CÁMARA DE DIPUTADOS
LXV LEGISLATURA

Gaceta Parlamentaria

Año XXVII | Palacio Legislativo de San Lázaro, miércoles 6 de diciembre de 2023 | Número 6421-II-6-1

CONTENIDO

Anexo II-6-1

Miércoles 6 de diciembre

INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY GENERAL DEL SISTEMA NACIONAL DE SEGURIDAD DIGITAL, PRESENTADA POR EL DIP. SALVADOR CARO CABRERA, INTEGRANTE DEL GRUPO PARLAMENTARIO DE MOVIMIENTO CIUDADANO.

El suscrito, **Diputado Salvador Caro Cabrera, integrante del Grupo Parlamentario de Movimiento Ciudadano de la LXV Legislatura en la Cámara de Diputados**, con fundamento en lo establecido en los artículos **71, fracción II de la Constitución Política de los Estados Unidos Mexicanos, y los artículos 6, numeral 1, fracción I y los Artículos 77 y 78 del Reglamento de la Cámara de Diputados,** sometemos a consideración del Pleno de la H. Cámara de Diputados la siguiente Iniciativa con base en la siguiente:

EXPOSICIÓN DE MOTIVOS

Ante el creciente uso de las tecnologías de la información y las comunicaciones (TIC), y la vulnerabilidad en la que estas ponen la seguridad y las libertades de las personas, es de la más alta importancia generar un Sistema que coordine a los organismos gubernamentales. Este debe buscar el pleno desarrollo seguro de las personas usuarias, enfatizando la protección a sus derechos humanos. Por tanto, se propone un Sistema que vele por el derecho a las TIC y por los derechos fundamentales de la Seguridad Digital: confidencialidad, integridad y disponibilidad de la información.

DERECHO A LAS TIC

El término de Tecnologías de la Información y las Comunicaciones (TIC) se refiere a aquellos recursos utilizados para procesar, administrar y compartir la información por medios tecnológicos como computadoras, teléfonos móviles,

televisores, reproductores portátiles de audio y video o consolas de juego.[1] Hoy en día, su papel en la sociedad es muy importante, toda vez que proveen servicios como: correo electrónico, búsqueda de información, banca online, descarga de música y video, comercio electrónico, etc.[2] De modo que se han posicionado como herramientas a las cuales tienen derecho las personas para subsistir en la actualidad.

El derecho a las TIC lo encontramos plasmado en el Artículo 6 de la Carta Magna:

> **Artículo 6o.** (…)
> El Estado **garantizará el derecho de acceso a las tecnologías de la información y comunicación**, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet.
> (…)
> B. En materia de radiodifusión y telecomunicaciones:
> I. El Estado **garantizará a la población su integración a la sociedad de la información y el conocimiento**, mediante una política de inclusión digital universal con metas anuales y sexenales.[3]

Por otro lado, citando a la **Comisión Nacional de Derechos Humanos (CNDH)**, el derecho a las TIC comprende:

> La libertad de las personas de acceder y usar eficazmente las tecnologías, navegar por la banda ancha y adquirir información de calidad por los diversos medios digitales, radiofónicos y

[1] Gobierno Federal (2018). "Tecnologías de la información y comunicación. Que la edad no sea un obstáculo". Gobierno Federal. Recuperado el 24 de octubre del 2023. Disponible en: https://www.gob.mx/profeco/documentos/tecnologias-de-la-informacion-y-comunicacion-que-la-edad-no-sea-un-obstaculo?state=published
[2] *Ibid.*
[3] (Constitución Política de los Estados Unidos Mexicanos, art. 6).

> televisivos. Asimismo, difundir cualquier contenido por los medios mencionados, interactuar y formar parte integral de la sociedad de la Información, sin importar condiciones sociales o económicas.[4]

A dichas **prerrogativas inherentes a los usuarios del mundo digital, se les ha clasificado como Derechos de Cuarta Generación.[5] Estos revisten derechos objetivos (degradación de derechos humanos por la evolución de la tecnología) y subjetivos (protección a la ciudadanía del mundo digital, comúnmente conocidos como cibernautas**).[6]

Al respecto de los Derechos de Cuarta Generación, el **Centro de Estudios de la Opinión Publica de la H. Cámara de Diputados** en su obra *Los derechos humanos de cuarta generación. Un acercamiento*, menciona:

