

**DICTAMEN DEL PLENO DEL INSTITUTO MICHOACANO DE TRANSPARENCIA,  
ACCESO A LA INFORMACION Y PROTECCION DE DATOS PERSONALES,  
CORRESPONDIENTE A LA EVALUACION DE IMPACTO EN LA PROTECCIÓN DE  
DATOS PERSONALES RESPECTO DEL CARÁCTER INTENSIVO O RELEVANTE EN  
EL TRATAMIENTO DE DATOS PERSONALES QUE SE EFECTUARÁ EN EL  
SISTEMA DE SERVIDORES PÚBLICOS QUE INTERVENGAN EN PROCEDIMIENTOS  
DE CONTRATACIONES PÚBLICAS, DE LA PLATAFORMA DIGITAL ESTATAL DEL  
SISTEMA ESTATAL ANTICORRUPCIÓN, NÚMERO DICT/EI/02/2021.**

**ANTECEDENTES:**

En fecha 13 de noviembre de 2017 se publicó en el Periódico Oficial del Estado de Michoacán de Ocampo, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, la cual es reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, así como del artículo 8 de la Constitución Política del Estado Libre y Soberano de Michoacán de Ocampo en materia de protección de datos personales en posesión de sujetos obligados.

En fecha 23 de enero de 2018 se publicó en el Diario Oficial de la Federación el Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, emitido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

En fecha 5 de noviembre de 2019 se publicó en el Periódico Oficial del Gobierno Constitucional del Estado de Michoacán de Ocampo el Acuerdo del Comité Coordinador



del Sistema Estatal Anticorrupción por medio del cual se emiten las Bases para el Funcionamiento de la Plataforma Digital Estatal.

En fecha 13 trece de julio de 2021 dos mil veintiuno se notificó al Instituto Michoacano de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, el oficio número SEA-SE-ST-1020/2021, suscrito por la Secretaría Técnica de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, para efectos de presentar la **EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES, RESPECTO AL CARÁCTER INTENSIVO Y RELEVANTE DEL TRATAMIENTO DE DATOS PERSONALES EN EL SISTEMA DE SERVIDORES PÚBLICOS QUE INTERVENGAN EN PROCEDIMIENTOS DE CONTRATACIONES PÚBLICAS, DE LA PLATAFORMA DIGITAL ESTATAL, DE CONFORMIDAD CON LO ESTABLECIDO EN LAS DISPOSICIONES ADMINISTRATIVAS DE CARÁCTER GENERAL PARA LA PRESENTACIÓN Y VALORACIÓN DE EVALUACIONES DE IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES**, de conformidad con lo que establece el artículo 10 de las *Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales*, emitidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, a efecto de que la evaluación presentada sea valorada y se emita, en su caso, el dictamen correspondiente, conforme lo establecen los artículos 72 y 73 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo.

#### CONSIDERACIONES:

El artículo 97 de la Constitución Política del Estado Libre y Soberano de Michoacán de Ocampo establece que, el Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales es un organismo autónomo,



especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley; se registrará por la ley en materia de transparencia y acceso a la información pública y por los principios de certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad.

De la misma manera, el artículo 97 de la Constitución Local establece que el Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales, tendrá competencia para conocer de los asuntos relacionados con el acceso a la información pública y la protección de datos personales de cualquier autoridad, entidad, órgano u organismo que forme parte de alguno de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicatos que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal.

Conforme lo que establece el artículo 3, fracción XV, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, la evaluación de impacto en la protección de datos personales es el documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normatividad aplicable.



El artículo 70 de la referida Ley establece que, cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con esta Ley o la Ley General impliquen el tratamiento intensivo o relevante de datos personales, deberá realizar una Evaluación de Impacto en la protección de datos personales, y presentarla ante el Instituto, el cual podrá emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.

El contenido de la evaluación de impacto a la protección de datos personales será determinado por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales de acuerdo con lo previsto en la Ley General de la materia.

Lo anterior se cumple con la remisión a este Instituto de la **EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES, RESPECTO AL CARÁCTER INTENSIVO Y RELEVANTE DEL TRATAMIENTO DE DATOS PERSONALES EN EL SISTEMA DE SERVIDORES PÚBLICOS QUE INTERVENGAN EN PROCEDIMIENTOS DE CONTRATACIONES PÚBLICAS, DE LA PLATAFORMA DIGITAL ESTATAL, DE CONFORMIDAD CON LO ESTABLECIDO EN LAS DISPOSICIONES ADMINISTRATIVAS DE CARÁCTER GENERAL PARA LA PRESENTACIÓN Y VALORACIÓN DE EVALUACIONES DE IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES**, por parte de la Secretaria Técnica de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción.

El artículo 71 del mismo ordenamiento legal establece que, para efectos de esta Ley se considerará que se está en presencia de un tratamiento intensivo o relevante de datos personales cuando:



- I. Existan riesgos inherentes a los datos personales a tratar;
- II. Se traten datos personales sensibles; y,
- III. Se efectúan o pretendan efectuar transferencias de datos personales.

El artículo 72 de la multicitada ley establece que, los sujetos obligados que realicen una Evaluación de impacto en la protección de datos personales, deberán presentarla ante el Instituto, treinta días anteriores a la fecha que se pretende poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, ante el Instituto a efecto de que emita las recomendaciones no vinculantes correspondientes.

El artículo 73 establece que, el Instituto emitirá, de ser el caso, recomendaciones no vinculantes sobre la Evaluación de impacto en la protección de datos personales presentado por el responsable.

El plazo para la emisión de las recomendaciones a que se refiere el párrafo anterior será dentro de los treinta días siguientes contados a partir del día siguiente a la presentación de la evaluación.

El artículo 84, fracción XIII de la referida Ley establece que es atribución del Instituto emitir, en su caso, las recomendaciones no vinculantes correspondientes a la Evaluación de impacto en la protección de datos personales que le sean presentadas.

Por lo anterior, este Pleno se avocará al estudio, análisis y emisión, en su caso, de las recomendaciones no vinculantes correspondientes, acerca de la Evaluación de Impacto presentada por la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, en los términos del párrafo que antecede y de las disposiciones administrativas de carácter



general para la elaboración, presentación y valoración de impacto en la protección de datos personales, emitido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

En una primera etapa, este Pleno concluye que la Evaluación de Impacto **cumplió** con los requisitos previstos en los artículos 14, 15, 16, 17, 18, 19, 20, 21 y 22 de las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de impacto en la protección de datos personales, emitido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Lo anterior, en virtud de que la Evaluación de Impacto, en su presentación cumplió con las siguientes disposiciones:

- I. La descripción de la política pública, programa, sistema o plataforma informativa, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales que pretenda poner en operación o modificar;
- II. La justificación de la necesidad de implementar o modificar la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales;
- III. La representación del ciclo de vida de los datos personales a tratar;
- IV. La identificación, análisis y descripción de la gestión de los riesgos inherentes para la protección de los datos personales;
- V. El análisis de cumplimiento normativo en materia de protección de datos personales de conformidad con la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables;
- VI. Los resultados de las o las consultas externas, que en su caso, se efectúen;



- VII. La opinión técnica del oficial de protección de datos personales respecto del tratamiento intensivo o relevante de datos personales que implique la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología, en su caso, y
- VIII. Cualquier otra información o documentos que considere conveniente hacer del conocimiento del Instituto o los organismos garantes en función de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología, que implique un tratamiento intensivo o relevante de datos personales y que pretenda poner en operación o modificar.

Una vez concluido lo anterior, este Pleno emitirá la respectiva valoración de la Evaluación de Impacto en la Protección de Datos Personales presentada por la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, tal y como lo dispone el artículo 27 de las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de impacto en la protección de datos personales, emitido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en concordancia con lo que establece el artículo 73 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, por las siguientes razones y consideraciones:

**Valoración de la evaluación de impacto en la protección de datos personales.**

**Artículo 27.** El Instituto o los organismos garantes deberán valorar la evaluación de impacto en la protección de datos personales tomando en cuenta lo siguiente:

- I. Los objetivos generales y específicos que persigue la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales;



**SE CUMPLE**, en los términos siguientes:

**Objetivo general.**

El objetivo del Sistema Informático es permitir que los distintos usuarios tengan acceso a la información relacionada con los servidores públicos, que intervienen en procedimientos de contrataciones públicas, tanto en la tramitación, atención y resolución para la adjudicación de contratos, otorgamiento de concesiones, licencias, permisos o autorizaciones y sus prórrogas, así como en la enajenación de bienes muebles y aquéllos que dictaminan en materia de avalúos, de tal manera que sea información de apoyo a las autoridades competentes en sus funciones de prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos; ya sea de conocimiento público para la detección de posibles conflictos de interés.

