PROYECTO DE ACUERDO DEL COMITÉ DE TRANSPARENCIA POR MEDIO DEL CUAL SE APRUEBA EL SISTEMA INTEGRAL DE SEGURIDAD DE DATOS PERSONALES DEL INSTITUTO ELECTORAL DE MICHOACÁN DOS MIL VEINTE

GLOSARIO

Código Electoral	Código Electoral del Estado de Michoacán de Ocampo
Comité de Transparencia	Comité de Transparencia del Instituto Electoral de Michoacán
Consejo General	Consejo General del Instituto Electoral de Michoacán
Constitución	Constitución Política de los Estados Unidos Mexicanos
Constitución Local	Constitución Política del Estado Libre y Soberano de Michoacán de Ocampo
Coordinación de Transparencia	Coordinación de Transparencia y Acceso a la Información del Instituto Electoral de Michoacán
DOF	Diario Oficial de la Federación
Instituto	Instituto Electoral de Michoacán
IMAIP	Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
Ley	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo.
Ley General	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
LGIPE	Ley General de Instituciones y Procedimientos Electorales

Lineamientos Generales	Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas.
Periódico oficial	Periódico Oficial del Gobierno Constitucional del Estado de Michoacán de Ocampo
Reglamento Interior	Reglamento Interior del Instituto Electoral de Michoacán

ANTECEDENTES

PRIMERO. Reforma constitucional en materia político-electoral. El 10 diez de febrero de 2014 dos mil catorce, se publicó en el Diario Oficial de la Federación, el Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia política-electoral.

SEGUNDO. Reforma constitucional en materia de transparencia. El 7 siete de febrero de 2014 dos mil catorce, se publicó en el Diario Oficial de la Federación, el Decreto por el que se reforma y adiciona el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos.

TERCERO. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. El 26 de enero de 2017 dos mil diecisiete, se publicó en el Diario Oficial de la Federación, el Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

CUARTO. Reforma local en materia electoral. El 25 veinticinco y 29 veintinueve de junio de 2014 dos mil catorce, se publicaron en el Periódico Oficial, los Decretos 316 y 323, respectivamente, en el primero se reformó la Constitución Local, y el segundo contiene el Código Electoral, en los que se armoniza la normativa a las disposiciones constitucionales y legales en materia político-electoral.

QUINTO. Expedición de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo. El 13 trece de noviembre d 2017 dos mil diecisiete, se publicó en el Periódico Oficial, la Ley de

Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo.

SEXTO. Reglamento para el funcionamiento de las Comisiones y de los Comités del Instituto Electoral de Michoacán. El 23 veintitrés de agosto de 2017 dos mil diecisiete, en Sesión Extraordinaria del Consejo General del Instituto, se aprobó el Acuerdo IEM-CG-25-2017 consistente en el *Reglamento para el funcionamiento de las Comisiones y de los Comités del Instituto Electoral de Michoacán,* mismo que entró en vigor al día siguiente de su publicación, es decir, el 24 veinticuatro de agosto de la anualidad en mención.

CONSIDERANDOS

PRIMERO. Atribuciones del Instituto. Los artículos 98 de la LGIPE, 98 de la Constitución Local, y 29 del Código Electoral, establecen que el Instituto es un organismo público autónomo depositario de la autoridad electoral, quien tiene a su cargo la organización, dirección y vigilancia de las elecciones y demás procesos que requieran consulta ciudadana en el Estado; que la certeza, imparcialidad, independencia, legalidad, objetividad, máxima publicidad, equidad y profesionalismo serán principios rectores en el ejercicio y desarrollo de esta función estatal.

Que, asimismo al tenor del artículo 34, fracciones I, II y XL, del Código Electoral, el Consejo General del Instituto tiene entre otras atribuciones vigilar el cumplimiento de las disposiciones constitucionales y las del Código Electoral; expedir el reglamento interior del Instituto y sus órganos internos, así como los que sean necesarios para el debido ejercicio de sus facultades y atribuciones; y; todas las demás que le confiere el Código y otras disposiciones legales.

De acuerdo con los artículos 1 y 6 de la Ley, el Instituto es sujeto obligado en materia de protección de datos personales, y como tal, garantizará la privacidad de los individuos y deberá velar porque terceras personas no incurran en conductas que puedan afectarla arbitrariamente.

SEGUNDO. Atribuciones del Comité de Transparencia. Que artículo 43 de la Ley General de Transparencia, así como el artículo 124 de la Ley, establecen que en cada sujeto obligado se integrará un Comité de Transparencia Colegiado e integrado por un mínimo de tres y máximo de cinco, quienes tendrán acceso a la

información para determinar su clasificación, conforme a la normatividad previamente establecida por los sujetos obligados para el resguardo o salvaguarda de la información.

Que de acuerdo con el artículo 79, fracción I, de la Ley, es atribución del Comité de Transparencia 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 Ley y en aquellas disposiciones aplicables en la materia.

