

## ANÁLISIS TÉCNICO PRELIMINAR

No. Expediente: 0972-1PO2-25

### I.- DATOS DE IDENTIFICACIÓN DE LA INICIATIVA

<b>1.- Nombre de la Iniciativa.</b>	Que adiciona diversas disposiciones a la Ley Nacional del Registro de Detenciones, en materia de seguridad de la base de datos.
<b>2.- Tema de la Iniciativa.</b>	Seguridad Nacional.
<b>3.- Nombre de quien presenta la Iniciativa.</b>	Dip. Julio César Moreno Rivera.
<b>4.- Grupo Parlamentario del Partido Político al que pertenece.</b>	MORENA.
<b>5.- Fecha de presentación ante el Pleno de la Cámara de Diputados.</b>	04 de noviembre de 2025.
<b>6.- Fecha de publicación en la Gaceta Parlamentaria.</b>	04 de noviembre de 2025.
<b>7.- Turno a Comisión.</b>	Seguridad Ciudadana.

### II.- SINOPSIS

Establecer los criterios que deberá considerar la Secretaría de Seguridad y Protección Ciudadana en casos de riesgos y vulneraciones a la base de datos del Registro Nacional de Detenciones.

### **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 XXIII y XXXII del artículo 73, 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.
- De conformidad con las reglas de técnica legislativa, verificar la estructura en el texto legal propuesto, respecto al orden de las fracciones del artículo 39 en el proyecto de decreto.

La iniciativa, salvo las observaciones antes señaladas, cumple en general con los requisitos formales que se exigen en la práctica parlamentaria y que de conformidad con el artículo 78 del Reglamento de la Cámara de Diputados, son los siguientes:

Encabezado o título de la propuesta; planteamiento del problema que la iniciativa pretenda resolver; problemática desde la perspectiva de género, en su caso; argumentos que la sustenten; fundamento legal; denominación del proyecto de ley o decreto; ordenamientos a modificar; texto normativo propuesto; artículos transitorios; lugar; fecha, nombre y rúbrica del iniciador.



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

TEXTO VIGENTE	TEXTO QUE SE PROPONE
<b>LEY NACIONAL DEL REGISTRO DE DETENCIONES.</b>	<b>PROYECTO DE DECRETO POR EL QUE SE ADICIONAN DIVERSAS DISPOSICIONES A LA LEY NACIONAL DEL REGISTRO DE DETENCIONES, EN MATERIA DE RIESGO Y VULNERACIÓN DE LA BASE DE DATOS DEL REGISTRO.</b>
<b>Artículo 11.</b> La Secretaría será la instancia encargada de la administración y operación del Registro y tendrá las siguientes facultades:	<b>Artículo Único.</b> Se <b>adiciona</b> una fracción IX, recorriéndose en su orden la actual fracción IX que pasa a ser X, del artículo 11 y <b>se adiciona</b> un Capítulo IX y los artículos 37, 38, 39, 40 y 41 a la Ley Nacional del Registro de Detenciones; para quedar como sigue:
<b>I.</b> a la <b>VIII.</b> ...	Artículo 11. ...  I. al VIII. ...
<b>No tiene correlativo</b>	<b>IX. Establecer las disposiciones necesarias para la gestión de riesgos y mitigación de vulneración a la base de datos del Registro, a que se refiere el Capítulo IX de esta ley.</b>
<b>IX.</b> Las demás que le confieran otras disposiciones jurídicas aplicables.	<b>X.</b> Las demás que le confieran otras disposiciones jurídicas aplicables.



