ANÁLISIS TÉCNICO PRELIMINAR

No. Expediente: 0172-1CP2-26

I.- DATOS DE IDENTIFICACIÓN DE LA INICIATIVA	
1.- Nombre de la Iniciativa.	Que reforma, adiciona y deroga diversas disposiciones de las Leyes de Seguridad Nacional; General de Protección de Datos Personales en Posesión de Sujetos Obligados; y Orgánica de la Administración Pública Federal, y del Código Penal Federal, en materia de protección de bases de datos poblacionales estratégicas del Estado.
2.- Tema de la Iniciativa.	Seguridad Nacional y Protección de Datos Personales.
3.- Nombre de quien presenta la Iniciativa.	Dip. Felipe Miguel Delgado Carrillo.
4.- Grupo Parlamentario del Partido Político al que pertenece.	PVEM.
5.- Fecha de presentación ante el Pleno de la Comisión Permanente.	21 de enero de 2026.
6.- Fecha de publicación en la Gaceta Parlamentaria.	21 de enero de 2026.
7.- Turno a Comisión.	Unidas de Seguridad Ciudadana y de Gobernación y Población, con opinión de Justicia

II.- SINOPSIS

Establecer como amenazas a la Seguridad Nacional cualquier acto dirigido a destruir, alterar, extraer, copiar, acceder o inutilizar, sin autorización, la información contenida en bases de datos poblacionales estratégicas bajo resguardo del Estado, los actos tendentes a facilitar, encubrir o aprovechar dichas conductas y todo atentado cibernético, intrusión, divulgación no autorizada o sabotaje que vulnere la integridad, confidencialidad o disponibilidad de las bases de datos poblacionales estratégicas del país. Precisar que las bases de datos poblacionales estratégicas en poder del Estado Mexicano se consideran parte de la infraestructura crítica nacional. Agregar las definiciones de Bases de Datos Poblacionales Estratégicas y Base de Datos Crítica del Estado. Establecer la obligación de los responsables de estas bases de datos críticos a implementar medidas de seguridad reforzadas de nivel alto, señalando los criterios mínimos. Señalar la obligación de las instituciones responsables estas bases a través de su Comité de Transparencia o equivalente, a designar un Enlace de Seguridad de la Información encargado de supervisar el debido cumplimiento de las medidas de protección reforzadas, el perfil de este servidor público, las funciones a desempeñar. Determinar en materia de transparencia y acceso a la información aplicable a las bases de datos críticas observar un equilibrio entre la máxima publicidad y la salvaguarda de la seguridad nacional y la privacidad señalando los criterios a considerar para tales efectos. Establecer como atribución de la Agencia de Transformación Digital y Telecomunicaciones coordinar, con las dependencias de la administración pública federal que sean responsables de estas de bases de datos críticas las acciones orientadas a la protección, estandarización e interoperabilidad de dichas bases de datos. Incluir el delito de acceso ilícito a una base de datos crítica del Estado; el de comercialización indebida de datos personales de una base de datos crítica del Estado; el de manejo ilícito de datos en bases de datos críticas del Estado, y el de omisión o negligencia grave en el manejo de bases de datos críticas del Estado, sus respectivas sanciones y agravantes.

III.- ANÁLISIS DE CONSTITUCIONALIDAD

El derecho de iniciativa se fundamenta en la fracción II del artículo 71 y la facultad del Congreso de la Unión para legislar en la materia se sustenta en la fracción XXIX-M del artículo 73 respecto a la Ley de Seguridad Nacional, en las fracciones XXIX-O, XXIX-S del artículo 73 en relación con los artículos 6º Apartado A, fracción VIII y 16, párrafo segundo respecto a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en la fracción XXXI del artículo 73 en relación con el artículo 90 respeto de la Ley Orgánica de la Administración Pública Federal; y en la fracción XXI, del artículo 73 del Código Penal Federal, todos de la Constitución Política de los Estados Unidos Mexicanos.

IV.- ANÁLISIS DE TÉCNICA LEGISLATIVA

En la parte relativa al texto legal que se propone, se sugiere lo siguiente:

- Conforme a la terminología y desarrollo del proceso legislativo, previstos por los artículos 70 y 72 constitucionales, respectivamente, usar el término "Iniciativa con Proyecto de Decreto", toda vez que éste aún se encuentra en proceso de aprobación.