TERCERO. Marco Jurídico. Que de conformidad con el Apartado A, fracciones I a III del artículo 6º de la Constitución, así como párrafo tercero, fracción I del artículo 8° de la Constitución Local, toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes; y toda persona, sin necesidad de acreditar interés alguno o justificar su utilización tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.

Que conforme al artículo 1, párrafos segundo, cuarto y quinto, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo son de aplicación y observancia directa para los sujetos obligados; su objeto es establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados, siendo éstos, en el ámbito estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Que de acuerdo con el artículo 3, fracción VIII, de la Ley, se consideran Datos Personales cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información.

Que el artículo 27 de la mencionada Ley, establece que con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, **el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales**, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Que asimismo **el artículo 29 de la misma Ley dispone las actividades que se deberán realizar para establecer y mantener las medidas de seguridad para la protección de los datos personales**, enlistando como mínimo las siguientes:

I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;

II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;

III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;

IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;

V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;

VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;

VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales; y,

VIII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

CUARTO. Justificación. Que el presente Proyecto de Acuerdo contiene el Documento del Sistema de Seguridad de Datos Personales del Instituto Electoral de Michoacán, con el cual se pretende dar cumplimiento a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, y proteger los Datos Personales en posesión del Instituto Electoral de Michoacán, describiendo en el mismo las medidas de seguridad que se deberán adoptar para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que se poseen.

Que en atención a lo dispuesto por el artículo 29 de la ley antes mencionada con detalle, el Sistema Integral de Seguridad de Datos Personales que se pone a consideración en el presente acuerdo esta integrado por seis anexos con los que se pretende cumplir con lo señalado, y se describen enseguida:

Anexo I. SISTEMA DE SEGURIDAD DE DATOS PERSONALES DEL INSTITUTO ELECTORAL DE MICHOACÁN. En este apartado se encontrarán las líneas básicas que comprende el Sistema de Seguridad que se propone, así como el detalle del objetivo que pretende lograr, a través de una serie de acciones mínimas, en cumplimiento a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados.

Para cumplir con todo ello se plantea una ruta de planeación, actuación y verificación, a fin de llevar un control de procesos que permita la claridad de todos los pasos y los sujetos que deben cumplir con ellos.

Anexo II. POLITICAS DE GESTIÓN DE DATOS PERSONALES. Como parte de las atribuciones conferidas al Instituto Electoral de Michoacán por parte de la Ley

de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, se tiene la atribución de establecer los principios generales que deben regir el tratamiento de los datos personales en cada una de las áreas que lo conforman, estableciendo los criterios mínimos específicos para el tratamiento de los datos personales, documento que deberá actualizarse periódicamente, a fin de conocer al menos semestralmente las condiciones y manejo de la información y los datos personales en cada una de las áreas que conforman este órgano.

En particular, las **Políticas de Gestión de Datos Personales** tiene la finalidad de garantizar el derecho a la protección de los datos de todas las personas físicas que se relacionan con el IEM, ya sea como parte del personal o de beneficiarios de su trabajo.

Todo lo anterior, observando los principios de legitimidad, licitud, lealtad, minimización, exactitud, limitación del plazo de conservación, integridad, confidencialidad, transparencia e información y responsabilidad proactiva.

- Principio de legitimidad, licitud y lealtad. Los datos personales deberán ser recogidos para uno o varios fines específicos y legítimos conforme a la legislación aplicable, en los casos que sea obligatorio deberá recabarse el consentimiento de los titulares de los datos, una vez informada la finalidad para la cual se recaba la información.
- Principio de minimización. Solo serán objeto de tratamiento aquellos datos personales que resulten estrictamente necesarios para la finalidad para la que se recojan o traten y adecuados a tal finalidad.
- Principio de exactitud. Los datos personales deberán ser exactos y estar actualizados. En caso contrario, deberán suprimirse o rectificarse.
- Principio de limitación del plazo de conservación. Los datos personales no se conservarán más allá del plazo necesario para conseguir el fin para el cual se tratan, salvo en los supuestos previstos legalmente.
- Principios de integridad y confidencialidad. Se deberá garantizar, mediante medidas técnicas, digitales u organizativas, una seguridad adecuada que los proteja del tratamiento no autorizado o ilícito y que evite su pérdida, su destrucción o que sufran daños accidentales.
- Principio de transparencia. El manejo y disposición de la información de cualquier tipo, y aquella que implique el tratamiento de datos personales,

siempre y en todos los casos debe cumplir con la característica de ser clara, accesible y comprensible en atención a que el sujeto interesado tenga clara la finalidad de la autorización o uso de sus datos.

- Principio de responsabilidad proactiva (rendición de cuentas). El Instituto deberá asumir como parte de su responsabilidad, y en los casos que la ley lo distinga las evaluaciones de riesgo como parte de sus actividades recurrentes, a fin de promover nuevas formas de protección y seguridad de los datos, que mitiguen o eviten los riesgos a los que se someten los datos tras su tratamiento.

Dicho lo anterior, se propone que todos quienes integran el Instituto Electoral sigan las directrices de lo que se plasma en el documento **Políticas de Gestión de Datos Personales (ANEXO II)** mismo que se deberá actualizar periódicamente en medida que se adopten nuevos criterios de protección de Datos.

