



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

Plan de Trabajo de la Comisión de Protección de Datos Personales 2021

Metepec, Estado de México, 15 de octubre de 2021



Introducción

El presente plan de trabajo establece las acciones diseñadas para continuar con la promoción de la educación y la cultura de protección de datos personales, así como el ejercicio de este derecho en el Estado de México. La Comisión, coordinada por el Comisionado Luis Gustavo Parra Noriega, e integrada por las Comisionadas Sharon Cristina Morales Martínez y Guadalupe Ramírez Peña, será la encargada de establecer las directrices para el cumplimiento de metas del presente plan, apoyados por la Dirección General de Protección de Datos Personales y con apego al Plan Estatal y Municipal de Protección de Datos Personales del Estado de México y Municipios y demás normatividad vigente.

Página | 2

Anteriormente, esta comisión ha trabajado en posicionar la protección de datos personales como un tema sustantivo, por medio de eventos de difusión y divulgación de información por diferentes medios.

Con base en el análisis de rubros a cubrir, este programa se integra por 6 estrategias, las cuales abarcarán temas que requieren la atención inmediata, y que guardan relación y son referentes con el fortalecimiento de la cultura de protección de datos personales, la profesionalización de las y los servidores públicos y Responsables, el reconocimiento de la figura de Oficial de Protección de Datos Personales, la socialización de esquemas de educación digital en torno a la privacidad, la Ciberseguridad bajo un esquema de prevención y gestión ante incidentes, la difusión y acompañamiento a la ciudadanía a fin de que conozca sus derechos



ARCOP, y finalmente el tratamiento de los datos personales en dispositivos y sistemas de Inteligencia Artificial.

Es de suma importancia destacar que la instalación de esta Comisión conlleva novedades y retos que emanan de la estrecha relación de la tecnología con el tratamiento de datos personales, por ello, presentar como innovación una vertiente enfocada en la Ciberseguridad para fortalecer los trabajos de los Responsables del tratamiento, sentará las bases de una nueva forma de proteger la información que las y los mexiquenses ponen en manos de las instituciones públicas de la entidad.

Esta meta, de auxiliar a mejorar los esquemas de protección en el sector público, nos permitirá que a partir de un enfoque preventivo y de acompañamiento, mejore los esquemas de gestión de riesgos que vislumbra la legislación estatal en la materia, pues será de amplia utilidad para evitar vulneraciones a los sistemas informáticos que son utilizados para almacenar y aprovechar información de carácter personal.

De esta manera, se prevé que cada una de las actividades que sean analizadas y aprobadas por la Comisión, posicionen, tanto en el plano nacional como internacional, al Infoem como un órgano garante vanguardista, pero sobre todo eficiente ante una sociedad cuyas necesidades aumentan día con día, a la par del desarrollo de la tecnología, en concordancia con la Estrategia Digital Nacional y sus desafíos.



Misión

Proveer a la ciudadanía herramientas teóricas y prácticas adaptables a los fenómenos de innovación, para el correcto uso de su derecho a la protección de datos personales.

Visión

Ser factor de cambio y concientización social en el conocimiento de los derechos de protección de datos personales, relacionados con las nuevas tendencias tecnológicas que ponen en riesgo la privacidad de los ciudadanos.

Objetivo General

Establecer los medios suficientes para facilitar el conocimiento y protección de los datos personales de la ciudadanía.

Objetivos específicos

- Desarrollar canales para democratizar la educación y una cultura de protección de datos personales entre la sociedad mexiquense.
- Fomentar la oficialización de los conocimientos de servidores públicos sobre la protección de datos personales para garantizar el alto desempeño en sus funciones.
- Realizar canales de comunicación amigables para educar sobre la privacidad en medios digitales.



- Reducir la brecha de seguridad de los Responsables del tratamiento de datos personales mediante la promoción e implementación de ejercicios de Ciberseguridad.
- Fortalecer los mecanismos de gestión de riesgo y medidas de seguridad que implementan los sujetos obligados a través de asesorías técnicas y especializadas por parte de especialistas en seguridad digital.
- Continuar con los ejercicios de acompañamiento relacionados con los derechos ARCO, tanto a los Responsables para que actúen como distribuidores de conocimiento, como para la ciudadanía que lo requiera.
- Concientizar a la ciudadanía sobre los riesgos del uso de datos personales al adquirir o contratar los servicios de Inteligencia Artificial.



ESTRATEGIA 1

Fortalecimiento a la cultura de protección de datos personales

Líneas de acción

1. Seguimiento y evaluación al Programa Estatal y Municipal de Protección de Datos Personales 2020-2022 de manera periódica.
2. Carta por los derechos digitales de niñas, niños y adolescentes. Además de una campaña de sensibilización sobre el ejercicio de los derechos digitales de los niños.
 - Para esta acción se prevé que el Instituto buscará trabajar en coordinación con organizaciones y Responsables, tanto en el diseño del documento como en las actividades de difusión de la misma.
3. Realizar conferencias con participación de ponentes nacionales e internacionales, llevados a cabo por plataformas electrónicas, con lenguaje ciudadano, cuyo público objetivo no necesariamente sea especialista en datos personales.