**Objetivos específicos.**

- a) Contar con la información de las personas servidoras públicas que intervienen en procedimientos de contrataciones públicas, para prevención de posibles conflictos de interés.
- b) Proporcionar información en una sola herramienta tecnológica, para que las autoridades cumplan con sus atribuciones en materia de investigación y sanción de faltas administrativas o hechos de corrupción;
- c) Abonar a los trabajos que realiza el Comité Coordinador del Sistema Estatal Anticorrupción para el diseño de políticas públicas en materia de combate a la corrupción, así como su evaluación periódica, ajustes y modificaciones correspondientes.
- d) Generar datos estadísticos para la realización de estudios y diagnósticos en materia anticorrupción.



**II. Las razones o motivos que justifican la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, en función de las atribuciones o facultades del responsable que la normatividad aplicable le confiera;**

**SE CUMPLE**, en los siguientes términos:

## **APARTADO II**

### ***I. La justificación de la necesidad de implementar el Sistema Informático.***

*La implementación y puesta en operación del Sistema de Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, es una obligación que deriva de la legislación de la materia como se ha señalado en el Apartado I del presente documento.*

*En efecto, la Ley de Sistema Estatal establece en su artículo 47 la obligación del Comité Coordinador de implementar la Plataforma Digital Estatal, con apego a los lineamientos señalados por la federación, que permita cumplir con los procedimientos, obligaciones y disposiciones señaladas en la propia Ley y en la Ley de Responsabilidades Administrativas, atendiendo a las necesidades de accesibilidad de los usuarios.*

*Asimismo, el numeral de referencia dispone que el Comité Coordinador será el responsable de proporcionar la información necesaria al Comité Coordinador del Sistema Nacional Anticorrupción, para que sea integrada a la Plataforma Digital Nacional.*



Por otra parte, la finalidad del Sistema de los Servidores Públicos que Intervienen en Procedimientos de Contrataciones Públicas, acorde a lo dispuesto en el artículo 50 de la Ley del Sistema Estatal Anticorrupción, en relación con el artículo 43 de la Ley de Responsabilidades Administrativas para el Estado, y 45 de las Bases para el funcionamiento de la Plataforma Digital Estatal, emitidas por el Comité Coordinador del Sistema Estatal Anticorrupción e permitir que los distintos usuarios tengan acceso a la información relacionada con los servidores públicos que intervienen en procedimientos de contrataciones públicas, de tramitación, atención y resolución para la adjudicación de un contrato, otorgamiento de una concesión, licencia, permiso o autorización y sus prórrogas, así como en la enajenación de bienes muebles y aquellos que dictaminan en materia de avalúos, de tal manera que sea utilizada por los integrantes del Sistema Estatal Anticorrupción y autoridades competentes en sus funciones de prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos.

Adicionalmente, es pertinente señalar que actualmente, la información del Sistema de Servidores Públicos que Intervienen en Procedimientos de contrataciones públicas, se encuentra dispersa en diversos formatos, bases de datos o en registros físicos; cada uno con particularidades y reglas distintas, dificultando la integración, consulta y la interoperabilidad de los datos. El estándar para la Interoperabilidad de Datos del Sistema de los Servidores Públicos que Intervienen en Procedimientos de Contrataciones Públicas surge a partir de la necesidad de distribuir, comparar y analizar la información de una manera uniforme e interoperable.

Conforme a lo anterior, la SESNA ha conceptualizado a la Plataforma Digital Nacional como una herramienta que permitirá la consulta de información de las diferentes instituciones de los tres niveles de gobierno en un solo punto, sin tener el objetivo de concentrarla o resguardarla. En ese sentido, resulta necesario dotar a la PDN de



*mecanismos que le permitan interconectarse con los diversos sistemas de gobierno para consultar la información que resulte necesaria, sin importar la tecnología con la que dichos sistemas fueron desarrollados (i.e., lenguajes programación bases de datos, etc)*

*La PDN logrará la interoperabilidad técnica con los diversos sistemas que la integrarán a través de la creación de estándares de datos y mediante el uso de Interfaces de Programación de Aplicaciones o APIs (por sus siglas en inglés). Los estándares de datos permitirán homologar la manera en que la información se debe representar para su entrega a la PDN, mientras que las APIs serán el mecanismo que permitirá la comunicación entre sistemas a través de Internet. Las APIs son ampliamente usadas para el desarrollo de aplicaciones a gran escala. El uso de APIs permitirá que las instituciones conserven el control de sus datos, gestionando el acceso a los mismos mediante reglas y perfiles de usuario.*

*De este modo, la PDE se interconectará con la PDN a través de APIs, para la consulta de datos públicos a nivel nacional; en tanto que la información, en particular en el Sistema de Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, que nos ocupa, se ingresará o registrará por dos vías, atendiendo a la particular condición de cada una de los Órganos del Estado (los escenarios descritos en el Apartado XII).*

*Por otra parte, atendiendo a que la legislación en materia de transparencia establece que, el tratamiento de datos personales es cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionados con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales; es que se estima que el tratamiento de datos personales que efectúe la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, está justificado por finalidades*



concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable le confiere, como se ha señalado con anterioridad.

Además, las medidas de seguridad con las que cooperará el Sistema de Servidores Públicos Intervengan en Procedimientos de Contrataciones Públicas, se estima que son adecuadas para garantizar el derecho a la protección de datos personales de sus titulares, ya que la información se encuentra protegida con accesos restringidos al equipo servidor donde se resguardará, contraseñas de usuarios, cifrado de información pública y privada, así como el monitoreo permanente del comportamiento y funcionamiento del Sistema Informático.

Asimismo, se considera que las medidas físicas, administrativas y tecnológicas propuestas son necesarias para garantizar el derecho a la protección de datos, teniendo en cuenta que su implementación tiene como finalidad reducir los riesgos que conlleva el proceso de resguardo de datos personales. Por consiguiente, las medidas, son moderadas puesto que no restringen a los titulares el uso de sus datos, ni impiden que se les dé la difusión que por ley corresponde.

Las medidas de seguridad también son las más idóneas en función al mayor número de beneficios o ventajas, que perjuicios en el tratamiento y protección de los datos personales de los titulares, ya que como se viene mencionando a lo largo de la presente evaluación, se persiguen como objetivos o finalidades:

- a) Contar con la información de las personas servidoras públicas que intervienen en procedimientos de contrataciones públicas, para prevención de posibles conflictos de interés.
- b) Contar con la información relativa a las contrataciones celebradas por servidores públicos que integran los Órganos del Estado.