> Este conjunto de derechos ha ido tomando forma en las últimas décadas, y abre el camino para un gran reto añadido en el siglo XXI: las nuevas formas que cobran los derechos de primera, segunda y tercera generación en el entorno del ciberespacio, es decir, la cuarta generación de los derechos humanos (…)
>
> En esta nueva etapa de la humanidad, **las libertades y derechos se han introducido en el espacio digital, lo que ha provocado que, por parte del Estado, su reconocimiento y protección constituya un reto en el sistema jurídico**.[7]

---

[4] CNDH (2015). "DERECHO DE ACCESO Y USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN". CNDH. Recuperado el 11 de octubre de 2023. Disponible en: http://appweb.cndh.org.mx/biblioteca/archivos/pdfs/foll_DerAccesoUsoTIC.pdf

[5] CESOP (2017). "Los derechos humanos de cuarta generación. Un acercamiento". Cámara de Diputados. Recuperado el 22 de octubre de 2023. Disponible en: http://www5.diputados.gob.mx/index.php/esl/content/download/91158/457163/file/CESOP-IL-72-14-DerHumaCuartaGeneracion-310817.pdf

[6] *Ibid.*

[7] *Ibid.*

De este modo**, los derechos humanos existen en el ciberespacio y así deben de ser respetados y protegidos**.

A lo largo de los años, se han elaborado cartas y declaraciones de la sociedad civil que pugnan por defender los derechos humanos en el ciber espacio. Por ejemplo, la *Declaración de Independencia del Ciberespacio* presentada en Davos, Suiza el 8 de febrero de 1996 por John Perry Barlow, fundador de la Electronic Frontier Foundation,[8] en la cual buscaba plasmar su visión del internet como un espacio diferente del mundo real. Asimismo, la *Carta de Derechos en Internet* de la Asociación para el Progreso de las Comunicaciones,[9] puntualiza que se trata de derechos que tienen como fin proteger el conocimiento,| la libertad de expresión y de asociación.

Por su parte, la Coalición Dinámica por los Derechos y Principios de Internet, localizada en el Foro para la Gobernanza de Internet de la Organización de las Naciones Unidas (ONU), emitió la *Carta de Derechos Humanos y Principios para Internet*. Dicha Carta recoge las declaraciones de principios emitidas en las Cumbres Mundiales para la Sociedad de la Información de Ginebra y de Túnez, y provee un marco normativo anclado en los Derechos Humanos internacionales para el cumplimiento y el avance de estos en el espacio *online*.[10] La Carta enfatiza que es esencial que todos que los agentes públicos y privados respeten y protejan los derechos humanos en internet. Por lo cual,

[8] Barlow, JP (1996). "Declaración de Independencia del Ciberespacio" Uhu.es. Recuperado el 22 de octubre de 2023. Disponible en: http://www.uhu.es/ramon.correa/nn_tt_edusocial/documentos/docs/declaracion_independencia.pdf

[9] APC (2006). "Carta de Derechos en Internet de la Asociación para el Progreso de las Comunicaciones". Recuperado el 22 de octubre de 2023. Disponible en: https://www.apc.org/sites/default/files/APC_charter_ES_2.pdf

[10] Foro para la Gobernanza de Internet de la Organización de las Naciones Unidas (2014). "Carta de derechos humanos y principios para internet". Dynamic Coalition: Foro de Gobernanza de Internet de las Naciones Unidas derechoseninternet.com. Recuperado el 22 de octubre de 2023. Disponible en: https://derechoseninternet.com/docs/IRPC_Carta_Derechos_Humanos_Internet.pdf

menciona que **se debe lograr que el internet funcione y evolucione de manera que sean cumplidos los derechos humanos.**[11]

Esto se encuentra en concordancia con el primer y segundo párrafo del Artículo 6° de la Constitución Política de los Estados Unidos Mexicanos.

> **Artículo 6o.** (…) El derecho a la información será garantizado por el Estado.
>
> Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión.[12]

Del mismo modo, ha habido diferentes acciones para proteger estos derechos. El **Consejo de Derechos Humanos de las Naciones Unidas**, en la ***Resolución A/HRC/20/L.132,*** titulada *Promoción, protección y disfrute de los derechos humanos en Internet*,[13] señaló que los derechos que se tienen en línea y fuera de línea deben protegerse:

> 1. Afirma que **los mismos derechos que tienen fuera de línea las personas también deben protegerse en línea**, en particular la **libertad de expresión,** lo que es aplicable independientemente de las fronteras y por conducto de cualquier medio de su propia elección, de conformidad con el artículo 19 de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos;
>
> 2. Reconoce la naturaleza global y abierta de **Internet como fuerza motriz de la aceleración de los progresos** en la

