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

DICTAMEN QUE EMITE EL INSTITUTO MICHOACANO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, CORRESPONDIENTE A LA EVALUACIÓN DE IMPACTO EI/01/2021 SOLICITADA POR LA SECRETARÍA EJECUTIVA DEL SISTEMA ESTATAL ANTICORRUPCIÓN MICHOACÁN.

El artículo 3, fracción XV de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, establece que 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 normativa aplicable; en ese tenor se contempla en el artículos74, de la citada Ley.

De conformidad con los citados ordenamientos, y con 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*, el Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales (IMAIP), emitirá un dictamen, luego de que un sujeto obligado, presente su proyecto de evaluación de impacto.

Las presentes recomendaciones y observaciones no son vinculantes, sino tienen carácter orientador, con la finalidad de proporcionar apoyo al responsable, asimismo difundir el conocimiento del derecho a la protección de datos personales y promover su ejercicio, mediante una serie de sugerencias basadas en estándares y mejores prácticas en materia de seguridad de la información, que pudieran resultar aplicables en atención a la naturaleza de los datos; las finalidades del tratamiento, y las capacidades técnicas del responsable.

SE CONSIDERA

1. Que el derecho a la información está reconocido como un derecho humano en el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos, dejando establecidos los principios y las bases que sustentan su ejercicio, además de establecer los límites del acceso a la información, en virtud de proteger la vida privada, el interés público y los datos personales.

2. Que el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, en el segundo párrafo establece que todas las personas tienen derecho a la protección, al acceso, rectificación y cancelación de sus datos personales, así como a manifestar su oposición en los términos que la legislación de la materia establezca; de igual forma, la fracción VII del numeral 116 del mismo ordenamiento, señala que las Constituciones de los Estados establecerán organismos autónomos especializados, imparciales y colegiados, responsables de garantizar el derecho de acceso a la información y de protección de datos personales.

3. Que el artículo 3, fracciones IX y XXXII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados entiende como **dato de carácter personal** cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información; asimismo define el **tratamiento de datos personales** cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

4. Que el tratamiento de los datos personales de los servidores públicos del Estado de Michoacán, en la medida que se refieran a personas físicas

identificables, se encuentra regulado por la normatividad de protección de datos personales.

5. Que a través del oficio SEA-SE-ST-2021 de fecha 20 de abril de la anualidad que transcurre, la Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Michoacán solicita la opinión del Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales para saber si es necesario realizar una evaluación de impacto relativa a la protección de datos que administrará y actualizará el *Sistema de Servidores Públicos y Particulares Sancionados* y que por tanto serán objeto de tratamiento. Hacen, además, especificaciones técnicas.

6. Que los artículos 10, 14, 15, 16, 17, 18 y 20 de las Disposiciones Administrativas de Carácter General para la Elaboración, Presentación y Valoración de Evaluaciones de Impacto en la Protección de Datos Personales del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, establecen los requisitos mínimos que deberán cumplir las evaluaciones de Impacto en la Protección de Datos Personales.

7. Que, de los requisitos señalados en los preceptos referidos en el punto anterior, el responsable **Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Michoacán,** dio cumplimiento a lo siguiente:

Descripción 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 que pretenda poner en operación o modificar.	
I. Su denominación	Inicio de funcionamiento del Sistema Informático.
II. Nombre de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento	Sistema de Servidores Púbicos y Particulares Sancionados, el cual integra la Plataforma Digital Estatal.

