



GOBIERNO DEL
ESTADO DE MÉXICO

Periódico Oficial

Gaceta del Gobierno

Gobierno del Estado Libre y Soberano de México

REGISTRO DGC NÚM. 001 1021 CARACTERÍSTICAS 113282801

Director: Lic. Aarón Navas Alvarez
legislacion.edomex.gob.mx

Mariano Matamoros Sur núm. 308 C.P. 50130

A: 202/3/001/02

Fecha: Toluca de Lerdo, Méx., jueves 31 de mayo de 2018

“2018. Año del Bicentenario del Natalicio de Ignacio Ramírez Calzada, El Nigromante”.

Sumario

INSTITUTO DE TRANSPARENCIA, ACCESO A LA
INFORMACIÓN PÚBLICA Y PROTECCIÓN DE
DATOS PERSONALES DEL ESTADO DE MÉXICO Y
MUNICIPIOS

PROGRAMA ESTATAL Y MUNICIPAL DE
PROTECCIÓN DE DATOS PERSONALES.

Tomo CCV
Número

96

SECCIÓN SÉPTIMA

Número de ejemplares impresos: 300

INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE MÉXICO Y MUNICIPIOS



Programa Estatal y Municipal de
Protección de Datos Personales

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

Programa Estatal y Municipal de Protección de Datos Personales

Índice

Presentación

Estructura del programa

I. Objetivo general, objetivos estratégicos y estrategias del programa

II. Desarrollo de ejes temáticos

1. Educación y cultura de protección de los datos personales de los mexiquenses
2. Capacitación de los responsables
3. Certificación de los sujetos obligados
4. Ejercicio de los derechos ARCO y la portabilidad
5. Implementación y mantenimiento de los sistemas de gestión de seguridad
6. Estándares en buenas prácticas en materia de protección de los datos personales
7. Gestión de recursos
8. Monitoreo, seguimiento y verificación de metas

Glosario

Presentación

El Programa Estatal y Municipal de Protección de Datos Personales tiene como objetivo general el reconocimiento y pleno ejercicio del derecho a la protección de los datos personales en el Estado de México.

Por ende, la misión del presente programa consiste en promover el efectivo ejercicio y la eficaz tutela de los derechos de acceso, rectificación, cancelación y oposición al tratamiento de los datos personales (ARCO) entre los mexiquenses e impulsar el desarrollo de la cultura de protección de los datos personales, obedeciendo no sólo a los ordenamientos legales de la materia, sino también al interés del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios (Infoem) por fortalecer el conocimiento, ejercicio y respeto por este derecho humano. Asimismo, tiene como visión constituirse como el instrumento rector de la política pública en materia de protección de los datos personales en la entidad.

La reforma constitucional del 7 de febrero de 2014 al artículo 6º constitucional fue no sólo una transformación en materia de transparencia y acceso a la información pública, sino una modificación en favor del derecho a la protección de los datos personales, ya que faculta al órgano garante autónomo para su salvaguarda.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados estipula, en su artículo 12, el objetivo de diseñar, ejecutar y evaluar un Programa Nacional de Protección de Datos Personales (Pronadatos) por parte del Sistema Nacional de Transparencia (SNT), para que funcione como instrumento rector de la política pública destinada a la integración y coordinación en la materia. Asimismo, prevé la implementación de los respectivos programas estatales y municipales. En un sentido semejante, el artículo 5º de la Constitución Política del Estado Libre y Soberano de México contempla el deber de garantizar el ejercicio del derecho a la protección de los datos personales.

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, en su artículo 14, contiene la obligación para el Infoem de diseñar, ejecutar y evaluar un programa estatal y municipal de protección de los datos personales, como política pública que atienda esta materia a partir de objetivos, estrategias, acciones y metas.

El Pronadatos 2018-2022 es el instrumento del SNT que coordina las bases de la política pública de protección de los datos personales en el país, dentro del sector público. Para ello, se auxilia de una estructura de política pública que incluye la identificación de problemáticas y el diseño de objetivos y acciones. Uno de sus ejes temáticos consiste en contar con una perspectiva normativa con enfoque de política pública en las entidades federativas.

El PEMPDP busca promover, entre la población, el ejercicio y tutela de los derechos ARCO y la portabilidad, así como impulsar el desarrollo de la cultura de protección de los datos personales. Se dirige a los responsables del tratamiento de datos personales de la población de esta entidad, definidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, pues, como política pública rectora en la materia, integra y exhorta a todos los actores sociales para que, desde su ámbito de competencia y actuación, se fortalezca este derecho humano en beneficio de nuestro sistema democrático.

El presente programa constituye la guía de las acciones de política pública en materia de protección de datos personales en el Estado de México en el periodo 2018-2020.

Estructura del programa

El Programa Estatal y Municipal de Protección de Datos Personales (PEMPDP) se ha estructurado con un esquema de política pública, utilizando la metodología de planeación estratégica y atendiendo a las disposiciones del artículo 14 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios y al propio Pronadatos 2018-2022.

El PEMPDP consta de un objetivo general, objetivos estratégicos y estrategias generales. Se encuentra organizado en 8 ejes temáticos que, en conjunto, llevan al cumplimiento de los objetivos estratégicos y las estrategias. Dichos ejes temáticos son los siguientes:

1. Educación y cultura de protección de los datos personales de los mexiquenses.
2. Capacitación de los responsables.
3. Certificación de los sujetos obligados.
4. Ejercicio de los derechos ARCO y la portabilidad.
5. Implementación y mantenimiento de los sistemas de gestión de seguridad.
6. Estándares en buenas prácticas en materia de protección de los datos personales.
7. Gestión de recursos
8. Monitoreo, seguimiento y verificación de metas.

Cada eje temático consta de un diagnóstico que describe la problemática detectada, un análisis FODA, líneas estratégicas y líneas de acción.

I. Objetivo general, objetivos estratégicos y estrategias del programa

El objetivo general del PEMPDP radica en el reconocimiento y pleno ejercicio del derecho a la protección de los datos personales en el Estado de México. Para su cumplimiento, se han establecido tres objetivos estratégicos:

1. Consolidar el marco de la cultura y la educación en materia de protección de los datos personales, así como la profesionalización de los responsables de su tratamiento.
2. Fortalecer el ejercicio de los derechos ARCO y la portabilidad.
3. Consolidar prácticas eficientes e innovadoras en la administración y gestión de los datos personales.

Cada objetivo estratégico tiene una estrategia general:

1. Alcanzar una amplia concientización ciudadana respecto del derecho a la protección de los datos personales, así como el óptimo desarrollo profesional de los responsables del tratamiento de los mismos.

2. Lograr una mayor participación de las personas en relación con el ejercicio de los derechos ARCO y la portabilidad, como instrumentos activos de ciudadanía.
3. Implementar acciones administrativas y de gestión que fortalezcan la protección de los datos personales.

II. Desarrollo de los ejes temáticos

Eje temático 1. Educación y cultura de protección de los datos personales de los mexicanos

Diagnóstico

Por lo que respecta a la educación y cultura del derecho de protección de datos personales encontramos un alto desconocimiento de la población mexicana sobre el derecho a la protección de los datos personales y su debido ejercicio; así como sobre las funciones del Infoem, entre ellas, la salvaguarda del mencionado derecho.

En el “Primer Estudio sobre Protección de Datos Personales entre Usuarios y empresas en México”, realizado por la Asociación Mexicana de Internet en 2016, consigna que 90% de un total de 734 internautas mexicanos encuestados no ha ejercido el derecho de acceso a los datos personales; 61% desconoce el tratamiento otorgado a sus datos personales en las redes sociales a las que pertenece, y 31% no sabe definir qué es un dato personal. Igualmente, dicho estudio señala que hace falta mayor difusión para el conocimiento del mencionado derecho (AMIPCI, 2016: 18, 22 y 30).

No obstante, existe preocupación de la población ante el mal uso de sus datos personales. La “Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales 2016”, que recaba información respecto al grado de conocimiento del derecho en cuestión, así como de los mecanismos para ejercerlo y garantizarlo, señala que en el país, 84% de la población de 18 años de edad y más que ha dado a conocer algún dato personal a alguna institución pública o empresa mostró preocupación por el uso indebido de su número telefónico personal. La encuesta reveló que 87.2% de la población mexicana de 18 años y más que ha dado a conocer algún dato personal a través de una red social o profesional se mostró preocupada por el uso indebido de su domicilio.

Otra problemática es que la población mexicana a la cual se debe garantizar este derecho es heterogénea. Si se toma en cuenta que en 2015 el Instituto Nacional de Estadística y Geografía (Inegi) contabilizó una población total para el Estado de México de 16 millones 187 mil 608 habitantes, se hace patente la necesidad de una planeación estratégica por regiones, así como por sectores de población que requieren atención focalizada con contenidos que cubran sus necesidades de lenguaje, cultura y conocimiento. Además, debe añadirse que la naturaleza de este derecho es fundamental, por lo que no existe una edad determinada para comenzar su difusión. En tal tenor, se requiere que la población de todas las edades acceda a este conocimiento, para que ejerza el derecho a la protección de los datos personales.

Aunado a ello, en el territorio mexicano existen grupos cuyas necesidades de difusión son diversas, como los hablantes de lenguas originarias y las personas que viven con alguna discapacidad visual, auditiva o motriz. El Inegi arrojó, en 2010, que la población de 5 años de edad y más hablante de alguna lengua indígena ascendía a 376 mil 830 habitantes en el territorio mexicano. Asimismo, se expone que la población con limitación en la actividad para ver ascendía a 162 mil 243 personas; en tanto que la población con limitación en la actividad para escuchar era de 57 mil 792 personas, en el mismo año.

El Infoem, como órgano garante, cuenta con la capacidad técnica para llevar a cabo acciones en materia de cultura y educación.

Actualmente funciona el *Programa de Cultura de la Transparencia y Protección de Datos Personales* mandatado en la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, y publicado en el Periódico Oficial Gaceta del Gobierno del 4 de noviembre de 2016. En este marco, el *Programa Monitor de la Transparencia*, en 2017 se realizaron 55 capacitaciones ciudadanas en 2017, con dos mil 460 beneficiados; en tanto que en lo que va del 2018, se han llevado a cabo 24 capacitaciones, en los cuales se ha beneficiado a mil 147 personas.