ESTRATEGIA 2

Fortalecimiento del Marco Normativo de la Dirección General de Protección de Datos Personales

1. Padrón de Sujetos Obligados en materia de Protección de Datos Personales.
2. Lineamientos para implementar los procedimientos de investigación y verificación, así como la práctica de auditorías voluntarias a los Responsables



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

3. Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios.
4. Implementación del Registro de Sistemas y Bases de Datos Personales del Estado de México (REDATOSEM).
5. Guía para la implementación de Sistemas de Gestión de Seguridad de Datos Personales.
6. Guía para elaborar el documento de seguridad de acuerdo con la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios; aplicable a los sistemas de datos personales en posesión de los Sujetos Obligados.
7. Guía para determinar el nivel de seguridad aplicable a los sistemas de datos personales en posesión de los Sujetos Obligados.
8. Reconocer las mejores prácticas en materia de protección de datos personales que realicen los Responsables del tratamiento de la entidad.



ESTRATEGIA 3

Socialización de esquemas de educación digital en torno a la privacidad y la Violencia

Líneas de acción

Página | 8

1. Realizar foros especializados para la prevención de la Violencia Digital y el mal uso de los datos personales en las plataformas digitales.
2. Generar materiales de difusión sobre prevención de la violencia digital, la protección de datos personales, los ciberdelitos y las sanciones.
3. Asesoramiento sobre denuncias y trámites a víctimas de violencia digital.
4. Establecer mecanismos directos de atención a eventos relacionados con la violencia digital y que resulten del acercamiento ciudadano con el Infoem, teniendo a un grupo de trabajo técnico y especializado en el Instituto, a fin de brindar orientación con los protocolos necesarios y su posterior direccionamiento a la Policía Cibernética (se propondrá convenio de colaboración en la materia con la SSC, el cual deberá comprender la capacitación de personal del Infoem en el tema, los trámites necesarios, los enlaces informáticos suficientes para la correcta comunicación y la coordinación en casos de actuación inmediata).
5. Buzón electrónico de denuncias. En caso de darse el convenio con la SSC, las denuncias se canalizarán de forma inmediata a la Policía Cibernética.



6. Generar un mapeo de actores políticos que contribuyan para alcanzar los objetivos referentes a la prevención de la violencia digital, en lo general y la violencia de género en Internet, en lo particular.
7. Trabajar en coordinación con instituciones educativas para incluir contenido referente al derecho a la protección de datos personales en los planes y programas de estudio de los distintos niveles educativos.
8. Capacitar a los docentes de las instituciones educativas para que dentro de sus actividades contribuyan a la difusión del derecho a la protección de datos personales.
9. Trabajar de manera colaborativa con la Secretaría de Educación del Estado de México para el diseño de acciones educativas enfocadas en la promoción de la educación digital.

ESTRATEGIA 4

Difusión y acompañamiento para el conocimiento de los derechos ARCOP con la ciudadanía

Líneas de acción

1. Elaborar manuales de orientación sobre el derecho a la privacidad, la protección de datos, Ciberseguridad y los derechos ARCOP de acuerdo con el perfil escolar, poblacional y de madurez digital.
2. Realizar campañas informativas sobre los derechos ARCOP.



3. Realizar sesiones de acompañamiento con los Responsables para que se conviertan en asesores de la ciudadanía que frecuente sus dependencias, sobre derechos ARCOP.



ESTRATEGIA 5

Concientización a la ciudadanía sobre las oportunidades y amenazas que conlleva el uso de Inteligencia Artificial

Líneas de acción

1. Elaborar un Manual Ciudadano sobre Inteligencia Artificial (IA) y protección de datos personales, que permita a las personas en general conocer lo siguiente:
 - Que al adquirir o utilizar IA supone el tratamiento y recolección de datos personales.
 - Que dichos tratamientos de datos personales están regulados.
 - Los riesgos y beneficios por su uso.
 - La información básica que deben conocer si pretenden comprar o utilizar IA.
 - Los derechos que deben garantizar los desarrolladores o prestadores de servicios de IA.
 - Dónde se almacenan sus datos personales y qué medidas de seguridad se deben implementar para su protección.



Para que esta acción tenga un mayor impacto, se buscará trabajar en coordinación con los Responsables del tratamiento de datos personales de la entidad, de tal manera que el manual que se diseña sea de observancia obligatoria y con acciones plausibles para su pronta implementación.



ESTRATEGIA 6

Profesionalización de servidores públicos y Responsables en materia de protección de datos personales y seguridad digital

Líneas de acción

1. Curso virtual en materia de protección de datos personales.
2. Fortalecimiento de la estructura de la Dirección General de Protección de Datos Personales a través de la integración de personal especializado en Ciberseguridad.
3. Programa de Acompañamiento para la implementación de medidas de seguridad digital.
4. Taller en materia de seguridad digital y Ciberseguridad.
5. Contar con una certificación para Oficiales de Protección de Datos Personales en el Estado de México.
6. Certificar al personal adscrito a la Dirección General de Protección de Datos Personales, a fin de que se puedan reconocer sus competencias en la materia.

