

ANÁLISIS TÉCNICO PRELIMINAR

No. Expediente: 0289-1PO2-25

I.- DATOS DE IDENTIFICACIÓN DE LA INICIATIVA

1.- Nombre de la Iniciativa.	Que adiciona y deroga diversas disposiciones de la Ley Nacional del Registro de Detenciones, en materia de gestión de riesgos y vulneraciones de la base de datos del Registro Nacional de Detenciones.
2.- Tema de la Iniciativa.	Justicia.
3.- Nombre de quien presenta la Iniciativa.	Dip. Teresa Ginez Serrano e integrantes del Grupo Parlamentario PAN.
4.- Grupo Parlamentario del Partido Político al que pertenece.	PAN.
5.- Fecha de presentación ante el Pleno de la Cámara de Diputados.	20 de noviembre de 2025.
6.- Fecha de publicación en la Gaceta Parlamentaria.	17 de septiembre de 2025.
7.- Turno a Comisión.	Seguridad Ciudadana.

II.- SINOPSIS

Establecer que, la Secretaría de Seguridad y Protección Ciudadana emitirá un protocolo para la gestión de riesgos y vulneraciones de la base de datos del Registro Nacional de Detenciones. Asimismo, incluir la definición y las medidas que regulen el funcionamiento de dicho protocolo.

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:

- De acuerdo con las reglas de técnica legislativa, así como con la integración actual de los preceptos que se busca reformar, referenciar en el texto aquéllos apartados cuyo contenido presenta alguna modificación.
- 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.

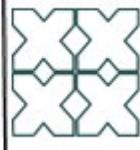
La iniciativa cumple en general con los requisitos formales que se exigen en la práctica parlamentaria y que de conformidad con el artículo 78 del Reglamento de la Cámara de Diputados, son los siguientes:

Encabezado o título de la propuesta; planteamiento del problema que la iniciativa pretenda resolver; 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
LEY NACIONAL DEL REGISTRO DE DETENCIONES	PROYECTO DE DECRETO POR EL QUE SE REFORMAN LOS ARTÍCULOS 11 Y 16, Y SE ADICIONA UN ARTÍCULO 16 BIS A LA LEY NACIONAL DEL REGISTRO DE DETENCIONES, EN MATERIA DE GESTIÓN DE RIESGOS Y VULNERACIONES DE LA BASE DE DATOS DEL REGISTRO NACIONAL DE DETENCIONES.
Artículo 11. La Secretaría será la instancia encargada de la administración y operación del Registro y tendrá las siguientes facultades:	ARTÍCULO ÚNICO. Se deroga el último párrafo del artículo 16 y se adiciona una fracción VIII, recorriéndose en su orden las actuales fracciones VIII y IX que pasan a ser IX y X, del artículo 11; y un artículo 16 Bis a la Ley Nacional del Registro de Detenciones, para quedar como sigue:
I. a VII. ...	Artículo 11. ...
No tiene correlativo	I. a VII. ...
VIII. Establecer y asignar las condiciones y perfiles de acceso de los sujetos obligados que hayan sido autorizados para acceder al Sistema, y	VIII. Emitir un Protocolo para la gestión de riesgos y vulneraciones de la base de datos; IX. Establecer y asignar las condiciones y perfiles de acceso de los sujetos obligados que hayan sido autorizados para acceder al Sistema, y



IX. Las demás que le confieran otras disposiciones jurídicas aplicables.

Artículo 16. Las condiciones y perfiles de acceso al Registro serán determinados por la Secretaría, conforme a los siguientes niveles:

I. a V. ...

La plataforma del Registro emitirá alertas y bloqueos respectivos cuando los sujetos obligados manipulen de manera inusual los datos del registro o se violenten los privilegios de acceso.

No tiene correlativo

No tiene correlativo

X. Las demás que le confieran otras disposiciones jurídicas aplicables.

Artículo 16. ...

I. a V. ...

Se deroga.

Artículo 16 Bis. La Secretaría emitirá un Protocolo para la gestión de riesgos y vulneraciones de la base de datos, que estará a lo dispuesto por el presente artículo.

Se considerará que la base de datos está en riesgo cuando se presenten intentos de acceso no autorizado, flujo inusual o irregular de datos, funcionamiento anómalo del sistema o de los equipos o cuando un Enlace Estatal o Institucional notifique al Administrador la vulneración de una base de datos de su dependencia o área.

Asimismo, se considerará que la base de datos fue vulnerada cuando se violenten los privilegios de acceso,



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

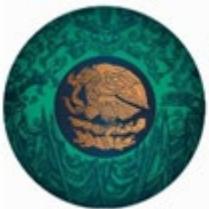
se detecte un acceso no autorizado al Registro, se detecte una extracción, modificación, transferencia o destrucción de datos no autorizada, o los sujetos obligados manipulen de manera inusual los datos del Registro.

No tiene correlativo

El Protocolo deberá establecer las medidas que permitan, al menos, lo siguiente:

No tiene correlativo

- I. Identificar la fuente del riesgo o vulneración de la base de datos;
- II. Documentar cada incidente de riesgo o vulneración;
- III. Evaluar en cada caso la magnitud del riesgo potencial o del daño sufrido;
- IV. Alertar a los sujetos obligados;
- V. Garantizar la continuidad de la operación de la plataforma y la integridad de la información;
- VI. En su caso, recuperar el control de la base de datos, y
- VII. Determinar acciones de mitigación para evitar repetición.



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

No tiene correlativo

No tiene correlativo

Las personas que desempeñen el nivel de Administrador y Supervisor serán las responsables de atender los hechos que pongan en riesgo o vulneren la base de datos, bajo la supervisión de la unidad administrativa designada por la Secretaría para tal efecto. El Protocolo establecerá las facultades específicas que tendrán para la atención de estos casos, sin que estas puedan exceder las facultades de la unidad administrativa designada por la Secretaría.

En casos de vulneración se deberá documentar cada incidente identificando, al menos, lo siguiente:

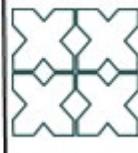
I. La fecha y hora en la que se tuvo conocimiento;

II. Los datos afectados;

III. La causa de la vulneración, y

IV. Las acciones desempeñadas para salvaguardar la información contenida en la base de datos.

La Secretaría desarrollará e implementará un sistema de detección de intrusiones que emita alertas y bloqueos automatizados desde la plataforma, en caso de que ocurran hechos que pongan en riesgo o vulneren su base de datos.



No tiene correlativo

La Secretaría implementará medidas preventivas que incluyan monitoreo permanente de la infraestructura tecnológica, evaluación periódica de vulnerabilidades y pruebas de penetración para mitigar riesgos, así como cooperación e intercambio de información sobre amenazas y mejores prácticas de ciberseguridad con otras instituciones gubernamentales.

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 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.