DOCUMENTO DE SEGURIDAD DEL INSTITUTO MICHOACANO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

CONTENIDO

INSTITUTO MICHOACANO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD

PRESENTACIÓN

Con fundamento en el artículo 19 de la Declaración Universal de Derechos Humanos, el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos, artículo 13 del Pacto de San José, el artículo IV de la Declaración Americana de los Derechos y Deberes del Hombre, artículo 4 de la Carta Democrática Interamericana, en tanto que en el orden Jurídico Nacional tiene su fundamento en el artículo 6 apartado A, fracciones I y II de la Constitución Política de los Estados Unidos Mexicanos, en los señala que toda persona tiene derecho al libre acceso a la información plural, oportuna y al derecho a la protección de sus datos personales, así como al acceso,rectificación, cancelación, oposición y portabilidad en los términos que determina la Ley.

En este sentido la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo[1], establece un conjunto de bases, principios y procedimientos para garantizar el derecho a la protección de datos con carácter personal y que se encuentra en posesión de sujetos obligados, entre los que figura el Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Michoacán.

El artículo 3 fracción XIII, de la Legislación Local, dice: Documento de Seguridad es el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

El Documento de Seguridad busca crear un sistema de gestión para el tratamiento de los datos personales, que integre las acciones interrelacionadas

[1] En lo sucesivo, Legislación Local

para operar, monitorear, mantener y mejorar el tratamiento y seguridad de los datos personales.

El tratamiento involucra acciones pertinentes para establecer y mantener las medidas de seguridad necesarias para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso acceso o tratamiento no autorizado o ilícito, así como garantizar los principios y obligaciones previstas en la ley.

El artículo 31 de la referida legislación, establece que los sujetos obligados deberán elaborar un documento de seguridad que contenga, al menos, lo siguiente:

I. El inventario de datos personales y de sus sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad;
VII. El programa general de capacitación.

Considerando que los datos personales constituyen el principal activo de información objeto del presente documento, es necesario señalar que todos y cada uno de los elementos que lo integran, constituyen un sistema interno para la gestión y tratamiento de los datos personales en posesión del Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales, tal como lo indica el artículo 30 de la Legislación Local al señalar que. se entiende por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

1. OBJETIVO DEL DOCUMENTO DE SEGURIDAD

El presente documento tiene como objetivo brindar las herramientas necesarias para la protección de los datos personales en posesión del Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales, como un medio para cumplir con las obligaciones que establece la Legislación Local y los Lineamientos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán[2], así como la normatividad que derive de los mismos; estableciendo los elementos y actividades de gestión para la operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua, además de promover la adopción de mejores prácticas en relación con la protección de datos personales, con la finalidad de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales.

2. RESPONSABILIDADES

De conformidad con lo dispuesto por los artículos 78 y 79 de la Legislación Local, el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales, y sin perjuicio de otras atribuciones que le sean conferidas en la normatividad que le resulte aplicable, tendrá las siguientes funciones:

I. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;
II. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;
III. Confirmar, modificar o revocar las determinaciones en las que se declare

[2] En lo posterior, Los Lineamientos.

la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO;

IV. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;

V. Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;

VI. Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto;

VII. Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales; y,

VIII. Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales; particularmente en casos relacionados con la declaración de inexistencia que realicen los responsables.

Para que el objetivo planteado se logre con éxito, se requiere del apoyo e impulso directo del más alto nivel de la institución. En ese sentido, el Documento de Seguridad se deberá hacer del conocimiento de la Presidencia y del Pleno del Instituto, a fin de que se tomen las medidas necesarias y sea de observancia general para este Organismo Garante.

La intervención del Comisionado Presidente tendrá la finalidad de impulsar la debida implementación del Documento de Seguridad al interior del sujeto obligado, pero no podrá suplir ni afectar las funciones del Comité de Transparencia, en su carácter de autoridad máxima en materia de protección de datos personales del Instituto.

Asimismo, para que la implementación del Documento de Seguridad tenga como resultado el cumplimiento integral de las obligaciones que establece la nuestra Legislación Local y los Lineamientos, será de observancia obligatoria para todas las personas servidoras públicas del sujeto obligado que en el ejercicio de sus funciones traten datos personales.

Las unidades administrativas deberán realizar las acciones necesarias para cumplir con las obligaciones que establece este Documento de Seguridad, debiendo asignar los recursos materiales y humanos necesarios, además de prever lo que se requiera en sus programas de trabajo.

Por lo anterior, resulta fundamental que el Documento de Seguridad se conozca al interior de este Organismo Garante, siendo responsabilidad del Comité de Transparencia difundirlo y socializarlo entre el personal.

3. ALCANCE DEL DOCUMENTO DE SEGURIDAD

El Documento de Seguridad aplica a todas las unidades administrativas que realicen tratamiento de datos personales en ejercicio de sus atribuciones, y a todos los tratamientos de datos personales que efectúen, mismos que se encuentran bajo su estricta responsabilidad, tanto en los espacios físicos como los medios electrónicos en los que se resguardan, operan y administran, con observancia de los principios, deberes y obligaciones que nuestra Legislación Local establece.

Acorde al artículo 3 fracción XIV, del Manual de Organización del Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales, las unidades administrativas que forman parte de este Organismo Garante, y que deberán observar el Programa de Protección de Datos Personales, son las siguientes:

1. Presidencia;
2. Ponencias de Comisionadas y/o Comisionados;
3. Secretaria General;
4. Órgano Interno de Control;
5. Coordinación Jurídica;
6. Coordinación de Investigación y Capacitación; y,
7. Coordinación Administrativa.

La Dirección de Protección de Datos Personales y Políticas de Promoción

de Derechos ARCOP y Subdirección de Protección de Datos Personales, integran este Documento de Seguridad con base en la información generada por las distintas unidades administrativas.

4. SISTEMA DE GESTIÓN DE DATOS PERSONALES

El Sistema de Gestión de Datos Personales es el medio por el cual el Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales, por sus siglas IMAIP, garantiza el tratamiento de los datos personales que lleva a cabo como parte de sus funciones, desde su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación correspondiente; es por ello que se establecen políticas y métodos orientados a salvaguardar la confidencialidad, integridad y disponibilidad de estos datos, de acuerdo con la Legislación Local y la Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo.

En ese tenor, se inició un proceso de organización y planeación de los medios para la protección de datos personales, tomando como punto de partida la identificación de los procesos y tareas en los que, conforme a sus atribuciones, las distintas áreas del Instituto desarrollan tratamientos de datos personales. Para tal fin, se elaboró un formulario que facilitó a cada Unidad Administrativa, la identificación de los tratamientos que llevan a cabo como parte de su responsabilidad, considerando las medidas de seguridad señaladas en el artículo 27 de la Legislación Local; logrando con ello el levantamiento del inventario de datos personales, tratando de identificar la categoría y tipo datos utilizados en cada tratamiento, incluyendo los de carácter sensible; los medios a través de los cuales se obtienen dichos datos; el sistema físico y/o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; las características del lugar donde seubican las bases físicas o electrónicas de datos; las finalidades del tratamiento, el nombre, cargo y adscripción de los servidores públicos que tienen acceso al tratamiento, además de si son objeto de transferencia identificando los destinatarios o receptores de los mismos, así como las causas que la justifican.

Además, el inventario será fundamental para la determinación del ciclo de vida de los datos personales; entendiendo que, una vez concluida la finalidad de éstos, deben ser sometidos a un proceso de bloqueo y, en su caso, de cancelación, supresión o destrucción, vinculado con el proceso de gestión documental que se desarrolla al interior del Instituto.

Una vez integrados los inventarios de tratamientos y de datos personales, se estableció la metodología para el análisis de riesgo, con la intención de que se identificara el valor de los datos y su ciclo de vida, así como el valor de exposición, las posibles consecuencias para los titulares por el uso indebido y/o posible vulneración y las condiciones de riesgo a los que podrían encontrarse expuestos por medidas de seguridad poco confiables. Lo anterior, permitió identificar la brecha entre las medidas de seguridad existentes y las medidas de seguridad administrativas, físicas y técnicas faltantes que garanticen la seguridad de los datos personales.

A partir de la identificación de posibles vulneraciones, establecer controles o mecanismos para que todas las personas que intervengan en cualquier fase del tratamiento de los datos personales guarden el debido sigilo, obligación que subsistirá aún después de finalizar sus relaciones con el mismo y sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.

Las amenazas que se buscan prevenir pueden ser de diferentes tipos:

1. Robo, extravío o copia no autorizada;
2. Uso, acceso o tratamiento no autorizado;
3. Daño, alteración o modificación no autorizado;
4. Pérdida o destrucción no autorizada.

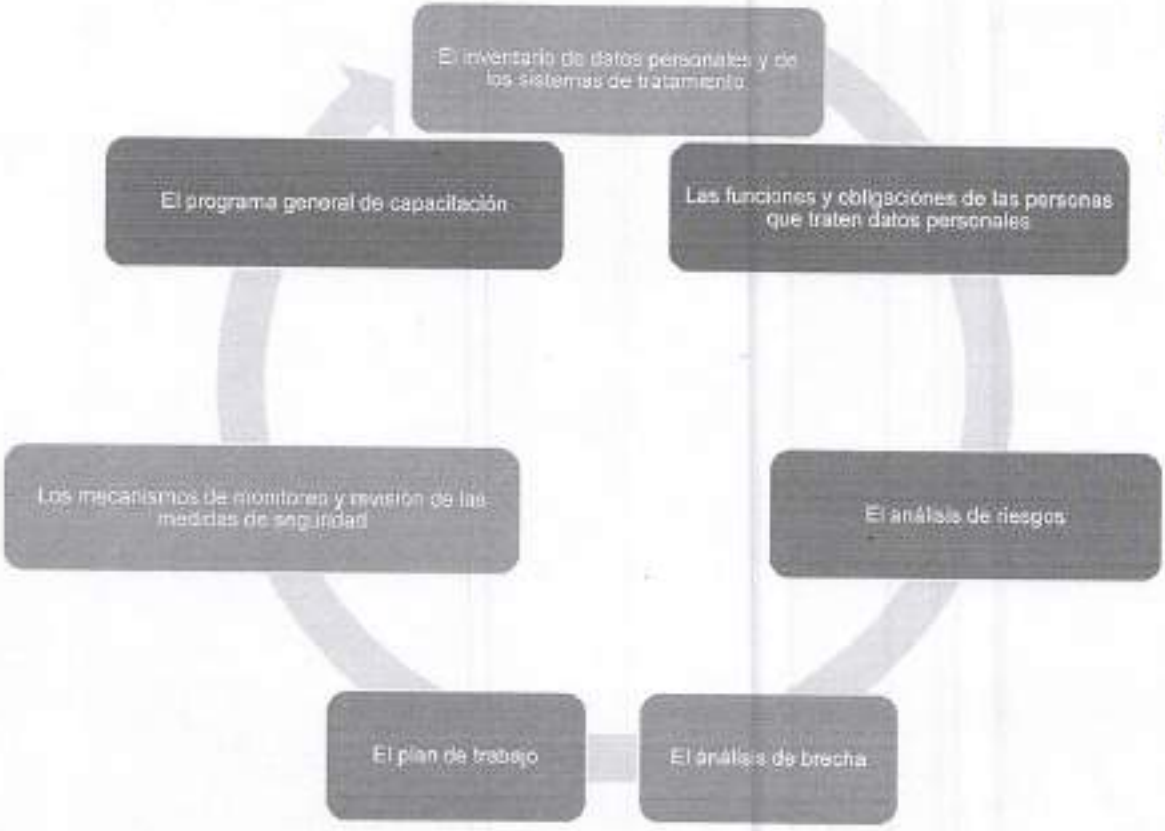
El riesgo que puede presentarse en caso de que las amenazas señaladas detonen las vulnerabilidades, es el acceso a los datos personales de manera no autorizada, comprometiendo con ello su confidencialidad, disponibilidad e integridad; en ese sentido, las medidas de seguridad adoptadas por cada Unidad Administrativa están orientadas a proteger los datos personales a su resguardo.