- c) *Proporcionar información en una sola herramienta tecnológica, para que las autoridades cumplan con sus atribuciones en materia de investigación y sanción de faltas administrativas o hechos de corrupción;*
- d) *Abonar a los trabajo que realiza el Comité Coordinador del Sistema Estatal Anticorrupción para el diseño de políticas públicas en materia de combate a la corrupción, así como su evaluación periódica, ajustes y modificaciones correspondientes.*
- e) *Generar datos estadísticos para la realización de estudios y diagnósticos en materia anticorrupción.*

*Además, son suficientes para asegurar la confiabilidad, integridad y confidencialidad de la información del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, como la tecnología utilizada, el resguardo en un servidor propio de la Secretaría Ejecutiva, accesos mediante usuarios y contraseñas específicos, con facultades también diferenciadas y específicas, entre otras que hayan sido descritas.*


**III. Las categorías de titulares, distinguiendo aquéllos que pertenezcan a grupos vulnerables en función de su edad; género; origen étnico o racial; estado de salud; preferencia sexual; nivel de instrucción y condición socioeconómica;**

**SE CUMPLE**, en los siguientes términos:


*De acuerdo con lo establecido en los artículos 3, fracción XXXI, de la Ley General de Protección de Datos, y 3, fracción VIII, de la Ley Local de Protección de Datos, el titular es la persona física a quien corresponden los datos personales.*



En virtud de lo anterior y una vez especificados los objetivos del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, de la Plataforma Digital Estatal, los titulares de los datos que almacenará y se actualizarán en el mismo son los siguientes:


- 
1. **Servidores públicos:** Información de los servidores públicos que intervengan en los procedimientos de contrataciones públicas, de tramitación, atención y resolución para la adjudicación de un contrato, otorgamiento de una concesión, licencia, permiso o autorización y sus prórrogas, así como en la enajenación de bienes muebles y aquellos que dictaminan en materia de avalúos; cuyos datos se inscribirán en el Sistema de los Servidores Públicos que intervengan en Procedimientos de Contrataciones Públicas, de la Plataforma Digital Estatal.
  2. **Superior inmediato:** Información del superior inmediato del servidor público que intervenga en los procesos descritos en el punto que antecede, que se inscribirá en el Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, de la Plataforma Digital Estatal.

#### IV. Los datos personales tratados y su volumen;



**SE CUMPLE**, en los términos siguientes:

#### **Datos de servidores públicos**



Los datos que administrará y actualizará el Sistema de Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas y que por tanto serán objeto de tratamiento, son los siguientes:



**DATOS DE REGISTRO CARACTERÍSTICAS DE LOS DATOS**

Ejercicio fiscal	<b>Datos públicos en el Sistema, para consulta de cualquier persona</b>
Tipo de procedimiento	
Ramo	
Institución	

**DATOS DE IDENTIFICACIÓN DEL  
SERVIDOR PÚBLICO**

**CARACTERÍSTICAS DE LOS DATOS**

Nombre(s) y apellidos	<b>Datos públicos en el Sistema, para consulta de cualquier persona.</b>
Registro Federal de Contribuyentes (RFC) con homoclave	<b>Datos no públicos en el Sistema, únicamente tendrán acceso a su consulta los servidores públicos designados para ello que deberán contar con un usuario y contraseña específico.</b>
Clave Única de Registro de Población (CURP)	
Género	

DATA

**DATOS DE LA DEPENDENCIA DONDE  
LABORA EL SERVIDOR PÚBLICO**

**CARACTERÍSTICAS DE LOS DATOS**

Nombre de la institución o dependencia a la que pertenece.	<b>Datos públicos en el Sistema, para consulta de cualquier persona.</b>
Siglas de la institución o dependencia a la que pertenece.	
Nombre del puesto del servidor público.	
Clave de la institución o dependencia a la que pertenece.	<b>Datos no públicos en el Sistema, únicamente tendrán acceso a su consulta los servidores públicos designados para</b>
Nivel o identificador del servidor público.	

/

0



	ello que deberán contar con un usuario y contraseña específico.
--	---

### Datos del superior inmediato

Los datos que contendrá y actualizará el Sistema de Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, respecto del superior del servidor público que interviene en procesos de contrataciones son los siguientes:

DATOS DEL SUPERIOR INMEDIATO	CARACTERÍSTICAS DE LOS DATOS
Nombre(s) y apellidos.	Datos no públicos en el Sistema, únicamente tendrán acceso a su consulta los servidores públicos designados para ello que deberán contar con un usuario y contraseña específico.
Nombre del puesto.	
Nivel del puesto.	
Registro Federal de Contribuyentes (RFC) con homoclave.	
Clave Única de Registro de Población (CURP)	

### V. Las finalidades del tratamiento intensivo o relevante de datos personales;

**SE CUMPLE**, en los siguientes términos:

Los datos que se inscriben en el Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas podrán ser utilizados para las siguientes finalidades:

- Integrar el Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas a que se refieren los artículos 37, fracciones X y XI;



47, 48, 50 de la Ley del Sistema Estatal Anticorrupción para el Estado de Michoacán de Ocampo; 45, 46 y 47 de las Bases para el funcionamiento de la Plataforma Digital Estatal.

- b) La consulta de los datos de los servidores públicos que intervengan en los procedimientos de contrataciones públicas esté al alcance en un mismo sitio y de manera inmediata de las autoridades cuya competencia lo requiera y para el conocimiento del público en general, respecto de datos públicos.
- c) Recibir e integrar la información que los distintos Órganos del Estado incorporen para su transmisión e integración a la Plataforma Digital Nacional, conforme a los lineamientos, estándares y políticas de dicte el Comité Coordinador del Sistema Nacional Anticorrupción, en términos de lo previsto en el artículo 48, fracción II, de la Ley del Sistema Estatal Anticorrupción.
- d) Contribuir al ejercicio de las atribuciones de las autoridades competentes para investigar y sancionar faltas administrativas y hechos de corrupción.
- e) Apoyar a los trabajos que realiza el Comité Coordinador del Sistema Estatal Anticorrupción para el diseño de políticas públicas en materia de combate a la corrupción, así como su evaluación periódica, ajustes y modificaciones correspondientes.
- f) Generar datos estadísticos para la realización de estudios y diagnósticos en materia anticorrupción.

**VI. Las transferencias nacionales o internacionales, de datos personales que, en su caso, pretendan efectuarse con la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales;**

**SE CUMPLE**, en los términos siguientes:



De conformidad con el artículo 3, fracción XXXI de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, que señala que una transferencia es toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado. **No se realizarán transferencia de datos personales en los términos de la disposición de referencia, dado que los datos contenidos en el Sistema que nos ocupa, únicamente serán consultables por las instituciones señaladas en el párrafo que antecede en tratándose de datos privados y públicos, y por toda persona en tratándose de datos públicos.** (Énfasis propio).

VII. La tecnología utilizada para efectuar el tratamiento intensivo o relevante de datos personales;

**SE CUMPLE**, en los términos siguientes:

En el sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, se realizará la captura y procesamiento de datos, resguardará y concentrará la información, y se generarán reportes y estadística. Este Sistema utilizará la siguiente tecnología para su funcionamiento:

### **Especificaciones Técnicas**

Para el registro de datos y lograr la interconexión del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas con los Órganos del Estado, la Secretaría Ejecutiva prevé tres posibles escenarios, siendo los siguientes:



**Escenario 1.** Los Órganos del Estado que cuenten con un Sistema Informático propio donde registren la información en relación con Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, el cual deberá atender a los estándares técnicos establecidas por la Secretaría Ejecutiva del Sistema Nacional Anticorrupción, serán conectados a la Plataforma Digital Estatal mediante APIs de interconexión.

**Escenario 2.** Para todo aquel órgano del Estado que no cuente con su Sistema de los Servidores Públicos que intervengan en Procedimientos de Contrataciones Públicas, la Secretaría Ejecutiva pondrá a disposición un servicio web, con el formulario para la captura y validación de la información correspondientes.

**Escenario 3.** De igual manera, para todos aquéllos Órganos del Estado que no cuenten con su Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, la Secretaría Ejecutiva ha previsto incluir en el servicio web, la opción de cargar el listado de datos correspondiente, a través de un archivo en formato Excel que de manera previa les será otorgado, ya que el mismo requiere de campos específicos para su correcto funcionamiento.

Con independencia de cualquiera de los tres escenarios antes mencionados, el Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas de la Plataforma Digital Estatal, se ha desarrollado de acuerdo con las especificaciones técnicas emitas por la Secretaría Ejecutiva del Sistema Nacional Anticorrupción, para lograr la interconexión con la Plataforma Digital Nacional, siendo los siguientes:

- **Open API Specification**

El Estándar para la Interoperabilidad de Datos de Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, está basado en el



formato conocido como Open API Specification (OAS), el cual es un formato de especificación que permite describir de manera precisa las características con las que deberán contar las APIs que integrarán a la PDN y la PDE.

- **Oauth 2.0**

El acceso a las APIs que se integrarán a la PDN se gestionará a través del protocolo de autorización OAuth 2.0, el cual es un estándar ampliamente usado por la industria de Internet. El estándar OAuth 2.0 que permitirá a la PDE obtener acceso necesario a las APIs de los órganos del Estado que sí cuenten con su Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas a través del uso de tokens de autorización.