**No tiene correlativo**

## **Capítulo IX Seguridad de la Base de Datos del Registro**

**Artículo 37. Se considera riesgo a cualquier acontecimiento potencialmente capaz de afectar la confidencialidad, integridad o disponibilidad de la información contenida en la base de datos del Registro, tales como:**

**I. Daño físico, incidental o deliberado a la infraestructura que soporta la base de datos;**

**II. Fallas técnicas, incluyendo el mal funcionamiento del hardware o software, sobrecarga o saturación del sistema, obsolescencia tecnológica, así como deficiencias o falta de mantenimiento preventivo y correctivo;**

**III. Presencia o ejecución de software malicioso;**

**IV. Ataques técnicos orientados a infringir el sistema, tales como explotación de vulnerabilidades, intentos de acceso no autorizado, ataques de denegación de servicio, filtración de contraseñas o modificación no autorizada de configuraciones;**



No tiene correlativo

**V. Incumplimiento de políticas, reglas de acceso o procedimientos de seguridad, ya sea por negligencia, omisión o acción deliberada;**

**VI. Cuando la plataforma emita las alertas a que se refiere el artículo 16, o**

**VII. Cualquier otra que, por su naturaleza, pueda comprometer su integridad o disponibilidad.**

**Artículo 38. Se considera que existe vulneración a la información contenida en base de datos del Registro cuando se afecte su confidencialidad, integridad o disponibilidad, por las siguientes causas:**

**I. Pérdida, destrucción, alteración o modificación no autorizada de la información que contiene;**

**II. Reproducción, sustracción o transferencia no autorizada de información;**

**III. Uso, acceso o tratamiento de la información con fines distintos o ajenos a los previstos por esta Ley;**

**IV. Se divulgue, exponga o transmita a personas no autorizadas, o a través de medios no permitidos, o**



No tiene correlativo

**V. Cualquier otra que, por su naturaleza y medios de ejecución, afecte su confidencialidad, integridad o disponibilidad.**

**Artículo 39. Para prevenir y mitigar la materialización de los riesgos previstos en el artículo 37, la Secretaría deberá implementar, al menos, las siguientes medidas de seguridad:**

**I. Establecer controles que impidan el acceso no autorizado o el daño a las instalaciones, áreas críticas y recursos que permiten el funcionamiento de la base de datos;**

**II. Garantizar la implementación de un programa de mantenimiento continuo a los sistemas y equipos involucrados en el almacenamiento y gestión de la información;**

**III. Asegurar que el acceso a la base de datos se realice únicamente por usuarios debidamente identificados, autenticados y autorizados;**

**IV. Implementar un esquema de control de accesos basado en roles, responsabilidades y niveles de acceso a la información acorde con las funciones asignadas;**



**CÁMARA DE  
DIPUTADOS**  
LXVI LEGISLATURA  
SOBERANÍA Y JUSTICIA SOCIAL



Dirección  
General de  
Apoyo  
Parlamentario

DIRECCIÓN GENERAL DE APOYO PARLAMENTARIO  
DIRECCIÓN DE APOYO A COMISIONES  
SUBDIRECCIÓN DE APOYO TÉCNICO-JURÍDICO A COMISIONES

No tiene correlativo

**V. Ejecutar el alta, modificación y cancelación de usuarios conforme a los lineamientos establecidos, para tal efecto, por el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública;**

**VI. Generar y conservar respaldos de la información, de manera periódica y segura, procurando su cifrado a efecto de mantener la confidencialidad e integridad de la información contenida en la base de datos del Registro;**

**I. Implementar y actualizar herramientas de ciberseguridad orientadas a la protección de la infraestructura tecnológica ante posibles ataques, software malicioso u otras amenazas, y**

**II. Realizar análisis periódicos de vulnerabilidades y amenazas, así como la evaluación de la eficacia de las medidas de seguridad implementadas para su mitigación.**

**Artículo 40. Cuando se identifique una vulneración a la base de datos que integra el Registro, la Secretaría deberá implementar de manera inmediata medidas orientadas a mitigar sus efectos y garantizar la continuidad operativa, que comprenderán, al menos las siguientes:**





**No tiene correlativo**

**I. Activar, en su caso, el procedimiento de recuperación de desastres, asegurando la continuidad en la operación del Registro;**

