INICIATIVA CON 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.

La suscrita, Diputada Teresa Ginez Serrano, integrante del Grupo Parlamentario del Partido Acción Nacional en la LXVI Legislatura de la Cámara de Diputados del H. Congreso de la Unión, con fundamento en lo dispuesto en los artículos 71, fracción II, y 72, apartado H, de la Constitución Política de los Estados Unidos Mexicanos; y los artículos 6, numeral 1, fracción I; 77, numeral 1, y 78, del Reglamento de la Cámara de Diputados, someto a consideración de esta Soberanía la **"Iniciativa con 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"**, la cual plantea la problemática y los argumentos establecidos en la siguiente:

EXPOSICIÓN DE MOTIVOS

Primero. Planteamiento del problema

La reforma constitucional que estableció el mandato legislativo de expedir la Ley Nacional del Registro de Detenciones determinó que dicha legislación debía regular el personal responsable, sus facultades, así como las medidas a desplegarse en casos de riesgo y vulneración de la base de datos del Registro Nacional de Detenciones. Sin embargo, la Ley promulgada no cumplió con dichos criterios, ante lo cual la Comisión Nacional de Derechos Humanos presentó la Acción de Inconstitucionalidad 63/2019 que, una vez resuelta por la Suprema Corte de Justicia de la Nación, determinó que el Congreso de la Unión incurrió en omisión legislativa por no prever dichas medidas. Por ello, mediante la

presente Iniciativa propongo legislar para superar la inconstitucionalidad y brindar certeza jurídica a la operación del Registro Nacional de Detenciones.

Segundo. Contexto

La reforma constitucional en materia de Guardia Nacional aprobada y publicada en 2019[1], entre otras modificaciones, le otorgó al Congreso de la Unión la facultad de expedir una Ley Nacional del Registro de Detenciones (en adelante "Ley"), con el objetivo de registrar las condiciones en las cuales se podría realizar el arresto o la detención de los infractores de la ley[2]. En el artículo Cuarto Transitorio del Decreto de reforma constitucional se establecieron los criterios que debía contener la Ley, que se transcriben a continuación:

> "**Cuarto.** Al expedir las leyes a que se refiere la fracción XXIII del artículo 73 de esta Constitución, el Congreso de la Unión estará a lo siguiente:
>
> **I.** a **III.** [...]
>
> **IV.** La **Ley Nacional del Registro de Detenciones** incorporará, al menos, las siguientes previsiones:
>
> **1.** Las características del Registro y los principios que rigen su conformación, uso y conservación;
> **2.** El momento de realizar el registro de la persona dentro del procedimiento de detención;
> **3.** El tratamiento de los datos personales de la persona detenida, en términos de las leyes en la materia;
> **4.** Los criterios para clasificar la información como reservada o confidencial;
> **5.** Las personas autorizadas para acceder a la base de datos del Registro y los niveles de acceso;

[1] Andrés Manuel López Obrador, "Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de Guardia Nacional." *Diario Oficial de la Federación*, Tomo DCCLXXXVI No. 20 Ciudad de México, martes 26 de marzo de 2019.
[2] Senado de la República, "Consideraciones de las Modificaciones al Proyecto de Decreto que reforma, adiciona y deroga diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de Guardia Nacional". *Gaceta del Senado de la República*, Número LXIV/1SPO-87/89770, jueves 21 de febrero de 2019.

6. Las atribuciones de los servidores públicos que desempeñen funciones en el Registro y sus responsabilidades en la recepción, administración y seguridad de la información, y

7. La actuación que deberá desplegar el Registro y su personal en caso de ocurrir hechos que pongan en riesgo o vulneren su base de datos."[3]

El 27 de mayo de 2019 se promulgó la Ley Nacional del Registro de Detenciones[4], con lo cual el Congreso de la Unión cumplió el mandato establecido en el artículo Primero Transitorio del Decreto de reforma constitucional en materia de Guardia Nacional, que otorgó 90 días naturales para tal efecto. En términos generales, la Ley le otorgó la administración y operación del Registro Nacional de Detenciones a la Secretaría de Seguridad Ciudadana y lo integró al Sistema Nacional de Información de Seguridad Pública.

Tras la publicación de la Ley, la Comisión Nacional de los Derechos Humanos (en adelante "CNDH") presentó acción de inconstitucionalidad el 26 de junio de 2019 en contra de la totalidad de la Ley y, particularmente, en contra de los artículos 19 y Quinto Transitorio. La demanda de acción, que fue radicada bajo el número de expediente 63/2019, presentó esencialmente dos conceptos de invalidez, de los cuales el que interesa a la materia de la Iniciativa es el relacionado con la omisión legislativa y se resume a continuación:

> "**1.- Omisión legislativa.** El Congreso de la Unión incurrió en omisión legislativa en competencia de ejercicio obligatorio al no determinar en la nueva Ley, las medidas de seguridad de carácter administrativo, físico y técnico para el resguardo de la base de datos y así proteger la información asentada contra cualquier daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado. Una obligación que se encontraba dispuesta en el artículo Cuarto Transitorio, fracción IV, numeral 7 del "Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de Guardia Nacional."

[3] Énfasis añadido.
[4] Andrés Manuel López Obrador, "Decreto por el que se expide la Ley Nacional del Registro de Detenciones." *Diario Oficial de la Federación*, Tomo DCCLXXXVIII No. 28 Ciudad de México, lunes 27 de mayo de 2019.