[11] *Ibidem*.
[12] (Constitución Política de los Estados Unidos Mexicanos, art. 6, primer y segundo párrafos)
[13] Consejo de Derechos Humanos de Naciones Unidas (2018). "Resolución A/HRC/20/L.13: Promoción, protección y disfrute de los derechos humanos en Internet". Consejo de Derechos Humanos de Naciones Unidas. Consultado el 10 de octubre del 2023. Disponible en: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_38_L10.pdf

consecución del desarrollo en sus diversas formas, especialmente el logro de los Objetivos de Desarrollo Sostenible;

(…)

5. Exhorta a todos los Estados a cerrar las brechas digitales, especialmente la existente entre los géneros, y a aumentar el uso de la tecnología de la información y las comunicaciones, para **promover el pleno disfrute de los derechos humanos para todos**, en particular:

a) Fomentando un **entorno en línea propicio, seguro y favorable** a la participación de todos

(…)

d) Aplicando un **enfoque integral basado en los derechos humanos en el suministro y la ampliación del acceso a la tecnología de la información y las comunicaciones**, y **promoviendo**, en **consulta con todos los sectores de la sociedad, especialmente las empresas comerciales y los actores de la sociedad civil,** políticas y directrices en materia de tecnología de la información y las comunicaciones que otorguen una atención específica a las consideraciones de género;

6. Exhorta a los Estados a **garantizar recursos eficaces en los casos de violaciones de los derechos humanos, en particular las relacionadas con Internet,** de conformidad con sus obligaciones internacionales;

Del mismo modo, en el año 2016, el **Consejo de Derechos Humanos de la ONU** aprobó la ***Resolución A/HCR/20/L***.[14] En ella, reafirmó lo dicho en la anterior

[14] Consejo de Derechos Humanos de Naciones Unidas (2016). "Resolución A/HRC/32/L.20: Promoción protección y disfrute de los Derechos Humanos en Internet". Recuperado el 11 de octubre de 2023. Disponible en: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_32_L20.pdf

resolución y **condenó las violaciones en contra de los derechos humanos de las personas al limitar su participación en las tecnologías**:

> 9. Condena inequívocamente todos los abusos y violaciones de los derechos humanos, como torturas, ejecuciones extrajudiciales, desapariciones forzadas y detenciones arbitrarias, así como la expulsión, intimidación y hostigamiento y la violencia de género **cometida contra las personas por ejercer sus derechos humanos y libertades fundamentales en Internet, y exhorta a todos los Estados a que garanticen la rendición de cuentas** a este respecto;
>
> 10. Condena inequívocamente **las medidas cuyo objetivo deliberado es impedir u obstaculizar el acceso o la divulgación de información en línea, vulnerando el derecho internacional de los derechos humanos,** y exhorta a todos los Estados a que se abstengan de adoptar estas medidas, o cesen de aplicarlas;
>
> (…)
>
> 12. Exhorta a todos los Estados a que consideren la posibilidad de formular, mediante **procesos transparentes e inclusivos con la participación de todos los interesados, y adoptar políticas públicas nacionales relativas a Internet que tengan como objetivo básico el acceso y disfrute universal de los derechos humanos**;[15]

De este modo, la Seguridad Digital abarca todo lo que tiene que ver con la protección de datos confidenciales, información biométrica, personal, software, compras y banca en línea, los sistemas de informática gubernamental y otros detalles de la vida moderna que dependen de las computadoras y otros dispositivos inteligentes

[15] *Ibid.*

La Seguridad Digital es uno de los desafíos clave del presente y el futuro, ya que las TIC han crecido y la dependencia en el ciber espacio. La cuestión estriba en que esto ha generado que los ataques cibernéticos se incrementen de forma significativa, porque a medida que crece la tecnología, también crecen las maneras de corromperla.

ACCIONES GUBERNAMENTALES FALLIDAS

Reconociendo la importancia de la tecnología, el Gobierno Mexicano se comprometió a tomar medidas de seguridad para proteger la información, así como prevenir y atender incidentes cibernéticos de las instituciones de la administración pública, en la Estrategia Digital Nacional 2021-2024.[16] De este modo, señaló objetivos específicos y líneas de acción en materia de seguridad, especificados a continuación:

Objetivos específicos	Líneas de acción
• 5. Promover una cultura de seguridad de la información que genere certeza y confianza a las personas usuarias de los servicios tecnológicos institucionales y gubernamentales.	• Promover una política general de seguridad de la información que procure la preservación de la confidencialidad, disponibilidad e integridad de la información resguardada por las Instituciones. • Promover la implementación de un Protocolo Homologado para la Gestión de Incidentes