Sin embargo, también se detecta que son prácticamente inexistentes los estudios a nivel estatal o municipal sobre las necesidades de la población del Estado de México en materia de protección de los datos personales, lo cual coadyuvaría a un mejor diseño de los planes y programas.

De este análisis se desprende que la necesidad de una estrategia de educación cívica para promover este derecho no es un asunto menor, tanto en el contexto internacional, caracterizado por el continuo flujo de datos en un mundo globalizado, como en el ámbito nacional, pues la protección de los datos personales es un derecho asociado a una concepción esencial para el fortalecimiento de las sociedades democráticas.

El “Estudio para fortalecer la estrategia de educación cívica y cultura para el ejercicio del derecho a la protección de datos personales por parte de los titulares”, publicado por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (Inai) en 2016, reconoce la necesidad de contar con instrumentos que den pauta a la

implementación de acciones encaminadas a la prevención de la violación del derecho a la protección de los datos personales, a través de una estrategia de educación cívica.

De lo anteriormente expuesto, emergen, por lo menos, dos esferas de atención. La primera es una esfera obligatoria para quienes entregan sus datos personales a los responsables, al ser solicitados para realizar algún trámite o servicio. La segunda se refiere a una esfera voluntaria para quienes exponen su información en el entorno digital, al realizar publicaciones en plataformas como redes sociales.

En el Estado de México se busca difundir a través de la educación, el conocimiento en torno al derecho de la protección de los datos personales, así como promover su ejercicio entre la población; es decir, edificar una cultura de protección de los datos personales.

En primera instancia, se requiere la difusión del derecho: extender, propagar o divulgar conocimientos, noticias, actitudes y costumbres.

La difusión abarca dos grupos:

- a) El primero es la población en general, a este grupo habrá que concientizarlo de la importancia de este derecho, a la autodeterminación informativa y sobre los derechos de acceso, rectificación, cancelación y oposición al tratamiento de los datos personales (ARCO), así como la portabilidad.
- b) El segundo grupo son los responsables del tratamiento de datos personales, con el fin de actualizar los conocimientos obtenidos en las capacitaciones impartidas por el Infoem, con miras a que se conviertan en agentes transmisores del conocimiento y tengan las herramientas necesarias para una mejor aplicación de la normatividad.

El presente eje temático tiene como destinatario al primer grupo.

Análisis FODA

Eje temático 1: Educación y cultura de protección de los datos personales de los mexiquenses

Fortalezas	Debilidades
<ul style="list-style-type: none"> • El Infoem cuenta con capacidad humana para implementar un programa de cultura de la protección de datos personales entre los habitantes del Estado de México. • El Infoem, como especialista en el tema, posee experiencia en la materia. • Al ser órgano garante, cuenta con las herramientas técnicas necesarias para implementar acciones de educación, promoción y difusión de este derecho, a través de las diversas plataformas digitales. 	<ul style="list-style-type: none"> • Existe desconocimiento del derecho a la protección de los datos personales entre la población habitante del Estado de México. • Los responsables no cuentan con la capacitación necesaria para difundir el derecho entre los servidores públicos ni entre la población. • El presupuesto para costear campañas publicitarias en medios de comunicación es limitado, en comparación al número de población al que se pretende llegar. • Brecha digital que limita la posibilidad del uso de plataformas para ejercer el derecho.
Oportunidades	Amenazas
<ul style="list-style-type: none"> • Legislación robusta que permite llevar a cabo acciones dirigidas a la población mexiquense. • Posibilidad de implementar programas de difusión del derecho e impactar a un número de población considerable. • Es posible establecer coordinación con los responsables e instituciones privadas. • Buena relación con las instituciones educativas, tanto públicas como privadas, lo cual permite la implementación del programa. 	<ul style="list-style-type: none"> • La rotación de personal al interior de los responsables limita la posibilidad de dar continuación a proyectos relacionados con la difusión del derecho. • Existe confusión entre la ponderación de este derecho y el de acceso a la información pública.

Problemática

1. Desconocimiento de la población mexiquense sobre el derecho a la protección de los datos personales.
2. Desconocimiento de la población mexiquense sobre la existencia del Infoem, sus funciones y atribuciones; entre ellas, la garantía del derecho a la protección de datos personales.
3. Preocupación de la población ante el mal uso de sus datos personales.

4. Heterogeneidad de la población mexiquense a la cual se debe garantizar este derecho.
5. Inexistencia de estudios a nivel estatal o municipal sobre las necesidades de la población del Estado de México en materia de protección de los datos personales.

Líneas estratégicas

- 1.1. Difusión del derecho a la protección de los datos personales entre la población del Estado de México.
- 1.2. Difusión de las funciones del Infoem en materia de protección de los datos personales entre la población del Estado de México.
- 1.3. Promoción del ejercicio del derecho a la protección de los datos personales, la autodeterminación informativa, los derechos ARCO y la portabilidad, entre la población del Estado de México.

Líneas de acción

- 1.1.1. Sensibilizar a la población mexiquense sobre el tema de protección de los datos personales, a través de la difusión de mensajes en los diversos medios de comunicación (corto plazo).
- 1.1.2. Sociabilizar el tema de la protección de los datos personales entre la población mexiquense, a través de foros, conferencias y cursos, en coordinación con los diversos responsables (mediano plazo).
- 1.1.3. Buscar la inclusión de contenidos en la materia en los programas educativos de los distintos grados académicos, a fin de generar una cultura de protección de los datos personales entre el alumnado (largo plazo).
- 1.2.1. Fortalecer la imagen institucional del Infoem como organismo garante de la protección de los datos personales, mediante mensajes en los medios de comunicación (corto plazo).
- 1.2.2. Dar a conocer a la población mexiquense las actividades realizadas por el Infoem en materia de protección de los datos personales, en ferias, congresos y seminarios (corto plazo).
- 1.2.3. Impulsar la formación de usuarios en materia de protección de los datos personales, mediante cursos en línea sobre el ejercicio de este derecho y sus beneficios (mediano plazo).
- 1.3.1. Desarrollar una campaña de difusión sobre el derecho a la protección de los datos personales, la autodeterminación informativa, la portabilidad y los derechos ARCO (mediano plazo).
- 1.3.2. Promover actividades culturales que impulsen el ejercicio de los derechos ARCO y la portabilidad (mediano plazo).

Eje temático 2. Capacitación de los responsables

Diagnóstico

La implementación de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, publicada en mayo de 2017, señala que el Infoem tiene la atribución de capacitar y certificar en materia de protección de los datos personales en posesión de los sujetos obligados en el ámbito material y territorial de competencia que le corresponde.

Si bien el Infoem ha impartido sesiones de capacitación orientadas a los temas de acceso a la información pública y protección de los datos personales, toda vez que la normatividad de la materia así lo establece, la expedición de la ley trajo consigo importantes avances, como el derecho a la portabilidad de los datos personales y la implementación de un sistema de gestión de seguridad.

Cabe destacar que, según los resultados del estudio de opinión llevado a cabo a los sujetos obligados en 2016 por el Infoem, cuya muestra aleatoria representativa fue de 506 cuestionarios para 153 servidores públicos entrevistados, 68.5% consideró que sus objetivos de capacitación están encaminados al cumplimiento del ejercicio del derecho de acceso a la información pública y 41.2%, opinó que están enfocados a la protección de los datos personales.

Respecto de los temas de las sesiones de capacitación, los servidores públicos entrevistados las evaluaron con 8, 9 y 10, puesto que las consideran completas e impartidas oportunamente. Sin embargo, casi la mitad de los participantes señaló el reto es que se ofrezcan talleres prácticos sobre los temas.

Por otro lado, 85% de los participantes declaró que es necesaria una mayor sensibilización de los servidores públicos en general, pues un alto porcentaje de los participantes no convoca al resto de los funcionarios de su dependencia para las capacitaciones. Este estudio resaltó la importancia de compartir contenidos con los compañeros de trabajo y evaluar el nivel de conocimientos al término de cada capacitación.

Sobre la aceptación de los servidores públicos de ser evaluados con base en los conocimientos adquiridos en las capacitaciones, los resultados demuestran que 79.7% señalaron estar de acuerdo, mientras que 13.1% se negó. Entre los

argumentos vertidos destaca que es una forma de examinar sus conocimientos y competencias laborales; sin embargo, 13.75% indicó que las capacitaciones no son suficientes para ser evaluados.

Por otro lado, el Infoem ha iniciado un proceso de rediseño de sus procesos de capacitación a servidores públicos, que incluye, por un lado, la integración de un equipo de capacitadores formados de manera integral tanto en los temas sustantivos del Instituto como en el desarrollo de competencias didácticas; y por otro, el diseño de diferentes herramientas de capacitación que incluyen cursos presenciales, en línea, seminarios, talleres y diplomados.

Análisis FODA

Eje temático 2: Capacitación de los responsables

Fortalezas	Debilidades
<ul style="list-style-type: none"> • Institución oficial experta en el tema de protección de datos personales. • Normatividad jurídica en la materia. 	<ul style="list-style-type: none"> • Pocos capacitadores en el tema de protección de datos personales. • Contenidos temáticos repetitivos en las capacitaciones. • Falta de contenidos didácticos como guías, folletos, trípticos, etc.
Oportunidades	Amenazas
<ul style="list-style-type: none"> • Obligatoriedad del cumplimiento de las nuevas disposiciones en materia de protección de datos personales. • Especialización de contenidos dependiendo de cada sujeto obligado. • Realización cursos de sensibilización. 	<ul style="list-style-type: none"> • Periodo electoral • Falta de interés • Alta demanda de capacitación derivada de nuevas leyes • Rotación constante de servidores públicos en los cargos de protección de datos personales • Condiciones geográficas de algunos municipios

Problemática

1. Falta de conocimiento sobre el derecho a la protección de los datos personales por parte de los sujetos obligados.
2. Énfasis en la capacitación en materia de acceso a la información pública, más que en la protección de los datos personales.

Falta de material bibliográfico y didáctico sobre los contenidos en la materia, como guías, cuadernillos o manuales.

Líneas estratégicas

- 2.1 Realización de actividades informativas sobre la importancia de la protección de datos personales dirigida a los responsables.
- 2.2. Desarrollo de nuevas herramientas de capacitación, que enriquezcan el proceso de enseñanza-aprendizaje de los responsables.
- 2.3. Elaboración de materiales didácticos innovadores que fortalezcan la capacitación en materia de protección de datos personales.