En el marco del sistema de gestión y política de seguridad institucional, se procurará:

I. Tratar a los datos personales conforme a la Ley;
II. Identificar a los servidores públicos de este Instituto, responsables del tratamiento de los datos personales;
III. Que los tratamientos de datos personales estén sujetos al principio de consentimiento, siempre que la Ley lo permita;
IV. Responder al principio de información a los titulares sobre tratamiento al que serán sometidos sus datos personales, el uso que se les dará y sus finalidades;
V. Mantener la actualización y pertinencia de los datos personales;
VI. Priorizar la supresión de los datos personales cuando haya concluido el proceso para el que fueron obtenidos;
VII. Ajustar el tratamiento de los datos personales a finalidades concretas, explícitas y lícitas para las que fueron solicitados, recabando estrictamente los necesarios;
VIII. Obtener datos personales a través de medios legales, con respeto a la expectativa de privacidad del titular;
IX. Velar por el cumplimiento de los principios, priorizando el deber de seguridad y de confidencialidad, durante el ciclo de vida de los datos personales sometidos a tratamiento, con estricto apego de los derechos de sus titulares;
X. Mantener actualizado el inventario de datos personales con el que cuenta el Instituto.

Para lograr lo anterior, se tomó como punto de partida la identificación de vulnerabilidades y amenazas, estableciendo medidas de seguridad generales que, de acuerdo con otras experiencias y mejores prácticas tomadas como referencia, se encaminan a la mejora continua por parte de las personas involucradas en el tratamiento, buscando lograr la salvaguarda del derecho a la privacidad y protección de datos los personales, actuando con estricto apego tanto a la Legislación Local como a los Lineamientos correspondientes.

INTEGRACIÓN DEL DOCUMENTO DE SEGURIDAD



5. INVENTARIO DE TRATAMIENTOS Y DATOS PERSONALES

Para el debido cumplimiento de las obligaciones, es necesario que cada una de las unidades administrativas que conforman este Instituto, realicen un diagnóstico de los tratamientos de datos personales que llevan a cabo, basado en la elaboración de un inventario que contenga la información básica de cada tratamiento de datos personales que realiza.

Por inventario de tratamientos de datos personales, se entenderá el control documentado que se llevará de los tratamientos que realizan las unidades

administrativas del Instituto.

Como resultado del proceso de análisis y actualización de la información, se logró identificar a las unidades administrativas que realizan tratamiento datos personales, a saber:

1. Presidencia;
2. Ponencias de Comisionadas y/o Comisionados;
3. Secretaría General;
4. Órgano Interno de Control;
5. Coordinación Jurídica;
6. Coordinación de Investigación y Capacitación; y,
7. Coordinación Administrativa.

Estos tratamientos se realizan en absoluto apego a sus funciones, a través de las diversas áreas que las integran y permiten el desarrollo de los procesos que realizan para el cumplimiento de dichas funciones. En relación con lo anterior, fue posible identificar 49 procesos que implican el tratamiento de datos personales, mismos que a continuación se describen:

UNIDAD ADMINISTRATIVA	TRATAMIENTO
PRESIDENCIA	Dar a conocer las actividades del Instituto (Entrevista)
	Promover y difundir el acceso a la información y la protección de datos personales y gestión documental (Boletines y comunicados)
	Celebración de convenios de colaboración
PONENCIA DE COMISIONADAS Y/O	Substanciación de Recursos de Revisión y Denuncias en Materia de Acceso a la Información Pública
	Substanciación de Denuncias y Verificaciones en

COMISIONADOS	Materia de Datos Personales
	Substanciación de Medios de Impugnación
SECRETARÍA GENERAL	Registro y Turno de Verificaciones de Datos Personales
	Actas y Acuerdos
	Certificaciones
	Notificaciones
	Recibir, Registrar y Distribuir los escritos y correspondencia a las Unidades Administrativas
	Sistema de Verificación de portales de Obligaciones de Transparencia (VERIPOT)
	Asistencia Informática
	Sistema de Seguimiento a Medios de Impugnación (SEGUIMAIP)
	Sistema de Declaración Patrimonial
	Solicitudes de Acceso a la Información (SAI)
	Atención a Sujetos Obligados en la Plataforma Nacional de Transparencia
	Resguardo de los Archivos en el Archivo de Concentración
ÓRGANO INTERNO DE CONTROL	Procedimiento para la verificación patrimonial y de conflicto de interés de las personas servidoras públicas
	Recepción de la declaración patrimonial y de interés (inicial, modificación y conclusión) y la constancia de declaración fiscal
	Procedimiento de responsabilidad administrativa cuya resolución corresponde a los tribunales
	Revisiones de control interno
	Substanciar el procedimiento de responsabilidad administrativa (faltas no graves)
	Investigación de faltas administrativas derivadas

	de quejas, denuncias, auditorías internas o externas
	Presentar denuncias por delitos ante la Fiscalía especializada en combate a la corrupción o sus homólogos en el ámbito local
	Resolución al Procedimiento de Responsabilidad Administrativa. (Faltas no graves)
COORDINACIÓN JURÍDICA	Seguimiento de Juicio de Amparo
	Cumplimiento de las Resoluciones de los Recursos de Revisión y Denuncias
	Cumplimiento de la Verificación de Datos Personales
COORDINACIÓN DE INVESTIGACIÓN Y CAPACITACIÓN	Programa Anual de Estado Abierto y Transparencia Proactiva
	Implementación de políticas y mecanismos aplicables en materia de Gobierno Abierto, Transparencia Proactiva, Partido Político Abierto y Rendición de Cuentas
	Declaratoria de Estado Abierto, Gobierno abierto, Congreso Abierto, Justicia Abierta y Municipio Abierto
	Reconocimiento en materia de Transparencia Proactiva
	Capacitación
	Campañas de difusión
COORDINACIÓN ADMINISTRATIVA	Registro de Asistencia del Personal del Instituto
	Elaboración y Control de Contratos con Proveedores de Bienes y Servicios al Instituto
	Permisos al Personal del Instituto para Ausentarse
	Cálculo y Pago de Finiquitos y Liquidaciones al Personal del Instituto
	Elaboración y Control de los Expedientes del Personal del Instituto
	Registro del Personal del Instituto y Deducciones

	Correspondientes ante el IMSS
	Cálculo y Pago de Impuestos Retenidos al Personal del Instituto
	Elaboración, Timbrado y Pago de Nómina del Personal del Instituto
	Elaboración de Matriz de Percepciones y deducciones del Personal del Instituto
	Pago a Proveedores del Instituto
	Resguardo y Control de Bienes Propiedad al Instituto
	Coordinación y Supervisión de los Programas de Servicio Social y Prácticas Profesionales en el Instituto
	Pago de los Vales de Despensa del Personal del Instituto
	Cálculo y Pago de Viáticos del Personal del Instituto

Como resultado del proceso de análisis, se identificaron también los datos personales utilizados en los tratamientos, mismos que corresponden a las tres categorías, tal como se señala a continuación:

De Identificación:

Nombre, estado civil, teléfono, sexo, nacionalidad, ocupación, firma, domicilio, curp, rfc, número de seguridad social, cédula profesional, fecha de nacimiento, antecedentes laborales, características físicas, correo electrónico, curriculum vitae, datos académicos, datos de identificación, datos laborales, datos familiares, datos personales contenidos en documento para acreditar personalidad del representante, datos personales contenidos en la identificación oficial presentada por la persona física, imagen en fotografía y/o video, huella dactilar, huella digital, menor de edad, clave de elector, entre otros.

Patrimoniales:

Número de cuentas bancarias, estados de cuenta, clabe interbancaria, institución bancaria, facturas, beneficiarios, datos contenidos en declaraciones

patrimoniales, como (descuentos personales, ahorro voluntario, hipoteca, seguro médico, entre otros).

Sensibles:

Creencias religiosas, filosóficas o morales, datos de salud, datos sobre procedimientos judiciales o seguidos en forma de juicio, discapacidad, estado de interdicción o incapacidad legal, información genética, migratoria, origen étnico o racial.