	intensivo o relevante de datos personales	
III.	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	**Objetivo general** El Sistema Estatal de Servidores Públicos y Particulares Sancionados tiene como finalidad que las sanciones firmes, impuestas a servidores públicos y particulares por la comisión de faltas administrativas en términos de la Ley de Responsabilidades Administrativas para el Estado de Michoacán de Ocampo y hechos de corrupción en términos de la legislación penal, queden inscritas en el mismo y su consulta deberá estar al alcance de las autoridades cuya competencia lo requiera, así como de la ciudadanía. **Objetivos específicos.** a) Servir de herramienta para la detección de servidores públicos o ex servidores públicos, que se encuentren impedidos por disposición legal o inhabilitado por resolución de autoridad competente para ocupar un empleo, cargo o comisión en el servicio público; o inhabilitado, en el caso de particulares, para realizar contrataciones con los Órganos del Estado. b) Contribuir al ejercicio de las atribuciones de las autoridades competentes para investigar y sancionar faltas administrativas o hechos de corrupción; c) Abonar a los trabajos que realiza el Comité Coordinador del Sistema Estatal Anticorrupción para la 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.
IV. Fundamento legal 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, conforme a sus facultades o atribuciones que la normatividad aplicable le confiera	- Artículo 113 de la *Constitución Política de los Estados Unidos Mexicanos.* - Artículos 9, fracción XII, 13, 48, 49, 52 y 53 de la *Ley General del Sistema Nacional Anticorrupción.* - Artículos 27, párrafos cuarto y quinto, 77 y 80, de la *Ley General de Responsabilidades Administrativas.* - Artículos 109 ter, de la *Constitución Política del Estado Libre y Soberano de Michoacán de Ocampo.* - Artículos 37, fracción X, 47, 48, 51 y 52 de la *Ley del Sistema Estatal Anticorrupción para el Estado de Michoacán de Ocampo.* -Artículos 25 y 59 de la *Ley de Responsabilidades Administrativas para el Estado de Michoacán de Ocampo.* - Artículo 18, fracción XXVI *Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción.* - Artículos 4, 5, fracción III, 48, 49 y 50 de las *Bases para el Funcionamiento de la Plataforma Digital Estatal,* emitidas por el Comité Coordinador.
V. Categorías de los 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	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 Servidores Públicos y Particulares Sancionados, de la Plataforma Digital Estatal, los titulares de los datos personales que almacenará y actualizara el mismo son los siguientes:

	Servidores Públicos Sancionados o ex servidores públicos: Información de los servidores públicos o ex servidores públicos sancionados, cuyas sanciones se inscriben en el Sistema de Servidores Públicos y Particulares Sancionados de la Plataforma Digital Estatal. **Particulares sancionados:** Información correspondiente a los licitantes, proveedores y contratistas sancionados, cuyas sanciones se inscriben en el Sistema de Servidores Públicos y Particulares Sancionados de la Plataforma Digital Estatal.
VI. Datos personales que serán objeto de tratamiento, distinguiendo, en su caso, los datos personales sensibles	**Datos de Identificación:** • Nombre(s) y apellidos • Registro Federal de Contribuyentes (RFC) con homoclave • Clave Única de Registro de Población (CURP) • Género **Datos del Empleo, Cargo o Comisión del Servidor Público o Ex Servidor Público Sancionado:** • Número de expediente del Procedimiento Administrativo de Responsabilidades • Nombre de la Institución o Dependencia a la que pertenece • Siglas de la Institución o Dependencia a la que pertenece • Clave de la Institución o Dependencia a la que pertenece. • Puesto del Servidor Público Sancionado • Clave del nivel del puesto del Servidor Público Sancionado • Autoridad encargada del proceso de sanción • Tipo de falta cometida

	• Tipo de sanción aplicada • Causa o motivo de la sanción • URL que apunta al documento en formato digital de la resolución emitida por el correspondiente Órgano Interno de Control • Fecha en la que se emite la resolución sancionatoria • Monto de la multa expresado en la moneda origen **Datos en caso de que el Servidor Público haya sido Inhabilitado:** • Plazo de la inhabilitación • Fecha inicial y final de la inhabilitación **Datos de particulares sancionados:** • Nombre(s) y apellidos del director general de la empresa al momento de la falta • CURP del director general de la empresa al momento de la falta • Nombre(s) y apellidos del apoderado legal de la empresa al momento de la falta • CURP del apoderado legal de la empresa al momento de la falta • Razón social de la empresa • Objeto social de la empresa • Nombre del país especificado en estándar ISO3166 • Código alpha 2 del país especificado en estándar ISO3166 • Tipo de persona • Nombre de la entidad federativa del Marco Geoestadístico Nacional • Clave de la entidad federativa del Marco Geoestadístico Nacional • Nombre del municipio del Marco Geoestadístico Nacional • Clave del municipio del Marco Geoestadístico Nacional