[16]Gobierno Federal (2020). "Acuerdo por el que se expide la Estrategia Digital Nacional 2021-2024". Diario Oficial de la Federación de fecha 6 de septiembre de 2021. Recuperado el 10 de octubre del 2023. Disponible en: https://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021#gsc.tab=0

	Cibernéticos entre las Instituciones. • Coordinar evaluaciones de seguridad en las Instituciones para la detección de amenazas y mejorar la gestión de riesgos de seguridad de la información. • Fortalecer la coordinación entre autoridades para mejorar los procesos de prevención y atención de incidencias cibernéticas. • Promover buenas prácticas de prevención y reacción a través de la colaboración con el Centro Nacional de Respuesta a Incidentes Cibernéticos • Proponer la adopción de acciones clave para fortalecer los mecanismos de seguridad de la información que prevengan riesgos

Tabla 1. Elaboración propia con información del Acuerdo por el que se expide la Estrategia Digital Nacional 2021-2024

Por otro lado, se creó el Protocolo Homologado para la Gestión de Incidentes Cibernéticos entre las Instituciones tiene como objetivo "gestionar de forma coordinada los incidentes cibernéticos (…) mediante la aplicación de

procedimientos y prácticas de Ciberseguridad, para la contención y mitigación de amenazas cibernéticas".[17] Esto se implementa mediante un Grupo Coordinador que articula los esfuerzos en materia de ciberseguridad entre las Instituciones de la administración pública Federal, Entidades Federativas, Organismos Constitucionales Autónomos, Academia e Instancias del Sector Privado del país involucradas.[18]

Asimismo, el ***ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la administración pública Federal*** establece que las instituciones deberán contar con un Marco de Gestión de Seguridad de la Información y un órgano interinstitucional en materia de Tecnologías de la Información y Comunicación y Seguridad de la Información que articule los esfuerzos de las dependencias de la administración pública Federal.[19]

A pesar de **los objetivos y compromisos con la ciudadanía,** estos **no se cumplieron** ya que diversas instituciones de la administración pública Federal han sufrido ataques cibernéticos que inevitablemente afectaron la Seguridad Digital de la ciudadanía.

---

[17] Gobierno Federal (2022). Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos. Gobierno Federal. Consultado el 24 de octubre del 2023. Disponible en: https://www.gob.mx/gncertmx/articulos/protocolo-283239

[18] Secretaría de Seguridad y Protección Ciudadana (2021). "Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos". Secretaria de Seguridad y Protección Ciudadana. Consultado el 24 de octubre del 2023. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/735044/Protocolo_Nacional_Homologado_de_Gestion_de_Incidentes_Ciberneticos.pdf

[19] Secretaría de Gobernación (2021). "ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la administración pública Federal". Diario Oficial de la Federación. Consultado el 24 de octubre del 2023. Disponible en: https://dof.gob.mx/nota_detalle.php?codigo=5628885&fecha=06/09/2021#gsc.tab=0

A continuación, se enlistan algunos de los ataques a la seguridad cibernética ocurridos en los últimos años:

- Durante abril y mayo de 2018 el **Banco de México** fue víctima de varios ataques cibernéticos que **vulneraron el Sistema de Pagos Electrónicos Interbancarios**.[20] **Se sustrajeron por lo menos 300 millones de pesos** de cinco instituciones bancarias.[21] Esto ocurrió pese a la existencia de la Gerencia de Seguridad de Tecnologías de la Información, del Centro de Defensa de Ciberseguridad y de la Dirección de Ciberseguridad, que en teoría son los responsables de procurar la ciberseguridad y hacer frente a los incidentes de la institución.

- En 2019, la empresa estatal **Petróleos Mexicanos** (PEMEX) fue *hackeada*. De este modo, **180,000 archivos de la petrolera fueron secuestrados** y los delincuentes demandaron 565 *bitcoins*, equivalente a **4.9 millones de dólares, para liberar los archivos**.[22] De este modo, en febrero de 2020 se filtraron en la *Deep web* documentos con información de la infraestructura de PEMEX, de proveedores y datos personales de empleados y clientes.[23]

[20] Banco de México (2018). "Información sobre los Ataques a Participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI)". Banco de México. Recuperado el 9 de octubre de 2023. Disponible en: https://www.banxico.org.mx/publicaciones-y-prensa/informes-trimestrales/recuadros/%7B86A498AE-5F8A-57CE-2C11-B5059AB9EB20%7D.pdf

[21] Forbes (2018). "Hackers roban al menos 300 mdp con ataque a bancos en México". Forbes México. Recuperado 10 de octubre de 2023. Disponible en: https://www.forbes.com.mx/hackers-roban-de-300-a-400-mdp-con-ataque-a-sistema-de-bancos/

