



PODER LEGISLATIVO FEDERAL  
CÁMARA DE DIPUTADOS

MESA DIRECTIVA  
LXVI LEGISLATURA  
OF. No. D.G.P.L. 66-II-3-1372  
**EXP. 4055**

Sen. Laura Itzel Castillo Juárez  
Presidenta de la Cámara de Senadores  
P r e s e n t e

Tenemos el honor de remitir a usted, para sus efectos Constitucionales, el expediente con la Minuta Proyecto de Decreto por el que se adicionan diversas disposiciones de la Ley Nacional del Registro de Detenciones, con número CD-LXVI-II-2P-136, aprobado en esta fecha por la Cámara de Diputados del Honorable Congreso de la Unión.

Ciudad de México, a 29 de abril de 2026



A handwritten signature in blue ink, appearing to read "Magdalena del Socorro Nuñez Monreal", written over a horizontal line.

Dip. Magdalena del Socorro Nuñez Monreal  
Secretaria



PODER LEGISLATIVO FEDERAL  
CÁMARA DE DIPUTADOS

**M I N U T A  
P R O Y E C T O  
D E  
D E C R E T O**

**POR EL QUE SE ADICIONAN DIVERSAS DISPOSICIONES DE LA LEY NACIONAL DEL REGISTRO DE DETENCIONES**

**Artículo Único.-** Se adiciona una fracción IX, recorriéndose en su orden la subsecuente, del artículo 11 y se adiciona un Capítulo IX, denominado "Seguridad de la Base de Datos del Registro"; y los artículos 37, 38, 39, 40 y 41 a la Ley Nacional del Registro de Detenciones, para quedar como sigue:

**Artículo 11. ...**

**I. a VIII. ...**

- 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;**
- X. Las demás que le confieran otras disposiciones jurídicas aplicables.**

**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;**





- 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 la 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
- 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;**
- 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;**
- VII. **Implementar y actualizar herramientas de ciberseguridad orientadas a la protección de la infraestructura tecnológica ante posibles ataques, software malicioso u otras amenazas, y**
- VIII. **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:**

- 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;**
- 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**





PODER LEGISLATIVO FEDERAL  
CÁMARA DE DIPUTADOS

**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 ciento ochenta días contados a partir de la entrada en vigor del presente Decreto, la Secretaría deberá realizar las adecuaciones reglamentarias necesarias a las disposiciones aplicables.

**Tercero.-** La Secretaría deberá implementar las acciones administrativas que estime necesarias que garanticen que las personas que desempeñen el nivel de Administradores y Supervisores cuenten con las aptitudes para gestionar riesgos y vulneraciones de la base de datos, dentro de un plazo de ciento veinte días contados a partir de la emisión de las adecuaciones a que se refiere el artículo anterior.

**Cuarto.-** 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.

S A L Ó N DE SESIONES DE LA CÁMARA DE DIPUTADOS DEL HONORABLE CONGRESO DE LA UNIÓN. Ciudad de México, a 29 de abril de 2026.



  
Dip. Kenia López Rabadán  
Presidenta

  
Dip. Magdalena del Socorro Núñez Monreal  
Secretaria

Se remite a la H. Cámara de Senadores  
para sus efectos Constitucionales la  
Minuta CD-LXVI-II-2P-136  
Ciudad de México, a 29 de abril de 2026



  
Mtro. Hugo Christian Rosas de León  
Secretario de Servicios Parlamentarios.