	• Código postal del domicilio • Nombre de la localidad o colonia • Clave de la localidad • Tipo de vialidad • Nombre de vialidad • Número exterior e interior del domicilio **Datos de identificación de la empresa en caso de que se encuentre en el extranjero:** • Código alpha 2 del país especificado en estándar ISO3166 **Datos del expediente derivado de la investigación de las autoridades investigadoras:** • Nombre de la Institución o Dependencia donde el contratista cometió la irregularidad • Siglas de la Institución o Dependencia donde el contratista cometió la irregularidad • Clave de la Institución o Dependencia donde el contratista cometió la irregularidad • RFC del contratista • Teléfono del contratista **Datos del contrato motivo:** • Objeto del contrato • OIC o Unidad responsable de la sanción • Tipo de falta • Tipo de sanción • Causa/motivo de la sanción • Acto que originó la investigación • Nombre(s) y apellidos del Titular del área de responsabilidades o Contralor del Órgano Interno de Control responsable de la información registrada • Sentido de la resolución

	• URL que apunta al documento en formato digital de la resolución emitida por el correspondiente Órgano Interno de Control • Fecha de notificación de la resolución **Datos en caso de que el particular haya tenido una sanción económica:** • Monto de la multa impuesta a la empresa • Moneda de la multa impuesta a la empresa, apegado al formato ISO 4217 • Valor de la moneda apegado al formato ISO 4217 **Datos en caso de que el particular haya sido inhabilitado:** • Plazo de la inhabilitación • Fecha inicial y final de la inhabilitación • Cualquier observación pertinente (sección que permite adjuntar referencias a cualquier documento que se considere de valor para transparentar el proceso de sanción).
VII. Finalidades del tratamiento intensivo o relevante de datos personales	a) Integrar el Sistema de Servidores Públicos y Particulares Sancionados a que se refieren los artículos 37, fracciones X y XI, 47, 48, 51, de la Ley del Sistema Estatal Anticorrupción; b) Que las sanciones impuestas a servidores públicos y particulares por la comisión de faltas administrativas en términos de la Ley de Responsabilidades Administrativas para el Estado de Michoacán de Ocampo y hechos de corrupción en términos de la legislación penal, queden inscritas dentro del mismo y su consulta deberá estar al alcance de las autoridades cuya competencia lo requiera.

	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 que dicte el Comité Coordinador del Sistema Nacional Anticorrupción, en términos de lo previsto en el artículo 48, fracción III, de la Ley del Sistema Estatal. d) Facilitar el ejercicio de las atribuciones de las autoridades competentes en la investigación y sanción de faltas administrativas y hechos de corrupción.
VIII. Procesos, fases o actividades operativas de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que involucren el tratamiento de datos personales, así como la descripción puntual de los mismos	Existen perfiles distintos, uno para ciudadanos y el otro para las autoridades. Se advierte que para cada órgano del Estado son 2 usuarios, es decir una persona encargada de capturar que deberá ser parte del Órgano Interno de Control y 1 validador que verificará que la información sea correcta, de preferencia el titular del Órgano Interno de Control. Ahora, respecto a los ciudadanos su vista será únicamente de datos públicos y el usuario de la autoridad que tenga acceso mediante una contraseña, podrá ver toda la información.
IX. Forma en que se recabarán los datos personales o, en su caso, las fuentes de las cuales provienen;	Se llevará a cabo de acuerdo al detalle explícito que se desarrolla en el apartado III de la Evaluación de Impacto.
X. Las transferencias 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	Se advierte en el documento de la evaluación de impacto que los datos públicos recabados y registrados a través del S3, serán transferidos a los siguientes órganos: -Poder Legislativo -Poder Judicial -Secretaría de Contraloría del Estado -Auditoría Superior de Michoacán

	tecnología, indicando las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales de carácter privado, nacionales y/o internacionales en su calidad de destinatarios de los datos personales, y las finalidades de estas transferencias.	-Fiscalía General del Estado -Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales -Tribunal de Justicia Administrativa del Estado de Michoacán -Instituto Electoral de Michoacán -Universidad Michoacana de San Nicolás de Hidalgo -Tribunal Electoral del Estado de Michoacán Comisión Estatal de Derechos Humanos -Al Fiscal Especializado en Delitos relacionados con Hechos de Corrupción -113 Órganos Internos de Control de los ayuntamientos del Estado de Michoacán de Ocampo. -Secretaría Ejecutiva del Sistema Nacional Anticorrupción a través de la Plataforma Digital Nacional. -Y, en su caso de ser requerida, a autoridades judiciales, instancias que conforme a lo previsto en el artículo 67 de la Ley General de Protección de Datos, se obligan a utilizarlos exclusivamente para los fines que fueron transferidos. Las transferencias de datos personales a dichos órganos se realizarán sin necesidad de recabar el consentimiento del titular, ya que se encuentra dentro de los supuestos de excepción previstos en los artículos 70 fracciones I y II de la Ley General de Protección de Datos; artículo 18, fracciones I y II de la Ley Local de Protección de Datos. Sin embargo, en la reunión de trabajo que se sostuvo el día 27 de mayo de la presente anualidad, una vez explicado que una transferencia de datos personales es toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona

		distinta del titular, del responsable o del encargado, los responsables del sistema especificaron que no harán transferencias de datos personales.
XI.	Tiempo de duración de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología, incluyendo aquél que corresponda específicamente al tratamiento intensivo o relevante de datos personales	La duración del S3, será por tiempo indefinido, ya que hasta la fecha no existe disposición legal, reglamentaria o administrativa, que establezca un plazo de vigencia para el funcionamiento del Sistema
XII.	La tecnología que se pretende utilizar para efectuar el tratamiento intensivo o relevante de datos personales	• Open API Specification • OAuth 2.0
XIII.	Las medidas de seguridad de carácter administrativo, físico y técnico a implementar de conformidad con lo previsto en la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables	**Administrativas** • Cada usuario posee un perfil de usuario específico para tener acceso únicamente a la información requerida para realizar sus funciones. • 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 con 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 un registro detallado sobre las peticiones realizadas por cada usuario, por lo tanto, es posible identificar quién y cuándo se tuvo acceso a la información. **Físicas** • Los datos son almacenados en un servidor físico ubicado en las instalaciones de la Secretaría.

	• El acceso al servidor se encuentra restringido con medidas estrictas 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 fallos 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 naciones que permiten el correcto aislamiento. **Tecnológicas** • Cada usuario posee 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. • La sesión del usuario tiene un límite de vida de 5 minutos después de la última acción del usuario, transcurrido dicho limite la sesión se cierra 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.
XIV. Nombre y cargo del servidor o de los servidores públicos que cuentan con facultad expresa para decidir, aprobar o autorizar la puesta en operación o modificación de la	Lic. Ana María Vargas Vélez, Secretaria Técnica de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción. Lic. Brenda Patricia Gamiño Cruzaley, Jefa de la Unidad de Transparencia, Acceso a la Información Pública y

	política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales	Protección de Datos Personales de la SESEA. Ing. Lizbeth Pureco Pedraza, Jefa del Departamento de Servicios Tecnológicos y Plataforma Digital de la Secretaría Ejecutiva.
XV.	Cualquier otra información o documentos que considere conveniente hacer del conocimiento del Instituto o los organismos garantes	No se presentaron.
Justificación de la necesidad de implementar o modificar la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología.		
I.	Si la o las medidas propuestas son susceptibles o idóneas para garantizar el derecho a la protección de datos personales de los titulares	Se advierte que las medidas propuestas son adecuadas, ya que se cumple con lo señalado en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán.
II.	Si la o las medidas propuestas son las estrictamente necesarias, en el sentido de ser las más moderadas para garantizar el derecho a la protección de datos personales de los titulares	De acuerdo a la documentación que maneja el proyecto de la PDN se deberá evaluar las capacidades de los sistemas de información en el caso del diseño de arquitectura informática, ya que la PDN no concentra información, más bien llama a la información de los diferentes servicios implementados en cada estado, que se conectan por medio de las API's y se autentifican por el protocolo OAuth 2.0, por lo que los niveles de seguridad son altos y de acuerdo a los roles de usuario que se manejan, la información podrá ser entregada de acuerdo a las facultades o rol de usuario. Open API Specification Una API es un conjunto de definiciones y protocolos que se utiliza para