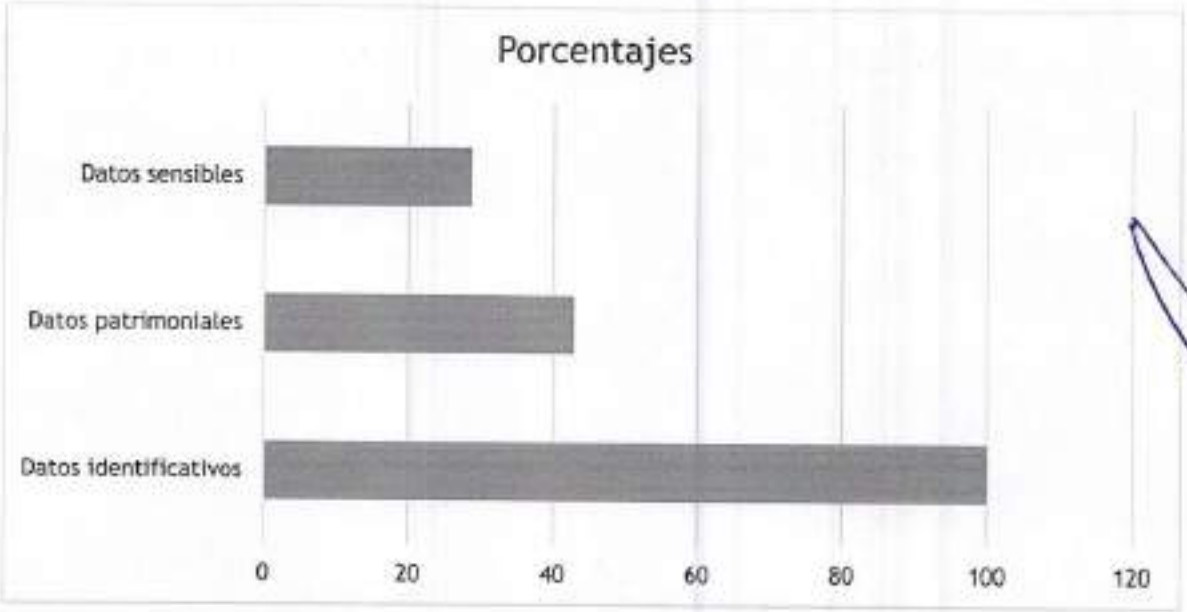
Estos datos son utilizados en 49 tratamientos, de los cuales 3 corresponden a la Presidencia, 3 a las Ponencias de las Comisionadas y/o Comisionados, 12 a la Secretaría General, 8 al Órgano Interno de Control, 3 a la Coordinación Jurídica, 6 a la Coordinación de Investigación y Capacitación, y 14 a la Coordinación Administrativa. Asimismo, en 49 tratamientos se utilizan datos personales de identificación, mientras que en 21 se recabaron datos personales patrimoniales; y, en lo que se refiere a datos sensibles se operan en 14 tratamientos.

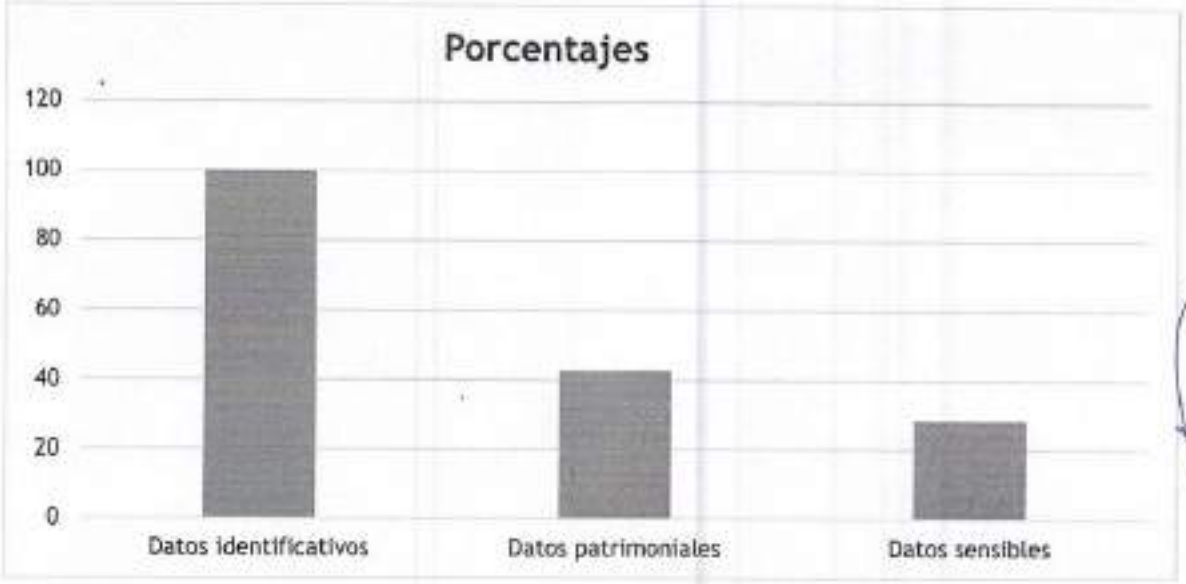
Como se puede apreciar, la unidad administrativa con mayor número de tratamientos es la Coordinación Administrativa con 14, mientras que la Presidencia, Ponencias y Coordinación Jurídica son las que menos procesos desarrollan, al tener solo 3 tratamientos.

En relación con los datos solicitados, todas las unidades administrativas solicitan datos de identificación, mientras que las Ponencias, la Secretaría General, el Órgano Interno de Control, la Coordinación Jurídica y la Coordinación Administrativa, solicitan datos patrimoniales; en esa tesitura, las Ponencias, el Órgano Interno de Control, la Coordinación Jurídica y la Coordinación Administrativa, manejan datos sensibles.

En ese sentido, se identificó también que, con relación a los procesos en los que se tratan datos, el 100% por ciento de los tratamientos usan datos identificativos; el 42.85% usa datos patrimoniales, y el 28.57% usa datos sensibles.

PROCESOS EN LOS QUE SE TRATAN DATOS





A partir de lo anterior, podemos identificar que la categoría de datos personales con mayor número procesos es la de carácter identificativo, en segundo término, los que incluyen datos patrimoniales; y, en el caso de datos sensibles, ocupan el tercer lugar en los tratamientos en los que se utilizan.

Tipo de datos tratados por unidad administrativa:

1. Identificativos;
2. Patrimoniales;
3. Sensibles.

Es posible apreciar que la Coordinación Administrativa es la unidad que desarrolla el mayor número de procesos en los que intervienen tratamientos de datos personales, dada la naturaleza de sus funciones; lo anterior, debido a que las áreas que la integran cuentan con atribuciones para administrar los recursos humanos, materiales y financieros del Instituto; esto implica que los procesos correspondientes a la protección de datos personales sean aplicados con mayor cuidado y puntualidad, para garantizar que este derecho se cumpla. No obstante, en las otras áreas, aunque en menor medida, también se efectúa el tratamiento de datos personales; por tanto, la estrategia de protección debe ser entendida como una acción de frecuencia generalizada.

TRATAMIENTOS DE LA COORDINACIÓN ADMINISTRATIVA		
NO.	**ÁREA**	**TRATAMIENTO O PROCESO:**
1	Coordinación Administrativa	Elaboración y Control de Contratos con Proveedores de Bienes y Servicios al Instituto
2	Coordinación Administrativa	Permisos al Personal del Instituto para Ausentarse
3	Coordinación Administrativa	Pago a Proveedores del Instituto
4	Coordinación Administrativa	Resguardo y Control de Bienes Propiedad del Instituto
5	Coordinación Administrativa	Coordinación y Supervisión de los Programas de Servicio Social y Prácticas Profesionales en el Instituto
6	Subcoordinación de Finanzas	Cálculo y Pago de Viáticos del

		Personal del Instituto
7	Subcoordinación de Finanzas	Cálculo y Pago de Impuestos Retenidos al Personal del Instituto
8	Subcoordinación de Finanzas	Cálculo y Pago de Finiquitos y Liquidaciones al Personal del Instituto
9	Jefatura de Recursos Humanos	Elaboración, Timbrado y Pago de Nómina del Personal del Instituto
10	Jefatura de Recursos Humanos	Elaboración de Matriz de Percepciones y Deducciones del Personal del Instituto
11	Jefatura de Recursos Humanos	Pago de los Vales de Despensa del Personal del Instituto
12	Jefatura de Recursos Humanos	Elaboración y Control de los Expedientes del Personal del Instituto
13	Jefatura de Recursos Humanos	Registro de Asistencia del Personal del Instituto
14	Jefatura de Recursos Humanos	Registro del Personal del Instituto y Deducciones Correspondientes ante el IMSS

Al respecto, se identificó que cada unidad administrativa tiene un medio propio para recabar datos personales y estos son: de manera personal, directamente del titular, a través de correo electrónico, vía telefónica, Plataforma Nacional de Transparencia.

Asimismo, las áreas responsables se encargan de desarrollar estrategias para la protección de los datos personales, mediante archivos o bases de datos electrónicas simples, resguardadas en las computadoras de las personas servidoras públicas.

Es por ello, que el Inventario de Datos Personales del Instituto, a partir de los hallazgos identificados en su actualización, se integra como un elemento del Sistema de Gestión de Datos Personales, que representa, junto con las medidas de seguridad, un instrumento útil para la implementación de las medidas correspondientes en materia de protección de datos personales.

Lo anterior favorece el trazo de rutas para la capacitación en materia de protección de datos personales al personal que integra este Instituto, como una vía de fortalecimiento en la operación de los procesos en que se tratan datos personales, en la búsqueda de sensibilizar y preparar a los responsables y encargados de los mismos, para que el tratamiento se realice de conformidad con los estándares nacionales e internacionales en la materia.

En apego a lo anterior, el Inventario de Datos Personales del Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales, se consolida como un elemento más de la política implementada para la observancia de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en su artículo 35 párrafo I, dando certeza a la ciudadanía sobre el destino de los datos recabados por este Organismo Garante.

6. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATAN DE DATOS PERSONALES

Con la finalidad de dar cumplimiento al principio de legalidad que todo servidor público debe atender al momento de llevar a cabo el tratamiento de datos personales, es menester definir las funciones establecidas en el Manual de Organización de este Instituto.