ANEXO III.- ANALISIS DE RIESGO. Este apartado contiene el cuestionario que se aplicará a cada área del Instituto y cuyo interés es el de realizar el **análisis de riesgos** que permitirá reconocer cuáles son las medidas de seguridad que el instituto debe adoptar para garantizar la **confidencialidad, la disponibilidad y la integridad** de la información y de los sistemas de información que utilizan para tratar los datos personales.

Así pues, el objetivo principal del Análisis de Riesgos es el de garantizar un nivel de seguridad adecuado al riesgo del tratamiento de datos personales, es decir, tomar en consideración aquellos eventos negativos, teniendo en cuenta factores internos o externos, que provoquen, pérdida total o parcial, maltrato, reproducción no autorizada, extravío de los dispositivos que contienen la información.

La pretensión con esto será en primer lugar identificar activos, es decir, qué datos son recabados y quiénes los procesan; reconocer los riesgos, así como identificar las medidas que actualmente se aplican, mejorarlas, o en su caso crear instrumentos de protección en el uso, trámite y manejo de los datos personales, siendo este último producto consecuencia del análisis de riesgos de los datos mencionados.

ANEXO IV y V.- AUTORIZACIÓN PARA EL USO DE DATOS PERSONALES y COMPROMISO DE CONFIDENCIALIDAD DEL PERSONAL DEL INSTITUTO.- De acuerdo con la Ley de Protección de Datos Personales en Posesión de Sujetos

Obligados, relativo a la adopción de mejores esquemas de protección que tengan por objeto el ejercicio, tratamiento, transferencia, actualización y cumplimiento de normativa en materia de Protección de Datos se propone que cada integrante del Instituto en funciones y quienes ingresen al mismo firmen el consentimiento tácito de uso de datos personales y el compromiso de confidencialidad, a fin de que este órgano pueda garantizar el buen uso y conservación de la información que maneja.

Ambos documentos, que se pretende se integren al expediente laboral del personal, buscan blindar la privacidad de los titulares de la información, por lo que el Comité de Transparencia, una vez aprobado y acordado por sus integrantes, deberá hacerlo de conocimiento a las áreas necesarias a fin de que se ejecute la disposición.

ANEXO VI. - INVENTARIO DE DATOS PERSONALES. - Como parte de los principios, bases generales y procedimientos para garantizar el derecho de seguridad, protección y confidencialidad de los datos personales que maneja este Instituto, se hace necesario realizar el inventario de datos personales con la información básica del tratamiento de datos personales señalado por las direcciones y coordinaciones de este Instituto.

Esto permitirá cumplir con la obligación de crear un inventario de datos, que renueve y se verifique en función de la información real que cotidianamente se maneja en cada área del IEM.

Una vez que se tengan los datos de cada área, se proceda a realizar el inventario de datos personales y se pongan a consideración los programas, tareas, acciones o capacitaciones que se crean convenientes, asimismo para que el propio titular del área, de acuerdo a sus necesidades proponga las vías más idóneas para que en los casos concretos y con base en la experiencia se ejerzan acciones para la protección y conservación de los datos y la documentación a su cargo.

De este modo, aunado a las medidas de seguridad que se presentan en este proyecto, el documento también contiene el formulario que deberá llenar cada área y actualizar de forma constante con la finalidad de contar con un inventario de datos personales, así como el tratamiento que se les dará y el personal que estará involucrado en el manejo de estos, así como el análisis de riesgo de los mismos en posesión de cada área.

Con fundamento en los antecedentes y considerandos señalados, este Comité emite el siguiente:

PROYECTO DE ACUERDO DEL COMITÉ DE TRANSPARENCIA POR MEDIO DEL CUAL SE APRUEBA EL SISTEMA INTEGRAL DE SEGURIDAD DE DATOS PERSONALES DEL INSTITUTO ELECTORAL DE MICHOACÁN DOS MIL VEINTE

UNICO.- Se aprueba el Sistema de Seguridad de Datos Personales del Instituto Electoral de Michoacán, así como sus anexos.

TRANSITORIOS

PRIMERO. El presente acuerdo entrará en vigor a partir del día de su aprobación.

TERCERO. Se instruye a la Secretaría Técnica del Comité de Transparencia y Acceso a la Información, Mtra. Miryam Elizabeth Camacho Suárez, para que realice lo conducente a efecto de que haga del conocimiento el presente acuerdo al Encargado de Despacho de la Secretaría Ejecutiva del Instituto Electoral de Michoacán, con la finalidad de que lo informe a los integrantes del Consejo General y demás instancias competentes. -

Así lo aprobó por unanimidad de votos en Sesión Ordinaria de 28 de agosto de 2020, dos mil veinte, el Comité de Transparencia, integrado por el Consejero Electoral Presidente del Comité Lic. Luis Ignacio Peña Godínez y la Consejera Electoral Lcda. Irma Ramírez Cruz, ante la Secretaria Técnica del Comité que autoriza, Mtra. Miryam Elizabeth Camacho Suárez. DOY FE.

