Documento en el cual se especifiquen los sistemas de supervisión y vigilancia de los tratamientos de datos personales del Instituto de Administración y Avalúos de Bienes Nacionales

CONTENIDO

I.- PRESENTACIÓN

El Instituto de Administración y Avalúos de Bienes Nacionales (INDAABIN) en términos del artículo 31, fracción XXIX, de la Ley Orgánica de la Administración Pública Federal, en relación con el Segundo Transitorio, del Decreto publicado el 18 de julio de 2016, en el Diario Oficial de la Federación, por el que se reforman, adicionan y derogan diversas disposiciones de la Ley Orgánica de la Administración Pública Federal, 2, apartado D, fracción VI, y 6°, fracción XXXV, del Reglamento Interior de la Secretaría de Hacienda y Crédito Público, es un órgano administrativo desconcentrado de la Secretaría de Hacienda y Crédito Público que le está jerárquicamente subordinado y tiene la organización y las atribuciones que le confiere su Reglamento, al que le corresponde el despacho de, entre otros asuntos, el de conducir la política inmobiliaria de la Administración Pública Federal salvo por lo que se refiere a las playas, zona federal marítimo terrestre, terrenos ganados al mar o cualquier depósito de aguas marítimas y demás zonas federales.

El INDAABIN al ser un órgano administrativo desconcentrado de la Secretaría de Hacienda y Crédito Público, forma parte de la administración pública federal, por lo que es considerado sujeto obligado en términos del artículo 1 párrafo quinto de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y en consecuencia, debe cumplir con las disposiciones establecidas en materia de protección de datos personales.

En ese sentido, el artículo 6, Base A, fracción II de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) establece que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes, en tanto que su diverso 16, segundo párrafo dispone que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, lo cual garantiza a los titulares el derecho a su privacidad, el buen uso de su información personal y su derecho a la autodeterminación informativa, el cual implica que toda persona decida de manera libre e informada, sobre el uso de la información que les pertenece.

Por otro lado, la LGPDPPSO, establece que es obligación de todo responsable proteger los datos personales que trate, garantizar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información, y responsabilidad, los deberes de seguridad y confidencialidad, y las obligaciones derivadas de dicha Ley.

Para tales efectos, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), emitió los Lineamientos Generales de Protección de Datos Personales para el Sector Público (LGPDPSP), en el que desarrolló y concentró en un solo

cuerpo normativo las obligaciones señaladas en la LGPDPPSO, con la finalidad facilitar y hacer más comprensible y simple el conocimiento y la exigibilidad del derecho a la protección de datos personales en el sector público federal, así como evitar la fragmentación o atomización en innumerables ordenamientos que pudiera repercutir en el cumplimiento efectivo de la dicha Ley por parte de los responsables del ámbito federal, o bien, hacer inaccesible el derecho para cualquier persona.

De esa manera, de conformidad a lo establecido en los artículos 16, último párrafo, 45, 54, 72, 107 y 118 de los LGPDPSP, la carga de la prueba para acreditar el cumplimiento de los principios, deberes y obligaciones relativas a la protección de datos personales en su tratamiento, en todo momento, recaerá en el responsable por lo que deberán adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la LGPDPPSO y los LGPDPSP.

Asimismo, el 26 de noviembre de 2021 el INAI emitió el Acuerdo mediante el cual se aprueban los Instrumentos Técnicos de Evaluación que refiere el Título Décimo de los LGPDPSP, en los cuales se estableció el tipo de evaluación, la metodología, los criterios, los formatos y los indicadores de cumplimiento que deberán observar los sujetos obligados en el tratamiento de datos personales.

En ese sentido, a efecto de salvaguardar el derecho humano a la protección de datos personales y en observancia al principio de responsabilidad que establece que el responsable del tratamiento de datos personales deberá implementar mecanismos para el cumplimiento de los principios, deberes y obligaciones establecidos en la LGPDPPSO y los LGPDPSP, se considera necesario establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales la cual de observancia obligatoria para el personal del Instituto que realice un tratamiento de datos personales, la cual instituya un programa de trabajo dirigido a la protección de los datos personales en posesión del INDAABIN.

II. OBJETO

Primero. – El presente instrumento tendrá por objeto regular el procedimiento de supervisión y vigilancia sobre el cumplimiento de la política de protección de datos personales del Instituto de Administración y Avalúos de Bienes Nacionales, y el programa de trabajo que observe las medidas necesarias para proteger los datos personales en su posesión.