Líneas de acción

- 2.1.1. Realizar jornadas de sensibilización con los titulares de los responsables, a fin de que conozcan los principales aspectos de la ley de la materia (corto plazo).
- 2.1.2 Llevar a cabo conferencias magistrales, foros y seminarios en diversas instituciones estatales (corto plazo).

2.2.1. Diseñar y realizar cursos especializados para los oficiales de Protección de Datos Personales (mediano plazo).

2.2.2. Realizar talleres basados en estudios de caso (mediano plazo).

2.3.1. Diseñar y promover contenidos impresos, a través de guías, folletos o trípticos para los responsables, sobre temas especializados en materia de protección de los datos personales (corto plazo).

2.3.2. Desarrollar cursos en línea con materiales visuales, auditivos y documentales (mediano plazo).

Eje temático 3. Certificación de los sujetos obligados

Diagnóstico

En el ámbito de la administración pública, la profesionalización de los servidores públicos ha transitado hacia lo que se ha denominado el desarrollo de competencias, que implica una combinación dinámica de conocimiento, comprensión, capacidades y habilidades.

La certificación de competencias laborales es el proceso mediante el cual se garantiza que el servidor público haga uso de sus capacidades, desarrolle y practique las habilidades adquiridas para el óptimo desempeño de sus funciones, según las siguientes etapas: capacitación, evaluación y emisión del certificado.

En el Estado de México, el artículo 14, fracción V, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios establece que el Infoem debe certificar a los sujetos obligados, organizaciones o asociaciones de la sociedad, así como a las personas en general que ofrezcan, en forma interdisciplinaria y profesional, la posibilidad de llevar a cabo cursos o talleres en materia de protección de los datos personales. Por otro lado, el artículo 92 de la citada ley determina, como uno de los requisitos para ser oficial de Protección de Datos Personales, contar con la certificación emitida por el Instituto.

El artículo 57 de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios señala que el titular de la Unidad de Transparencia debe contar con conocimientos o, tratándose de las entidades gubernamentales estatales y los municipios, la certificación en materia de acceso a la información pública, transparencia y protección de los datos personales que para tal efecto emita el Infoem.

La certificación se vuelve un reto impostergable para avanzar en la profesionalización de los servidores públicos en materia de protección de los datos personales. Un aspecto a favor de la certificación es el hecho de que la legislación ya la contempla como obligación para tres figuras: titulares de las Unidades de Transparencia, oficiales de Protección de Datos Personales e instancias que busquen impartir cursos o talleres sobre los temas mencionados.

La certificación debe efectuarse mediante un proceso de normalización (elaboración de un estándar de competencia laboral), capacitación en los criterios del estándar, evaluación y, finalmente, emisión del certificado por una instancia competente.

El Instituto se encuentra en el proceso de desarrollo de cuatro estándares de competencia laboral:

1. Estándar mexiquense de competencias en la garantía del derecho de acceso a la información pública.
2. Estándar mexiquense de competencias en la garantía del derecho de protección de los datos personales.
3. Estándar mexiquense de competencias en la impartición de cursos de capacitación en materia de acceso a la información pública.
4. Estándar mexiquense de competencias en la impartición de cursos de capacitación en materia de protección de los datos personales.

Aunque se cuenta con ordenamientos legales, existe un alto desconocimiento y baja especialización de los responsables de la protección de los datos personales. Tanto la capacitación como la certificación tienen el objetivo de proveer a los servidores públicos del conocimiento y las competencias para que desarrollen su función con la mayor eficiencia, coadyuvando de esta forma con la debida tutela del derecho.

El Estado de México se encuentra frente al reto de diseñar el proceso de certificación de acuerdo con las características de los sujetos obligados, para que se convierta en un procedimiento profesional, especializado y riguroso que sirva como modelo para el SNT.

Análisis FODA

Eje temático 3:
Certificación de sujetos obligados

Fortalezas	Debilidades
<ul style="list-style-type: none"> • Certificación obligatoria para el Oficial de Datos Personales • Certificación para las instancias que imparten cursos de capacitación en materia de datos personales. 	<ul style="list-style-type: none"> • Desconocimiento de los sujetos obligados acerca de la legislación en la materia. • Baja especialización de los servidores públicos responsables de datos personales. • Ausencia de una cultura de protección de datos personales y su tratamiento.
Oportunidades	Amenazas
<ul style="list-style-type: none"> • Diseño de un proceso de certificación acorde con las características del Estado de México y sus Municipios. • Diseño del primer estándar de competencia laboral en materia de datos personales a nivel nacional. 	<ul style="list-style-type: none"> • Riesgo de afectación del derecho de protección de datos personales de los ciudadanos, ante la falta de profesionalización de los responsables.

Problemática

1. Falta de conocimiento y especialización por parte de los responsables respecto de los datos personales.
2. Necesidad de profesionalización integral de los responsables.
3. Riesgo de afectación del derecho a la protección de los datos personales.
4. Falta de certificación de los oficiales de Protección de Datos Personales.

Líneas estratégicas

- 3.1. Diseño de un proceso metodológico integral de certificación para el Estado de México, dirigido a los oficiales de Protección de Datos Personales, así como a las personas y organizaciones que busquen impartir cursos en la materia.
- 3.2. Evaluación y actualización periódica del proceso de certificación.

Líneas de acción

- 3.1.1. Elaborar las normas, estándares o criterios generales de la competencia del oficial de Protección de Datos Personales, así como a las personas y organizaciones que busquen impartir cursos en la materia (corto plazo).
- 3.1.2. Diseñar y elaborar los contenidos de la capacitación de la norma o estándar (corto plazo).
- 3.1.3. Preparar los recursos humanos de capacitación y evaluación del proceso de certificación (mediano plazo).
- 3.1.4. Diseñar el plan de capacitación para la certificación (mediano plazo).
- 3.2.1. Revisar periódicamente la actualización de la norma o estándar (mediano plazo).
- 3.2.2. Evaluar el proceso de certificación de los responsables (mediano plazo).
- 3.2.3. Aplicar acciones de mejora al proceso de certificación, de acuerdo con la evaluación que se efectúe (mediano plazo).

Eje temático 4. Ejercicio de los derechos ARCO y la portabilidad

Diagnóstico

En el Estado de México, la protección de los datos personales se encuentra prevista en el artículo 5º de la Constitución Política del Estado Libre y Soberano de México y se rige por las disposiciones de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios (Ley de Protección de Datos). Ambas normas contemplan, entre otros aspectos, la creación del Infoem como un organismo autónomo garante, responsable de coordinar y evaluar las acciones relativas a la política pública transversal de protección de los datos personales en el ámbito estatal y municipal.

La mencionada Ley de Protección de Datos se constituye como un avance relevante en la materia, toda vez que subraya el enfoque de procesos a través de sistemas de datos personales y su registro; tipos y niveles de seguridad, y un marco base para la implementación de un sistema de gestión. Una de las figuras relevantes que incluye se refiere a la incorporación de planes de trabajo, análisis de riesgo, análisis de brechas, acciones preventivas, derecho a la portabilidad, registro de mejores prácticas, notificación de violaciones a la seguridad de los datos personales e imposición de medidas de apremio.

Además, este instrumento legal adiciona y adecua las figuras jurídicas que se estimaron necesarias para el correcto tratamiento de la información, como el Programa Estatal y Municipal de Protección de Datos Personales; la protección de los datos personales de menores y los datos personales de carácter sensible; la clasificación de los datos personales a través de acuerdos relativos a sus sistemas; los deberes y obligaciones a cargo de los responsables, su conceptualización e integración; la incorporación y actualización de diversas figuras jurídicas inmersas en el tratamiento de datos personales; la participación, mediante el Sarcoem, en la Plataforma Nacional de Transparencia; las obligaciones del oficial de protección de los datos personales y el responsable de seguridad cuando se esté frente al tratamiento relevante e intensivo de datos personales; la cláusula testamentaria para el ejercicio de los derechos ARCO, y la limitación del tratamiento.

En este sentido, el Infoem vigila la observancia de las disposiciones legales y normativas sobre protección de los datos personales en posesión de los sujetos obligados, promoviendo la adopción de las medidas de seguridad que garanticen la integridad, disponibilidad y confidencialidad de los datos personales, en congruencia con los principios, derechos, excepciones, obligaciones, sanciones y responsabilidades que rigen la materia, y contribuyendo con la implementación de procedimientos sencillos y expeditos para que toda persona pueda ejercer los derechos ARCO.

En materia de protección de los datos personales, es relevante destacar que, cuando los titulares desean conocer la información que obra en posesión de los sujetos obligados, tienen a su alcance el ejercicio de los derechos ARCO y la portabilidad, los cuales forman parte de las garantías primarias de ese derecho.

En este sentido, cada uno de los derechos ARCO tiene características específicas. El primero de ellos se encuentra al alcance toda persona para obtener información sobre sus datos. Por otro lado, el derecho de rectificación tiene como finalidad corregir datos inexactos. La cancelación es útil para solicitar el bloqueo de los datos personales cuando su tratamiento se efectúa en contravención con la legislación aplicable. Finalmente, la oposición consiste en solicitar el cese del tratamiento de los datos cuando se hayan recabado sin consentimiento o cuando existan razones legítimas y justificadas para ello.