Lcda. Irma Ramírez Cruz
Consejera Electoral integrante provisional
del Comité de Transparencia

Lic. Luis Ignacio Peña Godínez
Consejero Electoral
Presidente
del Comité de Transparencia

Mtra. Miryam Elizabeth Camacho Suárez
Secretaria Técnica
del Comité de Transparencia

ANEXO I

SISTEMA DE SEGURIDAD DE DATOS PERSONALES DEL INSTITUTO ELECTORAL DE MICHOACÁN

El presente documento contiene las líneas básicas del sistema de seguridad de protección de datos personales sugerido por el INAI, mismo que tiene por objeto colaborar en la dirección, operación y control de forma sistemática y transparente de los procesos que son responsabilidad de los sujetos obligados, a fin de lograr con éxito sus actividades.

Por tanto, resulta importante observar acciones tendientes a garantizar la seguridad de los Datos Personales, debido a que:

- La protección de datos personales es un derecho humano.
- Ayuda a mitigar los efectos de una vulneración a la seguridad.
- Evita daños a la reputación e imagen de la organización.
- Evita sanciones a los servidores públicos.

Es importante resaltar que las políticas de seguridad y las medidas de protección de datos deben, en todos los casos, ir orientadas a cumplir con la legislación, ya que dentro de ésta se prevé de manera implícita la garantía de los derechos de la ciudadanía de mantener seguros sus Datos Personales y darle un tratamiento legítimo y correcto, cumpliendo con las siguientes acciones mínimas:

a) El cumplimiento de todos los principios que establece el artículo 12 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, así como su Reglamento y demás normativa aplicable;
b) Tratar y recabar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley y demás normativa aplicable (principio de licitud);
c) Sujetar el tratamiento de datos personales al consentimiento del titular, salvo las excepciones previstas por la Ley (principio de consentimiento);
d) Informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad (principio de información);
e) Procurar que los datos personales tratados sean correctos y actualizados (principio de calidad);

f) Suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y para las cuales se obtuvieron (principio de calidad);
g) Tratar datos personales estrictamente el tiempo necesario para propósitos legales, regulatorios o legítimos organizacionales (principio de calidad);
h) Limitar el tratamiento de los datos personales al cumplimiento de las finalidades previstas en el aviso de privacidad (principio de finalidad);
i) No obtener los datos personales a través de medios fraudulentos (principio de lealtad);
j) Respetar la expectativa razonable de privacidad del titular (principio de lealtad);
k) Tratar los menos datos personales posibles, y sólo aquéllos que resulten necesarios, adecuados y relevantes en relación con las finalidades previstas en el aviso de privacidad (principio de proporcionalidad);
l) Velar por el cumplimiento de estos principios y adoptar las medidas necesarias para su aplicación (principio de responsabilidad);
m) Establecer y mantener medidas de seguridad (deber de seguridad);
n) Guardar la confidencialidad de los datos personales (deber de confidencialidad);
o) Identificar el flujo y ciclo de vida de los datos personales: por qué medio se recaban, en qué procesos de la organización se utilizan, con quién se comparten, y en qué momento y por qué medios se suprimen;
p) Mantener un inventario actualizado de los datos personales o de sus categorías que maneja la organización;
q) Respetar los derechos de los titulares en relación con sus datos personales;
r) Aplicar las excepciones contempladas en la normativa en materia de protección de datos personales;
s) Desarrollar e implementar un Sistema Integral de Seguridad de Datos Personales de acuerdo con las políticas de gestión de datos personales, y
t) Definir las partes interesadas y miembros de la organización con responsabilidades específicas y a cargo de la rendición de cuentas para el SGSDP.

Para cumplir con dicho objetivo, se cumplirá con las acciones mínimas tales como las de planificar, hacer, verificar y actuar, a través del cual se dirigen y controlan los procesos o tareas.

Dicha ruta cumple con los criterios que este instituto también ha adoptado, de planear, hacer, verificar y actuar; y mediante los cuales se pretende la mejora permanente de los procesos, a fin de cumplir con los estándares más estrictos, en este caso, en materia de Transparencia y Acceso a la Información, en apoyo al ejercicio de su función y proyección del derecho universal de libertad de expresión y al consecuente derecho a buscar, recibir y difundir información e ideas de todo tipo y por cualquier medio, sin más limitaciones que las establecidas en el artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos.

Por tanto, los objetivos generales de este documento se traducen en las siguientes acciones:

1. Proveer un marco suficiente para la protección de los datos personales en posesión del Instituto Electoral de Michoacán.
2. Cumplir con las obligaciones de la Ley General, la Ley del Estado y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo.
3. Implementar mecanismos que permitan el adecuado y eficiente manejo de los datos personales en posesión de los sujetos obligados, en el Instituto Electoral.
4. Integrar un documento de seguridad del Instituto, para el tratamiento de datos.