La CNDH también argumentó en su demanda que no contar con normas que describan la actuación que deberá desplegar el Registro ante hechos que pongan en riesgo o amenacen base de datos, se puede traducir en alteraciones que menoscaben su mantenimiento. Esto implicaría violentar diversos derechos de las personas detenidas, debido a que un mal seguimiento y constancia de la autoridad que realizó la detención dificultaría la protección de las garantías procesales que asisten a todos los detenidos y que están reconocidas en el artículo 20 de la Constitución Política de los Estados Unidos Mexicanos (en adelante "CPEUM").

En el estudio de fondo la Suprema Corte de Justicia de la Nación (en adelante "SCJN") reconoció que, tanto las normas nacionales como internacionales, conciben al Registro Nacional de Detenciones como una herramienta de protección de los derechos humanos. El Registro se relaciona con los artículos 16, 20 y 29 de la Constitución, los cuales establecen la obligación del Estado de contar con un registro de detenciones que debe ser entendido como un derecho del imputado.

Señaló que la Corte Interamericana de Derechos Humanos ha destacado en diversos precedentes que el Estado tiene una posición especial como garante de los derechos de los detenidos. Esta posición responde a la existencia de un sistema de información confiable sobre los registros de detenciones que se encuentran a disposición de los familiares y asesores de los detenidos y que puede ser empleado para establecer las posibles responsabilidades del sistema de justicia penal.

Otros instrumentos internacionales, tales como el artículo 17.3 de la Convención Internacional para la Protección de todas las Personas contra las Desapariciones Forzadas; el artículo 11, segundo párrafo, de la Convención Interamericana sobre Desaparición Forzada de Personas; las Reglas Mínimas de las Naciones Unidas para el Tratamiento de los Reclusos; las Reglas Mínimas de las Naciones Unidas para la Protección de los Menores Privados de Libertad; así como el Conjunto de Principios para la Protección de todas las Personas

Sometidas a Cualquier Forma de Detención o Prisión, coinciden en que los registros deben contener una serie de elementos mínimos, tales como:

a) Identidad de la persona privada de la libertad;
b) Día, hora y lugar donde la persona fue privada de la libertad;
c) Identidad de los funcionarios que hayan intervenido;
d) Elementos relativos a la integridad física de la persona privada de libertad;
e) En caso de fallecimiento durante la privación de la libertad, las circunstancias, y causas del fallecimiento y el destino de los restos, y
f) Día y hora de liberación o traslado a otro lugar de detención y la autoridad encargada del traslado.

Estos elementos mínimos conforman la información que debía contener el Registro y constituye el objeto de protección de la Ley y de la autoridad encargada de su operación. En este contexto, la SCJN se centró en analizar la existencia de una omisión legislativa por parte del Congreso de la Unión, tomando como referencia los criterios establecidos en la fracción IV del artículo Cuarto Transitorio del Decreto de reforma constitucional en materia de Guardia Nacional, que se transcribió con anterioridad.

Luego del análisis pormenorizado de todos los artículos de la Ley, la SCJN no identificó elementos en el proceso legislativo o disposiciones expresas que permitieran sostener la plena inclusión de las directrices establecidas en el artículo Cuarto Transitorio en la Ley. Sin embargo, luego de una lectura integral del artículo transitorio concluyó que, por lo menos, debían señalarse las acciones que tendrían que realizar los miembros del Registro ante algún evento que pusiera en riesgo la información o vulnerara el sistema.

Al respecto, es conveniente rescatar lo señalado en los informes justificados de las autoridades responsables en relación con la descripción de las acciones a cargo del personal del Registro. La Cámara de Senadores argumentó que el mandato fue atendido en los artículos 2, fracción VI, 9, 10, 11, 13, 15, 16, 24, 25, 29 y 35 de la Ley Nacional del Registro de Detenciones, mediante el establecimiento de la emisión de alertas y bloqueos, la existencia de claves exclusivas para

usuarios otorgadas sólo por la Secretaría, así como las constancias de actualizaciones de información.

Por otra parte, la Cámara de Diputados aclaró que existen disposiciones que describen las acciones que corresponden a la emisión de alertas y bloqueos cuando se violenten los privilegios de acceso, contempladas en el artículo 16 de la Ley. También argumentó que se previó un sistema de responsabilidades por omisiones de autoridad y mecanismos de seguridad y carácter operativo para el debido funcionamiento, autorización, cancelación y consulta del Registro.

Por último, la Consejería Jurídica de la Presidencia de la República sostuvo que, al haberse establecido principios en la Ley para la manipulación del Registro, también se previó que la Secretaría sería la encargada del manejo, administración y conservación contenida en el registro y, para ello, se le facultó para emitir un reglamento que regulara su actuación. En otras palabras, argumentó que se había dado cumplimiento a estos criterios mediante el otorgamiento de una cláusula habilitante a la Secretaría para la emisión de un reglamento que determine su actuar.

La SCJN no dio por válidos dichos argumentos y advirtió el incumplimiento del mandato del contenido del artículo Cuarto Transitorio del Decreto, en esencia, por las siguientes razones:

- **Sujetos externos.** El Poder reformador no limitó en el artículo transitorio la existencia de hechos que pongan en riesgo o vulneren la base de datos sólo a aquellos ocasionados por sujetos obligados, ya que el riesgo puede verificarse con independencia de la calidad de los sujetos que intervengan, sean sujetos obligados o externos. En este sentido, el artículo 16 solo prevé la manipulación de la base de datos por intervención de sujetos obligados y, si se adopta esta disposición como cumplimiento de las directrices, se ignorarían los casos en que sujetos externos vulneren la base de datos.

