes están expresamente autorizados para ingresar a las instalaciones donde se encuentren los sistemas y/o bases de datos personales, ya sea en soporte físico o electrónico. Este apartado aplica a los sistemas y/o bases de datos personales con un nivel de básico a alto de protección).*
Identificación y autenticación.	*(Se establecerá el procedimiento que permita la correcta identificación y autenticación, de forma inequívoca y personalizada, para ello se deberá agregar una relación actualizada por sistemas y/o bases de datos personales en posesión de los servidores públicos que tengan acceso autorizado conforme a sus facultades, competencias y funciones. Este apartado aplica a los sistemas y/o bases de datos personales con un nivel básico a alto de protección).*
Procedimientos de respaldo y recuperación de datos.	*(Se deberán describir los mecanismos para la realización de copias de respaldo y recuperación de datos personales.* *En caso de que los datos personales se encuentren en soporte físico se procurará que el respaldo se efectúe mediante la digitalización de los documentos.* *Cuando los datos personales se encuentren en soporte electrónico se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida involuntaria o destrucción accidental. Este apartado aplica a los sistemas y/o bases de datos personales con un nivel básico a alto de protección).*
Plan de contingencia.	*(Se deberá agregar la siguiente leyenda:* *"Se establecerá el conjunto de procedimientos alternativos a seguir en caso de que exista una violación a la seguridad de los datos personales, así como las acciones que serán definidas en el plan de contingencia institucional").*
Auditorías.	*(Se deberá agregar la siguiente leyenda en los sistemas y/o bases de datos personales de nivel medio y alto de protección:* *"Las medidas de seguridad implementadas a los sistemas y/o bases de datos personales, se sujetarán a una auditoría*

	por parte de la Contraloría General para verificar el cumplimiento de la ley". *En los sistemas y/o bases de datos personales de nivel básico de protección se deberá agregar la siguiente leyenda: "No aplica").*
Supresión y borrado seguro de datos.	*(Se precisarán por sistema y/o bases de datos personales los mecanismos para la supresión y borrado seguro de los datos personales una vez que se haya cumplido con la finalidad de su utilización.* *Nota: La áreas deberán tomar en consideración si la normatividad en materia electoral prevé reglas específicas para la destrucción de algún tipo de documento que contenga datos personales, ejemplo "listado nominal").*
El plan de trabajo.	*(Se deberá agregar la siguiente leyenda:* *"En caso de violación a la seguridad de los datos personales se aplicarán las acciones preventivas y correctivas a seguir para adecuar las medidas de seguridad y el tratamiento de los datos personales establecidos en el plan de trabajo si fuese el caso, a efecto de evitar que la violación se repita").*
Los mecanismos de monitoreo y revisión de las medidas de seguridad.	*(Se precisarán los mecanismos para monitorear y revisar de manera periódica las medidas de seguridad implementadas por el área, así como las amenazas y vulnerabilidades a las que están sujetos los datos personales contenidos en los sistemas y/o bases de datos personales).*
El programa general de capacitación.	*(Se deberá agregar la siguiente leyenda:* *"El personal será capacitado de manera permanente en coordinación con la Unidad de Transparencia conforme al programa anual de actividades aprobado por el Consejo General del IEEM").*

IEEM
Instituto Electoral del Estado de México

TRANSPARENCIA Y ACCESO A LA INFORMACIÓN

BITÁCORA DE VIOLACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES

Área responsable: _____

Nombre del sistema y/o base de datos personales:
_____

No.	Descripción de la Violación	Fecha en que ocurrió la violación	Motivo por el que ocurrió la violación	Acciones correctivas implementadas por el área