Segundo. – El presente instrumento normativo tiene como finalidad supervisar y vigilar que el personal que labora en el INDAABIN, realice un tratamiento de datos personales en estricto apego a la Política de Protección de Datos Personales de este Instituto, a los principios, deberes y obligaciones previstos en la LGPDPPSO y demás disposiciones aplicables, lo cual permitirá garantizar la adecuada protección de los datos personales y el ejercicio de los derechos de

Acceso, Rectificación, Cancelación, Oposición y Portabilidad al tratamiento de datos personales por parte de sus titulares.

Tercero. – Garantizar el cumplimiento de los principios, deberes y obligaciones en materia de protección de datos personales para otorgar certeza jurídica a sus titulares sobre el control su información personal; que incluyen el derecho a saber quién posee sus datos personales, el tratamiento al que están siendo sometidos y el poder de oponerse a esa posesión y tratamiento.

III. ALCANCE

El presente instrumento es de observancia obligatoria para todo el personal de las unidades administrativas del INDAABIN, involucrados en el tratamiento de datos personales, así como, para los integrantes de su Comité de Transparencia (en lo sucesivo CT), con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización, en la que se encuentren los datos personales, los cuales deben observar lo establecido en la Política de Protección de Datos Personales de este Instituto.

CAPÍTULO I. MARCO NORMATIVO

1. Que el artículo 6, Base A, fracción II de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) establece que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

2. Que el artículo 16, segundo párrafo de la CPEUM establece que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

3. Que el 26 de enero de 2017 se publicó en el Diario Oficial de la Federación el Decreto por el cual se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), misma que en su artículo 1, párrafo segundo y cuarto establece que todas sus disposiciones según corresponda en el ámbito de su competencia son de aplicación y observancia directa para los sujetos obligados pertenecientes al orden federal, asimismo que tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.

4. Que el artículo 2, fracciones II, IV y VI de la LGPDPPSO tiene entre sus objetivos, establecer las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, mediante procedimientos sencillos y expeditos; garantizar la observancia de los principios de protección de datos personales, así como garantizar que toda persona pueda ejercer el derecho a la protección de los datos personales, entre otros.

5. Que el artículo 16 de la LGPDPPSO, establece la observancia por parte del responsable, de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales, así como en su artículo 31 determina que el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

6. Que los artículos 29 y 30, fracciones I y VII, de la LGPDPPSO, el responsable deberá implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en dicha Ley, entre los cuales se encuentran, destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales, así como diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la LGPDPPSO y las demás que resulten aplicables en la materia.

7. Que los artículos 43 a 47 de la LGPDPPSO establecen los derechos de acceso, rectificación, cancelación y oposición (ARCO) que tienen los titulares de los datos personales y la forma en la que podrán ejercerlos.

8. Que el artículo 83 de la LGPDPPSO establece que cada sujeto obligado contará con un Comité de Transparencia (CT), mismo que se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y demás normatividad aplicable, el cual será la autoridad máxima en materia de protección de datos personales.

9. Que el artículo 30, fracciones I y II y 84, fracción I de la LGPDPPSO, prevé que los responsables tendrán que coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en

aquellas disposiciones que resulten aplicables en la materia; por su parte el CT, entre otras, tendrán facultades y atribuciones para coordinar, supervisar y realizar, en términos de las disposiciones aplicables, las acciones y procedimientos para garantizar el derecho a la protección de los datos personales en la organización del responsable.

Por su parte el artículo 30, fracción V, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece que entre los mecanismos que se deberán adoptar para cumplir con el principio de responsabilidad, se encuentra el de establecer un sistema de supervisión y vigilancia, incluyendo auditorías, que permita comprobar el cumplimiento de las políticas de protección de datos personales.

10. Que el 26 de enero de 2018, se publicaron en el Diario Oficial de la Federación los Lineamientos Generales de Protección de Datos Personales para el Sector Público (LGPDPSP), mismos que establece en su artículo 46, párrafo primero, que el responsable deberá adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la LGPDPPSO y en los referidos Lineamientos, así como establecer aquellos mecanismos necesarios para evidenciar dicho cumplimiento ante los titulares y el INAI.

11. El 12 de febrero de 2018 se publicó en el Diario Oficial de la Federación, el Acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, mediante el cual se aprueban los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, en cuyo artículo 14 dispone que para la portabilidad de datos personales el responsable deberá observar los requisitos, plazos, condiciones, términos y procedimientos establecidos en el Título tercero, Capítulo II de la LGPDPPSO.