- **Exceso de la facultad reglamentaria.** Los artículos 11, 13, 14, 15, 16, 27, 32 y 35 de la Ley establecen la facultad de la Secretaría de emitir disposiciones para el adecuado funcionamiento del Registro pero, contrario a lo que argumentan las autoridades, no habilitan a la Secretaría a emitir un reglamento para desarrollar el funcionamiento del Registro y la actuación de su personal ante una vulneración de la información. Si se asumen estas disposiciones como cumplimiento del mandato, se excederían los límites de la facultad reglamentaria, pues se avalaría la emisión de un reglamento que viole la reserva de ley que le corresponde al legislador.

Por lo anterior, el Tribunal Pleno concluyó que sí era fundada la omisión legislativa relativa en competencia de ejercicio obligatorio, ya que la Ley fue omisa en regular la actuación del personal del Registro cuando se susciten hechos o eventos, ya sean externos o internos, que pongan en riesgo la información contenida en la base de datos. En consecuencia, mandató al Congreso de la Unión subsanar tal omisión considerando al menos los siguientes aspectos:

> "i. El personal que será responsable de atender los hechos que pongan en riesgo o vulneren la base de datos.
> ii. Las facultades que tendrá el personal para atender las amenazas o vulneraciones a la información.
> iii. Las medidas que deberán desplegarse frente a los supuestos de riesgo y vulneración de la base de datos.
> iv. Los supuestos específicos en que podría estimarse que la base de datos que integra el Registro se encuentra en riesgo o ha sido vulnerada."[5]

No obstante, a pesar de haber transcurrido más de dos años desde la resolución de la acción de inconstitucionalidad, el Congreso de la Unión aún no ha legislado para superar la omisión legislativa relativa en competencia de ejercicio obligatorio. Por ello, resulta urgente reformar la Ley para brindar certeza a la información contenida en la base de datos del Registro.

[5] Suprema Corte de Justicia de la Nación, "Acción de Inconstitucionalidad 63/2019." *Semanario Judicial de la Federación y su Gaceta*, Comisión Nacional de los Derechos Humanos, 24 de enero de 2023, Ponente: Ministro Javier Laynez Potisek, Secretaria: Érika Yazmín Zárate Villa.

Tercero. Argumentos de la Iniciativa

El Registro Nacional de Detenciones es la base de datos que concentra la información nacional sobre las personas detenidas en ejercicio de las facultades de las autoridades civiles. Es una herramienta que coadyuva en la prevención de la violación de los derechos humanos de las personas detenidas por tortura, tratos crueles, inhumanos y degradantes o desaparición forzada, puesto que permite realizar el seguimiento de la persona desde el momento en que es detenida hasta que se define su situación jurídica ante un juez.

En términos del artículo 16 de la CPEUM, nadie puede ser molestado sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En caso que una autoridad ejecute una orden judicial de aprehensión, la persona detenida debe ser puesta a disposición del juez o presentada ante el Ministerio Público sin dilación alguna, ya que en caso contrario se pueden establecer responsabilidades administrativas y penales contra los responsables.

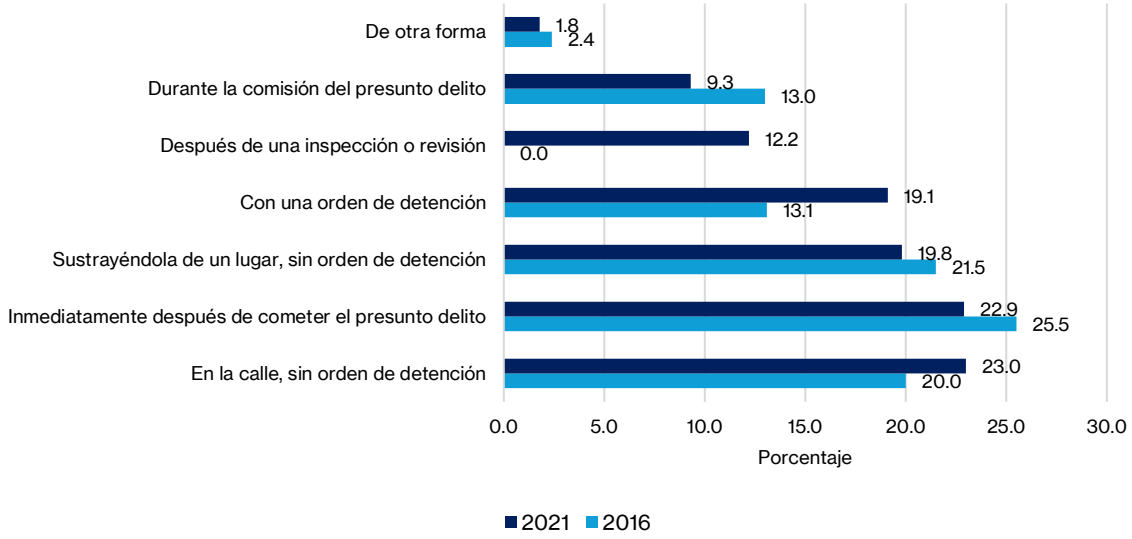
Incluso en escenarios específicos como la flagrancia o urgencia, el juez debe ratificar inmediatamente la detención o decretar la libertad con las reservas de ley. A pesar de lo dispuesto en la CPEUM, la Encuesta Nacional de Población Privada de la Libertad 2021 (ENPOL)[6] del INEGI evidenció un número significativo de detenciones arbitrarias o contrarias a la ley. De acuerdo con dicha encuesta, el 23% de la población en reclusión indicó que su detención se llevó a cabo en la calle sin orden de detención y el 19.8% sustrayéndola de un lugar sin orden de detención, como se muestra Gráfica 1.