La iniciativa, salvo la observación antes señalada cumple en general con los requisitos formales que se exigen en la práctica parlamentaria y que son los siguientes:

Ser formulada por escrito, tener un título, contener el nombre y firma de la persona que presenta la iniciativa, una parte expositiva de motivos, el texto legal que se propone, el artículo transitorio que señala la entrada en vigor, la fecha de elaboración y ser publicada en la Gaceta Parlamentaria.

V.- CUADRO COMPARATIVO DEL TEXTO VIGENTE Y DEL TEXTO QUE SE PROPONE

TEXTO VIGENTE	TEXTO QUE SE PROPONE
LEY DE SEGURIDAD NACIONAL	**DECRETO POR EL QUE SE REFORMAN, ADICIONAN Y DEROGAN DIVERSAS DISPOSICIONES DE LA LEY DE SEGURIDAD NACIONAL, DE LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS, DE LA LEY ORGÁNICA DE LA ADMINISTRACIÓN PÚBLICA FEDERAL Y DEL CÓDIGO PENAL FEDERAL, EN MATERIA DE PROTECCIÓN DE BASES DE DATOS POBLACIONALES ESTRATÉGICAS DEL ESTADO.**
	Artículo Primero. Se **reforman** las fracciones XII y XIII y se **adiciona** una fracción XIV al artículo 5; se adiciona un artículo 6 Bis a la Ley de Seguridad Nacional, para quedar como sigue:
Artículo 5.- Para los efectos de la presente Ley, son amenazas a la Seguridad Nacional:	Artículo 5.- …:
I. a **XI**. ...	I. a XI. ...
XII. Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos, y	XII. Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos**,**

XIII. [*Actos ilícitos en contra del fisco federal a los que hace referencia el artículo 167 del Código Nacional de Procedimientos Penales*.] Fracción declarada inválida por sentencia de la SCJN a Acción de Inconstitucionalidad notificada para efectos legales 25-11-2022 y publicada DOF 20-08-2025	XIII**.** Actos ilícitos en contra del fisco federal a los que hace referencia el artículo 167 del Código Nacional de Procedimientos Penales, **y**
No tiene correlativo	**XIV. Cualquier acto dirigido a destruir, alterar, extraer, copiar, acceder o inutilizar, sin autorización, la información contenida en bases de datos poblacionales estratégicas bajo resguardo del Estado, así como los actos tendentes a facilitar, encubrir o aprovechar dichas conductas. En general, se considerará amenaza a la seguridad nacional todo atentado cibernético, intrusión, divulgación no autorizada o sabotaje que vulnere la integridad, confidencialidad o disponibilidad de las bases de datos poblacionales estratégicas del país.**
No tiene correlativo	**Artículo 6 Bis.- Las bases de datos poblacionales estratégicas en poder del Estado Mexicano se consideran parte de la infraestructura crítica nacional, por ser indispensables para la seguridad nacional y el interés público. Se entiende por bases de datos poblacionales estratégicas aquellas administradas por autoridades públicas que contienen datos personales de una proporción significativa de la población o datos de identidad de los habitantes, cuya alteración, destrucción, divulgación o uso ilícito podría:**

No tiene correlativo	**I. Comprometer la seguridad nacional, la seguridad interior o la seguridad pública;** **II. Afectar la continuidad de servicios esenciales del Estado o la garantía de derechos fundamentales de la población a gran escala, o** **III. Lesionar la gobernabilidad democrática, la integridad de procesos electorales, la estabilidad económica o la confianza ciudadana en las instituciones, mediante el uso indebido de dicha información.**
LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS. **No tiene correlativo** **No tiene correlativo**	**Artículo Segundo.** Se **adiciona** un Capítulo III, denominado "*De las Bases de Datos Críticas del Estado*", que contiene los artículos 76 Bis, 76 Ter, 76 Quáter y 76 Quintus, al Título Sexto de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, para quedar como sigue: **Capítulo III** **De las Bases de Datos Críticas del Estado** **Artículo 76 Bis. Para efectos de esta ley, se considera Base de Datos Crítica del Estado aquella base de datos en posesión de sujetos obligados que, por su naturaleza estratégica o por el volumen o sensibilidad de los datos personales que contiene,**