- **Implementación del estándar**

La implementación del estándar de Datos del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas se harán mediante un proceso de API que puede ser dividido en los siguientes pasos:

**Diagnóstico.**

**Diseño de arquitectura.**

**Desarrollo.**

- **Modelo de comunicación**

A través de la PDE, los usuarios podrán realizar consultas a las APIs de los Órganos del Estado, escenario que se llevará a cabo cuando los Órganos del Estado cuentan con un Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas y de no ser así, se realizará la consulta en el mismo servidor. Dichas consultas se configurarán usando parámetros.

El API tendrá la tarea de recibir la consulta y aplicar la lógica de negocio al interior de los Órganos del Estado para generar la respuesta correspondiente; y, hacia el exterior para



enviarla a la PDN, dicha respuesta deberá estar apegada al estándar de Datos del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas.

### **Herramientas para desarrollo web**

La interconexión entre los sistemas de información de los órganos del Estado y la PDE se establecerá a través de internet, usando servicios web o APIs con arquitectura REST (Representational State Transfer). REST es un modelo ampliamente usado para el desarrollo de sistemas web, cuando se esté en alguno de los dos escenarios donde se prevé el servicio web como medios de interconexión, la consulta será local.

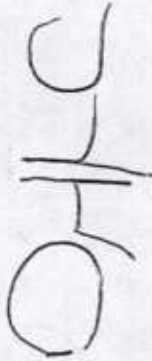
Las herramientas utilizadas en el desarrollo del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, cumplen con las especificaciones dictadas por la PDN y se desarrolló con las siguientes herramientas:

- **Anaconda:** Distribución del lenguaje de programación Python, es software gratuito y de código abierto.
- **Elastic Search:** Servidor de búsqueda para grandes cantidades de datos. Cuenta con una API de búsqueda, es software gratuito y de código abierto.
- **Kibana:** Es una herramienta para visualizar y explorar los datos que se encuentran indexados en ElasticSearch, es software gratuito y de código abierto.
- **APM Server:** Monitoreo del sistema mediante logs y métricas de rendimiento, es software gratuito y de código abierto.
- **Nginx:** Servidor web diseñado para ofrecer un bajo uso de memoria y alta concurrencia, es software libre y de código abierto.




- **PostgreSQL 12:** Es un sistema de gestión de bases de datos relacional orientado a objetos y de código abierto diseñado específicamente para ambientes con alto volumen de datos, es software gratuito y de código abierto.


En el mismo sentido, la Secretaría Ejecutiva cuenta con las siguientes tecnologías para almacenar y administrar toda la información referente al Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, siendo las siguientes:

- 
1. **Servidor:** HPE Proliant DL380 Gen 10 Procesador Intel Xeon 4114 10 Core 2.26GHZ
  2. **Sistema Operativo:** Windows Server 2019 Standar Edition.
  3. **Firewall:** SONICWALL NSA 2656.
  4. **Internet:** Internet dedicado: 50 MB, fibra óptica.

VIII. Las medidas de seguridad de carácter administrativo, físico y técnico que se pretendan adoptar;

 **SE CUMPLE**, en los siguientes términos:

#### **Administrativas**

- 
- Cada usuario tendrá un perfil de usuario específico para tener acceso únicamente a la información requerida para realizar sus funciones, de acuerdo con las facultades que serán otorgadas y que han quedado precisadas en apartados que preceden.
  - Capacitación para cada usuario sobre el uso adecuado de la información a la que tiene acceso, así como su nivel de responsabilidad en cuanto al resguardo de la información confidencial que maneja.



- *Manual de usuario que contiene sugerencias e indicaciones para el resguardo de contraseñas y las medidas de seguridad que se deben implementar para evitar que personas no autorizadas obtengan acceso a la información del Sistema.*
- *El sistema cuenta con un registro detallado sobre las peticiones realizadas por cada usuario (peticiones que se hagan al Sistema para realizar altas, bajas, consultas o modificaciones dependiendo el tipo de usuario) por lo tanto, es posible identificar la persona y fecha en que se tuvo acceso a la información.*
- *En el supuesto de que un usuario extravié sus credenciales deberá comunicarse inmediatamente a la Secretaría Ejecutiva a fin de que la cuenta sea bloqueada y le sea reasignada una nueva contraseña.*
- *Todos los usuarios deberán firmar un acuerdo de confidencialidad del Sistema de servidores públicos que intervengan en procedimientos de contratación.*

### **Físicas**

- *Los datos son almacenados en un servidor físico ubicado en las instalaciones de la Secretaría Ejecutiva, en un cuarto frío con todas las medidas pertinentes en cuanto a cableado, organización y configuración.*
- *El acceso al servidor se encuentra restringido con medidas de seguridad, solamente personal autorizado cuenta con acceso físico.*
- *El sitio del servidor cuenta con un sistema de refrigeración para evitar el aumento de temperatura evitando posibles fallas por causa del sobrecalentamiento del equipo de cómputo.*
- *Se cuenta con un sistema de respaldo de energía con autonomía de 4 horas para uso exclusivo del servidor.*
- *El cableado eléctrico respeta las normas y estándares nacionales que permiten el correcto aislamiento.*



- El servidor cuenta con un respaldo espejo en un disco duro adicional para evitar la pérdida de datos.

### **Tecnológicas**

Además de la tecnología usada en el Servidor es de señalarse lo siguiente:

- A cada usuario se le proporcionará una cuenta con una contraseña única donde se definen los permisos y roles de usuario que le permiten tener acceso a la información del sistema conforme a sus funciones y atribuciones.
- Los usuarios son responsables del resguardo de sus contraseñas e información a la que tengan acceso.
- El tráfico de red está protegido por un Firewall SonicWALL con filtrado por dirección IP y MAC, evitando con ello el riesgo de hackeo de datos.
- La sesión del usuario tiene un límite de vida de 5 minutos después de la última acción del usuario, transcurrido dicho tiempo la sesión se cerrará automáticamente, lo cual evita el acceso a usuarios no autorizados en un equipo con la sesión abierta.
- Monitoreo constante del servidor y funcionamiento del sistema.

Las medidas de seguridad de carácter administrativo, físico y técnico mencionadas anteriormente serán supervisadas y actualizadas de manera mensual a fin de reducir los riesgos inherentes y residuales en el tratamiento de la información.

**IX. Los posibles riesgos y amenazas, así como el daño o consecuencias que pudieran producirse o presentarse si llegasen a materializarse con la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales;**



**SE CUMPLE**, en los términos siguientes:

**APARTADO V.**

**IDENTIFICACIÓN, ANÁLISIS Y GESTIÓN DE LOS RIESGOS PARA LA  
PROTECCIÓN DE DATOS PERSONALES.**

*En este apartado se incluye la gestión de riesgos, que tiene por objeto identificar, analizar y responder a los factores de riesgo en la seguridad de los datos y amenazas de intrusos en la red, al igual que posibles efectos negativos y consecuencias que pudieran producirse con la puesta en operación del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, tales como la pérdida de información, hackeo de datos, daño técnico en el equipo servidor, intrusión de extraños, esto mediante el Plan General para Gestionar los Riesgos Identificados. En este Plan se considera lo siguiente:*

- A. Se identifican y describen de forma específica los riesgos administrativos, físicos o tecnológicos que podrían presentarse con la puesta en operación del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas;*
- B. Se pondera de forma cuantitativa, la probabilidad de que los riesgos identificados sucedan, así como su nivel de impacto en los titulares en lo que respecta al tratamiento de sus datos personales; y*
- C. Se puntualizan las medidas y controles concretos que se adoptarán con la finalidad de eliminar, mitigar, transferir o retener los riesgos detectados, de tal manera que no tengan un impacto en la esfera de los titulares de los datos, en lo que respecta al tratamiento de sus datos personales.*



## **PLAN GENERAL PARA GESTIONAR LOS RIESGOS IDENTIFICADOS**

### ***I. Identificación y descripción específica de los riesgos administrativos, físicos o tecnológicos que podrían presentarse con la puesta en operación del Sistema de los Servidores Públicos que intervengan en Procedimientos de Contrataciones Públicas.***

En todo sistema informático existen riesgos inherentes a la puesta en marcha, así como situaciones extraordinarias que escapan a su control, por lo tanto, es de suma importancia establecer medidas preventivas para eliminar, mitigar y retener esos riesgos.