Así pues, como parte de las atribuciones del Comité y la Coordinación de Transparencia, contenidas en la ley, y en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, que implican 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 y; supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad, es preciso señalar que este documento se elabora con la pretensión de contar con la participación de las diversas áreas del Instituto, mismas que fungen como enlaces de transparencia, las cuales son:

- Secretaría Ejecutiva
- Dirección Ejecutiva de Educación Cívica y Participación ciudadana
- Dirección Ejecutiva de Administración, Prerrogativas y Partidos Políticos
- Dirección Ejecutiva de Organización electoral

- Dirección Ejecutiva de Vinculación y Servicio Profesional Electoral
- Coordinación de Fiscalización
- Coordinación de Comunicación social
- Coordinación de Transparencia
- Coordinación de Igualdad de Género, No Discriminación y Derechos Humanos
- Coordinación de Archivos
- Coordinación Pueblos Indígenas
- Unidad Técnica del Voto de los Michoacanos en el extranjero
- Contraloría
- Secretaría Particular

ANEXO II

POLITICAS DE GESTIÓN DE LOS DATOS PERSONALES

De acuerdo con el artículo 29 de la Ley General de Transparencia, el Instituto electoral deberá realizar las acciones necesarias que permitan establecer y mantener las **medidas de seguridad para la protección** de los **datos personales**, así como su correcto uso, almacenamiento y procesamiento de estos.

Para lo anterior debe cumplir con los siguientes criterios mínimos específicos:

Medidas de seguridad generales

- ✓ Evita dejar documentos a la mano.
- ✓ Resguarda tus contraseñas en un lugar seguro.
- ✓ Usar archiveros con llave.

- ✓ Evita tirar documentos con datos personales sin triturar.
- ✓ No dejar documentos en la fotocopiadora.
- ✓ Evitar el reúso de papel con datos personales.
- ✓ No dejar a la vista datos personales

Medidas de seguridad físicas

- ✓ Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
- ✓ Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- ✓ Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización; y
- ✓ Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Medidas de seguridad técnicas

- ✓ Prevenir que el acceso a las bases de datos personales o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
- ✓ Generar un esquema de privilegios de acceso y tratamiento, para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
- ✓ Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware; y
- ✓ Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Medidas de seguridad procedimentales

- ✓ Utilizar el formato de testaje de datos cuando sea necesario
- ✓ Firmar la carta compromiso de confidencialidad del Instituto
- ✓ Firmar el documento de Cesión de Datos al ingresar como parte del personal del Instituto

ANEXO III

ANALISIS DE RIESGOS

El análisis de riesgos es un ejercicio que debe realizarse al momento de llevar a cabo el tratamiento de datos personales, e idealmente cada seis meses, la finalidad es establecer parámetros de seguridad que garanticen los derechos de protección de datos de los posibles afectados, de ahí que en este documento se intente identificar los riesgos y evitar las amenazas potenciales, tales como:

- La confidencialidad,
- La integridad,
- La disponibilidad,
- La eficacia de las medidas de seguridad adoptadas
- La licitud de los tratamientos de datos personales.

De este modo identificaremos el tipo y ubicación de los Datos Personales en posesión del Instituto. Para tales efectos comenzaremos por establecer claramente cuál es el tipo de información que es susceptible de considerarse en un Análisis de Riesgos Protección de Datos, área respectiva, señalando con un SI o un No si en su área se trabaja con cierto tipo de datos.

Categorías según su naturaleza:

TIPO DE INFORMACIÓN	SI/NO
a) Nivel estándar. Esta categoría considera **información de identificación**, contacto, datos laborales y académicos de una persona física identificada o identificable, tal como: nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo, lugar de trabajo,	

experiencia laboral, datos de contacto laborales, idioma o lengua, escolaridad, trayectoria educativa, títulos, certificados, cédula profesional, entre otros.	
b) Nivel sensible. Datos que permiten conocer la ubicación física de la persona, tales como la dirección física e información relativa al tránsito de las personas dentro y fuera del país. También son datos de nivel sensible aquéllos que permitan inferir el **patrimonio** de una persona, que incluye entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores y fianzas. Incluye el número de tarjeta bancaria de crédito y/o débito. Son considerados también los datos de **autenticación** con información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica y cualquier otro que permita autenticar a una persona. Dentro de esta categoría se toman en cuenta los **datos jurídicos** tales como antecedentes penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa. Finalmente, se contemplan los datos personales sensibles de la Ley, es decir, aquéllos que afecten a la esfera más íntima de su titular. Por ejemplo, se consideran sensibles los que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave a la integridad del titular.	
c) Nivel especial. Los que de acuerdo con su naturaleza y contexto pueden causar un daño excepcional a los titulares, por ejemplo: **Información adicional de tarjeta bancaria** que considera el número de la tarjeta de crédito y/o débito mencionado anteriormente en combinación con cualquier otro dato relacionado o contenido en la misma, por ejemplo, fecha de	

vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal (PIN). Los datos personales de titulares de alto riesgo, cuya profesión, oficio o condición los expone a una mayor probabilidad de ser atacados debido al beneficio económico o reputacional que su información representa para una persona no autorizada. Por ejemplo, líderes políticos, religiosos, empresariales, de opinión y cualquier otra persona que sea considerada como personaje público. Asimismo, se considera a cualquier persona cuya profesión esté relacionada con la impartición de justicia y seguridad nacional.	