El Sistema de Acceso, Rectificación, Cancelación y Oposición de Datos Personales del Estado de México (Sarcoem) es el medio electrónico establecido por el Infoem para registrar las solicitudes de derechos ARCO. Existe el registro de un total de 908 solicitudes en 2017. Además, hasta el primer bimestre de 2018, se han contabilizado 184 solicitudes, las cuales se presentan a continuación:

Sujeto obligado	2017	2018
Poder Ejecutivo	524	212
Poder Legislativo	4	2
Poder Judicial	13	9
Ayuntamientos	291	121
Órganos autónomos	60	36
Tribunales administrativos	0	0
Partidos políticos	9	13
Fideicomisos y fondos públicos	0	0
Sindicatos	5	4
Personas jurídicas colectivas	2	0
Total	908	397

Fuente: www.infoem.org.mx/est_/index.php

De acuerdo con las cifras de la tabla anterior, las solicitudes de derechos ARCO han aumentado, ya que el total de las solicitudes registradas en el primer cuatrimestre de 2018 representa 43.7% en relación con la totalidad de las solicitudes reportadas en 2017. A fin de identificar el incremento de las solicitudes de derechos ARCO, a continuación se presenta el número de solicitudes registradas en 2016 y 2017, identificando los sujetos obligados, el tipo de solicitud y la variación de un periodo a otro:

Sujeto obligado	Acceso			Rectificación			Cancelación			Oposición			Total		
	2016	2017	Variación %	2016	2017	Variación %	2016	2017	Variación %	2016	2017	Variación %	2016	2017	Variación %
Poder Ejecutivo	371	509		10	7		7	5		3	3		391	524	
Poder Legislativo	8	3		0	0		0	1		0	0		8	4	
Poder Judicial	9	11		0	0		0	1		1	1		10	13	
Ayuntamientos	275	285		2	1		9	3		3	2		289	291	
Organismos autónomos	70	51		0	2		1	4		2	3		73	60	
Partidos políticos	1	3		0	0		0	5		1	1		2	9	
Sindicatos	0	5		0	0		0	0		0	0		0	5	
Fideicomisos y fondos públicos	0	0		0	0		0	0		0	0		0	0	
Personas jurídicas colectivas	0	1		0	0		0	1		0	0		0	2	
Total	734	868	18	12	10	-17	17	20	-18	10	10	0	773	908	17%

Fuente: <http://www.infoem.org.mx/src/php/solicitudesTipoYear.php>

En consecuencia, se aprecia que el Poder Ejecutivo tiene registrado el mayor número de solicitudes de derechos ARCO y, en segundo lugar, los ayuntamientos; mientras que, los fideicomisos y fondos públicos no cuentan con registros:

Derechos	2016	2017	Total	% representativo
Acceso	734	868	1602	95.3
Rectificación	12	10	22	1.3
Cancelación	17	20	37	2.2
Oposición	10	10	20	1.2
Total	773	908	1681	100

En atención a la tabla anterior, se identifica que el derecho de acceso a los datos personales es el más ejercido entre los derechos ARCO, mientras que el derecho de oposición al tratamiento de los datos personales resulta el menos frecuente. A efecto de contrastar estas cifras, la siguiente tabla reúne la cantidad de recursos de revisión atendidos por los sujetos obligados en 2016 y 2017:

2016		2017	
Sujeto obligado	Total	Sujeto obligado	Total
Poder Ejecutivo			
Instituto de Seguridad Social del Estado de México y Municipios	265	Instituto de Seguridad Social del Estado de México y Municipios	402
Secretaría de Finanzas	15	Instituto de Salud del Estado de México	43
Instituto de Salud del Estado de México	15	Secretaría de Finanzas	10
Secretaría de Educación	10	Secretaría de Educación	10
Comisión Estatal de Seguridad Ciudadana	9	Servicios Educativos Integrados al Estado de México	5
Servicios Educativos Integrados al Estado de México	9	Comisión Estatal de Seguridad Ciudadana	5
Secretaría de la Contraloría	8	Secretaría de Salud	4
Secretaría de Movilidad	6	Secretaría de Movilidad	4
Instituto de la Función Registral del Estado de México	5	Instituto de la Función Registral del Estado de México	3
Gubernatura	4	Colegio de Bachilleres del Estado de México	3
Municipios			
Ayuntamiento de Teotihuacán	92	Ayuntamiento de Teotihuacán	119
Ayuntamiento de Zumpango	32	Ayuntamiento de Zumpango	43
Ayuntamiento de Tlalnepantla de Baz	15	Ayuntamiento de Ixtapaluca	32
Ayuntamiento de Toluca	13	Ayuntamiento de Ecatepec de Morelos	13

Ayuntamiento de Ecatepec de Morelos	12	Ayuntamiento de Nezahualcóyotl	10
Ayuntamiento de Papalotla	9	Ayuntamiento de Tlalnepantla de Baz	9
Ayuntamiento de Huixquilucan	8	Ayuntamiento de Toluca	8
Ayuntamiento de Metepec	8	Ayuntamiento de Papalotla	6
Ayuntamiento de Nezahualcóyotl	7	Ayuntamiento de Valle de Chalco Solidaridad	5
Ayuntamiento de Oztolotepec	6	Ayuntamiento de Chimalhuacán	4

Cabe señalar que la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios constituye un avance relevante en la materia en la entidad, ya que prevé acciones y figuras jurídicas que se consideran necesarias para su correcto tratamiento; entre ellas, el derecho a la portabilidad de los datos personales.

La portabilidad abre la posibilidad de que los titulares tengan mayores facultades respecto de sus datos personales, al trasladarlos, copiarlos o transmitirlos fácilmente vía electrónica en un formato estructurado y comúnmente utilizado. Los titulares tienen derecho a obtener de los sujetos obligados ante los cuales hayan entregado su información una copia de los datos objeto de tratamiento en el mismo formato que les permita seguir utilizándolos y, en su caso, entregarlos a otro responsable para su reutilización y aprovechamiento. Ello, según las condiciones tecnológicas específicas para su realización, de acuerdo con los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.

Actualmente, el Infoem está incorporando elementos y adecuando las características del Sarcoem para favorecer el pleno ejercicio de este derecho, considerando aspectos puntuales en materia de transmisiones, puesto que se debe informar al titular sobre los tipos de formato disponibles para realizarlas, lo cual involucra la adopción de protocolos, herramientas, aplicaciones o servicios que permitan el enlace eficiente al atender las medidas de seguridad administrativas, físicas y técnicas para efectuar dicha transmisión, que comprende la autenticación de usuarios, conexiones seguras o utilizar medios electrónicos de transmisión cifrados.

Ante tal escenario, resulta imprescindible dar a conocer a la población el ejercicio de tales derechos y promover el uso del Sarcoem como una herramienta tecnológica destinada a la gestión de las mencionadas solicitudes.

Análisis FODA

**Eje temático 4:
Ejercicio de los derechos ARCO y portabilidad**

Fortalezas	Debilidades
<ul style="list-style-type: none"> • El Infoem cuenta con una infraestructura informática robusta con capacidad para atender la demanda social, en materia de protección de datos. • El Instituto cuenta con personal altamente capacitado capaz de enfrentar los retos que se presenten en el ejercicio de los derechos ARCO. • Se ha dado en la entidad mexiquense un cumplimiento. 	<ul style="list-style-type: none"> • Al ser derechos de tercera generación, existe la posibilidad de que el marco normativo aplicable al procedimiento para el ejercicio de estos derechos se vea transgredido por una incorrecta interpretación. • Los procedimientos seguidos por los responsables carecen de metodología cuando se está frente al ejercicio de los derechos ARCO. • El desconocimiento de la sociedad de los procedimientos para el ejercicio de estos derechos.
Oportunidades	Amenazas
<ul style="list-style-type: none"> • Al ser la portabilidad un derecho novedoso en México, se cuenta con la oportunidad de crear bases sólidas para que la ciudadanía conozca y ejerza este derecho. • Las herramientas tecnológicas con las que cuenta el Instituto, permiten llevar un adecuado control y seguimiento de las solicitudes en materia de derechos ARCO. 	<ul style="list-style-type: none"> • El bajo nivel de especialización de los responsables en el tratamiento de datos personales. • La falta de atención en el fomento del ejercicio de los derechos ARCO, así como el derecho a la portabilidad.

Problemática

1. El ejercicio de los derechos ARCO es muy reducido en la población mexiquense.
2. La población no conoce los procedimientos para solicitar el ejercicio de los derechos ARCO.
3. La población desconoce el Sarcoem.
4. Los sujetos obligados no cuentan con una metodología para el ejercicio de los derechos ARCO.

El derecho a la portabilidad de los datos personales es reciente y exige condiciones tecnológicas específicas.

Líneas estratégicas

- 4.1. Sensibilización, promoción y difusión de los derechos ARCO y la portabilidad de los datos personales.
- 4.2. Vinculación del ejercicio de los derechos ARCO y la portabilidad con el enfoque de otros derechos.
- 4.3. Creación e implementación de las condiciones tecnológicas específicas para la realización del derecho a la portabilidad.

Líneas de acción

- 4.1.1. Fortalecer la promoción y difusión del ejercicio de los derechos ARCO y la portabilidad en las actividades emprendidas por el Infoem Establecer los temas de interés y población a la que se dirigirá el mensaje (corto plazo).
- 4.1.2. Crear y difundir material relacionado con el ejercicio de los derechos ARCO y la portabilidad (mediano plazo).
- 4.2.1. Visibilizar el ejercicio de los derechos ARCO y la portabilidad entre los distintos sectores de la población mexiquense, como medio para mejorar el acceso a la salud, educación, empleo, seguridad y justicia (mediano plazo).
- 4.2.2. Impulsar el desarrollo de asesorías en materia de protección de los datos personales (mediano plazo).
- 4.2.3. Impulsar la mejora continua del Centro de Atención Telefónica (CAT) del Infoem, para beneficio de los titulares en el ejercicio de los derechos ARCO y la portabilidad (mediano plazo).
- 4.3.1. Desarrollar un modelo que establezca los objetivos y la forma de ejecución del ejercicio del derecho a la portabilidad de los datos personales en el Infoem (corto plazo).
- 4.3.2. Promover la implementación de acciones por parte de los responsables acordes con el modelo de referencia (mediano plazo).
- 4.3.3. Desarrollar herramientas de seguimiento, medición y evaluación de los mecanismos de portabilidad (mediano plazo).

Eje temático 5. Implementación y mantenimiento de los sistemas de gestión de seguridad*Diagnóstico*

El tema de la protección de datos resulta vital importancia derivando del avance tecnológico y los riesgos en el manejo de la información, especialmente cuando se trata de datos personales y que además se encuentra en posesión de entes públicos, ya que la información se utiliza, almacena y transfiere para propósitos diversos que inciden en la vida privada de las personas.