La primera etapa del presente Plan consiste en identificar los riesgos que pudieran presentarse, y proponer las medidas y controles concretos para evitarlos y en todo caso contar con un plan de acción para minimizarlos.

Por consiguiente, es necesario prever todos los escenarios posibles tomando en cuenta las variables y factores que tengan la capacidad de causar perjuicio o poner en una situación de vulnerabilidad a los titulares de los datos sobre los que se realiza el tratamiento.

Se analizará el ciclo de vida del tratamiento de datos desde el inicio hasta el final, examinando los recursos involucrados con la gestión de datos, esto con la finalidad de identificar las etapas en las que los datos tratados son susceptibles a sufrir algún tipo de riesgo.

### ***II. La ponderación cuantitativa y cualitativa de la probabilidad de que los riesgos identificados sucedan, así como su nivel de impacto en los titulares en lo que respecta al tratamiento de sus datos personales.***



En el presente numeral, se enlistan y explican todos los riesgos y amenazas que pudieran presentarse y para ello, en necesario determinar el nivel que tienen para causar perjuicio o colocar en una situación de vulnerabilidad a los titulares de los datos sobre los que se realiza el tratamiento, por lo tanto, es necesario clasificarlos para dar mayor prioridad a los que pudieran tener consecuencias negativas de mayor alcance.

Para realizar dicha clasificación se usan dos tipos de enfoques: análisis cuantitativo y análisis cualitativo, en los siguientes términos:

### **Análisis cualitativo de riesgos**

Se atiende a que el enfoque cualitativo no tiene como finalidad medir los riesgos, sino comprenderlos, consiste en investigar cada uno de los posibles escenarios que puedan ocurrir. No parte de la idea de una realidad existente, sino de muchas realidades que pudieran presentarse, midiendo la posibilidad subjetiva de que cierto riesgo suceda, haciendo énfasis en el nivel de impacto como consecuencia de que surgiera dicho riesgo. Una vez que los riesgos han sido identificados el siguiente paso será analizarlos y priorizarlos, otorgándoles una calificación numérica según la probabilidad de que puedan presentarse, el daño que pudieran llegar a causar y el tiempo de respuesta para ser solucionados.

La metodología empleada está basada en los siguientes niveles posibles:

Probabilidad de ocurrencia
1. Baja
2. Limitada
3. Alta



#### 4. Máxima

Por otro lado, el impacto se determina con base a los posibles daños que pueden ocurrir en caso de que el riesgo o la amenaza se llegara a presentar, por lo tanto, el impacto también se evalúa con la misma escala de cuatro niveles:

1. **Impacto bajo:** No hay consecuencias negativas que generen perjuicio o pongan en una situación de vulnerabilidad a los titulares de los datos sobre los que se realiza el tratamiento de datos.
2. **Impacto limitado:** Las consecuencias negativas no son suficientes para generar perjuicio a los titulares de los datos sobre los que se realiza el tratamiento de datos.
3. **Impacto alto:** Las consecuencias implican un daño elevado generando perjuicio a los titulares de los datos sobre los que se realiza el tratamiento de datos.
4. **Impacto máximo:** Las consecuencias implican un daño muy alto con impacto crítico generando perjuicio elevado a los titulares de los datos sobre los que se realiza el tratamiento de datos.

Una vez que las escalas han sido definidas expresamente, es posible precisar el nivel de riesgo al que nos enfrentamos. Cada riesgo será evaluado en una escala siendo el nivel de daño mínimo el número 1 y el nivel de daño máximo el número 4.

Impacto	
Bajo	1
Limitado	2
Alto	3
Máximo	4



Cabe señalar que es imposible eliminar completamente el o los riesgos, y que cada actividad que se realiza implica cierto nivel de riesgo; la puesta en marcha del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas no es la excepción. Se pretende contar con la preparación adecuada para saber cómo responder ante cualquier eventualidad, a fin de mitigar o reducir los posibles daños inherentes al uso de tecnologías de la información y la comunicación. Se utilizará la herramienta conocida como "Matriz de probabilidad" con la cual se pueden observar claramente los riesgos a los que se requiere prestar más atención. En la matriz de probabilidad se utilizan dos criterios que son: la probabilidad de que un riesgo ocurra y el impacto que tendrá dicho riesgo en caso de ocurrir.

Para calcular el riesgo se empleará la siguiente fórmula: Riesgo=Probabilidad x Impacto.

**X. Las medidas o controles concretos que el responsable adoptará para eliminar, mitigar, transferir o retener los riesgos identificados;**

<b>Medidas de control administrativas</b>	
<b>Medidas para mitigar el riesgo</b>	
<b>Riesgo</b>	<b>Descripción de la medida de control</b>
Eliminación de datos de los servidores públicos del sistema, de forma accidental o intencional.	Se implementarán perfiles de acceso, gestión y obligaciones para cada usuario conforme a sus responsabilidades; lo cual se establecerá en el Catálogo de Perfiles de Usuario del Sistema de los Servidores Públicos que Intervengan en Contrataciones Públicas.
Acceso al Sistema por un tercero no autorizado usando credencial de acceso	Se solicitará oficialmente la designación de los usuarios capturador y validador de



<p>de otro usuario y que ponga en riesgo la integridad y veracidad de los datos almacenados en el Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas.</p>	<p>datos; y se brindará capacitación con una guía sobre cómo mantener las credenciales de acceso seguras, indicando las medidas de seguridad que deberán implementar en sus equipos de cómputo y/o dispositivos móviles de donde se realicen conexiones a la PDE. Adicionalmente, el Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas contará con un mecanismo de seguridad que cierra la sesión después de 5 minutos de inactividad.</p> <p><b>Valor:</b> -1 en la probabilidad de ocurrencia en cada uno de los riesgos.</p>
<p>Proporcionar acceso al sistema a personal no capacitado en el correcto uso de datos personales.</p>	<p>Los usuarios recibirán una capacitación sobre el manejo y uso correcto de los datos personales, según corresponda, en coordinación con las autoridades competentes.</p> <p><b>Valor:</b> -1 en la probabilidad de ocurrencia en cada uno de los riesgos.</p>
<p>Captura de datos erróneos por parte del Usuario capturados del Órgano Interno de Control.</p>	<p>Antes de dar de alta un registro, los datos deberán ser verificados y validados por el Usuario validador para que ingresen al Sistema y se den de alta.</p>



	<p><i>El Sistema cuenta con niveles de acceso sumamente estrictos para cada usuario de acuerdo a sus responsabilidades, por lo tanto, ningún otro usuario (ni siquiera el usuario administrador del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas) tiene acceso para validar los datos.</i></p> <p><b>Valor:</b> -1 en la probabilidad de ocurrencia en cada uno de los riesgos.</p>
<p><i>Desconocimiento sobre el Catálogo de Perfiles de Usuarios del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas.</i></p>	<p><i>Capacitación sobre el uso del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas y los perfiles de usuario con el manual de usuario correspondiente.</i></p> <p><b>Valor:</b> -2 en la probabilidad de ocurrencia del riesgo.</p>
<p><i>Desconocimiento de los usuarios sobre el tratamiento de datos personales y las consecuencias del incumplimiento de las disposiciones regulatorias del uso del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas.</i></p>	<p><i>Contar con el aviso de privacidad del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas y hacerlo de conocimiento público.</i></p>