12. Que conforme a lo dispuesto por el artículo 247 de los Lineamientos Generales, el Instituto aprobará los Instrumentos Técnicos de Evaluación que sean necesarios para medir el desempeño de los responsables respecto al cumplimiento de las obligaciones previstas en la Ley General y demás disposiciones aplicables en la materia; los cuales contemplarán, al menos, el tipo de evaluación, la metodología, los criterios, los formatos, por lo que el 26 de noviembre de 2021 se publicó en el Diario Oficial de la Federación el ACUERDO mediante el cual se aprueban los Instrumentos Técnicos que refiere el Título Décimo de los LGPDPSP en los cuales se estableció el tipo de evaluación, la metodología, los criterios, los formatos y los indicadores de cumplimiento que deberán cumplir los sujetos obligados en el tratamiento de datos personales.

Por las razones expuestas y con fundamento en lo dispuesto por los artículos 6, Base A, fracción II y 16, segundo párrafo de la Constitución Política de los Estados Unidos

Mexicanos; 30, fracción V de la LGPDPPSO, así como el diverso 49 y 63 de los LGPDPSP, el CT emite el presente instrumento normativo en el cual se especifiquen los sistemas de supervisión y vigilancia.

DE LAS BASES PARA ESTABLECER LOS SISTEMAS DE SUPERVISIÓN Y VIGILANCIA

Primero. El procedimiento de verificación se llevará de conformidad con lo dispuesto en el presente instrumento jurídico.

Segundo. El Comité de Transparencia a través de la Unidad de Transparencia llevará a cabo las acciones de verificación del cumplimiento de la Política de Protección de Datos Personales de este Instituto, que se implementará en cada tratamiento de datos personales que se realice al interior del mismo (censal o muestral).

Tercero. Las acciones de verificación se realizarán al menos una vez cada año y de acuerdo a lo establecido en el Programa de Protección de Datos Personales que emita el Comité de Transparencia, o bien, en casos extraordinarios como consecuencia de alguna denuncia por vulneración de datos personales que formule cualquier titular de los mismos. De conformidad con el artículo 30, fracciones IV y V de la Ley General, en relación con el artículo 49 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Cuarto. Las verificaciones se realizarán a los tratamientos de datos personales que realice cada una de las unidades administrativas del Instituto, en las cuales se hará el monitoreo de las siguientes actividades:

1) Las medidas de seguridad implementadas en el tratamiento de datos personales.

2) La implementación de las políticas, programas, lineamientos, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua, aprobados por el Comité de Transparencia.

3) Los nuevos tratamientos que se incluyan en la gestión de riesgos.

4) Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras.

5)Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas.

6) La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.

7) Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.

8) El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.

9) Los incidentes y vulneraciones de seguridad ocurridas.

10) Las que determine el Comité de Transparencia en el Programa que para tal efecto emita.

Quinto. Para minimizar la interferencia entre las actividades de verificación y los procesos de trabajo del ente verificado, se considerará lo siguiente:

a) Planificar la visita.

– Asegurar la autorización y acceso a aquellas partes del ente verificado, para visitarlas de acuerdo con el alcance del Programa de Protección de Datos Personales que emita el Comité de Transparencia;

– Proporcionar la información adecuada a las personas responsables de verificar sobre seguridad física de la información a consultarse;

– Confirmar los acuerdos con el ente verificado sobre el uso de dispositivos móviles y cámaras, incluyendo la grabación de la información como fotografías de ubicaciones y equipos, copias de capturas de pantalla o fotocopias de documentos, videos de actividades y entrevistas, considerando en todo momento las cuestiones de seguridad y confidencialidad;

– Asegurarse de que el personal auditado será informado sobre los objetivos y el alcance de la verificación;

b) Actividades en sitio: – Evitar cualquier interrupción innecesaria de los procedimientos operativos.

Sexto.- En ese sentido, el Instituto desarrollará el cumplimiento de dicha obligación a través de los siguientes mecanismos:

Para efecto de realizar las verificaciones, le corresponderá a la Unidad de Transparencia ejecutar el mecanismo de monitoreo y supervisión de las medidas de seguridad implementadas en la protección de datos personales, a través de los siguientes ejes:

a) Etapa de Monitoreo. La Unidad de Transparencia requerirá a cada una de las áreas que reportaron tratamientos de datos personales, a través de sus inventarios, la elaboración de un reporte, en el que deberán precisarse:

	Sí	No
1. Se han definido y se establecen y mantienen las medidas de seguridad administrativas, técnicas y físicas necesarias para la protección de los datos personales.	☐	☐
2. Se ha revisado el marco normativo que regula en lo particular el tratamiento de datos personales en cuestión, a fin de identificar si éste contempla medidas de seguridad específicas o adicionales a las previstas en la LGPDPPSO y los Lineamientos Generales, y se ha definido la procedencia de su implementación.	☐	☐
3. Se han definido las funciones, obligaciones y cadena de mando de cada servidor público que trata datos personales, por unidad administrativa.	☐	☐
4. Se ha comunicado a cada servidor público sus funciones, obligaciones y cadena de mando con relación al tratamiento de datos personales que efectúa.	☐	☐
5. Se ha elaborado el inventario de datos personales con los siguientes elementos:	☐	☐