La autodeterminación informativa adquiere matices interpretativos y fragmentarios que se traducen en la delimitación de acciones concretas a nivel institucional, a fin de identificar oportunidades de mejora continua, para establecer procesos y mecanismos para la operatividad de la Ley de Protección de Datos; cabe destacar, que actualmente nuestra normatividad contempla el derecho de portabilidad; por ende, para el Infoem preciso desarrollar un marco teórico y jurídico que permita a los sujetos obligados desarrollar acciones encaminadas a sentar el escenario idóneo para el pleno ejercicio de dicho derecho, considerando como parte fundamental las condiciones tecnológicas específicas para su realización y las particularidades y características propias de los sujetos obligados, dado que cada institución tiene una forma específica de resguardar la información ya sea de manera física o electrónica y con controles de seguridad que en estricto sentido deben obedecer a parámetros de gestión documental y cuestiones archivísticas relacionados con la implementación de cuadros generales de clasificación archivística y catálogos de disposición documental, de acuerdo a la normatividad aplicable en materia de archivos.

Así mismo, el propio marco normativo contempla el derecho de obtener del responsable la limitación del tratamiento de los datos personales cuando el titular impugne la exactitud de los datos, el tratamiento sea ilícito y el titular se oponga a la supresión de los datos y el responsable ya no necesite los datos personales para los fines del tratamiento. De igual manera, la seguridad de los datos personales en el sector público constituye una problemática, ya que hasta el día de hoy existe incertidumbre por parte de los responsables en la implementación de documentos normativos exigibles en la Ley de Protección de Datos, tal es el caso del documento de seguridad que consiste en el 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, dicho documento en términos de la Ley contiene el inventario de datos personales y de los sistemas de tratamiento, las funciones y obligaciones de las personas que traten datos personales, el análisis de riesgos y de brecha, el plan de trabajo y contingencia, los mecanismos de monitoreo y revisión de las medidas de seguridad y el programa general de capacitación.

En este sentido, la Ley de Protección de Datos Personales, establece las atribuciones conferidas al Infoem en materia de protección de datos personales, destacando las siguientes: orientación, asesoría y capacitación de sujetos obligados y particulares en la materia; diseño y aprobación de formatos de solicitudes de derechos ARCO; el registro de Sistemas de Datos Personales en posesión de sujetos obligados; promover y difundir el derecho a la protección de datos personales; elaborar y publicar estudios e investigaciones, así como, organizar seminarios, cursos, talleres y demás actividades para difundir y ampliar el conocimiento en la materia; formular observaciones y recomendaciones a los sujetos obligados que incumplan con las disposiciones previstas en materia de protección de datos personales; verificación del cumplimiento, a través de procedimientos de revisión que resulten compatibles; imposición de medidas de apremio e investigación de posibles violaciones a la seguridad de los datos personales.

Cabe subrayar que todas las acciones vinculadas con las medidas de seguridad para el tratamiento de los datos personales deben estar documentadas y contenidas en el sistema de gestión, con el propósito de preservar la confidencialidad, integridad y disponibilidad de los datos y evitar una vulneración a la seguridad.

El sistema de gestión implica la implementación de medidas físicas, técnicas y administrativas que deben incluirse en el documento de seguridad, el cual resulta de observancia obligatoria para los sujetos obligados. Asimismo, la ley de la materia dispone que, en caso de que ocurra una violación a la protección de los datos personales, los responsables deben tomar las acciones definidas en su plan de contingencia y, posteriormente, analizar las causas que originaron esta situación, con el fin de establecer en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas y el tratamiento de los datos personales, a efecto de que la violación no se repita.

En este orden de ideas, la falta de implementación del sistema de gestión ocasiona la vulnerabilidad de los responsables para que se susciten violaciones a la protección de los datos personales bajo su resguardo, destacando el incumplimiento del deber de confidencialidad, lo que se traduce en la ineficiencia de las medidas físicas, técnicas y administrativas, así como la falta de implementación de los documentos normativos que guardan relación con el sistema en su conjunto.

En tal virtud, el Infoem, en ejercicio de sus atribuciones de vigilancia y verificación del cumplimiento de las disposiciones de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, desarrolla investigaciones previas, en una etapa disuasiva, en contra de diversos sujetos obligados por posibles violaciones a la seguridad de los datos personales, para lo cual, en el registro correspondiente, se cuenta con un total de 145 expedientes de investigación en 2017.

De este modo, los ayuntamientos registran el mayor número de posibles violaciones en materia de protección de los datos personales.

En consecuencia, el registro de procedimientos de investigación y verificación a cargo de la Dirección de Protección de Datos Personales del Infoem versa sobre posibles violaciones a la seguridad de los datos personales, debido a la falta de implementación de un sistema de gestión. De igual manera, es importante citar que el artículo 165 de la Ley de Protección de Datos Personales en Posesión de Sujetos

Obligados del Estado de México y Municipios fija las causales de responsabilidad administrativa por incumplimiento de sus disposiciones, entre las que sobresalen las violaciones a la salvaguarda de los datos personales generadas por la falta de implementación de medidas de seguridad físicas, técnicas y administrativas; es decir, los responsables deben documentarlas en un sistema de gestión, a fin de garantizar el tratamiento adecuado de los datos personales, considerando el tipo y nivel de seguridad aplicable.

Por ende, los responsables deben cumplir con los principios, deberes y obligaciones en materia de protección de los datos personales, con la adopción de las medidas y mecanismos para garantizar su integridad, disponibilidad y confidencialidad y para promover fomentar y difundir la cultura de protección de los datos personales. En el mismo sentido, cabe considerar la imposición de medidas de apremio en caso de incumplimiento de las resoluciones emitidas por el Infoem, que consisten en amonestación pública y multas según la gravedad del hecho, la condición económica del infractor y la reincidencia.

Análisis FODA

Eje temático 5:
Implementación y mantenimiento de sistemas de gestión de seguridad

Fortalezas	Debilidades
<ul style="list-style-type: none"> • Considerado por la Ley como un instrumento necesario para la implementación del Programa Estatal y Municipal de Protección de Datos Personales en el Estado de México. • El establecimiento de medidas de seguridad esta previsto en la legislación en la materia, con la finalidad de garantizar a los titulares de datos personales que las bases de datos en donde se encuentre contenida su información estará segura. 	<ul style="list-style-type: none"> • Falta de conocimiento de las medidas de seguridad desarrolladas por los responsables. • El personal de los responsables no están debidamente capacitados en materia de protección de datos personales. • Falta de interés por parte de los responsables para dar cumplimiento a las obligaciones que en materia de protección de datos personales que establece la Ley.
Oportunidades	Amenazas
<ul style="list-style-type: none"> • Desarrollo de plataformas y/o sistemas que cumplen con los niveles de seguridad necesarios y suficientes que garanticen el debido tratamiento y resguardo de los datos personales en posesión de los responsables. • Establecimiento de seguridad de carácter administrativo, físico y técnico para la protección de los datos, que permitan protegerlos (confidencialidad, integridad y disponibilidad) 	<ul style="list-style-type: none"> • Que los Responsables no cuenten con los recursos financieros, técnicos y administrativos para implementar un sistema de medidas de seguridad. • Incompatibilidad de las medidas de seguridad desarrolladas por los responsables. • Corrupción en el manejo y tratamiento de los datos personales.

Problemática

1. Desconocimiento de la normatividad aplicable en la implementación del sistema de gestión de seguridad por parte de los responsables.
2. Insuficiencia general de las medidas de seguridad implementadas por los responsables, pues no cumplen con un nivel aceptable para proteger los datos personales.
3. Falta de elaboración e implementación de los documentos de seguridad por parte de los responsables.
4. Incremento y reincidencia en posibles vulneraciones a la seguridad de los datos personales por parte de los responsables.

Líneas estratégicas

- 5.1. Desarrollo de herramientas y metodologías para la implementación de los sistemas de gestión de seguridad.
- 5.2. Desarrollo de diagnósticos, herramientas y metodologías para la implementación y mejora continua de los sistemas de gestión de seguridad.
- 5.3. Promoción de acciones preventivas por parte de los responsables para la implementación y mejora continua de los sistemas de gestión de seguridad.
- 5.4. Promoción de acciones correctivas por parte de los responsables para la implementación y mejora continua de los sistemas de gestión de seguridad.

Líneas de acción

- 5.1.1. Construir metodologías para el mapeo de los flujos y tratamientos de los datos personales para su uso al interior de los responsables (corto plazo).
- 5.1.2. Elaborar una herramienta de autodiagnóstico que permita a los responsables identificar sus necesidades de seguridad en el tratamiento de los datos personales (corto plazo).
- 5.1.3. Trazar las acciones generales para la atención de las necesidades identificadas a partir del análisis de las respuestas de la herramienta de autodiagnóstico realizada por los responsables (corto plazo).
- 5.2.1. Construir metodologías para la identificación de las violaciones a la seguridad de los datos personales (mediano plazo).
- 5.2.2. Dar seguimiento a la atención de las necesidades y vulnerabilidades detectadas en los sistemas de gestión de seguridad operados por los responsables (mediano plazo).
- 5.3.1. Facilitar a los responsables las metodologías para la elaboración de análisis de riesgos y análisis de brecha, para que cuenten con un nivel aceptable de protección de los datos personales (mediano plazo).

5.3.2. Impulsar la elaboración e implementación del plan de contingencia a cargo de los responsables (mediano plazo).

5.4.1. Dar seguimiento a la implementación de las acciones recomendadas a los responsables para la instalación del sistema de gestión de seguridad (largo plazo).

5.4.2. Contribuir con apoyo técnico para la implementación de acciones en caso de una vulneración a la seguridad de los datos personales (largo plazo).

5.4.3. Facilitar a los responsables las metodologías para la elaboración de su plan de trabajo, con el fin de evitar la repetición de las violaciones a la seguridad de los datos personales (largo plazo).

Eje temático 6. Estándares en buenas prácticas en materia de protección de los datos personales

Diagnóstico

Actualmente, el creciente uso de las tecnologías favorece el manejo e intercambio de información, lo que promueve el flujo indiscriminado de los datos personales, por lo que es necesario impulsar la cultura de protección de los mismos entre la sociedad mexicana.

Por otro lado, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios prevé que los responsables puedan adoptar o desarrollar, individualmente o de acuerdo con otros responsables, encargados u organizaciones, esquemas de mejores prácticas. Asimismo, se refiere a la validación y el reconocimiento de mejores prácticas por parte del Infoem.