DRH







	<p><b>Valor: -1 en la probabilidad de ocurrencia del riesgo.</b></p>
<p><b>Medidas de control físicas y tecnológicas</b></p>	
<p><u>Medidas para mitigar el riesgo</u></p>	
<p>Eliminación de datos almacenados en el equipo servidor de forma intencional o accidental.</p>	<p>Una vez que la información ha sido validada, se bloqueará el registro para cualquier tipo de modificación.</p> <p>En caso de que se requiera hacer correcciones, modificaciones, se requerirá solicitud por oficio por parte del Órgano Interno de Control a la Secretaría Ejecutiva, a fin de habilitar el registro correspondiente para realizar las modificaciones pertinentes; se contará con un plazo de 15 días naturales para su modificación, transcurrido ese tiempo el registro volverá a bloquearse y no se permitirán modificaciones.</p> <p>Cada uno de los usuarios será responsable de resguardar sus credenciales de acceso.</p> <p>El usuario validador perteneciente al Sujeto obligado será responsable de verificar que la información sea la correcta. Todos los usuarios han sido</p>
<p>Contraseñas expuestas por robo o extravío (equipo de cómputo o dispositivo móvil).</p>	
<p>Presencia de información errónea, de los servidores en el Sistema de los Servidores Públicos que Intervengan en</p>	



<p>Procedimientos de Contrataciones Públicas de los Órganos del Estado.</p>	<p>capacitados para el uso y llenado de datos del Sistema de Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas.</p> <p><b>Valor:</b> -1 en la probabilidad de ocurrencia en cada uno de los riesgos.</p>
<p>Servidor inaccesible debido a un ataque de denegación de servicio.</p>	<p>El tráfico que recibe el servidor es monitoreado por un cortafuegos con la capacidad de bloquear ataques de denegación de servicio.</p> <p><b>Valor:</b> -1 en la probabilidad de ocurrencia del riesgo.</p>
<p>El Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, no valida el acceso o perfil de usuario.</p>	<p>Los niveles de acceso estarán definidos conforme a las atribuciones y responsabilidades de cada perfil de los usuarios del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas.</p> <p><b>Valor:</b> -1 en la probabilidad de ocurrencia del riesgo.</p>
<p>Base de datos parcial o totalmente copiada sin autorización.</p>	<p>La asignación de los usuarios y contraseñas, estableciendo niveles de acción.</p>

07/10

/

0



<p><i>Datos personales disponibles durante las pruebas de los ajustes al desarrollo del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas.</i></p>	<p><i>Antivirus con análisis heurístico para la detección de software malicioso conocido y desconocido.</i></p> <p><i>Monitoreo de tráfico entrante y saliente del servidor mediante un firewall, lo cual permite la detección de tráfico inusual como descarga de software y posibles fugas de información.</i></p> <p><i>Conexión segura mediante un certificado de seguridad.</i></p> <p><i>Conexiones entrantes limitadas para la administración del servidor mediante un filtrado de direcciones IP, lo cual evita accesos remotos no autorizados.</i></p> <p><b>Valor:</b> -1 en la probabilidad de ocurrencia del riesgo.</p>
<p><i>Venta de la base de datos parcial o total copiada sin autorización.</i></p>	<p><i>Capacitación a los usuarios sobre el uso de datos personales y las responsabilidades en que se pudiera incurrir en su mal uso.</i></p> <p><i>Se llevará un registro detallado de cada vez que un usuario realiza una consulta o</i></p>



	<p><i>modificación de los datos, con la finalidad de poder realizar un rastreo ante fuga de información.</i></p> <p><i>Ningún usuario, excepto el administrador tiene acceso a toda la base de datos de forma directa; para poder ver los datos es necesario entrar o acceder mediante la interfaz del usuario del sistema.</i></p> <p><i>Se cuenta con un registro de los usuarios que se conectan al servidor de forma directa.</i></p> <p><b>Valor:</b> -1 en la probabilidad de ocurrencia en los riesgos.</p>
<p><i>Datos de interoperabilidad erróneos por ausencia de verificación de la integridad de los datos interconectados.</i></p>	<p><i>El desarrollo del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, observa el estándar de datos emitido por la SESNA, para el funcionamiento con la Plataforma Digital Nacional.</i></p> <p><i>Se realizaron todas las pruebas requeridas por la SESNA, por lo tanto, la consistencia de datos entre la Plataforma</i></p>



	<p>Digital Estatal y la Plataforma Digital Nacional es del 100%.</p> <p><b>Valor:</b> -1 en la probabilidad de ocurrencia en el riesgo.</p>
<p>Eliminación o destrucción de la base de datos del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas.</p>	<p>Se tiene expresamente prohibido el uso de software ilegal, así como la descarga de software de dudosa procedencia.</p> <p>Antivirus con análisis heurístico para la detección de software malicioso conocido y desconocido.</p> <p>Monitoreo de tráfico entrante y saliente del servidor mediante un firewall, lo cual permite la detección de tráfico inusual como descarga de software y posibles fugas de información.</p> <p>Conexión segura mediante un certificado de seguridad, instalado en el Servidor.</p> <p>Conexiones entrantes limitadas para la administración del servidor mediante un filtrado de dirección IP, lo cual evita accesos remotos no autorizados.</p>



	<p>Ningún usuario, excepto el administrador tiene acceso a la base de datos de forma directa, para poder ver los datos es necesario entrar mediante la interfaz de usuario del sistema.</p> <p><b>Valor:</b> -2 en la probabilidad de ocurrencia del riesgo.</p>
Ejecución de un código malicioso.	<p>Se tiene expresamente prohibido el uso de software ilegal, así como la descarga de software de dudosa procedencia.</p> <p>Antivirus con análisis heurístico para la detección de software malicioso conocido y desconocido.</p> <p>Monitoreo de tráfico entrante y saliente del servidor mediante un firewall, lo cual permite la detección de tráfico inusual como descarga de software y posibles fugas de información.</p> <p><b>Virus:</b> -1 en la probabilidad de ocurrencia en el riesgo.</p>
El Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas no se encuentra en operación debido a daño físico por falta	<p>Mantenimiento preventivo mediante limpieza al site donde se encuentra físicamente el servidor.</p>

CHC  
OHC  
/



<p>de mantenimiento, corrosión, congelamiento, fuego, agua, contaminación o radiación electromagnética.</p>	<p>El site se encuentra en un área elevada para evitar inundaciones y no cuenta con conexiones de agua o tuberías cercanas.</p> <p>La temperatura es monitoreada constantemente para evitar el sobrecalentamiento de los componentes físicos del servidor.</p> <p>Tanto el cableado eléctrico como el cableado de red cuentan con un aislamiento según las normas oficiales mexicanas.</p> <p>Se cuenta con un no-break para el servidor con capacidad de 2.5 horas aproximadamente de energía eléctrica en caso de ser requerido.</p> <p>Valor: -2 en la probabilidad de ocurrencia en los riesgos.</p>
<p>Pérdida de información, por robo de bienes como el equipo servidor físico.</p>	<p>La base de datos cuenta con cifrado de información.</p> <p>Valor: -1 en la probabilidad de ocurrencia en el riesgo.</p>



**XI. Los mecanismos o procedimientos que adoptará el responsable para que la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales cumpla, desde el diseño y por defecto, con las obligaciones previstas en la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables;**

**SE CUMPLE**, en los siguientes términos:

*De acuerdo a lo que establece la Ley General de Protección de Datos Personales, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales y demás disposiciones aplicables, se señalan los mecanismos o procedimientos que adoptará el Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas para cumplir por defecto con los principios, deberes, derechos y obligaciones establecidos en la ley:*

**PRINCIPIOS DE LICITUD, FINALIDAD, LEALTAD, CONSENTIMIENTO, CALIDAD,  
 PROPORCIONALIDAD, INFORMACIÓN Y RESPONSABILIDAD EN EL  
 TRATAMIENTO DE DATOS PERSONALES**

PRINCIPIO	FUNDAMENTO	MECANISMO DE CUMPLIMIENTO
<b>LICITUD</b>	Artículo 16 de la Ley General de Protección de Datos Personales y 12 de la Ley de	<ul style="list-style-type: none"> <li>Se cumple, ya que el ejercicio de las facultades y atribuciones a cargo de la Secretaría Ejecutiva en su</li> </ul>