FUNCIONES DE LAS PERSONAS SERVIDORAS PÚBLICAS EN LOS SISTEMAS DE TRATAMIENTOS				
No.	Unidad Administrativa	Nombre de la Persona Servidora Pública	Función que desempeña	Tratamiento o Proceso:
1	Presidencia	Abraham Montes Magaña	Comisionado Presidente (Representación del Instituto, Coordinación y vinculación con medios de comunicación)	Dar a conocer las actividades del Instituto (Entrevista)
		Estefanía Ayala Bravo	Director de Ponencia de Presidencia (Coordinación y supervisión)	
		Ibeth Cruz Alonzo	Asesora de Vinculación de Presidencia (Vinculación con medios de comunicación)	
		Christopher Fernando López López	Jefe del Departamento de Comunicación Social (Vinculación con medios de comunicación, promoción y difusión)	
		Nilda Tamara Bautista Guerrero	Analista B en el Departamento de Comunicación Social (Promoción y difusión)	
2	Presidencia	Abraham Montes Magaña	Comisionado Presidente (Representación del Instituto, Coordinación y vinculación con medios de comunicación, coordinación de campañas)	Promover y difundir el acceso a la información y la protección de datos personales y gestión documental

		Estefanía Ayala Bravo	Director de Ponencia de Presidencia (Coordinación y supervisión)	(Boletines y comunicados)
		Ibeth Cruz Alonzo	Asesora de Vinculación de Presidencia (Vinculación con medios de comunicación)	
		Christopher Fernando López López	Jefe del Departamento de Comunicación Social (Coordinación y elaboración de campañas, vinculación con medios de comunicación, promoción y difusión)	
		Nilda Tamara Bautista Guerrero	Analista B en el Departamento de Comunicación Social (Elaboración de campañas, promoción y difusión)	
3	Presidencia	Abraham Montes Magaña	Comisionado Presidente (Coordinación, proyecto, firma y aprobación de los convenios)	Celebración de convenios de colaboración
		Estefanía Ayala Bravo	Director de Ponencia de Presidencia (Coordinación y supervisión)	
		Ibeth Cruz Alonzo	Asesora de Vinculación de Presidencia (Proyecto y elaboración de convenios y seguimiento)	

		Christopher Fernando López López	Jefe del Departamento de Comunicación Social (Promoción y difusión)	
		Nilda Tamara Bautista Guerrero	Analista B en el Departamento de Comunicación Social (Promoción y difusión)	
4	Ponencia Mtro. Abraham Montes Magaña	Abraham Montes Magaña	Comisionado (Análisis, discusión y, en su caso, aprobación de los acuerdos de cumplimiento y resoluciones)	Substanciación de Recursos de Revisión y Denuncias
		Estefanía Ayala Bravo	Director de Ponencia (Análisis de acuerdos de cumplimiento, firma de acuerdos diversos)	
		Raymundo Sánchez Arredondo	Secretario Técnico (Análisis de acuerdos y resoluciones, coordinación de proyecto y socialización entre ponencias)	
		Carlos Ruano Sánchez	Asesor (Análisis de acuerdos y resoluciones, coordinación de proyecto y socialización entre ponencias)	
		Dulce Rubí Méndez Walle	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)	

		José Ángel Santoyo Bautista	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)
		Rosa Elvira Saldivar Quintero	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)
		Yatziri Guadalupe Jiménez Rivera	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)
		Gael Javier Méndez Salmón	Secretaria Particular (Análisis de acuerdos y registro de expedientes)
	Ponencia Mtra. Ruth Noemí Espinoza Pérez	Ruth Nohemí Espinoza Pérez	Comisionada (Análisis, discusión y, en su caso, aprobación de los acuerdos de cumplimiento y resoluciones)
		Esperanza Elizabeth Torres Melgoza	Director de Ponencia (Análisis de acuerdos de cumplimiento, firma de acuerdos diversos)
		Estephania García Ayala	Secretaria Técnica (Análisis de acuerdos y resoluciones, coordinación de proyecto

			y socialización entre ponencias)	
		Zadquiel Leopoldo González Vargas	Asesor (Análisis de acuerdos y resoluciones, coordinación de proyecto y socialización entre ponencias)	
		José Guadalupe Guillén Rojas	Asesor (Análisis de acuerdos y resoluciones, coordinación de proyecto y socialización entre ponencias)	
		Jonathan Moncada Chávez	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)	
		Estefani Serrato Marín	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)	
		Carina Elizabeth Reyes Huitrón	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)	
		Estefanía Sánchez Sánchez	Secretaria Particular (Análisis de acuerdos y registro de expedientes)	

	Ponencia Mtra. Areli Yamilet Navarrete Naranjo	Areli Yamilet Navarrete Naranjo	Comisionada (Análisis, discusión y, en su caso, aprobación de los acuerdos de cumplimiento y resoluciones)	
		Cinthia Hernández Gallegos	Directora de Ponencia (Análisis de acuerdos de cumplimiento, firma de acuerdos diversos)	
		Carolina Pérez Juárez	Secretario Técnico (Análisis de acuerdos y resoluciones, coordinación de proyecto y socialización entre ponencias)	
		Carolina Pérez Juárez	Asesor (Análisis de acuerdos y resoluciones, coordinación de proyecto y socialización entre ponencias)	
		María Dolores Arredondo González	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)	
		Brenda Mariana Jiménez Castillo	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución	

		José Luis Luna Ramírez	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución	
		Frida Janese Villa Prado	Secretaria Particular (Análisis de acuerdos y registro de expedientes)	
5	Ponencia Mtro. Abraham Montes Magaña	Abraham Montes Magaña	Comisionada (Análisis, discusión y, en su caso, aprobación de los acuerdos de cumplimiento y resoluciones)	Substanciación de Denuncias y Verificaciones en Materia de Datos Personales
		Estefania Ayala Bravo	Director de Ponencia (Análisis de acuerdos de cumplimiento, firma de acuerdos diversos)	
		Raymundo Sánchez Arredondo	Secretario Técnico (Análisis de acuerdos y resoluciones, coordinación de proyecto y socialización entre ponencias)	
		Carlos Ruano Sánchez	Asesor (Análisis de acuerdos y resoluciones, coordinación de proyecto y socialización entre ponencias)	
		Dulce Rubí Méndez Walle	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de	

			expedientes y proyectos de resolución)	
		José Ángel Santoyo Bautista	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)	
		Rosa Elvira Saldivar Quintero	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)	
		Gael Javier Méndez Salmón	Secretaria Particular (Análisis de acuerdos y registro de expedientes)	
	Ponencia Mtra. Ruth Noemí Espinoza Pérez	Ruth Nohemí Espinoza Pérez	Comisionada (Análisis, discusión y, en su caso, aprobación de los acuerdos de cumplimiento y resoluciones)	
		Esperanza Elizabeth Torres Melgoza	Director de Ponencia (Análisis de acuerdos de cumplimiento, firma de acuerdos diversos)	
		Estephania García Ayala	Secretaria Técnica(Análisis de acuerdos y resoluciones, coordinación de proyecto y socialización entre ponencias)	

		Zadquiel Leopoldo González Vargas	Asesor (Análisis de acuerdos y resoluciones, coordinación de proyecto y socialización entre ponencias)	
		José Guadalupe Guillén Rojas	Asesor (Análisis de acuerdos y resoluciones, coordinación de proyecto y socialización entre ponencias)	
		Jonathan Moncada Chávez	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)	
		Estefani Serrato Marín	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)	
		Paulina Gallegos Ramírez	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)	
		Estefanía Sánchez Sánchez	Secretaria Particular (Análisis de acuerdos y registro de expedientes)	
	Ponencia Mtra. Areli Yamilet	Areli Yamilet Navarrete Naranjo	Comisionada (Análisis, discusión y, en su caso, aprobación de los acuerdos de	

	Navarrete Naranjo		cumplimiento y resoluciones)
		Cinthia Hernández Gallegos	Directora de Ponencia (Análisis de acuerdos de cumplimiento, firma de acuerdos diversos)
		Carolina Pérez Juárez	Secretario Técnico (Análisis de acuerdos y resoluciones, coordinación de proyecto y socialización entre ponencias)
		María Dolores Arredondo González	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)
		Brenda Mariana Jiménez Castillo	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)
		José Luis Luna Ramírez	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)
		Frida Janese Villa Prado	Secretaria Particular (Análisis de acuerdos y registro de expedientes)

6	Ponencia Mtro. Abraham Montes Magaña	Abraham Montes Magaña	Comisionada (Análisis, discusión y, en su caso, aprobación de los acuerdos de cumplimiento y resoluciones)	Substanciación de Medios de Impugnación
		Estefanía Ayala Bravo	Director de Ponencia (Análisis de acuerdos de cumplimiento, firma de acuerdos diversos)	
		Raymundo Sánchez Arredondo	Secretario Técnico (Análisis de acuerdos y resoluciones, coordinación de proyecto y socialización entre ponencias)	
		Carlos Ruano Sánchez	Asesor (Análisis de acuerdos y resoluciones, coordinación de proyecto y socialización entre ponencias)	
		Dulce Rubí Méndez Walle	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)	
		José Ángel Santoyo Bautista	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)	

		Rosa Elvira Saldivar Quintero	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)	
		Gael Javier Méndez Salmón	Secretaria Particular (Análisis de acuerdos y registro de expedientes)	
	Ponencia Mtra. Ruth Nohemí Espinoza Pérez	Ruth Nohemí Espinoza Pérez	Comisionada (Análisis, discusión y, en su caso, aprobación de los acuerdos de cumplimiento y resoluciones)	
		José Guadalupe Guillén Rojas	Director de Ponencia (Análisis de acuerdos de cumplimiento, firma de acuerdos diversos)	
		Estephanía García Ayala	Secretaria Técnica(Análisis de acuerdos y resoluciones, coordinación de proyecto y socialización entre ponencias)	
		Zadquiel Leopoldo González Vargas	Asesor (Análisis de acuerdos y resoluciones, coordinación de proyecto y socialización entre ponencias)	
		Jonathan Moncada Chávez	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de	

			expedientes y proyectos de resolución)
		Estefani Serrato Marín	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)
		Alejandra Alitzel Vieyra Cortés	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución)
		Estefanía Sánchez Sánchez	Secretaria Particular (Análisis de acuerdos y registro de expedientes)
	Ponencia Mtra. Areli Yamilet Navarrete Naranjo	Areli Yamilet Navarrete Naranjo	Comisionada (Análisis, discusión y, en su caso, aprobación de los acuerdos de cumplimiento y resoluciones)
		Cinthia Hernández Gallegos	Directora de Ponencia (Análisis de acuerdos de cumplimiento, firma de acuerdos diversos)

		Carolina Pérez Juárez	Secretario Técnico (Análisis de acuerdos y resoluciones, coordinación de proyecto y socialización entre ponencias)	
		María Dolores Arredondo González	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución	
		Brenda Mariana Jiménez Castillo	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución	
		José Luis Luna Ramírez	Secretario de Acuerdos y Proyectista (Elaboración y certificación de acuerdos, integración de expedientes y proyectos de resolución	
		Frida Janese Villa Prado	Secretaria Particular (Análisis de acuerdos y registro de expedientes)	
7	Secretaría General	Giselle Alzati Valdés	Jefatura de Departamento de Oficialía de Partes (Registro del recurso)	Registro y Turno de Verificaciones de Datos Personales
		Ma. Del Carmen Guzmán Pérez	Analista B (Turno a las ponencias)	

		Araceli Guerrero Tapia	Analista B (Elaboración de Turno del Recurso de Revisión)	
		Clara Magali Clemente Ruiz	Analista B (Integración de Expediente de Recurso de Revisión para Turno)	
		Omar Alexandro Negrón Villafán	Secretario General (Firma de los expedientes)	
8	Secretaría General	Omar Alexandro Negrón Villafán	Secretario General	Actas y Acuerdos
		Monserrat Canales Melchor	Elaboración de Actas y Acuerdos	
9	Secretaría General	Omar Alexandro Negrón Villafán	Secretario General	Certificaciones
		Monserrat Canales Melchor	Elaboración de Certificaciones	
10	Secretaría General	Yosira Isabel Compiant Barragán	Jefa del Departamento de Actuaría	Notificaciones
		Natalia Pallares Mora	Analista en funciones de notificador	
		Abraham Soto González	Analista en funciones de notificador	