Para comprender el concepto de mejores prácticas, Ximena Tocornal y Paola Tapia (2011) señalan que una buena práctica consiste en “un calificativo al cual se llega luego de un juicio de valor sobre méritos o aportes que nos deja una determinada iniciativa. Su identificación considera un proceso de evaluación, que, como todo acto intencionado, contempla objetivos respecto de lo que se busca alcanzar”. Por ende, se identifican oportunidades de mejora.

En el ámbito internacional, las prácticas relevantes aluden al uso de las tecnologías de la información y la comunicación (TIC) como fuente principal de difusión, capacitación, promoción y sensibilización en materia de protección de los datos personales. Así, cabe enunciar el caso del trabajo realizado por la Unión Europea denominado “Tú decides en internet”, el cual tiene por objetivo general sensibilizar y subrayar la importancia del tema y cómo éste repercute en la vida de las personas, además de priorizar y puntualizar el trabajo de las instituciones obligadas a proteger y salvaguardar la información.

La Agencia de Acceso a la Información Pública en Argentina cuenta con un Campus Virtual de Protección de Datos Personales que capacita y difunde diversas temáticas en la materia. Por otra parte, existe el Programa “Con Vos en la Web”, cuya misión radica en ayudar a generar un cambio de conducta respecto de las TIC, señalando sus ventajas y sus riesgos.

La Unidad Reguladora de Control de Datos Personales en Uruguay desarrolla un programa alusivo a la Ley de Protección de Datos Personales, el cual incluye un conjunto de guías prácticas de protección de los datos personales, al que se suma un curso en línea cuyas características se centran en la inclusión, la integralidad y un código de ética.

En el contexto nacional, el Inai cuenta con el proyecto “Corpus Iuris” en materia de protección de los datos personales, que surge en el seno de la Red Iberoamericana de Protección de Datos, cuyo objetivo es contar con una herramienta que acceda a un conjunto de documentos, normas y precedentes que muestren el desarrollo de la protección de los datos personales en el entorno internacional y nacional. También cuenta con un generador de avisos de privacidad y una guía para su elaboración, además de un vulnerómetro, que mide los riesgos de compartir información personal.

Por otro lado, destaca el trabajo de los organismos garantes de Veracruz, Jalisco, Nuevo León, Ciudad de México y Aguascalientes. El primero presenta un concurso denominado “Datos Personales: Yo me cuido, yo respeto, yo no publico”, cuya finalidad es sensibilizar a jóvenes y niños en la materia. Por otra parte, se presenta un “Plan de contingencia”, que se implementa ante la existencia de una interrupción no planificada de recursos informáticos.

En Nuevo León, cabe subrayar el trabajo realizado a través del diseño y elaboración de un portal interactivo para niños y jóvenes, se promueve la protección de los datos personales y se pone a disposición una guía de acción. En la Ciudad de México, existen programas integrales e incluyentes centrados en la participación ciudadana y en la vinculación institucional y gubernamental para el cumplimiento de la Ley de Protección de Datos Personales, enfatizando lo concerniente a los riesgos y ventajas de las TIC, para lo cual destaca la Feria de la Transparencia y Protección de Datos Personales, el Programa “Juventud en línea” y el Programa “Correspondes”. De igual manera, sobresale la labor de Aguascalientes, que ha impulsado una Agenda Ciudadana en la que se vigila y promueve el cumplimiento de los derechos ARCO.

El Infoem se ha encargado de construir una red institucional para vincularse con instancias internacionales y nacionales, a fin de compartir sus experiencias y actuar coordinadamente. En este sentido, ha celebrado diversos convenios internacionales en la materia, entre los que sobresale su aceptación como miembro de la Red Iberoamericana de Protección

de Datos con el carácter de observador el 8 de junio de 2016 en Santa Marta, Colombia, en el marco del XIV Encuentro Iberoamericano de Protección de Datos. En 2017, se dio la acreditación del Infoem como miembro de la Red Iberoamericana de Protección de Datos, en el marco del XV Encuentro Iberoamericano de Protección de Datos en Santiago de Chile, Chile.

Adicionalmente, fue aceptado como miembro de la Conferencia el 26 de octubre de 2015, en la 37ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada en Ámsterdam, Holanda, y el 20 de octubre de 2016, el Infoem y la Autoridad Regulatoria de Gibraltar firmaron un memorándum de entendimiento, a fin de establecer mecanismos de coordinación y cooperación para avanzar en una tutela efectiva de los derechos de acceso a la información pública y protección de los datos personales en ambas regiones. Por otro lado, desde 2016, este órgano garante conmemora el Día de Internet Seguro, el cual se celebra en febrero. Desde 2017, encabeza el Comité del Día del Internet Seguro en México.

En 2016, se llevó a cabo la firma del convenio de colaboración entre el Infoem y la Secretaría de Educación del Estado de México. Cabe destacar que este instrumento tiene el fin de promover la cultura de la transparencia, el acceso a la información pública, la protección de los datos personales y la rendición de cuentas entre el personal docente y el alumnado mexiquense en general, marco en el cual se inserta el Programa "Monitor de la Transparencia y Protector de mis Datos Personales".

Asimismo, sobresalen los avances del Infoem en la implementación de mejores prácticas en el contexto local, con el Sarcoem, único en su tipo y cuya finalidad es que la población ejerza los derechos ARCO. Destacan también algunas actividades de buenas prácticas, como la realización del Concurso de Dibujo Infantil "¿Cómo Protejo Mis Datos Personales?", del Concurso Estatal de Ensayo "El Acceso a la Información Pública y la Protección de los Datos Personales: Derechos para Todos" y del Concurso Estatal de Spot de Radio "El Acceso a la Información Pública y la Protección de los Datos Personales: Derechos para Todos".

De este modo, el Infoem tiene el gran reto de implementar mecanismos de mejores prácticas que promuevan que los responsables cumplan con las disposiciones previstas en la normatividad en materia de protección de los datos personales, el ejercicio de los derechos ARCO y la transferencia de los datos personales.

Análisis FODA

Eje temático 6:

Estándares en buenas prácticas en materia de protección de datos

Fortalezas	Debilidades
<ul style="list-style-type: none"> • Legislación a la vanguardia en estándares internacionales. • Sistema electrónico propio para el ejercicio de los derechos ARCO. • Órganos de control en materia de protección de datos. • Formar parte de instituciones internacionales en la materia. 	<ul style="list-style-type: none"> • Carencia de programas de buenas prácticas para la ciudadanía. • Necesidad de establecer mecanismos de buenas prácticas con los sujetos obligados. • Ejercicio limitado de los derechos ARCO en el <u>Sarcoem</u>. • Desconocimiento de la normatividad en materia de protección de datos personales.
Oportunidades	Amenazas
<ul style="list-style-type: none"> • Implementación de estándares internacionales de buenas prácticas en el contexto local. • Promoción de los derechos ARCO, a través de buenas prácticas. • Establecer convenios de colaboración interinstitucional con los responsables y con las instituciones educativas. 	<ul style="list-style-type: none"> • Tratamiento inadecuado de los datos personales por parte de los responsables. • Rotación constante de los titulares de los responsables, sobre todo en los municipios. • Transferencia inadecuada de datos personales. • Vulneración en la seguridad de los datos personales.

Problemática

1. Ausencia de incentivos que permitan a los responsables adoptar mejores prácticas en la protección de los datos personales.
2. Falta de mecanismos que permitan el cumplimiento adecuado de la normatividad de la materia.
3. Carencia de armonización en el tratamiento de los datos personales en sectores específicos.
4. Falta de un repositorio de información sobre estándares de protección de los datos personales en el ámbito nacional e internacional.
5. Necesidad de establecer mecanismos proactivos en el cumplimiento de los derechos ARCO.

Líneas estratégicas

- 6.1. Promoción de los estándares nacionales e internacionales de seguridad y mejores prácticas en materia de protección de los datos personales.
- 6.2. Coordinación con los responsables para que cumplan con las disposiciones previstas en la normatividad aplicable en la materia.
- 6.3. Impulso a los responsables en el uso de mejores prácticas desde su campo de trabajo.

Líneas de acción

- 6.1.1. Realizar un repositorio electrónico de información sobre mejores prácticas nacionales e internacionales como medio de consulta para los responsables (mediano plazo).
- 6.1.2. Crear documentos impresos y electrónicos con los estándares de mejores prácticas nacionales e internacionales, para difundirlos a través de las redes sociales, el sitio electrónico institucional y las sesiones de capacitación (mediano plazo).
- 6.2.1. Difundir los beneficios de la adopción de mejores prácticas en materia de protección de los datos personales en las capacitaciones (mediano plazo).
- 6.2.2. Realizar talleres con los responsables, con el fin de promover la adopción de esquemas de mejores prácticas (mediano plazo).
- 6.3.1. Promover certámenes de mejores prácticas con los responsables, a través de estímulos económicos o en especie (mediano plazo).
- 6.3.2. Identificar y publicar los resultados de experiencias más relevantes sobre los esquemas de mejores prácticas (mediano plazo).

Eje temático 7. Gestión de recursos*Diagnóstico*

La Constitución Política del Estado Libre y Soberano de México y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios contemplan, entre otros aspectos, la creación del Infoem como un organismo autónomo garante, responsable de coordinar y evaluar las acciones relativas a la política pública transversal de protección de los datos personales en el ámbito estatal y municipal.

La mencionada Ley de Protección de Datos se constituye como un avance relevante en la materia, toda vez que subraya el enfoque de procesos a través de sistemas de datos personales y su registro; tipos y niveles de seguridad, y un marco base para la implementación de un sistema de gestión. Una de las figuras relevantes que incluye se refiere a la incorporación de planes de trabajo, análisis de riesgo, análisis de brechas, acciones preventivas, derecho a la portabilidad, registro de mejores prácticas, notificación de violaciones a la seguridad de los datos personales e imposición de medidas de apremio.

Además, este instrumento legal adiciona y adecua las figuras jurídicas que se estimaron necesarias para el correcto tratamiento de la información, como la protección de los datos personales de menores y los datos personales de carácter sensible; la clasificación de los datos personales a través de acuerdos relativos a sus sistemas; los deberes y obligaciones a cargo de los responsables, su conceptualización e integración; la incorporación y actualización de diversas figuras jurídicas inmersas en el tratamiento de datos personales; las obligaciones del oficial de protección de los datos personales y el responsable de seguridad cuando se esté frente al tratamiento relevante e intensivo de datos personales; la cláusula testamentaria para el ejercicio de los derechos ARCO, y la limitación del tratamiento.