Tabla I. Identificar el tipo de información que se maneja y conserva en cada una de las áreas. Esto permitirá tener claridad del tipo de información que se posee y crear medidas de seguridad y tratamiento de dichos datos. Este formato deberá ser respondido y devuelto a la Coordinación de Transparencia, con lo cual se integrará el análisis de riesgos respectivo.

Una vez identificados los activos, entendidos estos como valores del Instituto que requieren de ser protegidos, existen riesgos que deben ser prevenidos, disminuidos o, si fuera posible, erradicados, por tanto será de vital importancia que los responsables de las áreas identifiquen el riesgo que mayor impacto puede tener sobre los datos personales en su poder, con el fin de dar un panorama amplio y claro respecto de la situación en la que se encuentran y se tomen las medidas necesarias de control para incrementar la seguridad de los mismos.

DATOS PERSONALES	**NIVEL**	**APLICA/NO APLICA**
Información adicional al número de tarjeta bancaria	Especial	
Ubicación física	Sensible	
Patrimonio	Sensible	
Autenticación	Sensible	
Jurídicos	Sensible	
Salud, creencias, opiniones políticas	Sensible	
Identificación y contacto	Estándar	

Tabla II. La finalidad de esta gráfica es dar claridad y precisión respecto de la clasificación en la que se encuentra el tipo de información que posee el sujeto obligado por área, lo cual le permitirá elaborar un semáforo de riesgo de la información de uso.

A partir del diagnóstico anterior, podremos verificar si es exigible al instituto establecer medidas de seguridad adicionales a las existentes o si, por el contrario, el estado actual de la custodia de los Datos Personales permite que sean suficientes las medidas de protección y en consecuencia el cumplimiento con la ley vigente en la materia.

De este modo, el Instituto como responsable deberá establecer y mantener las medidas de seguridad:

- Administrativas
- Físicas
- Técnicas
- Legales

Para evitar:	Y garantizar:
× Daño	× Confidencialidad
× Pérdida,	× Integridad
× Alteración,	× Disponibilidad
× Destrucción o	
× Uso, acceso o tratamiento no autorizado,	

Visto lo anterior y habiendo hecho una detallada observación de las potenciales amenazas les solicitamos que a continuación nos compartan lo que en sus áreas se trabaja respecto de las medidas de seguridad en el uso y posesión de datos personales:

DATOS PERSONALES	**MEDIDAS DE SEGURIDAD EXISTENTES**	**MEDIDAS DE SEGURIDAD EXISTENTES QUE OPERAN CORRECTAMENTE**	**MEDIDAS DE SEGURIDAD FALTANTES (favor hacer la propuesta conveniente al área y uso de información)**
Información adicional al número de tarjeta bancaria			

Ubicación física			
Patrimonio			
Autenticación			
Jurídicos			
Salud, creencias, opiniones políticas			
Identificación y contacto			

TIPOLOGÍA DE DATOS

¿En tu área se trata con Datos Personales?

- ☐ SI
- ☐ NO

FINALIDADES DEL TRATAMIENTO

¿Los datos de cuántos sujetos van a ser objeto de protección de datos?

- ☐ 0 a 100
- ☐ 101 a 1000
- ☐ 1001 a 10,000
- ☐ 10,001 a más

Carácter de la información que tiene trámite en tu área

- ☐ Datos especialmente protegidos
- ☐ Datos de autenticación
- ☐ Datos económicos, financieros y de seguro
- ☐ Características personales
- ☐ Circunstancias sociales
- ☐ Datos académicos y profesionales
- ☐ Detalles de empleo
- ☐ Información comercial
- ☐ Transacciones de bienes o servicios
- ☐ Otro especifique_____

Duración del tratamiento

Instantáneo
Días
Semanas
Meses
Años

Cobertura de los datos a los que se da tratamiento

- ☐ Locales
- ☐ Regionales
- ☐ Nacionales
- ☐ Internacionales

La finalidad del uso de los datos es:

- ☐ Monitorizar
- ☐ Observar
- ☐ Trámite
- ☐ Estadístico
- ☐ Referencial
- ☐ Identificación
- ☐ Judicial
- ☐ Otro especifique _____

¿Los información que se recaban con la finalidad de tratar datos especialmente protegidos en tema de ...?

- ☐ Ideología u opiniones políticas
- ☐ Afiliación sindical
- ☐ Religión u opiniones religiosas
- ☐ Creencias filosóficas
- ☐ Origen étnico o racial
- ☐ De salud
- ☐ Vida u orientación sexual
- ☐ Violencia de género o maltrato
- ☐ Datos biométricos
- ☐ Genéticos
- ☐ Para fines policiales o procedimientos judiciales
- ☐ Condenas o delitos penales

¿El tratamiento implica contacto con los titulares de los datos personales?