	resulte indispensable para la continuidad de funciones esenciales del Estado o cuya afectación pudiera comprometer la seguridad nacional, la seguridad pública o causar un daño grave a un amplio conjunto de personas. **En todo caso, tendrán carácter de bases de datos críticas del Estado, entre otras, las bases de datos poblacionales estratégicas determinadas conforme a la Ley de Seguridad Nacional y aquellas que sean calificadas como infraestructura de información crítica mediante lineamientos del Sistema Nacional de Transparencia y del Consejo de Seguridad Nacional.**
No tiene correlativo	**Artículo 76 Ter. Los responsables de bases de datos críticas del Estado deberán implementar medidas de seguridad reforzadas de nivel alto, superiores a las establecidas con carácter general, a fin de garantizar la integridad, disponibilidad, confidencialidad, autenticidad y resiliencia de la información. Entre dichas medidas, que serán proporcionales a la criticidad de la base de datos, se incluirán al menos:** **I. Controles de acceso estrictos y monitoreo continuo, con mecanismos de autenticación robusta y registro permanente de cualquier acceso, consulta, modificación o transferencia de datos;**

	II. Cifrado criptográfico de los datos personales sensibles o de identificación en reposo y en tránsito, así como medidas de seudonimización o disociación cuando aplique, para minimizar riesgos en caso de filtración; **III. Planes periódicos de evaluación de vulnerabilidades y pruebas de penetración en los sistemas informáticos que soportan la base de datos, para detectar y subsanar oportunamente posibles brechas de seguridad;** **IV. Protocolos de respuesta a incidentes de seguridad orientados a contener, mitigar y notificar cualquier vulneración de la seguridad de los datos personales. En caso de detectarse acceso no autorizado o pérdida/alteración de información en una base de datos crítica, el responsable deberá notificar de inmediato al órgano garante competente en materia de protección de datos personales y al Consejo de Seguridad Nacional, para la coordinación de acciones de contención y las investigaciones conducentes, y** **V. Auditorías de seguridad y cumplimiento normativo al menos una vez al año a cargo del órgano interno de control o unidad equivalente, con participación, en su caso, de la autoridad garante en**

No tiene correlativo	**materia de datos personales, para verificar la eficacia de las medidas implementadas y formular recomendaciones. Los resultados de estas auditorías serán documentados y, tratándose de bases de datos poblacionales estratégicas, podrán ser clasificados como información reservada por seguridad nacional, conforme a la Ley General de Transparencia, siempre que su publicidad ponga en riesgo la protección de los datos o la seguridad de los sistemas.** **Artículo 76 Quáter. Las instituciones responsables de bases de datos críticas del Estado deberán designar, en el ámbito de su Comité de Transparencia u órgano colegiado equivalente, a un Enlace de Seguridad de la Información encargado de supervisar el debido cumplimiento de las medidas de protección reforzadas. Este Enlace de Seguridad deberá ser un servidor público de nivel directivo con conocimientos especializados en seguridad de la información y protección de datos personales, cuyas funciones incluirán:** **I. Coordinar la elaboración e implementación del Documento de Seguridad específico para la base de datos crítica, detallando políticas, procedimientos y controles particulares;**

No tiene correlativo	**II. Fungir como punto de contacto institucional con la Agencia de Transformación Digital y Telecomunicaciones, con el Consejo de Seguridad Nacional y con el órgano garante de transparencia, para la atención de recomendaciones, lineamientos técnicos y eventuales incidentes relacionados con la base de datos crítica, y** **III. Promover la capacitación continua del personal que maneja la base de datos crítica, en temas de seguridad de la información, ciberseguridad y manejo ético de los datos, estableciendo controles de confianza cuando la naturaleza de la información lo amerite.** **Artículo 76 Quintus. El régimen de transparencia y acceso a la información aplicable a las bases de datos críticas del Estado deberá observar un equilibrio entre la máxima publicidad y la salvaguarda de la seguridad nacional y la privacidad. En ese sentido:** **I. La existencia, finalidad y marco normativo de cada base de datos crítica del Estado serán públicos. Los sujetos obligados deberán publicar en sus sitios electrónicos y en la Plataforma Nacional de Transparencia descripciones generales de dichas bases de datos, incluyendo su denominación,**