Por otra parte, de acuerdo con el Censo Nacional de Derechos Humanos Federal y Estatal (2024 elaborado por el INEGI, las detenciones arbitrarias ocupan el tercer lugar entre los hechos presuntamente violatorios registrados en los expedientes de queja calificados como presuntamente violatorios de derechos

[6] INEGI, *Encuesta Nacional de Población Privada de la Libertad (ENPOL) 2021. Principales Resultados*. México: INEGI, 2021. https://www.inegi.org.mx/programas/enpol/2021/ (Fecha de consulta: 10 de septiembre de 2025)

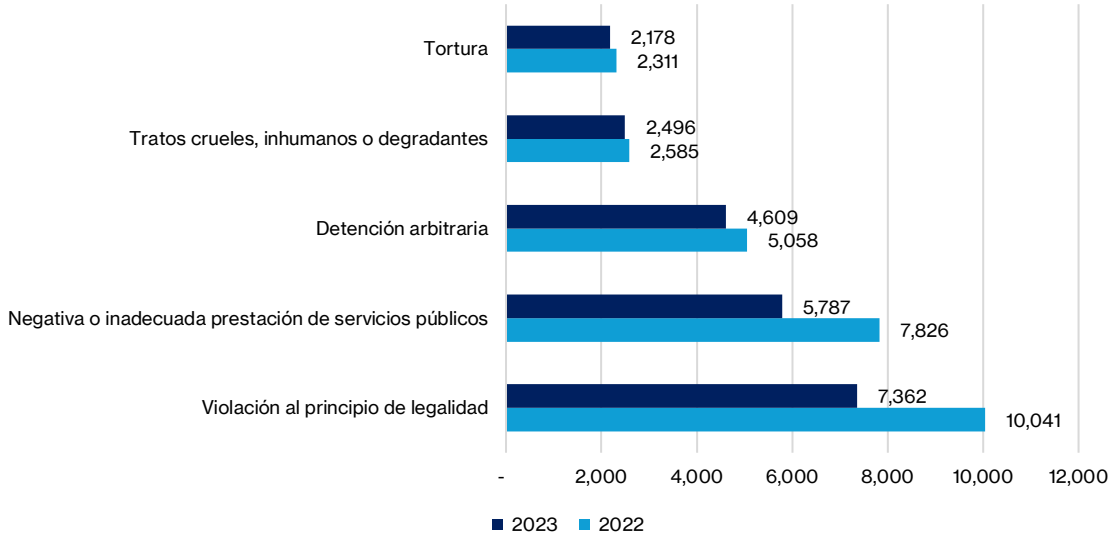
humanos, tal como se muestra en la Gráfica 2. A pesar de que disminuyeron de 5,058 casos en 2022 a 4,609 en 2023, sigue siendo un problema fundamental que demuestra que las autoridades que intervienen en las detenciones aún no garantizan los derechos humanos plenamente.

Gráfico 1. Situación en la que se llevó a cabo la detención



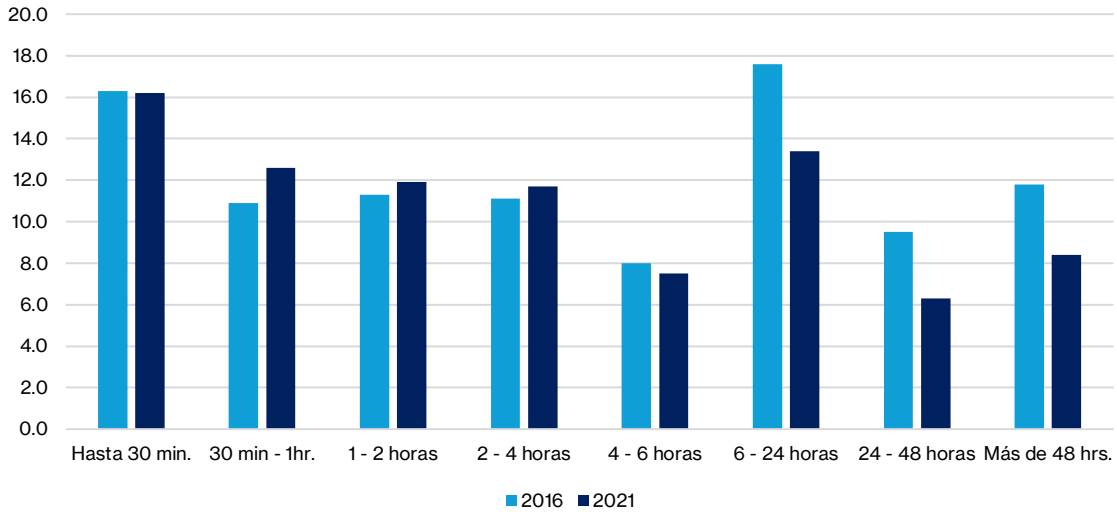
Fuente: ENPOL 2021, INEGI.

