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

Política de Gestión Datos Personales del Instituto Electoral del Estado de México

Política de Gestión de Datos Personales del Instituto Electoral del Estado de México

1.- Presentación

En términos de los artículos 29, 30 fracción II, 33 fracción I y 34 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 27, 28 fracción II, 46 fracción I y 47 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, este órgano electoral debe implementar mecanismos con el objeto de acreditar la observancia a los principios, deberes y obligaciones que derivan de la legislación aplicable.

Entre los mecanismos que se deben establecer, se encuentra el relativo a elaborar políticas obligatorias para la gestión y tratamiento de los datos personales que tomen en cuenta su ciclo de vida.

En este sentido, y a efecto de que el Instituto Electoral del Estado de México como Sujeto Obligado dé estricto cumplimiento a la normatividad en la materia, se emite la presente política.

2.- Política de Gestión de Datos Personales del Instituto Electoral del Estado de México

En el Instituto Electoral del Estado de México las y los servidores públicos electorales, en estricto cumplimiento a los ordenamientos aplicables en la materia, nos comprometemos a proteger, así como a mantener la confidencialidad, integridad y disponibilidad de los datos personales; así como de la documentación en soporte físico y electrónico que, con motivo del ejercicio de nuestras atribuciones normativas, damos tratamiento y se encuentran almacenados en Sistemas y/o Bases de Datos Personales.

Para ello, implementamos medidas de seguridad para así evitar su daño, alteración, pérdida, destrucción, uso indebido, transferencia y acceso no autorizado, conforme a los niveles de riesgo que identificamos.

Por otra parte, contamos con un Sistema de Gestión de Seguridad de Protección de Datos Personales que establece, implementa, opera, monitorea, revisa, mantiene y mejora de manera continua el tratamiento y la seguridad de los datos personales, así como de la documentación en soporte físico y electrónico contenida en Sistemas y/o Bases de Datos Personales, en función del riesgo de los activos.

3.- Alcance

El alcance de la presente política está orientado a proteger los datos personales, así como la documentación en soporte físico y electrónico que, con motivo del ejercicio de nuestras atribuciones normativas, damos tratamiento y se encuentran almacenados en Sistemas y/o Bases de Datos Personales.

4.- Objetivo

El objetivo de la presente política es establecer acciones e implementar medidas de seguridad en cumplimiento a los principios, deberes y obligaciones que derivan de la normatividad en la materia, para proteger los datos personales, así como la documentación en soporte físico y electrónico que el Instituto Electoral del Estado de México, en ejercicio de sus atribuciones legales, da tratamiento y los cuales se encuentran almacenados en Sistemas y/o Bases de Datos Personales.

5.- Términos y Definiciones

Activo: Datos personales, documentación en soporte físico y electrónico, así como cualquier elemento valioso para que el Instituto Electoral del Estado de México cumpla sus objetivos.

Administrador (a): La o el servidor público facultado para llevar a cabo el tratamiento y que tiene bajo su responsabilidad Sistemas y/o Bases de Datos Personales.

Alta dirección: Comité de Transparencia del Instituto Electoral del Estado de México.

Análisis de brecha: Proceso que permite comparar las medidas de seguridad existentes contra las faltantes.

Análisis de riesgos: Proceso que permite comprender la naturaleza y determinar el nivel del riesgo.

Base de Datos: 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: Cualquier información personal concerniente a personas físicas identificadas o identificables, establecida en cualquier formato o modalidad, y que esté almacenada en los sistemas y bases de datos.

Escenario de riesgo: Descripción de una amenaza que deriva de una vulnerabilidad determinada o un conjunto de vulnerabilidades que ponen en riesgo la documentación en soporte físico y electrónico, así como los datos personales que se encuentran almacenados en los Sistemas y/o Bases de Datos Personales administrados por las áreas del Instituto Electoral del Estado de México.

IEEM: Instituto Electoral del Estado de México.

Medidas de seguridad: Acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten proteger los activos que no son datos personales y los activos de datos personales.

Nivel de Riesgo: Grado de afectación a cualquier activo.

Organismos Garantes: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales e Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios.

Responsable en materia de seguridad: Servidoras y servidores públicos electorales que tienen como función principal atender y vigilar el cumplimiento de las medidas de seguridad establecidas por la o el administrador.

Riesgo: Es la probabilidad o posibilidad de que un evento desfavorable ocurra. Tiene un impacto negativo si se materializa.