	desarrollar e integrar el software de las aplicaciones, en este caso es una especificación para archivos de interfaz legibles por máquina para describir, producir, consumir y visualizar servicios web (RESTful). Las características más importantes de OpenAPI son las siguientes: Ayuda a establecer un buen diseño de las APIs Documentación completa Testing más rápido gracias a la generación de un sandbox Mejora el Time to market Generación de un portal de documentación que describe la API, en formaato human-readable OAuth 2.0 Es un estándar abierto para la autorización de APIs, que nos permite compartir información entre sitios sin tener que compartir la identidad. Es un mecanismo utilizado a día de hoy por grandes compañías como Google, Facebook, Microsoft, Twitter, GitHub o LinkedIn, entre otras muchas, por lo que su respaldo en seguridad es muy confiable. Implementación del estándar.
III. Si la o las medidas son equilibradas en función del mayor número de beneficios o ventajas que perjuicios para el garantizar el derecho a la protección de datos personales de los titulares	Se advierte que la implementación del Sistema de Servidores Púbicos y Particulares Sancionados (S3), genera más beneficios que perjuicios, ya que permite conocer las sanciones de los servidores públicos, sin vulnerar datos personales, lo que además de ser una obligación legal es un ejercicio de anticorrupción.

Ciclo de vida de los datos personales	
I. Las fuentes internas y/o externas, así como los medios y procedimientos a través de los cuales se recabarán los datos personales, o bien, son recabados	No se especifican.
II. Las áreas, grupos o personas que llevarán a cabo operaciones específicas de tratamiento con los datos personales	La información del sistema podrá ser consultada por entidades federativas, organismos de gobierno y público en general. Los ciudadanos en general solamente pueden ver los datos de servidores públicos que han sido inhabilitados por resolución firme de la autoridad competente, mientras que el usuario autoridad puede ver todos los datos (públicos y privados) de servidores públicos que han recibido una o más sanciones graves y no graves por resolución firme de la autoridad competente.
III. Los plazos de conservación o almacenamiento de los datos personales	Una vez que el plazo de la sanción ha expirado, el acceso al registro será bloqueado al público en general, teniendo acceso al registro histórico únicamente una autoridad competente que lo requiera para llevar a cabo sus funciones.
IV. Las técnicas a utilizar para garantizar el borrado seguro de los datos personales	No se especifican.

El artículo 74 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y el artículo 70 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, prevén la obligación de llevar a cabo una evaluación de impacto relativa a la protección de datos, cuando implique el tratamiento intensivo o relevante de datos personales; en términos de los numerales 75 y 71 de las mismas leyes respectivamente, 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 efectúen o pretendan efectuar transferencias de datos personales.

Con base en lo anteriormente expuesto, en apego al artículo 70, 72 y 73 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo y al 28 de las Disposiciones Administrativas de Carácter General para la elaboración, presentación y valoración en Evaluaciones de Impacto, el Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales, visto el proyecto de evaluación de impacto de protección de datos personales del *Sistema de Servidores Públicos y Particulares Sancionados, de la Plataforma Digital Estatal*, que presenta la Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Michoacán, y el oficio número SEA-SE-ST-461/2021 de fecha veinte de abril de la presente anualidad, en el que se formula una consulta sobre la necesidad o no de realizar una evaluación de impacto relativa a la protección y tratamiento de datos personales; se **emite** el siguiente **dictamen**, previo estudio técnico y jurídico de la información para evaluar los riesgos de esta nueva plataforma.

DICTAMEN

PRIMERO. Por lo expuesto en el punto número 7 de las consideraciones del presente instrumento, se determina que el *Sistema de Servidores Públicos y Particulares Sancionados, de la Plataforma Digital Estatal,* desarrollado por el responsable **Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Michoacán, cumple** con lo establecido en el numeral 71 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, así como 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 en Evaluaciones de Impacto, por lo cual para la implementación del sistema en mención, si se requiere una evaluación de impacto relativa a la protección de datos y resulta necesario emitir recomendaciones al respecto.

SEGUNDO. En el proyecto de evaluación de impacto de protección de datos personales del *Sistema de Servidores Públicos y Particulares Sancionados, de la*

Plataforma Digital Estatal, se advierte que con la finalidad de que las sanciones firmes, impuestas a servidores públicos y particulares por la comisión de faltas administrativas en términos de la *Ley de Responsabilidades Administrativas para el Estado de Michoacán de Ocampo* y hechos de corrupción en términos de la legislación penal, queden inscritas en el mismo y su consulta esté al alcance de las autoridades cuya competencia lo requiera, así como de la ciudadanía.