<p>UHO</p> <p><i>[Handwritten signature]</i></p> <p><i>[Handwritten scribble]</i></p>	<p>Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, que señalan que el tratamiento de datos personales deberán sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.</p>	<p>calidad de administradora del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, deriva de lo previsto en la normatividad nacional y local aplicable, y que ha quedado expuesto en el Apartado I del presente.</p> <ul style="list-style-type: none"> <li>• Mecanismos de regulación y supervisión que ejerce el Comité Coordinador del Sistema Estatal Anticorrupción, conforme a los artículos 47 de la Ley del Sistema Estatal Anticorrupción para el Estado de Michoacán de Ocampo y el Acuerdo del Comité Coordinador del Sistema Estatal Anticorrupción por medio del cual se emiten las Bases para el funcionamiento de la Plataforma Digital Estatal.</li> </ul>
	<p>Al tenor de los artículos 18 de la Ley General de</p>	<ul style="list-style-type: none"> <li>• Se cumple, ya que las finalidades del Sistema, son</li> </ul>

<b>FINALIDAD</b>	<p>Protección de Datos y 14 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.</p>	<p>concretas, porque atienden a la consecuencia de fines específicos o determinados; son explícitas porque se encuentran expresamente establecidas y se dan a conocer de manera clara; y sus finalidades son lícitas y legítimas, ya que derivan de las leyes de la materia. Esas finalidades han quedado referidas en el apartado III de la presente.</p>
<b>LEALTAD</b>	<p>Los artículos 19 de la Ley General de Protección de Datos Personales y 15 la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, señalan que, el</p>	<p>Este principio se cumple, ya que los datos serán oficiales, en virtud a que se obtendrán directamente de los Sujetos obligados que corresponden a los Órganos del Estado, en términos de la Ley local de Responsabilidades, quienes alimentarán o ingresarán al Sistema de información según corresponda.</p>



	<p>responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.</p>	<p>Establecimiento de mecanismos de seguridad, otorgando usuarios y claves específicas, a fin de que registren la información que corresponde, esto de conformidad con lo previsto en el Catálogo de perfiles de usuario del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, que integra la Plataforma Digital Estatal de Michoacán, de conformidad al artículo 48, fracción II, de la Ley del Sistema Estatal Anticorrupción para el Estado de Michoacán de Ocampo.</p>
<p><b>CONSENTIMIENTO</b></p>	<p>Los artículos 20, 21, 22 y 65 de la Ley General de Protección de Datos, y 16, 17 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo,</p>	<ul style="list-style-type: none"><li>• Se cumple, ya que se actualizan las hipótesis previstas en los artículos 22 fracciones I y II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, por lo</li></ul>

	<p>establecen que el titular de los datos personales debe autorizar el tratamiento o transferencia de manera libre, específica e informada, salvo que se actualice alguna de las hipótesis previstas en los artículos 22 y 70 de la Ley General en cita, así como 18 de la Ley Local.</p>	<p>que la Secretaría Ejecutiva a través del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, no está obligada a recabar el consentimiento del titular de los datos en virtud a que se realiza un ejercicio de las facultades conferidas en los artículos 9 fracción XIII, 36 fracción I, 48 y 49 fracción III de la Ley General del Sistema Nacional Anticorrupción; 8 fracción XI; 37 fracción X; 47, 48 fracción III y 49 de la Ley del Sistema Estatal Anticorrupción para el Estado de Michoacán de Ocampo.</p> <ul style="list-style-type: none"><li>• Además, es pertinente resaltar que salvo los datos correspondientes al Registro Federal de Contribuyentes, Clave Única de Registro de Población y género, los datos de los servidores públicos son públicos, atendiendo al</li></ul>
--	---	--



		diccionario de datos emitido por la Secretaría Ejecutiva del Sistema Estatal Anticorrupción para el sistema que nos ocupa.
<b>CALIDAD</b>	Los numerales 23 y 24 de la Ley General de Protección de Datos; y 19 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, disponen que el responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos. Se cumple con la calidad en los datos personales cuando éstos son	<ul style="list-style-type: none"> <li>• Se cumple, pues como ya se señaló los datos se obtienen directamente de las autoridades competentes a través de usuarios que sean designados, conforme a las facultades señaladas en el Catálogo elaborado para tal efecto, por lo que se actualiza la presunción de calidad en los datos personales.</li> <li>• El cumplimiento del principio de calidad, se garantiza mediante mecanismos de seguridad, otorgando usuarios y claves específicas, a fin de que sea registrada la información que corresponda, conforme a las facultades previstas en el Catálogo de perfiles de usuario del Sistema de los Servidores Públicos que Intervengan en</li> </ul>

	proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.	Procedimientos de Contrataciones Públicas, que integra la Plataforma Digital Estatal de Michoacán, de conformidad al artículo 48, fracción II, de la Ley del Sistema Estatal Anticorrupción para el Estado de Michoacán de Ocampo.
<b>PROPORCIONALIDAD</b>	Los artículos 25 de la Ley General de Protección de Datos, y 21 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, establecen que, el responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.	<ul style="list-style-type: none"> <li>Se cumple, pues como se señala en los apartados V y VI de la presente Evaluación de Impacto, los datos que se registrarán en el Sistema han sido definidos en el estándar técnico emitido por la Secretaría Ejecutiva del Sistema Nacional Anticorrupción, y son los estrictamente necesarios. De tal modo que el tratamiento de datos personales en el Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, guarda relación adecuada con lo dispuesto por la Ley,</li> </ul>

OK

/

○



		con lo que se persigue cumplir con las finalidades constitucionales en materia anticorrupción.
<b>INFORMACIÓN</b>	Los artículos 26 de la Ley General de Protección de Datos, y 22 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, establecen que, el responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.	<ul style="list-style-type: none"> <li>• Se cumple, ya que se pondrá a disposición de los Usuarios, el aviso de privacidad del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas cuando así corresponda, al margen de que los datos personales no serán recabados de origen en el Sistema, ya que los datos ingresarán al mismo a través de las autoridades competentes quienes tienen la responsabilidad de recabar los datos personales de los servidores públicos.</li> <li>• Difundir, por medios electrónicos y físicos, el aviso de privacidad del Sistema de los Servidores Públicos que Intervengan en</li> </ul>

		Procedimientos de Contrataciones Públicas.
<b>RESPONSABILIDAD EN EL TRATAMIENTO DE DATOS PERSONALES.</b>	<p>Los artículos 29 de la Ley General de Protección de Datos y 25 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, establecen que, el responsable deberá implementar los mecanismos previstos en la Ley para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la Ley y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular e Instituto.</p>	<ul style="list-style-type: none"><li>Se cumple con la elaboración de la presente Evaluación de Impacto en la Presentación de Datos Personales del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, de la Plataforma Digital Estatal para su presentación ante el Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales, para el procedimiento de valoración establecido en el artículo 23 del Acuerdo mediante el cual se aprueban las disposiciones de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales aprobado por el Instituto Nacional de Transparencia, Acceso a la</li></ul>

C  
H  
C







		Información y Protección de Datos Personales.
--	--	--

Para el cumplimiento de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales, con independencia de que se observan mediante los mecanismos y procedimientos que han quedado señalados, el titular de los datos tiene a disposición el Procedimiento previsto en la Ley General de Protección de Datos y en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, para solicitar el Acceso, Rectificación, Cancelación y Oposición sobre el tratamiento de sus datos.

XII. La opinión técnica del oficial de protección de datos personales respecto del tratamiento intensivo o relevante de datos personales que implique la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier tecnología, en su caso, y

**SE CUMPLE**, en los siguientes términos:

En base a lo expuesto en este documento que describe de manera detallada el Sistema de Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas y considerando su implementación deriva de una obligación prevista en las leyes de la materia, que se ajusta a los lineamientos nacionales como lo disponer la Ley del Sistema Estatal, que persigue finalidades específicas, lícitas y legítimas, que para su desarrollo se han seguido los estándares técnico emitidos por la Secretaría Ejecutiva del Sistema Nacional Anticorrupción; que las medidas de seguridad físicas, administrativas y tecnológicas que se han previsto para el resguardo de los datos, su temporalidad y permanencia en el Sistema, se puede concluir que si bien existen riesgos inherentes al

funcionamiento de todo el sistema informático, se han tomado las medidas necesarias para disminuirlos o mitigarlos y se prevé un estricto control en la información por medio de la asignación de usuarios y contraseñas seguras que estarán asignadas oficialmente a los servidores públicos que sean designados.