[22] Riquelme, R. (2019). "El rescate por el hackeo a Pemex es el segundo mayor por ransomware". El Economista. Recuperado 10 de octubre de 2023. Disponible en: https://www.eleconomista.com.mx/empresas/El-rescate-por-el-hackeo-a-Pemex-es-el-segundo-mayor-por-ransomware-20191115-0035.html

[23] Badillo, D. (2021). "Flotan" en internet 180,000 archivos de Pemex sustraídos por hackers". El Economista. Recuperado 10 de octubre de 2023. Disponible en: https://www.eleconomista.com.mx/empresas/Flota-en-internet-informacion-sensible-de-Pemex-sustraida-por-hackers-20210216-0103.html

- En 2020, la **Secretaría de Economía**, sufrió un ataque cibernético que impactó a los servidores[24] y afectó los trámites para la exportación.[25]

- En 2020 la **Secretaría de Trabajo y Previsión Social** fue *hackeada,* afectando a la plataforma de legitimación de contratos colectivos.[26]

- En 2020, la **Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros** fue *hackeada*, dejando a su página fuera se servicio.[27]

- En 2021, la **Lotería Nacional,** fue hackeada por el grupo ruso Avaddon.[28] De este modo, fueron secuestrados por lo menos 800 archivosfinancieros, legales y contratos firmados desde 2009.[29] A cambio de liberarlos el grupo pidió dinero, pero al no recibir el pago el grupo publicó la información.[30]

---

[24] Secretaria de Economía (2022). "Controla Secretaría de Economía ataque informático" Secretaría de Economía. Recuperado 10 de octubre de 2023. Disponible en: https://www.gob.mx/se/articulos/controla-secretaria-de-economia-ataque-informatico?idiom=es

[25] Saldaña, I. (2020). "Por hackeo a Secretaría de Economía, trámites de azúcar, jitomate y llantas serán por correo". El Universal. Recuperado 10 de octubre de 2023. Disponible en: https://www.eluniversal.com.mx/cartera/por-hackeo-economia-tramites-de-azucar-jitomate-y-llantas-seran-por-correo

[26] Excélsior (2020). "Incidente afecta la Secretaría del Trabajo". Excélsior. Recuperado 10 de octubre de 2023. Disponible en: https://www.excelsior.com.mx/nacional/incidente-afecta-la-secretaria-del-trabajo/1368850

[27] Armenta, MH (2020). "Hackean la página de la Condusef y la dejan fuera de servicio". Forbes México. Recuperado 10 de octubre de 2023. Disponible en: https://www.forbes.com.mx/hackean-la-pagina-de-internet-de-la-condusef/

[28] Guillén, Beatriz (2021). "Un grupo de hackers de origen ruso secuestra información confidencial de la Lotería Nacional". El País. Consultado el 21 de agosto del 2023, en: https://elpais.com/mexico/2021-06-01/un-grupo-de-hackers-de-origen-ruso-secuestra-informacion-confidencial-de-la-loteria-nacional.html

[29] Guillén, Beatriz (2021). "Los hackers que robaron información a la Lotería Nacional filtran 800 archivos confidenciales". El País. Consultado el 21 de agosto del 2023, en: https://elpais.com/mexico/2021-06-09/los-hackers-que-robaron-informacion-a-la-loteria-nacional-filtran-800-archivos-confidenciales.html

[30] *Ibid.*

- En 2021, la **Plataforma Nacional de Transparencia** sufrió ciberataques por medio del método conocido como *ramsonware*. Este es un *software* con el que los cibercriminales secuestran datos a través de un cifrado de archivos que se libera pagando un rescate.[31]

Esto vulnera el bienestar de la ciudadanía mexicana, ya que las personas que *hackean* los sistemas acceden a información confidencial. Por lo tanto, pudo haber sido importante implementar las medidas propuestas en la Estrategia Digital Nacional 2021-2024.

De este modo, es particularmente importante el ***hackeo* del cual fue víctima la Secretaría de la Defensa Nacional**, ya que **dejó al descubierto 6 *terabytes* de información** clasificada, documentos sin testar y estrategias de seguridad, poniendo en riesgo a la población del país.