• El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales; • Las finalidades de cada tratamiento de datos personales; • El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no; • El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales; • La lista de servidores públicos que tienen acceso a los sistemas de tratamiento; • En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y • En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que las justifican.		
6. En el inventario de datos personales se tomó en cuenta el ciclo de vida de los datos personales, conforme a lo siguiente: • La obtención de los datos personales; • El almacenamiento de los datos personales; • El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin; • La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen; • El bloqueo de los datos personales, en su caso, y • La cancelación, supresión o destrucción de los datos personales.	☐	☐
7. Se ha realizado el análisis de riesgo, considerando lo siguiente: • Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico; • El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida; • El valor y exposición de los activos involucrados en el tratamiento de los datos personales; • Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida; • El riesgo inherente a los datos personales tratados, contemplando el ciclo de vida de los datos personales, las amenazas y vulnerabilidades existentes para los datos personales y los recursos o activos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal o cualquier otro recurso humano o material, entre otros; • La sensibilidad de los datos personales tratados; • El desarrollo tecnológico; • Las transferencias de datos personales que se realicen; • El número de titulares; • Las vulneraciones previas ocurridas en los sistemas de tratamiento, y • El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.	☐	☐
8. Se ha realizado el análisis de brecha, tomando en cuenta lo siguiente: • Las medidas de seguridad existentes y efectivas; • Las medidas de seguridad faltantes, y	☐	☐

• La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.		
10. Se monitorea y revisa de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, tomando en cuenta lo siguiente: • Los nuevos activos que se incluyan en la gestión de riesgos; • Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras; • Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas; • La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes; • Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir; • El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y • Los incidentes y vulneraciones de seguridad ocurridas.	☐	☐

2) Etapa de Supervisión. La Unidad de Transparencia analizará los reportes de las áreas, verificando aquellos puntos en los que se hubiera reportado "No" como respuesta y se emitirá un dictamen o ficha técnica en el que se plasmarán las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad, con la finalidad de proteger los datos personales.

Las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad de datos personales se harán de conocimiento del Comité de Transparencia a efecto que niegue, modifique o apruebe la procedencia de las observaciones detectadas en los tratamientos de datos personales de las unidades administrativas del Instituto, las cuales se harán de conocimiento al área competente con la finalidad que las unidades administrativas atiendan y remitan las evidencias de su cumplimiento.

Concluido dicho periodo, se emitirán las acciones de mejora que deban implementar las unidades administrativas de en sus respectivos tratamientos con la finalidad de salvaguardar los principios de protección de datos personales previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia.

SÉPTIMO. - Mecanismos de auditoría en materia de datos personales. Entre los mecanismos que se deben adoptar para cumplir con el principio de responsabilidad el artículo 30, fracción V, de la Ley General de Datos Personales en Posesión de Sujetos Obligados, establece que se deberá mantener un sistema de supervisión y vigilancia, incluyendo auditorías, que permita comprobar el cumplimiento de las políticas de datos personales.

El artículo 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales), dispone que además del monitoreo y supervisión periódica de las medidas de seguridad, se deberá contar con un **programa de auditoría para revisar la eficacia y eficiencia del sistema de gestión.**

Por tanto, resulta necesario establecer un mecanismo que permita dar cumplimiento a las disposiciones antes citadas, mismo que se desarrolla de la siguiente manera:

Las auditorías en materia de datos personales tendrán las finalidades siguientes:

- ✓ Verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Es importante señalar que las auditorías que se realicen tendrán por objeto analizar el cumplimiento de los deberes y principios en los tratamientos de los datos personales que fueron documentados a través de los inventarios por cada una de las áreas, por lo que, la Unidad de Transparencia propondrá al Comité de Transparencia la programación por inventario y, el deber o principio que deberá ser objeto de la auditoría.

Lo anterior, permitirá identificar de forma ordenada las acciones y mejoras que habrán de implementarse para el adecuado manejo y protección de los datos personales.

TRANSITORIOS

PRIMERO. – Los presentes Lineamientos entrarán en vigor una vez que sean oficialmente notificados a las diversas áreas del INDAABIN.

SEGUNDO. – Que a través de la Unidad de Transparencia, se publiquen los presentes Lineamientos en el SIPOT de esta dependencia.