**XIII. Cualquier otra información que considere pertinente atendiendo a las circunstancias del caso en particular.**

**SE CUMPLE**, en los siguientes términos:

**Responsables conjuntos que presentan la Evaluación de Impacto en la protección de datos personales.**

- Lic. Ana María Vargas Vélez, Secretaria Técnica de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción.
- Ing. Lizbeth Pureco Pedraza, Jefa del Departamento de Servicios Tecnológicos y Plataforma Digital de la Secretaría Ejecutiva.
- Lic. Brenda Patricia Gamiño Cruzaley, Jefa de la Unidad de Transparencia, Acceso a la Información y Protección de Datos Personales de la Secretaría Ejecutiva.

**Denominación del responsables líder del proyecto.**

- Lic. Ana María Vargas Vélez, Secretaria Técnica de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción.

**Las obligaciones, deberes, responsabilidades, límites y demás cuestiones con la participación de todos los representantes.**



Servidor Público	Obligaciones, deberes, responsabilidades y límites de su participación en la presente evaluación
<p><b>Lic. Ana María Vargas Vélez, Secretaria Técnica de la Secretaría Ejecutiva.</b></p>	<ul style="list-style-type: none"><li>• Administradora de la Plataforma Digital Estatal y del Sistema de Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas.</li><li>• Responsable de la revisión y aprobación final de la Evaluación de Impacto.</li><li>• Deber de suscribir la presentación de la Evaluación de Impacto ante el IMAIP.</li><li>• Líder del proyecto de la implementación del Sistema de Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas.</li></ul>
<p><b>Ing. Lizbeth Pureco Pedraza, Jefa del Departamento de Servicios Tecnológicos y Plataforma Digital de la SESEA.</b></p>	<ul style="list-style-type: none"><li>• Responsable de la operación y buen funcionamiento de los servicios del Sistema de Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas.</li><li>• Deber de aportar la información necesaria para la elaboración de la Evaluación de Impacto.</li></ul>

	<ul style="list-style-type: none"><li>• Deber de aportar sugerencias y/o modificaciones de mejora a la Evaluación de Impacto.</li></ul>
<b>Lic. Brenda Patricia Gamiño Cruzaley,</b> <i>Jefa de la Unidad de Transparencia, Acceso a la Información Pública y Protección de Datos Personales de la SESEA.</i>	<ul style="list-style-type: none"><li>• Deber de revisar y presentar la propuesta inicial de Evaluación de Impacto.</li></ul>

De acuerdo con lo anteriormente expuesto, y previo a la determinación del sentido del Dictamen de éste Organismo Garante, resulta preciso resaltar la importancia del Sistema de Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas que se incorporará a la Plataforma Digital Estatal.

La Plataforma Digital Estatal, al igual que la Plataforma Digital Nacional, es una fuente de inteligencia para construir integridad y combatir la corrupción, que creará valor para el gobierno y la sociedad, a partir de la información de los Sistemas que la componen.

La Plataforma es un medio para la concentración y consulta de datos en la materia anticorrupción, que busca eliminar barreras y romper silos de información para que los datos sean comparables, accesibles, utilizables y estén dispuestos en un solo lugar para su consulta inmediata.

Busca ser una herramienta tecnológica especialmente para que las autoridades encargadas de prevenir, investigar y sancionar faltas administrativas y hechos de corrupción, así como las que tienen a su cargo la fiscalización y control de los recursos públicos, accedan a la información necesaria, en forma expedita y oportuna para el



ejercicio de sus atribuciones, contenida en los Sistemas que se conecten con dicha Plataforma.

En este sentido, los artículos 8, fracción XI, y 47 de la Ley del Sistema Estatal Anticorrupción para el Estado de Michoacán de Ocampo, establecen que el Comité Coordinador del Sistema Estatal Anticorrupción, implementará la Plataforma Digital Estatal, con apego a los lineamientos señalados por la federación, que permita cumplir con los procedimientos, obligaciones y disposiciones señaladas en dicha Ley y la Ley de Responsabilidades Administrativas para el Estado de Michoacán de Ocampo, así como para los sujetos que la misma ley del Sistema Estatal establece, atendiendo a las necesidades de accesibilidad de los usuarios.

Corresponde al Comité Coordinador y a los demás sujetos obligados en el ámbito de sus competencias, proporcionar los datos e información a la Plataforma Digital Estatal.

La administración de la Plataforma Digital Estatal, está a cargo de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, tal como lo establecen los artículos 37, fracción X, y el 47 de la Ley del Sistema Estatal Anticorrupción para el Estado de Michoacán de Ocampo.

La Plataforma Digital del Sistema Estatal contará con al menos 6 Sistemas electrónicos, que consisten en los siguientes:

- I. Sistema de evolución patrimonial de declaración de intereses y constancia de presentación de declaración fiscal;
- II. **Sistema de los servidores públicos que intervengan en procedimientos de contrataciones públicas;**
- III. Sistema de servidores públicos y particulares sancionados;



- IV. Sistema de información y comunicación con el sistema nacional y con el sistema nacional de fiscalización;
- V. Sistema de denuncia pública de faltas administrativas y hechos de corrupción;
- VI. Sistema de información pública de contrataciones.

(Énfasis propio)

En este sentido, se justifica la importancia de la realización de la Evaluación de Impacto que nos ocupa por parte del Sujeto Obligado, así como el análisis, valoración y dictamen de su contenido y alcance en la protección de datos personales por parte de este Instituto, toda vez que, una evaluación de impacto a la protección de datos personales tiene por objeto determinar, *ex ante* de la puesta en operación de un determinado tratamiento de datos personales, los impactos y amenazas que puedan comprometer los principios, deberes, derechos y demás obligaciones en el tratamiento de datos personales.

Con estas evaluaciones se busca detectar, prevenir y minimizar riesgos que pudieran producirse en los titulares respecto al tratamiento de su información personal, y más aún, prevenir el impacto en costos y recursos económicos respecto aquellos tratamientos que, desde su origen, no estén alineados a la normatividad en materia de protección de datos personales.

En este sentido, la elaboración de una evaluación de impacto a la protección de datos personales constituye una enorme aportación en materia de protección de datos personales, eminentemente por su efecto preventivo que no sólo abarca el respeto de los derechos y libertades de las personas involucradas, sino también el impacto económico que representaría en caso de que el tratamiento de datos personales no resultara conforme a lo dispuesto en la normatividad de datos personales aplicable.



Por lo anteriormente expuesto y con fundamento en los artículos 70, 72 y 73 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo; y, el artículo 28 de las Disposiciones Administrativas de Carácter General para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, emitido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, vista la Evaluación de Impacto en la Protección de Datos Personales, respecto al carácter intensivo o relevante del tratamiento de Datos Personales en el Sistema de Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, de la Plataforma Digital Estatal, de conformidad con lo establecido en las Disposiciones Administrativas de carácter general para la presentación y valoración de Evaluaciones de Impacto en la Protección de Datos Personales, presentada por la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, previo estudio técnico y jurídico de la información para evaluar los riesgos de esta nueva plataforma, se emite el siguiente:

#### DICTAMEN:

**PRIMERO.** El Sistema de Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, desarrollado por el responsables Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Michoacán, cumple con lo dispuesto en el artículo 71 la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, así como con lo establecido en los artículos 3, 4, 6, 7, 10, 14, 15, 17, 18, 19, 20, 21 y 22 de las Disposiciones Administrativas de Carácter General para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, emitido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, por lo que no será necesario emitir recomendaciones no vinculantes al respecto.

**SEGUNDO.** Notifíquese a la Lic. Ana María Vargas Vélez, Secretaria Técnica de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción.

Así lo acordó y aprobó el Pleno del Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales, en la Vigésima Tercera Sesión Extraordinaria del día 15 de septiembre de 2021.

**Pleno del Instituto Michoacano de Transparencia, Acceso a la Información y  
Protección de Datos Personales.**

**Mtra. Areli Yamilet Navarrete Naranjo**




**Comisionada Presidenta**

**Mtro. Abraham Montes Magaña**



**Comisionado**



**Lic. Diego Anita Gutiérrez**

**Comisionado**



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