- ☐ Si
- ☐ No

¿Se utilizan datos personales de algún grupo vulnerable? Menciónalo

- ☐ Si
- ☐ No

¿los datos personales que se recaban se utilizan para tomar alguna decisión?

- ☐ Si
- ☐ No

¿La información que recaba y procesa implica compartirla con otras áreas o entidades?

- ☐ Si
- ☐ No

¿Este tratamiento podría implicar perdida o alteración de la información?

☐ Si
☐ No

¿Implementa alguna medida de seguridad para las bases de datos personales en su poder?

☐ Si
☐ No

En caso de haber contestado a la pregunta anterior con un sí, describa las medidas de seguridad que implementa actualmente:

¿Han sucedido incidentes con la información contenida en las bases de datos personales, tales como, perdida, robo, alteración, etc.?

☐ Si
☐ No

En caso de haber contestado con un Si, describa los incidentes que han sucedido:

¿Se implementaron acciones correctivas después de los hechos?, descríbalas en caso de haber implementado alguna.

¿Se utiliza documentación en papel para tratar los datos personales?

- ☐ Si
- ☐ No

¿Qué medidas de conservación y/o resguardo se utilizan? Alguno otro, menciónalo

- ☐ En escritorio
- ☐ Bajo llave
- ☐ Se destruye al ser utilizada
- ☐ Se realiza un registro y se guarda
- ☐ Se transcribe y se guarda en electrónico

¿Interviene alguien ajeno al instituto en el tratamiento de los datos? Si, menciónalo

- ☐ Si
- ☐ No

¿El tratamiento de los Datos Personales en su área implica que un número elevado de personas intervenga?

- ☐ Si
- ☐ No

¿En el periodo que comprende los seis meses previos a esta fecha se ha implementado algún mecanismo técnico, humano o material nuevo que permita la salvaguarda de la información y los datos personales?

Cuando se depura información de las bases de datos personales, ¿lo hace con apego alguna norma?

- ☐ Si
- ☐ No

¿Qué procedimiento o protocolo utiliza para depurar las bases de datos personales físicos?

¿Qué procedimiento o protocolo utiliza para depurar las bases de datos personales electrónicos?

Este cuestionario pretende recoger las necesidades de cada área en materia de protección de datos, si existe alguna inquietud y/o propuesta relativa a este tema te solicitamos lo señales enseguida.

ANEXO IV

AUTORIZACIÓN PARA EL USO DE DATOS PERSONALES

Estimado/a_____

Con base en lo aprobado en el acuerdo IEM-CT-02/2020 y la intención de mantenerle informado del tratamiento que realizamos de sus datos personales, garantizándoles la protección de éstos conforme a la normativa vigente, le informamos que:

Los Datos Personales recogidos en su contrato y todos aquellos facilitados por usted han sido incorporados a su respectivo expediente, que se conserva con la finalidad de gestionar su relación con el Instituto.

De igual forma y con la intención de cumplir con todas las responsabilidades administrativas y fiscales, sus datos son compartidos con las entidades que la ley exige, en cumplimiento de la normativa laboral, de Seguridad Social y tributaria, por lo que, en caso de oponerse a este tratamiento de sus datos, deberá expresarlo tácitamente, ya sea mediante documento por escrito, o bien en este documento.

- ☐ Me doy por enterado y consiento que mis Datos Personales sean guardados en el expediente del contrato laboral y en su caso cedidos por el Instituto a las entidades que sean necesarias para el cumplimiento de la normativa laboral, a la Seguridad Social, Tributaria o administrativa.

Le solicitamos que en caso de alguna modificación en sus datos le comunique al Instituto por cualquiera de las vías puestas a su disposición, con la finalidad de mantener su información actualizada.

Es preciso recordarle que, en cualquier caso, queda a salvo su derecho de Acceder, Rectificar, Cancelar u Opositar los datos incluidos en el expediente que se conserva en el Instituto.

Morelia, Michoacán a _____ de _____ de 202____.

Nombre y firma del trabajador .____

ANEXO V

COMPROMISO DE CONFIDENCIALIDAD DEL PERSONAL DEL INSTITUTO

En _____ a _____ de _____ de 202 ___.

De acuerdo la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados, relativo a la adopción de mejores esquemas de protección que tengan por objeto el ejercicio, tratamiento, transferencia, actualización y cumplimiento de normativa en materia de Protección de Datos, establecido en el artículo 68 y 77, le informamos que:

Sus datos pasarán a formar parte de un fichero titularidad del Instituto Electoral del Estado de Michoacán, con domicilio en Bruselas 118, colonia Villa Universidad.

Y la finalidad del uso de los datos señalados serán:

Recursos Humanos: desarrollar, mantener, cumplir y controlar su actividad, y dar cumplimiento a las obligaciones y funciones del departamento de Recursos Humanos relativas a las actividades de formación, control de asistencia al trabajo,

formalización de las nóminas, deberes en materia de prevención de riesgos laborales, así como la gestión de canales de comunicación/denuncias implementados por la entidad de conformidad con requisitos previstos en las normativas en materia de cumplimiento vigentes.