11	Secretaría General	Giselle Alzati Valdés	Jefe de Departamento	Recibir, Registrar y Distribuir los escritos y correspondencia a las Unidades Administrativas
		Ma. Del Carmen Guzmán Pérez	Analista B	
12	Secretaría General	Manuel Magaña Guevara	Subdirector de Informática, desarrollo e Infraestructura Tecnológica	Veripot (Sistema de Verificación de Portales de Obligaciones de Transparencia)
		Ivonne Peraldi Rodríguez	Subcoordinadora de Verificaciones	
		Michael Patricio	Jefe de Departamento de Verificaciones	
13	Secretaría General	Manuel Magaña Guevara	Subdirector de Informática, desarrollo e Infraestructura Tecnológica	Asistencia Informática
14	Secretaría General	Manuel Magaña Guevara	Subdirector de Informática, desarrollo e Infraestructura Tecnológica	SEGIMAIP (Sistema de Seguimiento a Medios de Impugnación)
		Andrés Raymundo Muñoz Bucio	Analista B	
15	Secretaría General	Manuel Magaña Guevara	Subdirector de Informática, desarrollo e Infraestructura Tecnológica	Sistema de Declaración Patrimonial

		Yolanda Soto Morales	Jefa del Departamento de Investigación de Quejas y Denuncias, adscrita al Órgano Interno de Control	
		Dulce Eduviges Avellaneda Naranjo	Directora de Control Interno	
16	Secretaría General	Manuel Magaña Guevara	Subdirector de Informática, desarrollo e Infraestructura Tecnológica	SAI (Solicitudes de Acceso a la Información)
		Andrés Raymundo Muñoz Bucio	Analista B	
17	Secretaría General	Cristian Lizeth Bustos Murillo	Subdirectora de Plataforma, Sistemas y Asistencia Técnica a Sujetos Obligados IMAIP	Atención a Sujetos Obligados en la Plataforma Nacional de Transparencia
18	Secretaría General	Krishna Gandy Medina Uribe	Directora de Gestión Documental	Resguardo de los Archivos en el Archivo de Concentración
		Jesús Eduardo Pérez Escoto	Subdirector de Archivo de Concentración e Histórico	
19	Órgano Interno de Control	Dulce Eduviges Avellaneda Naranjo	Directora de Control Interno	Procedimiento para la verificación patrimonial y de conflicto de interés

		Yolanda Soto Morales	Jefatura de Investigación de Quejas y Denuncias (en cuanto a autoridad investigadora)	de las personas servidoras públicas
20	Órgano Interno de Control	Yolanda Soto Morales	Jefatura de Investigación de Quejas y Denuncias (en cuanto a autoridad investigadora)	Recepción de la declaración patrimonial y de interés (inicial, modificación y conclusión) y la constancia de declaración fiscal
21	Órgano Interno de Control	Dulce Eduviges Avellaneda Naranjo	Directora de Control Interno	Procedimiento de responsabilidad administrativa cuya resolución corresponde a los tribunales
22	Órgano Interno de Control	Dulce Eduviges Avellaneda Naranjo	Directora de Control Interno	Revisiones de control interno
23	Órgano Interno de Control	Dulce Eduviges Avellaneda Naranjo	Dulce Eduviges Avellaneda Naranjo	Substanciar el procedimiento de responsabilidad administrativa. (faltas no graves)
24	Órgano Interno de Control	Dulce Eduviges Avellaneda Naranjo	Directora de Control Interno	Investigación de faltas administrativas derivadas de quejas,

		Yolanda Soto Morales	Jefatura de Investigación de Quejas y Denuncias	denuncias, auditorías internas o externas
25	Órgano Interno de Control	Dulce Eduviges Avellaneda Naranjo	Directora de Control Interno	Presentar denuncias por delitos ante la Fiscalía especializada en combate a la corrupción o sus homólogos en el ámbito local
26	Órgano Interno de Control	Dulce Eduviges Avellaneda Naranjo	Directora de Control Interno	Resolución al Procedimiento de Responsabilidad Administrativa. (Faltas no graves)
27	Coordinación Jurídica	José Omar Reyes Herrera	Coordinador Jurídico (Dar atención y seguimiento a los asuntos administrativos, jurisdiccionales y contenciosos en los que el Instituto sea parte, así como dar vista a Presidencia de los mismos cada mes)	Seguimiento de Juicio de Amparo
		Mariela Merlos García	Analista B (coadyuvar con las actividades que se realizan en la unidad o en el área administrativa de adscripción)	

28	Coordinación Jurídica	Guadalupe Osornio Quezadas	Subcoordinadora de Cumplimiento y Medidas de Apremio, (proponer a la Coordinación Jurídica los proyectos de acuerdos a efecto de que el sujeto obligado cumpla con las resoluciones recaídas dentro de los procedimientos que resuelva el Pleno)	Cumplimiento de las Resoluciones de los Recursos de Revisión y Denuncias
		Irma Ríos Villegas	Jefa del Departamento de Cumplimiento (Proponer a la Subcoordinación de Cumplimiento y Medidas de Apremio los proyectos de acuerdo a efecto de que el sujeto obligado cumpla recaídas dentro de los procedimientos que resuelva el Pleno)	
		Gema Corolina González y Sandoval	Jefa de Departamento de Medidas de Apremio (Proponer a la Subcoordinación de Cumplimiento y Medidas de Apremio los proyectos de acuerdo a efecto de imponer las medidas de apremio necesarias para asegurar el cumplimiento de las resoluciones emitidas por el Pleno)	

		Paola Fuentes Velázquez	Analista A (coadyuvar con las actividades que se realizan en la unidad o en el área administrativa de adscripción)	
		Tatiana Marcela Cardiel Reyes	Analista B (coadyuvar con las actividades que se realizan en la unidad o en el área administrativa de adscripción)	
		Mariela Merlos García	Analista B (coadyuvar con las actividades que se realizan en la unidad o en el área administrativa de adscripción)	
29	Coordinación Jurídica	Guadalupe Osornio Quezadas	Subcoordinadora de Cumplimiento y Medidas de Apremio, (proponer a la Coordinación Jurídica los proyectos de acuerdos a efecto de que el sujeto obligado cumpla con las resoluciones recaídas dentro de los procedimientos que resuelva el Pleno)	Cumplimiento de la Verificación de Datos Personales
		Irma Ríos Villegas	Jefa del Departamento de Cumplimiento (Proponer a la Subcoordinación de Cumplimiento y Medidas de Apremio los proyectos de acuerdo a efecto de que el sujeto obligado cumpla recaídas dentro de los procedimientos que resuelva el Pleno)	

		Gema Corolina González y Sandoval	Jefa de Departamento de Medidas de Apremio (Proponer a la Subcoordinación de Cumplimiento y Medidas de Apremio los proyectos de acuerdo a efecto de imponer las medidas de apremio necesarias para asegurar el cumplimiento de las resoluciones emitidas por el Pleno)	
		Paola Fuentes Velázquez	Analista A (coadyuvar con las actividades que se realizan en la unidad o en el área administrativa de adscripción)	
		Tatiana Marcela Cardiel Reyes	Analista B (coadyuvar con las actividades que se realizan en la unidad o en el área administrativa de adscripción)	
		Mariela Merlos García	Analista B (coadyuvar con las actividades que se realizan en la unidad o en el área administrativa de adscripción)	
30	Coordinación de Investigación y Capacitación	Roberto García Escobar	Subcoordinador de Estado Abierto y Transparencia Proactiva	Programa Anual de Estado Abierto y Transparencia Proactiva
		Naín Rodríguez Torres	Analista B	

31	Coordinación de Investigación y Capacitación	Roberto García Escobar	Subcoordinador de Estado Abierto y Transparencia Proactiva	Implementación de políticas y mecanismos aplicables en materia de Gobierno Abierto, Transparencia Proactiva, Partido Político Abierto y Rendición de Cuentas
		Naín Rodríguez Torres	Analista B	
32	Coordinación de Investigación y Capacitación	Roberto García Escobar	Subcoordinador de Estado Abierto y Transparencia Proactiva	Declaratoria de Estado Abierto, Gobierno abierto, Congreso Abierto, Justicia Abierta y Municipio Abierto
		Naín Rodríguez Torres	Analista B	
33	Coordinación de Investigación y Capacitación	Roberto García Escobar	Subcoordinador de Estado Abierto y Transparencia Proactiva	Reconocimiento en materia de Transparencia Proactiva
		Naín Rodríguez Torres	Analista B	
24	Coordinación de Investigación y Capacitación	Norma Patricia González Arroyo	Jefe del Departamento de Capacitación	Capacitación
		Rosa María Zúñiga García	Analista B	
35	Coordinación de Investigación	Norma Patricia González Arroyo	Jefe del Departamento de Capacitación	Campañas de difusión

	y Capacitación	Rosa María Zúñiga García	Analista B	
36	Coordinación Administrativa	Erik Negrón Romero	Coordinador Administrativo	Registro de Asistencia del Personal del Instituto
		Bryan Baldomero Romero Valladares	Jefe de Recursos Humanos	
37	Coordinación Administrativa	Erik Negrón Romero	Coordinador Administrativo	Elaboración y Control de Contratos con Proveedores de Bienes y Servicios al Instituto
		Juan Antonio Color Vázquez	Subcoordinador de Finanzas	
		Esmeralda Saldaña Díaz	Analista B	
38	Coordinación Administrativa	Erik Negrón Romero	Coordinador Administrativo	Permisos al Personal del Instituto para Ausentarse
		Bryan Baldomero Romero Valladares	Jefe de Recursos Humanos	
39	Coordinación Administrativa	Erik Negrón Romero	Coordinador Administrativo	Cálculo y Pago de Finiquitos y Liquidaciones al Personal del Instituto
		Juan Antonio Color Vázquez	Subcoordinador de Finanzas	
		Bryan Baldomero Romero Valladares	Jefe de Recursos Humanos	