***HACKEO* A LA SEDENA**

El 29 de septiembre de 2022, el grupo *hacktivista* Guacamaya ingresó a los sistemas de la Secretaría de la Defensa Nacional (SEDENA) y obtuvo 6 terabytes[32] de información. Entre los documentos filtrados, se encontraban comunicaciones, fotografías y documentos de diversos temas, como contratos de obra pública, seguridad, contratos del ejército, correos, el estado de salud del Presidente López Obrador, **informes de inteligencia sobre líderes** criminales y **políticos**,[33] **transcripciones de intervenciones telefónicas, directorios y reportes sobre seguimiento a personas, como el Embajador de**

[31] *Ibid*.
[32] Abi-Habib, M. (2022). "El hackeo del ejército mexicano expone secretos de la institución más poderosa del país". The New York Times. Recuperado 8 de octubre de 2023. Disponible en: https://www.nytimes.com/es/2022/10/06/espanol/mexico-sedena-guacamaya-hackeo.html
[33] BBC News Mundo. (2022). "Guacamaya Leaks: 5 revelaciones del hackeo masivo que sufrió el ejército de México". Recuperado 8 de octubre de 2023. Disponible en: https://www.bbc.com/mundo/noticias-america-latina-63167331

Estados Unidos en México,[34] y el despliegue detallado de las fuerzas armadas.[35] **La información obtenida son 36 millones de documentos PDF, 1.5 millones de fotos y 3 mil horas de video. Esto es el triple de la información divulgada en los *Pandora Papers*.**[36]

Diversos expertos en ciberseguridad y sociedad civil mencionan que el *hackeo* a la SEDENA evidencia **la vulnerabilidad del Ejército de México en ciberseguridad**. En este sentido, Luis Fernando García, director ejecutivo de R3D explicó lo siguiente: "**Revela incompetencia o un descuido por parte del Gobierno** en la **protección de ciberseguridad** de sus instituciones".[37] Por su parte Leopoldo Maldonado, director para México y Centroamérica de Artículo 19 aseveró que el Ejército y el Gobierno tienen la responsabilidad por omisión, "por las vulnerabilidades que hay en sus redes internas, en sus sistemas de seguridad cibernética".[38]

Sin embargo, esta vulnerabilidad fue detectada de manera oportuna, pero no fue atendida. Francisco Solano, director de tecnologías de la información (TI) y portafolio de Logicalis para el norte de Latinoamérica explicó que el grupo Guacamaya aprovechó **una flaqueza del servidor Microsoft Exchange detectada en el primer semestre del año pasado por el gobierno, la cual no se pudo corregir por falta de recursos.**[39] Mientras que Adolfo Grego, especialista en investigación forense refiere que los hackers necesitaron por lo

[34] Loret, C. (2022). "Loret Capítulo 96". Latin US. Recuperado 8 de octubre de 2023. Disponible en: https://latinus.us/2022/09/29/loret-capitulo-96/

[35] *Ibidem.*

[36] BBC News Mundo. (2022). "Guacamaya Leaks: 5 revelaciones del hackeo masivo que sufrió el ejército de México". Recuperado 8 de octubre de 2023. Disponible en: https://www.bbc.com/mundo/noticias-america-latina-63167331

[37] Forbes. (2022). "Hackeo a Sedena revela incompetencia y pone en riesgo a personas: R3D". Forbes México. Recuperado 8 de octubre de 2023. Disponible en: https://www.forbes.com.mx/espionaje-al-ejercito-mexicano-vulnera-y-viola-los-ddhh-r3d/

[38] *Ibid.*

[39] *Ibid.*

menos de tres días para copiar la información de la SEDENA, lo cual supone inacción por parte de las autoridades.[40]

Ante esto, cabe mencionar que el 18 de mayo de 2017, la SEDENA obtuvo el registro ante la Secretaría de Hacienda y Crédito Público del programa denominado "Adquisición de Plataformas Tecnológicas para implementar un Centro de Operaciones del Ciberespacio". Dicho **programa tiene como fin dotar de recursos tecnológicos y de capacitación** de personal. Por lo **que a partir de 2018 se han dado recursos para la adquisición de plataformas para habilitar capacidades de ciber inteligencia** y de especialización de recursos humanos en la **SEDENA,** e incluso desarrollar actividades de investigación en el ciberespacio. Hasta ahora, la inversión ha sido de por lo menos **340 millones 491 mil 578 de pesos**. Sin embargo, ni esta inversión pudo detener el *hackeo*.[41]

La profundidad del problema radica en que la Secretaría encargada de velar por la seguridad nacional del país, establecido en la Ley de Seguridad Nacional, puso en riesgo a cada una de las personas que habitan el país.[42] Sin embargo, las vulnerabilidades de SEDENA en materia de Seguridad Digital no son nuevas. Tras realizar una revisión exhaustiva a la dependencia, con motivo de la Cuenta Pública del 2020, **la Auditoría Superior de la Federación reportó en 2021 las deficiencias de SEDENA en Seguridad Digital**:

- **Deficiencias en los controles de ciberdefensa para la infraestructura de hardware y software** de la Secretaría, relacionadas con las directrices, infraestructura y herramientas informáticas en esta materia, que podrían afectar la integridad, disponibilidad y confidencialidad de la

[40] *Ibid.*
[41] Rosa, Y. de la. (2022). "Sedena gasta más de 340 mdp en ciberseguridad. . . y aun así la hackean". Forbes México. Recuperado 9 de octubre de 2023. Disponible en: https://www.forbes.com.mx/sedena-gasta-mas-de-340-mdp-en-ciberseguridad-y-aun-asi-la-hackean/
[42] (Ley de Seguridad Nacional, art. 3)

información, poniendo en riesgo la operación de la SEDENA.

- Falta de control en la configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores, evaluación continua de la vulnerabilidad y solución, así como protección de correo electrónico y navegador web.[43]

Ante esto, se plantean los siguientes cuestionamientos: Si Guacamaya pudo, ¿qué no podrán hacer células criminales, cárteles y terroristas, ahora que saben lo vulnerable que es SEDENA? Por tanto, el cuestionamiento más importante es: ¿existe Seguridad Digital en México? La respuesta a esto es "no", y menos se respetan los derechos de las persona en el ciberespacio. Por ejemplo, el Caso Pegasus que puso a México como uno de los principales consumidores de tecnologías de vigilancia utilizada por funcionarios del gobierno para perpetuar intervenciones ilegales de las comunicaciones en contra de políticos, líderes comunitarios, activistas y periodistas.[44] Es inadmisible que esto siga ocurriendo.[45]

VÍCTIMAS DE ATAQUES

Por otro lado, las personas también son víctimas de ataques directos, ya sea mediante sus negocios o en la vida privada. Esto vulnera los derechos de todas y todos ya que las empresas más importantes lidian con datos e información de nuestro día a día, mientras que las más pequeñas cuentan con información

[43] Hackeo: Desde 2021 ASF reprobó a Sedena por deficiencias graves en ciberseguridad. Recuperado 9 de octubre de 2023, de https://m-x.com.mx/al-dia/hackeo-desde-2021-asf-reprobo-a-sedena-por-deficiencias-graves-en-ciberseguridad

[44] Davis, K., & Fry, W. (2022, febrero 20). En México no hay secretos: Cómo el espionaje se hizo rutina para políticos y otras personas en el poder. The Los Angeles times. https://www.latimes.com/espanol/mexico/articulo/2022-02-20/en-mexico-no-hay-secretos-como-el-espionaje-se-hizo-rutina-para-politicos-y-otras-personas-en-el-poder

[45] Cid, A. S. (2021, noviembre 9). El espionaje del 'caso Pegasus' en México se cobra su primer detenido. Ediciones EL PAÍS S.L. https://elpais.com/mexico/2021-11-09/el-espionaje-del-caso-pegasus-en-mexico-se-cobra-su-primer-detenido.html

sensible de sus trabajadores, proveedores y clientes. Por ejemplo, en 2022, por lo menos **12 empresas** del sector industrial y manufacturero sufrieron ataques por parte del grupo BlackCat, que se dedica a secuestrar información, archivos y servidores, pidiendo un rescate económico.[46]

Sin embargo, no son sólo los grupos delictivos los que cometen violaciones, sino también el Gobierno. De este modo, la **ciudadanía** también ha sido **víctima de espionaje** en múltiples ocasiones, con lo cual se violenta su derecho a la privacidad y sus derechos digitales. A continuación, se enlistan algunos casos:

- En 2014, tras la desaparición forzada de los 43 estudiantes de la Escuela Normal Rural de Ayotzinapa, los padres de familia acudieron a distintas autoridades internacionales para que investigaran el caso.[47] El Grupo Interdisciplinario de Expertos Independientes (GIEI) en julio de 2023 presento su sexto y ultimo informe sobre el caso Ayotzinapa. En dicho informe **el GIEI señala que el Ejército** fue el principal obstáculo para la búsqueda de verdad y justicia. Obstaculizó el acceso a información importante para la investigación, **y el Centro Militar de Inteligencia, una estructura internada secreta de espionaje del Ejército que entre sus funciones hace intercepciones telefónicas y de mensajería**, **se encargó de ocultar información privilegiada al GIEI respecto de los hechos ocurridos en Iguala**.[48]