Sistema de datos personales: Conjunto de datos personales contenidos en los archivos del Instituto Electoral del Estado de México que puede comprender el tratamiento de una o diversas bases de datos para el cumplimiento de una o diversas finalidades.

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

Titulares: Persona física o jurídica colectiva a la que corresponden los datos personales que sean objeto de tratamiento.

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

Usuarias o Usuarios: Personas autorizadas para tratar los datos personales, distintos al responsable, al encargado y al administrador de los datos.

Violación a la seguridad de datos personales: Es la materialización de las amenazas que pueden estar enfocadas a la pérdida, robo, extravío, daño, destrucción, alteración, copia, uso o tratamiento no autorizados.

6.- Marco Legal

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

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

7.- Referencias Normativas

- ISO/IEC 27001:2013 Tecnologías de Información – Técnicas de Seguridad y Sistemas de Gestión de la Seguridad de la Información.

- Lineamientos Generales en Materia de Protección de Datos Personales para el sector público aprobados por el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

- Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales emitidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

8.- Roles y responsabilidades.

ROLES	RESPONSABILIDADES
Comité de Transparencia	• Coordinar las acciones necesarias para garantizar la protección de los datos personales, así como de la documentación en soporte físico y electrónico que con motivo del ejercicio de las atribuciones normativas del IEEM, se da tratamiento y se encuentran

ROLES	RESPONSABILIDADES
	contenidos en Sistemas y/o Bases de Datos Personales. • Supervisar, en coordinación con quienes funjan como administradores (as) y responsables en materia de seguridad, el cumplimiento de las medidas y acciones que se implementen en observancia a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios; así como, demás normatividad aplicable. • Aprobar el "Programa de capacitación en materia de protección de datos personales". • Modificar y aprobar la presente política.
Administrador (a)	• Establecer al interior de las áreas acciones que garanticen la protección de los datos personales, así como de la documentación en soporte físico y electrónico que con motivo del ejercicio

ROLES	RESPONSABILIDADES
	de las atribuciones normativas del IEEM, se da tratamiento y se encuentran contenidos en Sistemas y/o Bases de Datos Personales.
Responsable en materia de seguridad	• Atender y vigilar el cumplimiento de las medidas de seguridad que garanticen, cuando menos, la autenticidad, confidencialidad, disponibilidad e integridad de los datos personales. • Establecer los criterios específicos sobre el manejo, mantenimiento, seguridad y protección de los sistemas o bases de datos personales. • Establecer procedimientos de control de acceso a la red que incluyan perfiles de usuarios (as) o grupos de usuarios (as) para el acceso restringido a las funciones y programas de los Sistemas o Bases de Datos Personales. Para tal efecto, podrán solicitar la asesoría técnica correspondiente.

<table>
<tr><th>ROLES</th><th>RESPONSABILIDADES</th></tr>
<tr><td>Usuario (a)</td><td>• Cumplir con las medidas, controles y acciones que se implementen en observancia a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios.</td></tr>
<tr><td colspan="2">Adicionalmente a las responsabilidades señaladas anteriormente, quien funja como administrador (a), responsable en materia de seguridad y usuario (a), debe:

• Proteger los datos personales, así como la documentación en soporte físico y electrónico que con motivo del ejercicio de las atribuciones normativas del IEEM, se da tratamiento y se encuentran contenidos en Sistemas y/o Bases de Datos Personales.

• Dar cumplimiento a los principios, deberes, obligaciones y demás normatividad aplicable.</td></tr>
<tr><td>Unidad de Informática y Estadística

Subdirección de Administración de Documentos

Unidad de Transparencia</td><td>• Concientizar y capacitar en el ámbito de sus atribuciones, al personal del IEEM que da tratamiento a los datos personales, así como a la documentación en soporte físico y electrónico de los Sistemas y/o Bases de Datos Personales administrados por las áreas.</td></tr>
</table>

ROLES	RESPONSABILIDADES
La Unidad de Transparencia deberá además: • Realizar las gestiones correspondientes para que la presente Política esté actualizada y disponible en los medios de comunicación oficiales. • Monitorear el cumplimiento de la presente política. • Informar a la Alta Dirección los resultados del monitoreo.	

9.- Gestión de datos personales del IEEM

Quien funja como Administrador (a), Responsable en Materia de Seguridad y Usuario (a), debe proteger los datos personales, así como la documentación en soporte físico y electrónico que con motivo del ejercicio de sus atribuciones normativas dé tratamiento y se encuentren contenidos en Sistemas y/o Bases de Datos Personales.