40	Coordinación Administrativa	Erik Negrón Romero	Coordinador Administrativo	Elaboración y Control de los Expedientes del Personal del Instituto
		Bryan Baldomero Romero Valladares	Jefe de Recursos Humanos	
41	Coordinación Administrativa	Erik Negrón Romero	Coordinador Administrativo	Registro del Personal del Instituto y Deducciones Correspondientes ante el IMSS
		Bryan Baldomero Romero Valladares	Jefe de Recursos Humanos	
		Martha Elisa Morales Solorio	Analista A	
42	Coordinación Administrativa	Erik Negrón Romero	Coordinador Administrativo	Cálculo y Pago de Impuestos Retenidos al Personal del Instituto
		Juan Antonio Color Vázquez	Subcoordinador de Finanzas	
		Roxana Espinoza Acosta	Analista A	
43	Coordinación Administrativa	Erik Negrón Romero	Coordinador Administrativo	Elaboración, Timbrado y Pago de Nómina del Personal del Instituto
		Bryan Baldomero Romero Valladares	Jefe de Recursos Humanos	
44	Coordinación Administrativa	Erik Negrón Romero	Coordinador Administrativo	Elaboración de Matriz de Percepciones y

		Bryan Baldomero Romero Valladares	Jefe de Recursos Humanos	Deducciones del Personal del Instituto
		Roxana Espinoza Acosta	Analista A	
45	Coordinación Administrativa	Erik Negrón Romero	Coordinador Administrativo	Pago a Proveedores del Instituto
		Fernando Villicaña Martínez	Analista B	
46	Coordinación Administrativa	Erik Negrón Romero	Coordinador Administrativo	Resguardo y Control de Bienes Propiedad del Instituto
		Jesús Castillo Gutiérrez	Analista B	
		Israel Hernández Maldonado	Analista B	
47	Coordinación Administrativa	Erik Negrón Romero	Coordinador Administrativo	Coordinación y Supervisión de los Programas de Servicio Social y Prácticas Profesionales en el Instituto
		Juan Antonio Color Vázquez	Subcoordinador de Finanzas	
48	Coordinación Administrativa	Erik Negrón Romero	Coordinador Administrativo	Pago de los Vales de Despensa del Personal del Instituto
		Bryan Baldomero Romero Valladares	Jefe de Recursos Humanos	
49	Coordinación Administrativa	Erik Negrón Romero	Coordinador Administrativo	

		Juan Antonio Color Vázquez	Subcoordinador de Finanzas	Cálculo y Pago de Viáticos del Personal del Instituto
		Esmeralda Saldaña Díaz	Analista B	

7. ANÁLISIS DE RIESGOS

De acuerdo con el artículo 31 fracción III, de la Legislación Local, el análisis de riesgos forma parte del documento de seguridad, como un medio para identificar las medidas de seguridad implementadas y, en relación con ello, las amenazas de vulneración en que se encuentran los datos personales.

El análisis sirve para identificar el riesgo inherente a los datos personales en el tratamiento a que son sometidos en el ejercicio de las funciones del Instituto, con respeto a la integridad de las personas.

La evaluación de riesgos de los datos personales forma parte de la serie de elementos que integran el documento de seguridad, cuyo propósito es garantizar la confidencialidad integridad y disponibilidad de los datos personales en posesión del Instituto.

Asimismo, para el análisis de riesgo se ha tomado en cuenta lo establecido en los Lineamientos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Michoacán de Ocampo, que en su artículo 46, define que para el cumplimiento al artículo 29 fracción IV de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, el responsable deberá realizar un análisis de riesgo de los datos personales tratados considerando lo siguiente:

I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;

II. El valor de los datos personales de acuerdo con su clasificación previamente definitiva y su ciclo de vida;

III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;

IV. Las consecuencias y negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida; y,

V. Los factores previstos en el artículo 28 de la Ley.

Bajo esta premisa, para analizar los riegos de los datos personales que son objeto de tratamiento por el Instituto, se aplicó un instrumento para clasificar los datos utilizados, a partir de la categorización existente en la ley:

1. DATOS DE IDENTIFICACIÓN O CONTACTO

Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, estado civil, firma, firma electrónica, cartilla militar, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), nombres de familiares, dependientes y/o beneficiarios.

2. DATOS PATRIMONIALES

Se refiere a los bienes muebles e inmuebles, ingresos y egresos, cuentas bancarias, seguros, fianzas, afores, historial crediticio, información fiscal, servicios contratados y afines.

3. DATOS SENSIBLES

Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y

morales, opiniones públicas y preferencia sexual.

De los anteriores, se identificaron principalmente dos categorías: datos de identificación y datos sensibles, en razón a que como datos patrimoniales se recaba número de cuentas bancarias, estados de cuenta, CLABE interbancaria, institución bancaria, facturas, beneficiarios, datos contenidos en declaraciones patrimoniales, y deducciones personales (ahorro voluntario, hipoteca, seguro de vida).

En un segundo momento se valoró la probabilidad y el impacto que pudiera tener para el titular, en caso de que llegara a materializarse uno o más factores (amenazas) durante el ciclo de vida de los datos sometidos a tratamiento (obtención, almacenamiento, transferencia, remisión, bloqueo y/o supresión).

Para el desarrollo del análisis, se detectaron cuatro tipos de amenazas previstas en la Ley:

1. Robo, extravío o copia no autorizada;
2. Uso, acceso o tratamiento no autorizado;
3. Daño, alteración o modificación no autorizado;
4. Pérdida o destrucción no autorizada.

A partir de lo anterior, se consideró una probabilidad baja, media, alta o muy alta, de que la amenaza suceda en las distintas etapas del tratamiento y tipo de datos personales, tomando en consideración las afectaciones que podría sufrir el titular de los datos en caso de vulneración, misma que puede ser leve, moderada o grave.

En cuanto a la valoración del riesgo, que por el tipo de dato llevan a cabo las Unidades Administrativas en cada proceso del tratamiento de datos personales, en una escala del 0 al 4, se representa de la siguiente manera:

TIPO DE DATO	RIESGO INHERENTE	NIVEL DE RIESGO
Datos identificativos	Bajo	1
Datos laborales, patrimoniales, procedimientos administrativos	Medio	2
Datos de tránsito y movimientos migratorios; de salud, biométricos	Alto	3
Datos sensibles	Muy alto	4

Al riesgo inherente, es necesario sumarle el volumen de titulares contenidos en la base de datos, a saber:

NÚMERO DE TITULARES	NIVEL DE RIESGO
Menos de 100	Bajo
Menos de 1,000	Medio
Menos de 10,000	Alto
Más de 10,000	Muy alto

En ese tenor, para el análisis de riesgo, se identifican 7 Unidades Administrativas con las que cuenta el Instituto y que llevan a cabo el tratamiento de Datos Personales durante el desarrollo del tratamiento de datos personales.

La unidad administrativa con mayor estado de vulnerabilidad y riesgo de los datos personales en tratamiento es la Coordinación Administrativa, seguida en orden descendente por el Órgano Interno de Control.

Al respecto, hay que señalar además que la etapa del ciclo de vida (obtención, uso, almacenamiento, transferencia, bloqueo y eliminación) en la que

los datos personales se encuentran más vulnerables, es en el periodo de almacenamiento; mientras que el periodo que implica menor riesgo es el de bloqueo.

1. Obtención;
2. Uso;
3. Almacenamiento;
4. Transferencia;
5. Bloqueo;
6. Eliminación.

Las amenazas a las que se ven expuestos son básicamente:

1. Robo, extravío o copia no autorizada;
2. Uso, acceso o tratamiento no autorizado;
3. Daño, alteración o modificación no autorizado;
4. Pérdida o destrucción no autorizada.

Siendo la más alta, la de robo, extravío o copia no autorizada, en tanto que la de menor riesgo es daño, alteración o modificación no autorizada.

Finalmente, como parte del análisis, es posible establecer que el nivel de riesgo es mayormente medio, debido que se trabaja sobre todo con datos de identificación, en algunos casos con datos patrimoniales y se utilizan en menor cantidad de procesos datos sensibles. Además, los datos personales corresponden a menos personas, lo que reduce el nivel de riesgo y se mantienen a resguardo en computadoras personales con contraseña y en archiveros ubicados en las unidades administrativas.

De acuerdo con las funciones que se desempeñan en las unidades administrativas, el riesgo prevalece en el nivel medio con mayor porcentaje, tomando en consideración que de las 7 unidades administrativas que conforman este Instituto, se mantienen en el número 2 equivalente a nivel medio, por tratar datos identificativos, patrimoniales y sensibles en sus procesos. Solo Presidencia, Secretaría General y la Coordinación de Investigación y Capacitación se

encuentran en un nivel bajo, debido a que los datos que se solicitan para realizar el tratamiento son únicamente identificativos.

8. ANÁLISIS DE BRECHA

Las medidas de seguridad administrativas, físicas y técnicas que actualmente se aplican en el Instituto para mantener la confidencialidad e integralidad de la información, protegiendo los datos personales contra daño, pérdida, destrucción o alteración, así como evitar el uso, acceso o tratamiento no autorizado e impedir la divulgación no autorizada, son las siguientes:

A) MEDIDAS ADMINISTRATIVAS:

1. Diseño y desarrollo de un modelo de capacitación permanente en materia de la Legislación Local, impartido a quienes laboran en el Instituto;
2. Aplicación de estrategias de seguridad, para el resguardo de los expedientes, con observancia de criterios vinculados con el sistema de gestión documental;
3. Diseño y ejecución de formatos de entrada y salida de préstamo de documentos por parte del área encargada del archivo del IMAIP;
4. Diseño e implementación de una carta responsiva por parte del personal con acceso a sistemas de datos personales, acerca del deber de confidencialidad;
5. Previsión de reportes de incidencias, mediante la elaboración e implementación de los formularios correspondientes.

B) MEDIDAS FÍSICAS:

1. Protección de documentos e información resguardándolos en archivos físicos de trámite y concentración, asegurados con llave;
2. Disponer de instalaciones aseguradas con llave para mantener control

de acceso de personas a espacios de resguardo de información;
3. Aplicar la firma de cartas de confidencialidad con el personal que trata datos personales.

c) MEDIDAS TÉCNICAS:

1. Garantizar la seguridad de los datos personales, utilizando claves de usuario y contraseñas de manera individual evitando compartirlas, prestarlaso registrarlas a la vista de otras personas; incluir caracteres alfanuméricos y especiales, considerando que éstas sean fáciles de recordar, pero difíciles de descifrar por un tercero;
2. Cuando se detecte que la clave de usuario o contraseña haya sido vulnerada o utilizadas por un tercero, notificar de manera inmediata a la Subdirección de Informática, Desarrollo e Infraestructura de este Instituto, para lo conducente;
3. Siempre utilizar la cuenta de correo electrónico oficial para fines relacionados con las actividades laborales, evitando remitir datos personales;
4. Mantener los documentos electrónicos bajo la protección de contraseñas; en lugares físicos, dentro de cajones cerrados, bajo llave, a fin de restringir el acceso a los datos personales que se tienen a resguardo;
5. Evitar que en los equipos de impresión se dejen olvidados documentos que contengan datos personales.

9. CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS

Los sistemas tecnológicos del Instituto son básicos, por lo que no se aplican controles de identificación y autenticación de usuarios sofisticados. La medida que se implementa es el uso de contraseñas para el acceso a los equipos de cómputo, repositorios y cuentas de correo institucionales; mismas que son controladas por

la Subdirección de Informática, Desarrollo e Infraestructura.

10. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES

El IMAIP cuenta con un contrato de servicios con la empresa google, que provee de repositorios para el almacenar y respaldar la información, especialmente de aquellos equipos de cómputo que tratan los correos institucionales y la página web institucional, lo que posibilita los procedimientos de respaldo y recuperación de la información; además, en cada área, los respaldos de datos personales se llevan a cabo de acuerdo con las posibilidades identificadas de manera particular. En algunos casos se realizan respaldos en la nube de diferentes sistemas operativos, así como en discos duros y otros medios portátiles controlados y administrados por los responsables de cada tratamiento de datos personales.

11. PLAN DE CONTINGENCIA PARA LA PROTECCIÓN DE LA INFORMACIÓN DEL IMAIP

Clasificación de la contingencia:

Según sea el tipo de contingencia se le puede asignar un grado de afectación:

1. **Grado 1:** Son las más bajas que van desde fallas eléctricas, fallas en la conexión de internet y que pueden ser resueltas por el mismo personal del Instituto;
2. **Grado 2:** Requiere tanto el apoyo del personal del Instituto, así como de personal externo (ejemplo: en un incendio, apoyo de bomberos y protección civil);
3. **Grado 3:** Son contingencias que por su alcance pueden afectar severamente la operatividad del Instituto y se requiere además del apoyo externo.

Consideraciones Principales:

1. Se debe realizar una evaluación de riesgos;
2. Dentro de la implementación del plan de contingencia se debe contar con un responsable general quien guiará la implementación de éste, así como la toma de decisiones;
3. Se designe un encargado de cada área para que apoye en cualquier desastre que ocurra y genere la contingencia, capacitándolos para el manejo de éstas, como el uso de extintores, planes de evaluación, entre otros;
4. Es necesario hacer las pruebas previas del plan de contingencia para garantizar su funcionalidad en caso de siniestro (las pruebas generalmente se hacen en tiempo real y lo más aproximado a la realidad);
5. Reunión con las comisiones o brigadas de las áreas del Instituto (capacitación y evaluaciones);
6. Revisión del Plan e integración de las recomendaciones y decisiones adoptadas de acuerdo con las lecciones aprendidas del ejercicio;
7. Difusión del documento del plan de contingencia una vez aprobado.

Lugar alternativo de trabajo

En caso de algún desastre mayor (terremoto o incendio) que implique pérdidas estructurales, se plantea en algunos casos, la posibilidad de contar con un lugar alternativo de trabajo; los sitios alternos de trabajo pueden ser propios, de una entidad con la que haya acuerdo o reciprocidad, instalaciones alquiladas (se debe contar con presupuesto).

En caso de contar con un ambiente alterno debe contar con los siguientes recursos:

1. Mesas para monitores y teclados de los servidores principales;
2. Sillas;
3. Switches;
4. Router para la conexión a internet;
5. UPS;

6. Teléfono;
7. Extinguidor;
8. Útiles de oficina.

Medidas preventivas ante siniestros

Medidas de prevención y conservación de los archivos:

1. El archivo de concentración o histórico debe situarse en el primer piso del edificio (no sótanos);
2. Espacios con luz natural y sin humedad;
3. Los muebles de archivo deben garantizar la conservación de los documentos que guardan; los documentos deben guardar uniformidad;
4. Evitar archivar documentación cerca de aparatos eléctricos, las instalaciones eléctricas deben estar en buenas condiciones;
5. Los estantes de los archivos deben estar entre 10 y 15 cm del suelo (facilitan la limpieza y evita a su vez la acumulación de humedad y proliferación de plagas);
6. Todos los equipos eléctricos que estén en el archivo deben quedar apagados y desconectados durante la noche o cuando no se utilicen;
7. Se recomienda no colocar vasos con líquido que puedan derramarse fácilmente sobre los aparatos eléctricos.

INCENDIOS

Medidas preventivas en caso de incendios

1. Se recomienda tener un conocimiento básico de primeros auxilios;
2. Para la pronta detección de un incendio se debe contar con detectores de humo;
3. En caso de incendio no abrir puertas y ventanas, el aire es factor para la propagación del fuego;
4. Si se tienen almacenadas sustancias inflamables como gasolina, acetona, aguarrás, alcohol o tiner, se sugiere colocarlos en lugares ventilados y lejos

de las flamas, fuentes de calor y aparatos eléctricos (si no los necesita deséchelos preferentemente);
5. Si el incendio es pequeño, se procurará apagarlo mediante un extintor. Si el fuego es de origen eléctrico no se deberá intentar apagarlo con agua; y,
6. No sobrecargar los contactos eléctricos, desconectando los que no se utilicen.

Sobre el resguardo de la información en caso de incendio:

1. Respaldo de información en una zona segura de preferencia, donde el calor de un incendio no alcance los dispositivos, esto es en lugares, cercanos a los extintores (sugerencias para realizar el almacenamiento de la información: CD, disco duro, bases de datos, la nube únicamente si es segura);
2. Tener identificados los documentos con mayor relevancia para resguardarlos en una zona segura (como en una caja de seguridad o realizar la digitalización de éstos con resguardo en la nube).

Durante un incendio:

1. Ubicar los extintores, cerciorarse de saber usarlos y que éstos sean reutilizables;
2. Si detecta un incendio procure mantener la calma y repórtelo inmediatamente o presione alguna señal de alarma;
3. No abra puertas ni ventanas, el fuego se extiende con el aire;
4. Si es un incendio que no pueda controlar usted mismo llame a los bomberos;
5. No pierda tiempo buscando objetos personales y salga del inmueble lo antes posible;
6. Si hay gas o humo humedezca un trapo y cubra su nariz y boca;
7. Si existe una puerta que deba atravesar toque con precaución la perilla; si está caliente no la abra;
8. Si su ropa se enciende, tírese al piso y ruede lentamente.

Después del incendio:

Un técnico debe revisar las instalaciones de gas y electricidad antes de utilizarlas nuevamente.

TERREMOTO

El daño ocasionado por un terremoto puede dañar principalmente la estructura del edificio, es por ello que los datos almacenados se encuentran en discos duros, cd, usb, se tiene un respaldo inmediato que nos permitiría recuperar la información; dado el supuesto que los respaldos electrónicos se dañaran, si contamos con información en la nube, podremos tener acceso a ellos apenas se tenga conexión a internet, auxiliados de algún aparato electrónico que nos permita su consulta.

Medidas preventivas en caso de sismo

1. No colocar muebles, equipos o cajas que bloqueen las rutas y salidas de emergencia del archivo;
2. Contar con un teléfono celular de emergencia en caso de falla de líneas telefónicas fijas;
3. Contar con un plan de evacuación y realizar simulacros de manera cotidiana;
4. Tener a la mano una radio de baterías, linterna y los principales documentos personales;
5. Contar con un botiquín de primeros auxilios;
6. Si se tienen anaqueles, los objetos pesados se colocan al final;
7. Localizar los lugares seguros en cada oficina; bajo mesas sólidas y escritorios resistentes;
8. Ubicar los lugares peligrosos: ventanas donde los vidrios pueden estrellarse, libreros o muebles que podrían caerse en caso de sismo.

Durante un sismo

1. Mantener la calma y ubicarse en una zona segura;
2. Pararse bajo un marco de puerta con trabe o de espaldas a un muro de carga;
3. Adoptar posición fetal de cara al suelo, abrazándose usted mismo en un rincón; de ser posible protegerse la cabeza;
4. Alejarse de ventanas, espejos y objetos de vidrio, así como de objetos colgantes;
5. Retirarse de objetos calientes, libreros, gabinetes o muebles pesados;
6. Si se está en un edificio, evitar el uso de elevadores; si se va por la calle, evitar postes, árboles y ramas;
7. Si es posible cerrar llaves del gas, desconecte la alimentación eléctrica y no encender fuego.

Después de un Sismo

1. Si usted queda atrapado, conserve la calma y trate de comunicarse al exterior golpeando un objeto;
2. Evite pisar cables que hubieran quedado caídos o sueltos;
3. Encienda la radio para mantenerse informado (posibles réplicas);
4. En caso de visible daño estructural del edificio, debe ser evaluado por Protección Civil para evitar cualquier riesgo secundario;
5. Se deben revisar las instalaciones eléctricas y de gas principalmente para evitar un desastre secundario.

Inundaciones por lluvia

Medidas preventivas en caso de inundación

1. Es importante realizar la revisión y reparación de la hermeticidad de ventanas y puertas, por donde podría filtrarse el agua de la lluvia, así como impermeabilizar los techos en la temporada de lluvias esto para evitar goteras;

2. Evitar en lo posible colocar expedientes y/o documentos directamente sobre el piso;
3. Respetar, al menos, una altura de 10 a 15 cm de los archiveros;
4. Colocar barreras para el agua (cubrir los documentos con plásticos, cubetas o recipientes para las goteras) en la parte superior de los estantes dentro del espacio para el archivo;
5. Evacuar los documentos afectados hacia áreas ventiladas;
6. Inmediatamente colocar papel secante en cada hoja de los expedientes;
7. Si un documento se moja en su totalidad se puede realizar la congelación de éste para su recuperación; debe realizarlo preferentemente un especialista (restauración).

Durante una inundación

1. Desconectar servicios de luz, gas y agua;
2. Mantenerse alejado de árboles y postes de luz;
3. Evitar tocar o pisar cables eléctricos;
4. Cubrir con bolsas de plástico aparatos u objetos que puedan dañarse con el agua.

Después de la inundación

1. Se puede expulsar el agua con una bomba de achique con motor de combustión o eléctrico, si es que hay suministro; en caso de que no hubiere, mediante esponjas, baldes, recogedores, entre otros;
2. Desinfectar las áreas afectadas pisos, muros y mobiliarios rescatable, con agua, jabón y cloro para evitar inundaciones.

Si los documentos han sufrido daños y se encuentran mojados, se debe seguir el procedimiento de congelación para recuperarlos. A continuación, se describe este procedimiento para recuperar los documentos humedecidos.