No tiene correlativo	**propósito, categoría de información que contienen y medidas básicas de protección implementadas, siempre que dicha información general no comprometa la seguridad de la base de datos.** **II. Se considerará información reservada por motivos de seguridad nacional aquella que detalle la arquitectura de seguridad, los controles específicos, claves de cifrado, configuraciones técnicas o vulnerabilidades identificadas de la base de datos crítica, cuya divulgación pudiera facilitar riesgos o ataques. Asimismo, podrá reservarse la información cuyo acceso irrestricto pueda ser utilizado para fines que pongan en peligro la seguridad de las personas (por ejemplo, listados completos de población con datos personales). Estas reservas se harán conforme a los criterios y procedimientos de la Ley General de Transparencia y Acceso a la Información Pública, sujetas a prueba de daño y ponderación caso por caso.** **III. La información de carácter personal contenida en bases de datos críticas del Estado se regirá por lo dispuesto en la presente Ley y demás normas de protección de datos personales. En cualquier solicitud de acceso a datos personales contenida en dichas bases, el sujeto obligado deberá extremar precauciones para verificar la identidad y legitimidad del solicitante, aplicando controles**

	adicionales si es necesario, en virtud de la criticidad de los datos solicitados. **IV. En caso de que alguna base de datos crítica contenga información no personal de interés público (por ejemplo, estadísticas agregadas, indicadores no confidenciales), se procurará ponerla a disposición en formatos de datos abiertos, con periodicidad y nivel de agregación que no comprometan la seguridad ni revelen datos protegidos. La publicación proactiva de información derivada de bases de datos críticas deberá ser aprobada por el Comité de Transparencia respectivo, siguiendo la asesoría del Enlace de Seguridad de la Información y atendiendo a las recomendaciones del órgano garante.**
LEY ORGÁNICA DE LA ADMINISTRACIÓN PÚBLICA FEDERAL **Artículo 42 Ter**.- A la Agencia de Transformación Digital y Telecomunicaciones le corresponde el despacho de los siguientes asuntos: **I**. a **V**. ...	**Artículo Tercero.** Se **adiciona** una nueva fracción VI al artículo 42 Ter de la Ley Orgánica de la Administración Pública Federal, recorriéndose la actual en el orden subsecuente, para quedar como sigue: Artículo 42 Ter.- …: I. a V. ...

No tiene correlativo	VI. **Coordinar, con las dependencias y entidades de la administración pública federal que sean responsables de bases de datos críticas del Estado, las acciones orientadas a la protección, estandarización e interoperabilidad de dichas bases de datos. En ejercicio de esta atribución, la Agencia deberá emitir lineamientos y criterios técnicos para asegurar un nivel homogéneo y óptimo de seguridad informática en la administración de las bases de datos críticas, fomentando la adopción de mejores prácticas en ciberseguridad, respaldo de información, recuperación ante desastres y continuidad operativa. Asimismo, la Agencia impulsará la interoperabilidad regulada entre bases de datos críticas y otros sistemas gubernamentales, con el fin de aprovechar sinergias tecnológicas y evitar duplicidades, todo ello sin comprometer la confidencialidad de los datos ni vulnerar las disposiciones de protección de datos personales. La Agencia actuará en estrecha coordinación técnica con las dependencias titulares de cada base de datos crítica, brindándoles asesoría y apoyo en materia de innovación tecnológica y protocolos de seguridad, y coadyuvará con las autoridades competentes en seguridad nacional y protección de datos para garantizar el cumplimiento integral de los lineamientos de este ámbito.**

VI. Definir los protocolos de seguridad de la información y comunicaciones de la Administración Pública Federal;	**VII.** Definir los protocolos de seguridad de la información y comunicaciones de la administración pública federal; ... ...
CÓDIGO PENAL FEDERAL **No tiene correlativo** **No tiene correlativo**	**Artículo Cuarto.** Se **adiciona** un Capítulo III, denominado "*Delitos en Materia de Bases de Datos Críticas del Estado*", que contiene los artículos 211 Bis 8, 211 Bis 9, 211 Bis 10, 211 Bis 11 y 211 Bis 12, al Título Noveno del Libro Segundo del Código Penal Federal, para quedar como sigue: **Capítulo III** **Delitos en Materia de Bases de Datos Críticas del Estado** **Artículo 211 Bis 8. Comete el delito de acceso ilícito a una base de datos crítica del Estado quien, sin autorización y mediante cualquier medio, acceda a una base de datos crítica del Estado, u obtenga, copie, extraiga, interfiera o altere total o parcialmente los datos personales contenidos en la misma, o los sistemas o equipos que la soportan.**