Gráfica 2. Hechos presuntamente violatorios de derechos humanos



Fuente: CNDHF 2024, INEGI.

Gráfica 3. Tiempo transcurrido entre la detención y la presentación ante el Ministerio Público o un Juez de lo Penal



Fuente: ENPOL 2021, INEGI.

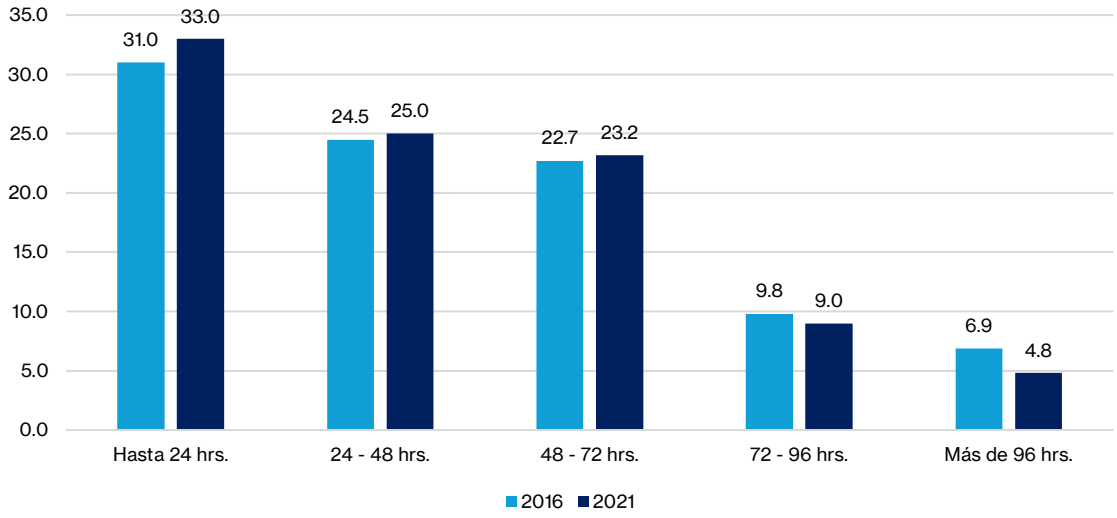
Esta información demuestra que se contradice abiertamente lo que establece la CPEUM, en el sentido que ningún indiciado podrá ser retenido por el Ministerio Público por más de 48 horas, plazo en que deberá ordenarse su libertad o ponérsele a disposición de la autoridad judicial. Si bien, en algunos casos se obtiene una determinación sobre la situación jurídica del detenido con celeridad, en la práctica este periodo también suele extenderse más allá de lo estipulado.

De acuerdo con la ENPOL 2021, se estima que el 25% de las personas detenidas permaneció en la agencia del Ministerio Público por más de 24 y hasta 48 horas, el 23.2% señaló que estuvo detenida en un periodo de más de 48 y hasta 72 horas, mientras que el 9% estuvo ahí más de 72 hasta 96 horas y el 4.8% por más de 96 horas, como lo muestra la Gráfica 4.

La ENPOL también revela información sobre el estado de salud de las personas privadas de la libertad en relación con las lesiones sufridas en la detención, destacando que el 44.4% de ellas presentó algún tipo de lesiones. Al menos en el 25.9% de los casos, el médico registró por escrito las lesiones causadas durante la detención. En cuanto al trato recibido durante la estancia en el

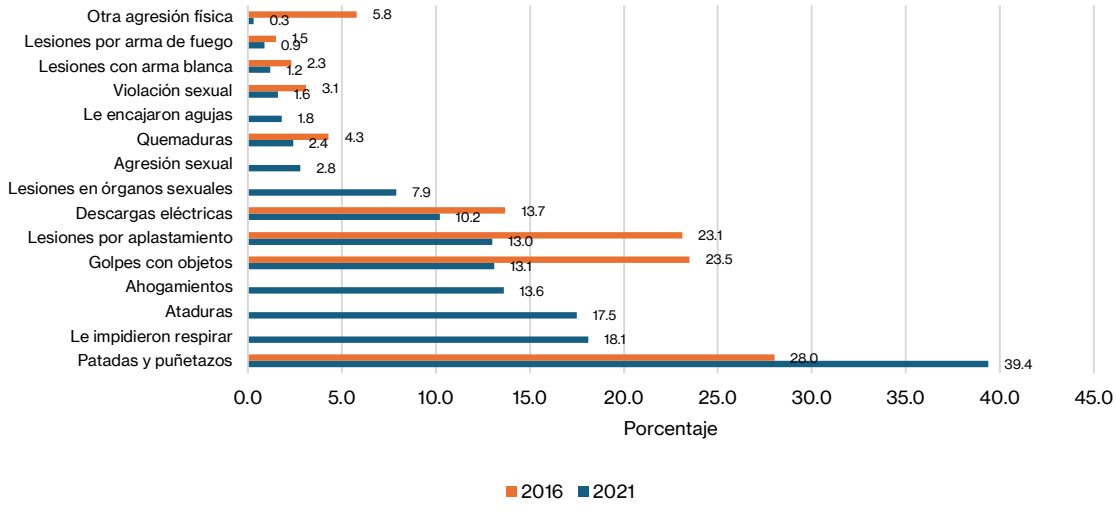
Ministerio Público, el 51% de los detenidos manifestó haber sido incomunicado o aislado como parte de violencia psicológica ejercida en su contra.