**II. Realizar el análisis y documentar las causas que originaron el incidente;**

**III. Adoptar las medidas preventivas y correctivas necesarias para evitar su repetición;**

**IV. Registrar cada incidente en una bitácora, precisando su naturaleza, fecha de ocurrencia, causas y acciones implementadas, e**

**V. Informar oportunamente a los sujetos obligados y demás áreas usuarias sobre la disponibilidad del servicio.**

**Artículo 41. La Secretaría será responsable de ejecutar las acciones necesarias para prevenir riesgos y atender las vulneraciones a la base de datos del Registro, contando para tal efecto con las siguientes atribuciones:**

**I. Coordinar la elaboración y actualización del plan de acción en materia de seguridad de la información;**





**No tiene correlativo**

**II. Coordinar el análisis de vulnerabilidades y amenazas, así como la evaluación de la eficacia de las medidas de seguridad implementadas y, de ser el caso, proponer las acciones de mejora que correspondan;**

**III. Supervisar la asignación y control de permisos de acceso a las aplicaciones del registro;**

**IV. Establecer mecanismos de supervisión, incluyendo monitoreo tecnológico, para verificar el cumplimiento de las medidas de seguridad;**

**V. Coordinar el proceso de alta, baja o cancelación de usuarios;**

**VI. Ordenar, en caso de contingencia, el bloqueo, restricción o revocación de accesos y permisos;**

**VII. Determinar, cuando sea necesario, la ejecución del procedimiento de recuperación de desastres;**

**VIII. Coordinar el análisis de causas de un incidente de vulneración e instruir la implementación de medidas correctivas y preventivas para mitigar sus efectos y evitar su repetición, y**



**CÁMARA DE  
DIPUTADOS**  
LXVI LEGISLATURA  
SOBERANÍA Y JUSTICIA SOCIAL



Dirección  
General de  
Apoyo  
Parlamentario

DIRECCIÓN GENERAL DE APOYO PARLAMENTARIO  
DIRECCIÓN DE APOYO A COMISIONES  
SUBDIRECCIÓN DE APOYO TÉCNICO-JURÍDICO A COMISIONES

**No tiene correlativo**

**IX. Las demás que les confiera la presente Ley y demás ordenamientos aplicables.**

**TRANSITORIOS.**

**PRIMERO.** El presente decreto entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación.

**SEGUNDO.** En un plazo no mayor a noventa días contados a partir de la entrada en vigor del presente Decreto, la Secretaría deberá emitir el Protocolo para la gestión de riesgos y vulneraciones de la base de datos del Registro Nacional de Detenciones, y realizar las adecuaciones necesarias a las disposiciones aplicables.

**TERCERO.** La Secretaría deberá iniciar programas de capacitación continua para las personas que desempeñen el nivel de Administradores y Supervisores para garantizar su aptitud para gestionar riesgos y vulneraciones de la base de datos, dentro de un plazo de ciento veinte días contados a partir de la emisión del Protocolo a que se refiere el artículo anterior.



**CÁMARA DE  
DIPUTADOS**  
LXVI LEGISLATURA  
SOBERANÍA Y JUSTICIA SOCIAL



Dirección  
General de  
Apoyo  
Parlamentario

**DIRECCIÓN GENERAL DE APOYO PARLAMENTARIO  
DIRECCIÓN DE APOYO A COMISIONES  
SUBDIRECCIÓN DE APOYO TÉCNICO-JURÍDICO A COMISIONES**

**CUATRO.** Las erogaciones que pudieran presentarse con motivo de la entrada en vigor del presente Decreto se realizarán con cargo a los presupuestos aprobados a los ejecutores de gasto correspondientes para el ejercicio fiscal que corresponda, por lo que no se autorizarán ampliaciones a su presupuesto para el presente ejercicio fiscal ni subsecuentes.

*Concepción Sarmiento Sarmiento*