Derechos de imagen: utilización de su imagen para la elaboración de publicaciones internas, y para su utilización con finalidades de promoción del voto o la finalidad específica del área que coordina, así como a la publicación de su CV e información de su trayectoria profesional en nuestra página oficial.

Puede ejercer sus derechos de Acceso, Rectificación, Cancelación y Oposición, así como revocar su autorización para el uso de sus imágenes.

Con la intención de cumplir con lo dispuesto en la normativa mencionada, le informamos que bajo ningún concepto usted debe utilizar ni incorporar a los sistemas informáticos y archivos documentales de este Instituto la información de carácter personal o empresarial a la que haya tenido acceso durante el desempeño de sus tareas o funciones en otras entidades, cuando ello pueda implicar la vulneración de las legislaciones anteriormente mencionadas, de igual modo no podrá extraer información de este órgano hacía otras, con la finalidad de favorecerse con el manejo de dicha información.

En cumplimiento de la legislación anteriormente mencionada, usted asume el compromiso de guardar secreto profesional respecto de los datos personales y cualquier otra información a la que tenga acceso con el motivo de las funciones asignadas, aún después de finalizar la relación laboral.

Asimismo, como parte del personal del Instituto se compromete a cumplir las normas internas de seguridad que permitan el desarrollo de sus funciones, así como el uso de los equipos informáticos, correo electrónico y demás aplicaciones a las que va a tener acceso; tiene además la responsabilidad y el deber de realizar los programas formativos y aplicar los procedimientos y normas que se le comuniquen a tal efecto.

Por último, en virtud de las responsabilidades que implica la protección de datos y las que se tienen como consecuencia de la entrada en vigor de la Ley General de Archivos, el integrante se compromete a aplicar y tener en consideración los protocolos y procedimientos que establezca el Instituto, a través de su Consejo

General, la Presidencia, las áreas de Acceso a la Información, Archivos o Administración en el ámbito de protección de datos de carácter personal en los términos previstos en este documento.

Ante cualquier duda, incidente, o imposibilidad de aplicación adecuada de los procedimientos y normas lo comunicará al responsable que se le designe en cada uno de los supuestos tal como quede establecido a tal efecto.

Nombre y firma de la o el interesado

ANEXO VI

INVENTARIO DE DATOS PERSONALES

Marcar con una **X** los datos personales que existen y son necesarios o que existen más no son necesarios en los procesos administrativos de su Unidad Administrativa.

Datos personales recabados	**Existente**	**Necesario**	**No necesario**
Datos de identificación y contacto			
Nombre			
Estado Civil			
Registro Federal de Contribuyentes (RFC)			
Clave Única de Registro de Población (CURP)			
Lugar de nacimiento			

Fecha de nacimiento			
Nacionalidad			
Domicilio			
Teléfono particular			
Teléfono celular			
Correo electrónico			
Firma autógrafa			
Firma electrónica			
Edad			
Fotografía			
Referencias personales			
Datos sobre características físicas			
Color de piel			
Color de cabello			
Señas particulares			
Estatura			
Peso			
Cicatrices			
Tipo de sangre			
Datos biométricos			
Imagen del iris			
Huella dactilar			
Palma de la mano			
Datos laborales			
Puesto o cargo que desempeña			
Domicilio de trabajo			
Correo electrónico institucional			
Teléfono institucional			
Referencias laborales			
Información generada durante los procedimientos de reclutamiento, selección y contratación			

Datos personales recabados	Existente	Necesario	No necesario
Experiencia/Capacitación laboral			
Datos académicos			
Trayectoria educativa			
Títulos			
Cédula profesional			
Certificados			
Reconocimientos			
Datos migratorios			
Entrada al país			
Salida del país			
Tiempo de permanencia en el país			
Calidad migratoria			
Derechos de residencia			
Aseguramiento			
Repatriación			
Datos patrimoniales y/o financieros			
Bienes muebles			
Bienes inmuebles			
Información fiscal			
Historial crediticio/Buró de crédito			
Ingresos			
Egresos			
Cuentas bancarias			
Números de tarjetas de crédito			
Información adicional de tarjeta (fecha de vencimiento, códigos de seguridad, datos de banda magnética, pin)			
Seguros			
Afores			

Datos sobre pasatiempos, entretenimiento y diversión			
Pasatiempos			
Aficiones			
Deportes que practica			
Juegos de su interés			
Datos legales			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)			
Otros datos personales (mencionar)			
Datos personales recabados	**Existente**	**Necesario**	**No necesario**
Datos personales sensibles			
Datos sobre la ideología			
Posturas religiosas/ ideológicas/morales/ filosóficas			
Pertenencia a un partido/Posturas políticas			
Pertenencia a un sindicato			
Datos de salud			
Estado de salud físico presente, pasado o futuro			
Estado de salud mental presente, pasado o futuro			
Información genética			
Datos sobre vida sexual			
Preferencias sexuales			
Prácticas o hábitos sexuales			
Datos de origen étnico o racial			

Pertenencia a un pueblo, etnia o región			
Otros datos personales (mencionar)			