1. Se introduce la obra en una bolsa de polietileno con cierre de cremallera o termo sellable. Es muy importante envolver el libro en plástico y reducir el volumen de aire para evitar la formación de condensación. Para que la

congelación se realice de forma correcta, se debe dejar un amplio espacio entre los libros;

2. La cámara de congelación debe alcanzar una temperatura de -20 °C. En un proceso acelerado de descenso de la temperatura, el tratamiento será más efectivo. La temperatura debe ser constante y el congelador no ha de formar hielo ya que se puede acumular humedad. Se recomienda que en el momento de aplicación combinada de los tratamientos de congelación y vacío para la desinfección de documentos. Se debe depositar la obra en la cámara de congelación hasta que esta haya alcanzado dicha temperatura para evitar la aclimatación de los organismos;
3. El tratamiento debe durar como mínimo 72 setenta y dos horas, dependiendo del grosor de la obra y la temperatura del congelador. No obstante, si es necesario, se puede alargar hasta un periodo de tres semanas;
4. La obra se ha de descongelar de forma paulatina sin ser extraída del envoltorio hasta alcanzar el equilibrio con la temperatura ambiente. Una vez descongelada y alcanzado el equilibrio, el envoltorio se puede retirar.

Robo

Robo común de equipos

En caso de robo a mano armada se sugiere contar con teléfonos de emergencia de diferentes dependencias, así como un botón de pánico por medio de una App instalada en el celular.

Huelga o manifestaciones

Manifestación o huelga:

Si el archivo tiene cerradura, asegúrese que quede bajo llave.

Amenazas informáticas

Medidas preventivas para amenazas informáticas

Es necesario contar con un inventario actualizado de los equipos de cómputo, impresoras, escáner, fotocopiadoras y tener contacto con proveedores de software, hardware, y medios de soporte.

1. Prevención de falla de los equipos: se debe procurar dar mantenimiento preventivo por lo menos dos veces al año, y contar con proveedores en caso de que se requiera algún reemplazo inmediato;
2. Los equipos pueden quedar dañados por fallas eléctricas, se requiere contar con estabilizadores/reguladores, en cada uno de los equipos principalmente en aquellos que su afectación implique la pérdida de información importante.

Hackeo informático:

Ante un evento de hackeo informático los pasos a seguir para mantener la seguridad de la información son los siguientes:

Cambiar contraseñas:

1. Debe tener al menos ocho caracteres;
2. No debe contener información personal como nombre real, nombre de usuario o incluso el nombre del Instituto;
3. Debe ser muy distinta a las contraseñas previas;
4. No debe contener palabras completas;
5. Debe contener caracteres de las cuatro categorías primarias: mayúsculas, minúsculas, números y caracteres especiales.

Mientras se está conectado a Internet el Hacker tendrá acceso a los archivos e información guardados en la computadora hackeada. Por lo que se debe **desconectar el cable de la red lo antes posible.**

Posteriormente:

1. Contactar al personal de soporte para que retire del aire la página;
2. Evalúe los daños causados: El experto debe evaluar qué información se perdió y cuál es la que se mantiene para restaurar el sitio lo antes posible.

Dentro de la seguridad informática se denomina plan de contingencia, a la definiciónde acciones a realizar, recursos a utilizar y personal a emplear en caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos informáticos o de transmisión de datos de este Organismo; es decir, es la determinación precisa del quién, qué, cómo, cuándo y dónde ocurrió; en el supuesto de producirse una anomalía en el sistema de información.

El plan de contingencia debe considerar todos los componentes del sistema: datos críticos, equipo lógico de base, aplicaciones, equipos físicos y de comunicaciones, documentación y personal. Además, debe contemplar también todos los recursos auxiliares, sin los cuales el funcionamiento de los sistemas podría verse seriamente comprometido: suministro de potencia, sistemas de climatización, instalaciones, entre otros.

Considerando que el IMAIP cuenta con sistema tecnológico no complejo, todo se deriva de las medidas de seguridad implementadas de manera específica en cada área.

Para contar con un sistema de seguridad más fortalecido, es necesario desarrollar el protocolo de actuación en caso de contingencia, que incluya:

1. Los reportes de vulneración;
2. Designación de personas encargadas de reportar la vulneración y de realizar la investigación para identificar posible causa y responsable;
3. Método de notificación a los titulares afectados; y,
4. Procedimientos para la recuperación de la información.

12. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DELOS DATOS PERSONALES

La destrucción y borrado de información es un tema de vital importancia para proteger la privacidad, confidencialidad, integridad y disponibilidad de la información y en particular de los datos personales; debe hacerse bajo procedimientos que garanticen que fueron eliminados en su totalidad y que no pueden ser recuperados y utilizarse de manera indebida.

Métodos Físicos

1. Trituración mediante corte cruzado o en partículas: cortar el documento de forma vertical y horizontal generando fragmentos diminutos, denominados "partículas", lo cual hace prácticamente imposible que se puedan unir;
2. Destrucción de los medios de almacenamiento electrónicos mediante desintegración, consistente en separación completa o pérdida de la unión de los elementos que conforman algo, de modo que deje de existir.

Métodos Lógicos Sobre-escritura:

Consiste en sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.

Lo anterior implica algunas acciones, entre las que podemos contar:

1. Capacitación al personal para acercarse al conocimiento de lo que son las técnicas para la supresión y el borrado seguro;
2. Diseño de un lineamiento para garantizar el proceso;
3. Adquisición de trituradoras para la destrucción de los documentos;
4. Implementación de herramientas digitales para:

a. Destrucción de medios de almacenamiento electrónicos;
b. Desmagnetización y sobre escritura de los equipos de cómputo.

13. PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

Conforme al análisis de brecha, es importante generar acciones que permitan la seguridad de la información, así como de su localización, para resolver de manera eficaz el acceso, rectificación, corrección u oposición de las personas titulares de lainformación; por lo que a continuación se presentan las actividades generales que se planea realizar:

1. Celebración de reuniones de trabajo con unidades administrativas a efecto identificar alternativas de solución técnicas, físicas y administrativas a desarrollar en el mediano y largo plazo;
2. Promover un sistema de gestión y administración de datos personales que permita centralizar mediante la identificación de datos por categorías, asociando los diversos tratamientos y procesos a las políticas de seguridad que resultan aplicables a cada caso, conforme a los estándares y mejores prácticas en la materia;
3. Elaborar un protocolo para la protección y el tratamiento de los datos personales;
4. Implementar mecanismos de divulgación y conocimiento de las políticas generales de seguridad y verificar de manera continua su cumplimiento;
5. Fortalecer los mecanismos de control de documentos e información en las distintas unidades administrativas, a efecto de evitar posibles vulneraciones.

14. MONITOREO DE LAS MEDIDAS DE SEGURIDAD

Como parte del programa de protección de datos personales, es importante la supervisión de las medidas de seguridad técnicas y físicas, como un elemento para la mejora continua, que permite definir nuevas formas de monitoreo, de acuerdo con las necesidades surgidas al interior del Instituto, como son:

1. Revisión y actualización permanente de las contraseñas utilizadas para resguardar los datos personales en equipos de cómputo;
2. Revisar de manera permanente el cumplimiento de protocolos implementados para la protección de los datos personales;
3. Vigilar que el ingreso de personas sea a través de los accesos correspondientes plenamente identificados.

15. PROGRAMA GENERAL DE CAPACITACIÓN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

La aplicación del Programa de Protección de Datos Personales en el Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales, requiere como factor esencial, la formación y sensibilización de las personas servidoras públicas que garantice la actualización y mejora continua del inventario de datos personales y la observancia de la normatividad vigente, a través de la temática siguiente:

1. Generalidades de la Ley de Protección de Datos Personales en Posesión de SujetosObligados del Estado de Michoacán de Ocampo;
2. Principios y deberes;
3. Sistema de Gestión, medidas de seguridad y acciones preventivas.

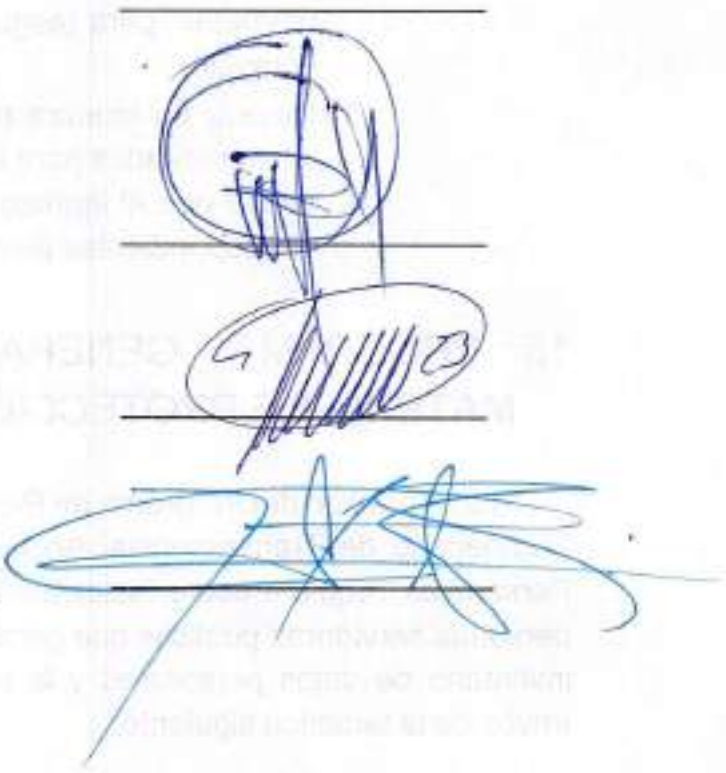
FIRMAN EL PRESENTE DOCUMENTO DE SEGURIDAD, LOS INTEGRANTES DEL COMITÉ DE TRANSPARENCIA DEL INSTITUTO MICHOACANO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

Omar Alexandro Negrón Villafán
Secretario General del IMAIP
Presidente del Comité de Transparencia

José Omar Reyes Herrera
Coordinador Jurídico del IMAIP
Secretario del Comité de Transparencia

Sarahí Esquivel Domínguez
Coordinadora de Investigación y Capacitación del IMAIP
Integrante del Comité de Transparencia

Erik Negrón Romero
Coordinador de Administración del IMAIP
Integrante del Comité de Transparencia



Las firmas que obran en la presente página forman parte del Documento Seguridad del Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales (IMAIP), aprobado en la Quinta Sesión Extraordinaria del Comité de Transparencia de este Instituto, mediante acuerdo: UNANIMIDAD/COMITÉ DE TRANSPARENCIA/ACTA 05-EXTRAORDINARIA/ACUERDO/02/10-10-2023, celebrada con fecha 10 diez de octubre del 2023 dos mil veintitrés y consta de 69 fojas incluida la presente.