Lo anterior, desde que se recaben, hasta que se proceda a su supresión y baja documental, previo bloqueo, una vez que se hayan cumplido los plazos de conservación establecidos en los instrumentos de control y consulta archivística, así como sus finalidades, dando siempre cumplimiento a los principios, deberes y obligaciones establecidas en la normatividad aplicable.

9.1.- Objetivos específicos

1. Concientizar y capacitar de manera permanente, a través de la Unidad de Transparencia, en colaboración con la Unidad de Informática y Estadística y la

Subdirección de Administración de Documentos, al personal del IEEM que da tratamiento a los datos personales, así como a la documentación en soporte físico y electrónico de los Sistemas y/o Bases de Datos Personales administrados por las áreas.

2. Identificar los escenarios que podrían poner en riesgo los datos personales, así como la documentación en soporte físico y electrónico que con motivo del ejercicio de las atribuciones normativas del IEEM, se da tratamiento y se encuentran contenidos en Sistemas y/o Bases de Datos Personales.

3. Implementar las medidas de seguridad necesarias para tratar, prevenir, mitigar, transferir o aceptar riesgos.

4. Realizar análisis de brecha que permitan determinar las medidas de seguridad faltantes, con el objeto de definir una estrategia de seguridad

5. Identificar incidentes y violaciones a la seguridad, conforme a la normatividad establecida para tal efecto.

9.2.- Medición

1. Para concientizar y capacitar al personal del IEEM que da tratamiento a los datos personales, así como a la documentación en soporte físico y electrónico de los Sistemas y/o Bases de Datos Personales, se realizarán por lo menos 2 capacitaciones anualmente.

   Aunado a ello, se le aplicará al personal 2 evaluaciones, una de diagnóstico y otra para medir los conocimientos adquiridos.

2. Se realizarán de manera aleatoria los análisis de riesgos por lo menos 2 veces al año.

3. Se monitorearán y revisarán las medidas de seguridad periódicamente.

4. Se monitorearán periódicamente las medidas de seguridad que se implementen derivado del análisis de brecha.

5. Se establecerán estrategias para el tratamiento de incidentes y de violaciones a la seguridad.

9.3.- Compromiso

El compromiso del IEEM es mantener actualizada y disponible la presente política para la consulta de las partes interesadas.

Aunado a ello, se llevará a cabo su monitoreo y revisión para medir su cumplimiento, eficacia, y así lograr su mejora continua.

9.4.- Comunicación

1. La presente política estará disponible en los medios de comunicación oficiales para la consulta de:

   - Las (os) titulares de los datos personales.
   - Personal del IEEM que da tratamiento a los datos personales, así como a la documentación en soporte físico y electrónico de los Sistemas y/o Bases de Datos Personales administrados por las áreas.
   - El Comité de Transparencia y la Unidad de Transparencia.
   - Organismos Garantes.
   - Ciudadanía en general.

2. Se revisará por lo menos cada 6 meses para determinar su eficacia y podrá ser modificada como parte de la mejora continua o cuando se presente alguna violación a la seguridad.

3. Cualquier cambio será informado a través de los medios de comunicación oficiales.

9.5.- Mejora Continua

A partir del monitoreo que se realiza a la política para medir su eficacia y cumplimiento, se podrán identificar acciones de mejora que impacten en los datos personales, así como en la documentación en soporte físico y electrónico que con motivo del ejercicio de las atribuciones normativas del IEEM, se da tratamiento y se encuentran contenidos en Sistemas y/o Bases de Datos Personales, conforme a lo establecido en la normatividad de la materia, los procesos internos y la metodología aplicable.

9.6.- Partes interesadas

Se consideran partes interesadas en la presente política, la o el Titular de los datos personales, Administrador (a), Responsable en Materia de Seguridad, Usuario (a), el Comité de Transparencia, la Unidad de Transparencia, los Organismos Garantes y ciudadanía en general.

9.7.- Medidas de seguridad

Se adoptarán, establecerán, mantendrán y documentarán 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.

Aunado a ello, se identificarán e implementarán medidas adicionales derivadas de los análisis de riesgos y brecha.

ANEXO

CONTROL DE CAMBIOS

Número de revisión	Páginas modificadas	Descripción del cambio	Fecha de modificación
Registrar de manera consecutiva las revisiones a la Política.	Señalar las páginas en las cuales se realizaron las modificaciones.	Especificar de manera concreta las modificaciones realizadas.	Anotar la fecha en que se realiza la modificación.