Por ende, las figuras jurídicas incorporadas a la referida ley surgen de la necesidad de generar un panorama más amplio en la materia, por lo que resulta una mayor carga de trabajo para los responsables del tratamiento de los datos personales.

El fortalecimiento presupuestal resulta primordial para la implementación de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, toda vez que se requieren recursos humanos y

materiales que permitan sentar las bases y condiciones para el desarrollo de las actividades de los sujetos obligados en el ámbito de sus atribuciones, destacando la vinculación entre la protección de los datos personales con la transparencia, el acceso a la información pública y la rendición de cuentas.

El Plan de Desarrollo del Estado de México 2017-2023 establece las bases de progreso económico de la entidad, con el fin de crear las condiciones para que la sociedad mexiquense cuente con mayor seguridad, más oportunidades de desarrollo y de empleo, reducción de la desigualdad, garantías de los derechos sociales y equidad de género, para tener una entidad más moderna, justa y con sentido social.

La primera de las cinco metas nacionales del Plan Nacional de Desarrollo 2013-2018, México en Paz, contempla el respeto a los derechos humanos, la erradicación de la violencia de género, el combate a la corrupción y el fomento a una mayor rendición de cuentas. Entre sus estrategias y líneas de acción transversales, el inciso ii) Gobierno cercano y moderno considera que deben garantizarse el acceso a la información pública y la protección de los datos personales, fomentando la rendición de cuentas.

Por su parte el Plan Estatal de Desarrollo 2017-2023 en su segundo eje, Gobierno capaz y responsable, considera los medios para impulsar el fortalecimiento institucional con transparencia, responsabilidad en el uso de los recursos públicos y vocación de servicio en favor de la ciudadanía. A su vez, el objetivo 5.5, promover instituciones de gobierno transparentes y que rindan cuentas, cuenta con siete estrategias relacionadas con la transparencia, el acceso a la información pública, el gobierno abierto y los archivos, como se enlista enseguida:

5.5.1. Impulsar la transparencia proactiva, la rendición de cuentas y el gobierno abierto.

5.5.2. Fortalecer el programa de servicio público sustentado en principios y valores éticos de los servidores públicos. Entre las líneas de acción de esta estrategia sobresale “fortalecer al instituto estatal de acceso a la información”.

5.5.3. Coordinar acciones de transparencia en la atención de observaciones y recomendaciones emitidas por entes externos de fiscalización.

5.5.4. Impulsar la Ley de Archivos de los Poderes Estatales. Entre las líneas de acción de esta estrategia destaca “crear proyectos en todas las dependencias del gobierno estatal para la conformación de sus archivos”.

5.5.5. Garantizar que las dependencias del gobierno estatal cumplan con la normatividad de transparentar las compras y contratos.

5.5.6. Apoyar a los ayuntamientos en el cumplimiento de la normatividad en materia de transparencia y acceso a la información pública. Entre las líneas de acción de esta estrategia destaca “capacitar a los funcionarios municipales en el manejo de los sistemas de información y transparencia”.

5.5.7. Fomentar la cultura de la denuncia, a través del desarrollo de medios electrónicos y móviles.

Como se desprende de estos ejes, metas, estrategias y líneas de acción, la transparencia, el acceso a la información pública y la protección de datos personales forman parte de la agenda pública federal y estatal. Así, al fortalecer al Infoem con la construcción del edificio sede, se consolidan su operatividad, eficacia y eficiencia, en cumplimiento de las obligaciones legales correspondientes. En idéntico sentido, este proyecto se alinea con los objetivos para el desarrollo sostenible de la Agenda 2030, de la cual forma parte México. Específicamente, se relaciona con el objetivo 16, promover sociedades pacíficas e inclusivas para el desarrollo sostenible, facilitar el acceso a la justicia para todos y construir a todos los niveles instituciones eficaces e inclusivas que rindan cuentas, de acuerdo con las siguientes metas:

16.5. Reducir considerablemente la corrupción y el soborno en todas sus formas.

16.6. Crear, a todos los niveles, instituciones eficaces y transparentes que rindan cuentas.

16.10. Garantizar el acceso público a la información y proteger las libertades fundamentales, de conformidad con las leyes nacionales y los acuerdos internacionales.

Las acciones ejecutadas por el Infoem contribuyen significativamente con el cumplimiento de las políticas públicas contenidas en el Plan Nacional de Desarrollo 2013-2018 y el Plan Estatal de Desarrollo 2017-2023. El Presupuesto de Egresos del Estado de México del Ejercicio Fiscal 2018, considera en el programa presupuestal denominado “Transparencia” una asignación de 190,325,506 pesos.

Análisis FODA

**Eje temático 7:
Gestión de recursos**

Fortalezas	Debilidades
<ul style="list-style-type: none"> • El reconocimiento internacional del derecho a la Protección de Datos Personales. • El derecho de protección de datos personales forma parte de la política de las estrategias y líneas de acción planteadas en el Plan Nacional de Desarrollo 2012-2018. • El carácter autónomo del Infoem le permite contar con autonomía de gestión y presupuestal. 	<ul style="list-style-type: none"> • La imposibilidad de una ampliación al presupuesto asignado al Instituto. • Insuficiencia de personal al interior del Infoem para atender en el menor tiempo posible las actividades de verificación, capacitación y procedimiento de impugnación. • Insuficiencia de vehículos de traslado aunado a la lejanía en que se ubican algunos sujetos obligados.
Oportunidades	Amenazas
<ul style="list-style-type: none"> • La posibilidad de convenir con los sujetos obligados el apoyo de instrumentación del Programa. • El conocimiento que los mexiquenses tienen con relación a sus derechos de protección de datos personales. 	<ul style="list-style-type: none"> • No contar con la suficiencia presupuestal para implementar el Programa. • Falta de recursos humanos, materiales y presupuestales de algunos sujetos obligados. • El desinterés que pudieran manifestarse los titulares de los sujetos obligados en relación con el tema. • El cambio de personal ya capacitado al interior de los sujetos obligados.

Problemática

1. No se identifica que los sujetos obligados destinen en su presupuesto de egresos recursos en materia de protección de los datos personales.
2. Insuficiencia para la operación de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios.

Líneas estratégicas

7.1. Desarrollo de herramientas y metodologías para crear un fondo o instrumentos de financiamiento para el apoyo a las acciones de implementación de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios.

Líneas de acción

- 7.1.1. Gestionar las acciones legislativas que permitan crear un fondo o instrumentos de financiamiento para el apoyo a las acciones de implementación de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios. (mediano plazo)
- 7.1.2. Desarrollar herramientas y metodologías para identificar las necesidades prioritarias que deben cubrirse para hacer equitativa la atención y garantía del derecho a la protección de los datos personales en el Estado de México. (mediano plazo)
- 7.1.3. Diseñar propuesta para la creación del instrumento de financiamiento de recursos estatales o federales que contribuya a la implementación de la Ley de Protección de Datos en los Sujetos Obligados del Estado de México. (mediano plazo)

Eje temático 8. Monitoreo, seguimiento y verificación de metas

Diagnóstico

El Programa Estatal y Municipal de Protección de Datos Personales es un nuevo instrumento de política pública en la garantía de este derecho humano. Si bien el Infoem ha diseñado e instrumentado acciones para difundir y salvaguardar este derecho, el programa que hoy se presenta, constituye un importante paso en la consolidación de éste.

El monitoreo y seguimiento de un programa es un proceso que comprende la recolección y análisis de datos para comprobar que durante su ejecución, se cumplen las líneas estratégicas y de acción.

La evaluación, por su lado, es un proceso mediante el cual se determina la pertinencia y el logro de sus objetivos y metas, así como la eficiencia, eficacia, calidad, resultados, impacto y sostenibilidad; es decir, si el programa en curso responde a atender las necesidades planteadas en el diagnóstico.

En el ámbito de las políticas públicas, el desempeño se define como la “medida en que una intervención para el desarrollo o una entidad que se ocupa de fomentar el desarrollo actúa conforme a criterios, normas y directrices específicos y obtiene resultados de conformidad con metas o planes establecidos” (OECD, 2002: 29).

Los indicadores para medir el desempeño, deben dar cuenta de dos aspectos importantes de las intervenciones para el desarrollo: 1, los resultados establecidos en la planificación (productos, efectos, impactos) y 2, los criterios, normas, directrices que guían la intervención del Instituto.

La elaboración de los indicadores es un paso crucial en el desarrollo de un sistema de seguimiento, ya que los indicadores son expresiones de las variables cuantitativas y cualitativas mediante las cuales pueden medirse los logros alcanzados, observar los cambios vinculados con una intervención o analizar los resultados del programa.

Las facultades que posibilitan al Infoem efectuar el monitoreo, seguimiento y verificación de metas se sustentan en los artículos 13 y 14 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de México y Municipios, que señalan el diseño, ejecución y evaluación de la política pública, al establecer que este órgano garante debe facilitar los mecanismos destinados a medir, reportar y verificar las metas establecidas.

El objetivo de estas acciones consiste en optimizar las actividades, operatividad y ejecución de los objetivos del programa, así como evaluar la aplicación y correcta implementación de la ley.

El Infoem cuenta con la Unidad de Información, Planeación, Programación y Evaluación (UIPPE), que, entre otras funciones, se encarga de evaluar el cumplimiento de indicadores y metas de los programas institucionales del Infoem.