	I. Si el agente modifica, daña, borra, destruye o inutiliza información contenida en la base de datos crítica, o provoca la interrupción de su funcionamiento, se le impondrán de cinco a quince años de prisión y multa de quinientos a mil quinientos días. **II. Si el agente accede, conoce, descarga o copia información de la base de datos crítica sin causar daños o alteraciones a los sistemas, se le impondrán de tres a diez años de prisión y multa de trescientos a ochocientos días.**
No tiene correlativo	**Artículo 211 Bis 9. Comete el delito de comercialización indebida de datos personales de una base de datos crítica del Estado quien, sin estar autorizado para ello, transfiera, venda, ceda, distribuya o divulgue a un tercero datos personales que formen parte de una base de datos crítica del Estado, con ánimo de lucro o beneficio propio o de un tercero, o con el objetivo de causar un perjuicio. A quien incurra en esta conducta se le impondrán de cuatro a doce años de prisión y de cuatrocientos a mil días multa.**
No tiene correlativo	**Artículo 211 Bis 10. Comete el delito de manejo ilícito de datos en bases de datos críticas del Estado**

No tiene correlativo	**por parte de personal autorizado aquel servidor público, funcionario, empleado o contratista que, estando autorizado para acceder o administrar una base de datos crítica del Estado en razón de su empleo o función, incumpla deliberadamente sus deberes de custodia o exceda los permisos otorgados con cualquiera de las finalidades siguientes: obtener, usar, sustraer, divulgar, alterar, falsificar o suprimir datos personales contenidos en la base de datos, fuera de los casos permitidos por la ley y sin consentimiento de la autoridad competente o de los titulares de los datos cuando se requiera.** **I. Si la persona autorizada alterare, falsificare, destruyere, dañare o suprimiere datos de la base de datos crítica, o provocare la interrupción no autorizada de su operación, se le impondrán de tres a ocho años de prisión y de trescientos a novecientos días multa.** **II. Si la persona autorizada obtiene, copia, extrae, divulga o transmite a terceros información contenida en la base de datos crítica, sin estar facultada para ello y al margen de los fines institucionales, se le impondrán de dos a seis años de prisión y de doscientos a seiscientos días multa.**

No tiene correlativo	**Además de las sanciones anteriores, al responsable de este delito que ostente la calidad de servidor público se le impondrá la destitución del cargo y la inhabilitación para ocupar cualquier empleo, cargo o comisión en el servicio público por un plazo de cinco a diez años, según la gravedad de la conducta. En todos los casos del presente artículo, se entenderá que el autor actuó deliberadamente cuando conocía las restricciones legales sobre el uso de la información y aun así actuó en contravención de éstas con intención de beneficio propio o ajeno, o para causar daño o ventaja indebida.** **Artículo 211 Bis 11. Comete el delito de omisión o negligencia grave en el manejo de bases de datos críticas del Estado el servidor público o encargado que, por falta de cuidado, inobservancia de sus deberes, incumplimiento de protocolos de seguridad o negligencia inexcusable, permita u origine con su conducta que personas no autorizadas accedan, obtengan, extraigan, alteren o difundan total o parcialmente los datos personales contenidos en una base de datos crítica del Estado, siempre que dicha conducta genere un riesgo efectivo o un daño a la seguridad de la información o a los derechos de los titulares de los datos.**

No tiene correlativo	**A quien incurra en esta conducta se le impondrán de dos a siete años de prisión y de doscientos a quinientos días multa. Tratándose de un servidor público, se le impondrá además la destitución e inhabilitación para cargo público hasta por cinco años.** **Artículo 211 Bis 12. Agravantes especiales. Las penas previstas en este Capítulo se aumentarán hasta en una mitad cuando concurra cualquiera de las siguientes circunstancias en la comisión de los delitos:** **I. Cuando la información personal obtenida, revelada o utilizada indebidamente sea empleada con fines de lucro, ventaja económica o beneficio político para el autor del delito o terceros, o bien fuere difundida masivamente.** **II. Cuando la conducta ilícita cause un perjuicio grave a la seguridad nacional, a la seguridad pública o a la defensa del Estado, ya sea porque los datos obtenidos se utilicen para cometer otros delitos de alto impacto (espionaje, terrorismo, extorsión masiva, etc.) o porque comprometan operaciones, planes o personal relacionado con la seguridad nacional.**

	III. Cuando el delito fuere cometido por un servidor público perteneciente a alguna institución de seguridad nacional, seguridad pública, procuración de justicia o fuerzas armadas, aprovechando los conocimientos, accesos o facilidades propios de su cargo.
	TRANSITORIO. **Único.** El presente decreto entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación.

Lucrecia Hermoso Santamaría.