Gráfica 4. Tiempo que la población privada de la libertad permaneció en el Ministerio Público



Fuente: ENPOL 2021, INEGI.

Gráfica 5. Actos de violencia física sufridos por la población privada de la libertad durante su estancia en la Agencia del Ministerio Público



Fuente: ENPOL 2021, INEGI.

Asimismo, la población privada de la libertad es víctima de violencia física en las instalaciones del Ministerio Público. De acuerdo con los datos de la ENPOL, el 28% de los detenidos declaró haber recibido patadas o puñetazos por parte de las autoridades o con el consentimiento de estas, al 18.1% les impidieron respirar, al 17.5% los ataron, al 13% les infligieron lesiones por aplastamiento, al 10.2% les administraron descargas eléctricas, entre otras agresiones, tal como se expone en la Gráfica 5.

La evidencia empírica hasta aquí expuesta permite afirmar que la detención es el escenario donde se llevan a cabo la mayoría de los hechos que violentan los derechos humanos de las personas privadas de su libertad, tales como tortura, tratos crueles, inhumanos y degradantes. Desde el instante en que la persona es detenida y durante las 48 horas subsecuentes, existe un espacio de oportunidad para proteger los derechos humanos, lo cual consolida a la detención como uno de los momentos claves de todo proceso penal.

En ese sentido, la función del Registro es fundamental para vigilar este momento procesal porque permite supervisar y monitorear cada detención con el fin de identificar los casos en los que las personas privadas de su libertad sufren una vulneración en su integridad. Por ello, es igualmente importante proteger adecuadamente la información contenida en la base de datos del Registro frente a eventos y amenzas que la pongan en riesgo o la vulneren.

La protección de la información contenida en plataformas digitales tiene una especial relevancia en el momento actual, ya que es una de las áreas más vulnerables del Estado Mexicano. Durante los últimos años se han registrado diversos casos de ataques a bases de datos y sistemas informáticos de instituciones gubernamentales con resultados muy negativos que han comprometido de manera crítica información sensible y reservada.

En noviembre de 2019 Petróleos Mexicanos (PEMEX) sufrió un ataque, denominado *ransomware* o secuestro de datos, en el 5% de las computadoras personales operadas por la empresa en su red corporativa. Los presuntos cibercriminales que cifraron la información pidieron un rescate de 565 bitcoins

(equivalente a 4.9 millones de dólares) para desencriptarla, cifra que no fue pagada de acuerdo con la entonces Secretaria de Energía, Rocío Nahle[7].

Un caso similar se suscitó el 23 de febrero de 2020, cuando la Secretaría de Economía recibió un ataque cibernético que provocó la suspensión de sus servicios digitales. De acuerdo con la dependencia, su información sensible y la de sus usuarios no se vio comprometida, pero como medida de precaución la Dirección General de Tecnologías de la Información (DGTI) solicitó a los proveedores el aislamiento de todas las redes y servidores[8].

En junio de 2021 la Lotería Nacional detectó de forma tardía el robo de información en su área administrativa por parte de delincuentes que operan internacionalmente. El grupo, autodenominado "Avaddon" exigió un rescate económico a cambio, cuyo monto y pago no fue aclarado por la dependencia. Sin embargo, para el caso contó con el apoyo y asesoría de la Coordinación de Estrategia Digital Nacional (CEDN) de Presidencia de la República e inició la modernización de sus sistemas informáticos[9].

A finales de 2022, la Secretaría de Defensa Nacional (SEDENA) fue hackeada por un grupo internacional denominado "Guacamayos", quienes sustrajeron cerca de 6 terabytes de datos sobre operativos realizados así como información acerca de la salud del Presidente[10]. También la Secretaría de Infraestructura, Comunicaciones y Transportes (SITC) sufrió vulneración en sus datos cibernéticos y, derivado de un secuestro de información, activó el "Protocolo

[7] Rodrigo Riquelme, "El rescate por el hackeo a Pemex es el segundo mayor por ransomware." *El Economista,* Sec. Empresas, 15 de noviembre de 2019. https://www.eleconomista.com.mx/empresas/El-rescate-por-el-hackeo-a-Pemex-es-el-segundo-mayor-por-ransomware-20191115-0035.html

[8] Ivette Saldaña, "Secretaría de Economía suspende trámites tras sufrir hackeo." *El Universal*, Sec. Economía, 24 de febrero de 2020. https://www.eluniversal.com.mx/cartera/economia/secretaria-de-economia-suspende-tramites-tras-sufrir-hackeo/

[9] Redacción, "Golpe 'gordo' a la Lotería: Admite robo de datos por hackeo." *El Financiero*, Sec. Nacional, 01 de junio de 2021. https://www.elfinanciero.com.mx/nacional/2021/05/31/golpe-gordo-a-la-loteria-admite-robo-de-datos-por-hackeo/

[10] Pablo Ferri, "El hackeo a Sedena deja al descubierto la estructura de la inteligencia mexicana." *El País*, Sec. México, 10 de octubre de 2022. https://elpais.com/mexico/2022-10-10/el-hackeo-a-sedena-deja-al-descubierto-la-estructura-de-la-inteligencia-mexicana.html

Nacional Homologado de Gestión de Incidentes Cibernéticos y Plan de Contingencia", a fin de contener posibles vulnerabilidades a la información y datos derivado de accesos ilícitos a equipos informáticos[11].