Análisis FODA

Eje temático 8: Monitoreo, seguimiento y verificación de metas

Fortalezas	Debilidades
<ul style="list-style-type: none"> • El Sarcoem coadyuva en la protección de datos personales, a través de la atención de las solicitudes de derechos ARCO, lo que permite el monitoreo, seguimiento y verificación de metas. • El Instituto cuenta con una Unidad de Información, Planeación, Programación y Evaluación (UIPPE), que se encarga de evaluar el cumplimiento de objetivos y metas institucionales. • Se cuenta con las posibilidades materiales para realizar las actividades de seguimiento del Programa Estatal y Municipal de Protección de Datos Personales. 	<ul style="list-style-type: none"> • El Infoem no cuenta con los recursos humanos y financieros necesarios para efectuar el monitoreo simultáneo en todo el Estado de México. • Desconocimiento que se traduce en incumplimiento de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, por parte de los responsables. • Gran parte de los responsables desconocen las funciones específicas de los sistemas informáticos que ofrece el Instituto. • Falta de tiempo para realizar el seguimiento, monitoreo y verificación de metas.
Oportunidades	Amenazas
<ul style="list-style-type: none"> • A través del Sarcoem, el Infoem puede dar seguimiento virtual a las solicitudes de derechos ARCO, así como las respuestas y resoluciones emitidas. • Uso de estadísticas generadas por el Sarcoem como insumo para la mejora continua del Programa Estatal y Municipal de Protección de Datos Personales. 	<ul style="list-style-type: none"> • Los sujetos obligados pueden tener poca disposición para el monitoreo, seguimiento y verificación de las metas. • Falta de personal que realice las actividades de verificación.

Problemática

La verificación, seguimiento y evaluación que se realizaba, era sobre acciones aisladas. Con el diseño del PEMPDF, como instrumento integral es posible elaborar un sistema de seguimiento y evaluación más completo.

Líneas estratégicas

- 8.1. Diseño del modelo de monitoreo, seguimiento y evaluación del Programa Estatal y Municipal de Protección de Datos Personales del Estado de México y Municipios.
- 8.2. Aplicación de medidas correctivas, de acuerdo con la evaluación de indicadores.

Líneas de acción

- 8.1.1. Definir metas e indicadores para cada línea de acción (corto plazo).
- 8.1.2. Determinar la periodicidad de la medición (corto plazo).
- 8.1.3. Definir la instancia o unidad que efectuará la evaluación (corto plazo).
- 8.1.4. Generar y utilizar estadísticas del Sarcoem para el proceso de evaluación (corto plazo).
- 8.2.1. Identificar las metas que presenten incumplimiento (mediano plazo).
- 8.2.2. Proponer acciones correctivas para las metas que presenten incumplimiento (mediano plazo).
- 8.2.3. Reformular las líneas de acción que lo ameriten (mediano plazo).

Glosario

1. **ACCIONES CORRECTIVAS:** cambios en los procesos, procedimientos o sistemas para la mejora de la calidad con el fin de evitar su repetición.
2. **ANÁLISIS DE BRECHA:** proceso que consiste en la identificación del patrón de control y de listas de seguridad correspondientes al nivel de riesgo.
3. **ANÁLISIS DE RIESGOS:** es el estudio de las causas de las posibles amenazas y probables eventos no deseados de los daños y consecuencias que éstas puedan producir.
4. **ÁREAS 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.
AVISOS DE PRIVACIDAD: 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.
5. **CAPACITACIÓN:** proceso educativo a corto plazo que utiliza un procedimiento planeado, sistemático y organizado a través del cual el personal administrativo designado por el Sujeto Obligado, adquirirá los conocimientos y las habilidades técnicas necesarias para acrecentar su eficacia en la protección de datos personales.
6. **CERTIFICACIÓN:** es la garantía que se entrega por una entidad referente en una materia y que se encarga además de velar el cumplimiento de determinadas condiciones, incluso las estudia y si las confirma positivamente dándole ese certificado.
7. **CONSENTIMIENTO:** a la manifestación de la voluntad libre, específica, informada e inequívoca de la o el titular de los datos personales para aceptar el tratamiento de su información.
DATOS PERSONALES: información concerniente a una persona física o jurídica colectiva identificada o identificable, establecida en cualquier formato o modalidad, y 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.
8. **DERECHOS ARCO:** a los derechos de Acceso, Rectificación, Cancelación y Oposición al tratamiento de datos personales.
9. **DESTINATARIO:** a la persona física o jurídica colectiva pública o privada a quien el responsable transfiere datos personales.
10. **DIAGNÓSTICO:** resultados que arroja un estudio, evaluación o análisis sobre determinado ámbito u objeto, con el propósito reflejar la situación o estado del sistema, para realizar una acción o tratamiento a partir de los resultados.
11. **DIFUSIÓN:** conjunto de acciones y actividades a partir de las cuales se interpreta y además se hace posible el acceso del público sobre el tratamiento de los datos personales.

12. **DISEÑAR:** actividad creativa y técnica y que tiene por misión la creación de campañas de difusión focalizadas para acercar el conocimiento de las leyes de la materia.
13. **EJE TEMÁTICO:** guion básico de organización programada para evaluar logros.
14. **EVALUACIÓN:** parámetros cualitativos y/o cuantitativos de impactos reales respecto de determinados tratamientos de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios y deberes aplicables al tratamiento y derechos de las y los titulares, así como los deberes de los responsables y encargados, previstos en esta Ley y demás disposiciones legales aplicables.
15. **GESTIÓN ADMINISTRATIVA:** forma en que se utilizan los recursos escasos para conseguir los objetivos en materia de protección de datos personales.
16. **GESTIÓN INNOVADORA:** conjunto de etapas técnicas, mecánicas y productivas que conducen al lanzamiento con éxito de nuevos procesos técnico en la impartición de materia de datos personales.
17. **GRUPOS VULNERABLES:** Persona o grupo que por sus características de desventaja por edad, sexo, estado civil; nivel educativo, origen étnico, situación o condición física y/o mental; requieren de un esfuerzo adicional para incorporarse al desarrollo y practica de los datos personales.
18. **INDICADORES:** elemento que se utiliza para indicar o señalar algo, que permita demostrar o señalar criterios para evaluar el desempeño de los responsables respecto del cumplimiento de la presente Ley y demás disposiciones que resulten aplicables.
19. **INSTRUMENTO RECTOR:** planificación institucional, destinado al cumplimiento de las funciones de una organización, por el cual se establece el orden de actuación, así como los objetivos o metas, cuantificables o no (en términos de un resultado final), que se cumplirán a través de la integración de un conjunto de esfuerzos y para lo cual se requiere combinar recursos humanos, tecnológicos, materiales y financieros; especifica tiempos y espacio en los que se va a desarrollar y atribuye responsabilidad a una o varias unidades ejecutoras debidamente coordinadas.
20. **LEY DE TRANSPARENCIA:** a la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios.
21. **LEY GENERAL:** a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
22. **LÍNEAS DE ACCIÓN:** estrategias de orientación y organización de diferentes actividades relacionadas con un campo de acción, de tal forma que se pueda garantizar la integración, articulación y continuidad de esfuerzos, de manera ordenada, coherente y sistemática.
23. **LÍNEAS ESTRATÉGICAS:** son la transformación de los factores claves detectados en el diagnóstico con efectos e impactos sobre otras.
24. **METAS:** parámetros establecidos para aquellos procesos en los que se persigue la obtención de un conocimiento o el cumplimiento de una expectativa.
25. **OBJETIVO:** Describe los propósitos que persigue el proyecto, especificando los de carácter general y los particulares.
26. **ÓRGANO GARANTE:** autoridad encargada de garantizar a toda persona la protección de sus datos personales que se encuentren en posesión de los sujetos obligados, a través de la aplicación de la presente Ley, en concordancia con lo establecido por las disposiciones legales y normatividad en la materia.
27. **PLAN DE CONTINGENCIA:** conjunto de procedimientos alternativos a la operatividad normal de cada institución. Su finalidad es la de permitir el funcionamiento de esta, aun cuando alguna de sus funciones deje de hacerlo por culpa de algún incidente tanto interno como ajeno a la organización.
28. **POLÍTICA PÚBLICA:** acciones con objetivos de interés público que surgen de decisiones sustentadas en un proceso de diagnóstico y análisis de factibilidad, para la atención efectiva de problemas públicos específicos, en donde participa la ciudadanía en la definición de problemas y soluciones.
29. **PORTABILIDAD:** posibilidad de traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tiene derecho a obtener de los sujetos obligados ante los cuales haya entregado su información una copia de los datos objeto de tratamiento en el mismo formato que le permita seguir utilizándolos
30. **PREVENCIÓN:** medidas precautorias necesarias y adecuadas con la misión de contrarrestar un perjuicio o algún daño que pueda producirse.
31. **SARCOEM:** Sistema de Acceso, Rectificación, Cancelación y Oposición de Datos Personales del Estado de México.
32. **SISTEMA DE GESTIÓN DE SEGURIDAD:** Documento que contiene las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales.

33. **SUJETOS OBLIGADOS:** Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos estatales y municipales, así como del gobierno y de la administración pública municipal y sus organismos descentralizados, asimismo de cualquier persona física, jurídica colectiva o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal, que deba cumplir con las obligaciones previstas en la presente Ley.
34. **TRANSMISORES DE CONOCIMIENTO:** Persona encargada de transmitir un conocimiento específico a través de aprendizaje, dentro del personal receptor de la información
35. **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.
36. **UIPE :** Unidad de Información, Planeación, Programación y Evaluación
37. **VERIFICACIÓN:** evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento de datos personales.
38. **VIOLACIONES A LA SEGURIDAD:** a la violación de la seguridad de los datos personales que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transferidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, o cualquier otra que afecte la confidencialidad, integridad y disponibilidad de los datos personales. Se encuentran comprendidas dentro de este concepto las vulneraciones a las que hace referencia la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

ASÍ LO APROBARON POR UNANIMIDAD DE VOTOS LOS INTEGRANTES DEL PLENO DEL INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE MÉXICO Y MUNICIPIOS, CONFORMADO POR LOS COMISIONADOS ZULEMA MARTÍNEZ SÁNCHEZ, EVA ABAID YAPUR, JOSÉ GUADALUPE LUNA HERNÁNDEZ Y JAVIER MARTÍNEZ CRUZ, EN LA VIGÉSIMA SESIÓN ORDINARIA CELEBRADA EL TREINTA DE MAYO DE DOS MIL DIECIOCHO, ANTE EL SECRETARIO TÉCNICO DEL PLENO, ALEXIS TAPIA RAMÍREZ.

Zulema Martínez Sánchez
Comisionada Presidenta
(Rúbrica).

Eva AbaidYapur
Comisionada
(Rúbrica).

José Guadalupe Luna Hernández
Comisionado
(Rúbrica).

Javier Martínez Cruz
Comisionado
(Rúbrica).

Alexis Tapia Ramírez
Secretario Técnico del Pleno
(Rúbrica).