El tratamiento de datos de identificación CURP, RFC, y género de los servidores y ex servidores públicos del estado de Michoacán de Ocampo descritos en el proyecto de evaluación de impacto, no es necesario, se sugiere tomar en cuenta que los datos personales recabados, deberán de ser exactos, completos y correctos, por ello, lo más útil sería pedir únicamente aquellos indispensables estrictamente para el trámite específico; teniendo en cuenta el riesgo detectado, aunque éste se considera obvio, es posible su reducción adoptando las sugerencias realizadas.

TERCERO. Se sugiere especificar cuál será el proceso para el borrado de datos, mediante una programación basada en el eliminado del texto original.

CUARTO. Es recomendable que cada una de las personas que tengan acceso para alimentar el sistema, así como los ingenieros involucrados en el mismo, los capturadores, validadores y las autoridades con usuario y contraseña firmen un acuerdo de confidencialidad.

QUINTO. Es conveniente especificar de donde se obtienen los datos de las sanciones que contienen datos personales, si derivan de algún expediente, etc.

SEXTO. El *Sistema de Servidores Públicos y Particulares Sancionados, de la Plataforma Digital Estatal,* de acuerdo con la opinión de la Dirección de Plataforma y Sistemas del Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales, al momento de su presentación no cuenta con algún riesgo de que no haga su función, para lo que fue creado, ya que el sistema hace lo que el usuario le solicita ejecutar.

SÉPTIMO. Es necesario realizar capacitaciones constantes sobre el conocimiento del uso y características, los perfiles de usuarios existentes, y el procedimiento con

la finalidad de garantizar la integridad, privacidad y seguridad de los datos personales de los involucrados en el sistema.

OCTAVO. Teniendo en cuenta este análisis, es fundamental señalar que debe existir un fluido canal de comunicación entre las áreas involucradas en las operaciones del tratamiento, de manera tal que pueda obtenerse información relevante sobre el ciclo de vida de los datos asociados al tratamiento de manera continua y el responsable del tratamiento siempre se encuentre en disposición de definirlo.

NOVENO. El responsable del tratamiento debe contar con un plan de acción que le permitirá demostrar, desde el momento en que aplique las medidas de manera efectiva, que se garantizan los derechos y libertades de las personas y la seguridad de los datos en el normal desarrollo de su actividad propia.

Sin embargo, la evaluación de impacto relativa a la protección de datos no es sino un ejercicio teórico que requiere su puesta en práctica de forma íntegra para garantizar los derechos y las libertades de los interesados.

Es fundamental que se realice una adecuada supervisión y una posterior revisión de la implantación de las medidas de control definidas en la evaluación de impacto para reducir el riesgo inherente hasta un riesgo residual que permita llevar a cabo el tratamiento garantizando los derechos y libertades de las personas físicas.

Debe tenerse en cuenta que el riesgo cero no existe, por lo que las medidas de control propuestas tienen como objetivo minimizar el riesgo asociado a una operación de tratamiento hasta un nivel aceptable para poder llevar a cabo las mismas garantizando los derechos y libertades de los interesados.

Por todo ello:

La evaluación de impacto relativa a la protección de datos en el *Sistema de Servidores Públicos y Particulares Sancionados, de la Plataforma Digital Estatal,* desarrollado por el responsable Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Michoacán, ha tenido un resultado **favorable,** lo que quiere decir, que por la forma de su desarrollo **no supone una amenaza para los derechos y libertades de los interesados en este momento,** por lo anterior, la implementación

de dicho sistema se podrá llevar a cabo siempre y cuando se apliquen todas las medidas de seguridad incluidas en el proyecto de la evaluación de impacto presentado ante este órgano garante, pues de esa manera no existirá un alto riesgo para los derechos y libertades de los interesados en relación con las operaciones de tratamiento analizadas.

En conclusión, debe señalarse que la evaluación de impacto es un proceso continuo que no se agota con la emisión del presente dictamen, ya que, constantemente, deberá revisarse si los tratamientos siguen siendo conformes con la evaluación a la que hubieran sido sometidos y, en todo caso, hacerlo cuando exista un cambio sustancial en alguna de las operaciones de tratamiento.

DÉCIMO. Notifíquese al responsable **Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Michoacán.**

Así lo acordó el Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales, el día 10 de junio de la anualidad en curso.

Dra. Reyna Lizbeth Ortega Silva

Comisionada Presidenta del Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales

Mtra. Areli Yamilet Navarrete Naranjo

Comisionada del Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales

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