En enero de 2024 el Sistema de Acreditaciones de Presidencia también fue objeto de vulneración mediante la cual se extrajo la información de 263 periodistas que cubrían la conferencia matutina del expresidente. De acuerdo con Jesús Ramírez Cuevas, vocero de la Presidencia, entre la información personal extraída sobre los periodistas se encuentran fotos, identificaciones de acreditación, datos personales, RFC, currículums, teléfonos, documentos expedidos por el Instituto Nacional de Migración, así como los medios de comunicación que representaban[12]. Al respecto, el entonces Coordinador de Estrategia Digital Nacional Carlos Emilio Calderón, indicó que durante el mes de enero de 2024 se detectaron 120 millones de peticiones potencialmente maliciosas en la plataforma gob.mx. Esto incrementó la sospecha de una posible tendencia de ciberataques a instituciones y direcciones de gobierno[13].

El 21 de febrero de 2024 el Portal del Empleo (empleo.gob.mx) del gobierno federal fue hackeado y la base de datos que incluye datos personales de 12 millones de mexicanos, fue vulnerada. Estos datos también fueron puestos a la venta en un sitio famoso entre los ciberdelincuentes, lo cual expone gravemente la seguridad de las personas cuyos datos fueron vulnerados, dado que las hace susceptibles de ser víctimas de otros delitos[14].

---

[11] Rodrigo Riquelme, "Todo lo que sabemos sobre el hackeo a la SICT del gobierno de México". *El Economista*, Sec. Tecnología, 2 de noviembre de 2022. https://www.eleconomista.com.mx/tecnologia/Todo-lo-que-sabemos-sobre-el-hackeo-a-la-SICT-del-gobierno-de-Mexico-20221102-0059.html

[12] Forbes, "Hackeo a datos de 263 periodistas fue con cuenta de exempleado desde España, revela Gobierno de México". *Forbes*, Sec. Portada, 29 de enero de 2024. https://www.forbes.com.mx/hackeo-a-datos-de-263-periodistas-fue-con-cuenta-de-exempleado-desde-espana-revela-gobierno-de-mexico/

[13] Luisa García, "Robo de datos de periodistas; gobierno federal detalla hackeo al Sistema de Acreditaciones de Presidencia". *El Universal*, Sec. Nación, 29 de enero de 2024. https://www.eluniversal.com.mx/nacion/filtracion-de-datos-de-periodistas-minuto-a-minuto-de-la-conferencia-de-prensa/

[14] Fernando Guarneros Olmos, "Hackean a la Sedena y el Portal del empleo; venden datos de los usuarios". *Expansión*, Sec. Tecnología, 27 de febrero de 2024. https://expansion.mx/tecnologia/2024/02/27/hackean-sedena-portal-del-empleo

Durante la presente administración, el 19 de noviembre de 2024 la Consejería Jurídica del Ejecutivo Federal sufrió un ciberataque por parte del grupo de hackers "RansomHub", vinculado a Rusia y a miembros de la organización cibercriminal "BlackCat", que sustrajo cerca de 313 gigabytes (GB) de información, incluyendo contratos, documentos financieros, correos electrónicos y datos personales de funcionarios. Este ha sido uno de los ataques más delicados, dado que al vulnerarse el sitio web del gobierno, se abrió la posibilidad de que más dependencias fueran vulneradas[15].

En marzo del presente año se descubrió una vulnerabilidad en el Servicio de Administración Tributaria (SAT) que permite a los ciberdelincuentes utilizar un dominio autorizado por la autoridad fiscal para distribuir un virus informático y robar información. Al respecto, la dependencia recomendó a los contribuyentes evitar abrir enlaces distribuidos por correo electrónico, ante el riesgo de sufrir una vulneración por parte del *malware*[16].En ese orden de ideas, a continuación se presentan los principales ataques a dependencias gubernamentales:

Gráfico 6. Principales ataques a dependencias del gobierno federal.

Fuente: elaboración propia con información pública

[15] Christopher Calderón, "Sheinbaum sufre primer hackeo; 'Secuestran' información confidencial de la Consejería de la Presidencia." *El Financiero,* Sec. Empresas, 19 de noviembre de 2024. https://www.elfinanciero.com.mx/empresas/2024/11/19/sheinbaum-sufre-primer-hackeo-secuestran-informacion-confidencial-de-la-consejeria-de-la-presidencia/

[16] Aldo Munguía, "SAT vulnerado: Fraude de ciberseguridad afecta cuentas autorizadas." *El Financiero*, Sec. Empresas, 10 de marzo de 2025. https://www.elfinanciero.com.mx/empresas/2025/03/10/sat-vulnerado-fraude-de-ciberseguridad-afecta-cuentas-autorizadas/

La frecuencia con la que se han verificado los ataques cibernéticos en los años recientes visibiliza la urgencia de contar con una política de Estado para garantizar la integridad de los sistemas informáticos y las bases de datos gubernamentales. Además, debe considerarse que las capacidades de la delincuencia para vulnerar los sistemas informáticos son cada vez mayores; así lo demuestra la reciente revelación del FBI que reconoció haber sido hackeado por el Cártel de Sinaloa en 2018, ataque que resultó en la muerte de varios informantes de la agencia[17].

En el marco de la reciente aprobación de una nueva reforma que militariza totalmente la Guardia Nacional, es indispensable fortalecer los mecanismos de control de su actuación, entre los cuales se encuentra el Registro Nacional de Detenciones. Por ello, estimo urgente emprender el proceso legislativo que brinde certeza a la información que contiene la base de datos del Registro, para lo cual propongo lo siguiente:

I. Determinar el personal que será responsable de atender los hechos que pongan en riesgo o vulneren la base de datos.

Propongo que las personas que desempeñen el nivel de Administrador y Supervisor dentro del Registro sean las responsables de atender los hechos que pongan en riesgo o vulneren la base de datos. También estimo necesario que la atención de estos hechos se realice bajo la supervisión de una unidad administrativa designada por la Secretaría.

II. Establecer las facultades que tendrá el personal para atender las amenazas o vulneraciones a la información.

Considero que las facultades del personal a cargo están necesariamente concatenadas con las medidas que deberán desplegarse en la atención de los hechos de riesgo o vulneración, por lo cual propongo establecer que la Secretaría definirá las facultades específicas, fijando como límite aquellas facultades otorgadas a la unidad administrativa encargada de la supervisión.

---

[17] Andrés Rodríguez, "El Cartel de Sinaloa hackeó al FBI para asesinar a sus informantes en México." *El País*, Sec. México, 27 de junio de 2025. https://elpais.com/mexico/2025-06-28/el-departamento-de-justicia-revela-que-el-cartel-de-sinaloa-hackeo-datos-de-un-telefono-del-fbi-para-asesinar-a-sus-informantes-en-mexico.html

III. Fijar las medidas que deberán desplegarse frente a los supuestos de riesgo y vulneración de la base de datos.

Propongo que las medidas a desplegarse en los supuestos de riesgo y vulneración permitan como mínimo:

1. Identificar la fuente del riesgo o vulneración de la base de datos;
2. Evaluar la magnitud del riesgo potencial o del daño sufrido;
3. Alertar a los sujetos obligados;
4. Garantizar la continuidad de la operación de la plataforma y la integridad de la información, y
5. En su caso, recuperar el control de la base de datos.

Adicionalmente propongo que la Secretaría desarrolle e implemente un sistema de alertas y bloqueos que emita la plataforma en caso de verificarse los supuestos de riesgo o vulneración.

IV. Definir los supuestos específicos en que podría estimarse que la base de datos que integra el Registro se encuentra en riesgo o ha sido vulnerada.

Propongo establecer una definición de “riesgo” cuando ocurra alguna de las siguientes situaciones:

1. Intentos de ingreso no autorizado,
2. Flujo inusual o irregular de datos,
3. Funcionamiento anómalo del sistema o de los equipos, o
4. Cuando un Enlace Estatal o Institucional notifique al Administrador la vulneración de una base de datos de su dependencia o área.

También propongo definir “vulneración” como aquella situación en que ocurra alguna de las siguientes acciones:

1. Se violenten los privilegios de acceso,
2. Se detecte un ingreso no autorizado al Registro,
3. Se detecte una transferencia de datos no autorizada, o

4. Los sujetos obligados manipulen de manera inusual los datos del Registro.

Cuarto. Cuadro comparativo

Para exponer con claridad la propuesta de modificación normativa, se presenta en el siguiente cuadro comparativo:

LEY NACIONAL DEL REGISTRO DE DETENCIONES	
TEXTO VIGENTE	**MODIFICACIÓN PROPUESTA**
Artículo 11. La Secretaría será la instancia encargada de la administración y operación del Registro y tendrá las siguientes facultades: **I.** a **VII.** ... **Sin correlativo.** **VIII.** 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 11.** ... **I.** a **VII.** ... **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 **X.** 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:	**Artículo 16.** ...

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.	**I.** a **V.** ... **Se deroga.**
Sin correlativo.	**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, 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. **El Protocolo deberá establecer las medidas que permitan, al menos, lo siguiente:** **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, y** **VI. En su caso, recuperar el control de la base de datos, y** **VII. Determinar acciones de mitigación para evitar repetición.** **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.** **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.

Quinto. Denominación del Proyecto de Decreto

La presente Iniciativa propone la siguiente denominación al Proyecto de Decreto:

"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"

Sexto. Ordenamientos por modificarse

A partir de lo aquí expuesto, el ordenamiento a modificar que considera esta propuesta es la **Ley Nacional del Registro de Detenciones**.

Séptimo. Texto Normativo Propuesto

Por lo anteriormente expuesto y fundado, someto a la consideración de esta Soberanía el siguiente:

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 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:

Artículo 11. ...

I. a **VII.** ...

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

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, 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.

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

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.

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.

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.

Dado en el Palacio Legislativo de San Lázaro, a los 17 días del mes de septiembre de 2025.

Dip. Teresa Ginez Serrano

Secretaría General

Secretaría de Servicios Parlamentarios

Gaceta Parlamentaria de la Cámara de Diputados

Director: Juan Luis Concheiro Bórquez, **Edición:** Casimiro Femat Saldívar, Ricardo Águila Sánchez, Antonio Mariscal Pioquinto.

Apoyo Documental: Dirección General de Proceso Legislativo. **Domicilio:** Avenida Congreso de la Unión, número 66, edificio E, cuarto nivel, Palacio Legislativo de San Lázaro, colonia El Parque, CP 15969. Teléfono: 5036 0000, extensión 54046. **Dirección electrónica: http://gaceta.diputados.gob.mx/**