[46] Redacción IT Masters Mag (2022). "Aparece ramsonware BlackCat en al menos 12 empresas de México, alertan". IT Masters Mag. Consultado el 21 de agosto del 2023, en: https://www.itmastersmag.com/noticias-analisis/aparece-ransomware-blackcat-en-al-menos-12-empresas-de-mexico-alertan/

[47] Centro Prodh (2023). "Ayotzinapa". Centro Prodh. Consultado el 21 de agosto del 2023, en: https://centroprodh.org.mx/casos-3/ayotzinapa/

[48] GIEI (2023). "Informe Ayotzinapa VI: Hallazgos, avances, obstáculos y pendientes". Grupo Interdisciplinario de Expertos Independientes. Consultado el 21 de agosto del 2023, en: https://drive.google.com/file/d/1_mRYLO9soOW5RoV8dLP2y1CkjlP8PIH1/view

- Entre enero de 2015 y julio de 2016, **periodistas, defensores de derechos humanos, científicos**, personal del Instituto Mexicano para la Competitividad, integrantes del colectivo **Mexicanos contra la Corrupción y la Impunidad**, miembros del Centro de Derechos Humanos Miguel Agustín Pro Juárez e integrantes del **GIEI**, sufrieron **intentos de infección con el *malware* Pegasus**, que es un sofisticado malware de vigilancia adquirido por la Secretaria de la Defensa Nacional, para llevar a cabo acciones de vigilancia.[49]

Sobre Pegasus, hay muchos ejemplos:

- En 2020, Raymundo Ramos, defensor de derechos humanos, fue atacado con el *malware* Pegasus.[50] Un informe The Citizen Lab de la Universidad de Toronto reporta que las **comunicaciones** de Ramos **fueron interferidas y esto solo pudo haber sido con el malware Pegasus**[51] con el objeto de **obtener conversaciones privadas** de Raymundo con otros periodistas e información relacionada con el caso de ejecuciones extrajudiciales por parte del Ejercito en Nuevo Laredo, Tamaulipas. Cabe mencionar que **él titular de SEDENA, Luis Cresencio Sandoval, estaba enterado** de esto y se le aconsejo presentar la información sobre Ramos a la Policía Ministerial Militar de forma confidencial.[52] El activista se pronunció al respecto de esto "Estás

[49] R3D (2017). "#GOBIERNOESPÍA: VIGILANCIA SISTEMÁTICA A PERIODISTAS Y DEFENSORES DE DERECHOS HUMANOS EN MÉXICO". Red en Defensa de los Derechos Digitales. Consultado el 21 de agosto del 2023, en: https://r3d.mx/2017/06/19/gobierno-espia/

[50] R3D (2023). "ESTRUCTURA SECRETA DEL EJÉRCITO ESPIÓ CON PEGASUS A RAYMUNDO RAMOS, CON PLENO CONOCIMIENTO DEL SECRETARIO DE LA DEFENSA". Red en Defensa de los Derechos Digitales. Consultado el 21 de agosto del 2023, en: https://r3d.mx/2023/03/07/estructura-secreta-del-ejercito-espio-con-pegasus-a-raymundo-ramos-con-pleno-conocimiento-del-secretario-de-la-defensa/

[51] The Citizen Lab (2023). "UPDATE: The Targeting of Jesús Raymundo Ramos Vázquez with Pegasus spyware". Muck School of Global Affairs & Public Policy. Consultado el 21 de agosto del 2023, en: https://r3d.mx/wp-content/uploads/Memo-Citizen-Lab-Raymundo-Ramos-230304.pdf

[52] R3D (2023). "ESTRUCTURA SECRETA DEL EJÉRCITO ESPIÓ CON PEGASUS A RAYMUNDO RAMOS, CON PLENO CONOCIMIENTO DEL SECRETARIO DE LA DEFENSA". Red en Defensa de los Derechos Digitales. Consultado el

hablando de un **ejército de personas con acceso a vigilancia**, a tu **información personal, a tus movimientos, a tus amistades, a todo… Ellos saben en todo momento en dónde estoy**".[53]

- En, 2019, el periodista Ricardo Raphael y su hijo, menor de 12 años, fueron **víctimas de espionaje con el *malware* Pegasus**, sumado a que el menor recibió amenazas.[54]

- En 2020, Renato Ramos Vázquez, defensor de derechos humanos en Tamaulipas y presidente del Comité Estatal de Derechos Humanos en Nuevo Laredo, **fue espiado con el *malware* Pegasus obteniendo mensajes de texto, llamadas, aplicaciones de mensajería instantánea, correos electrónicos, fotos, contactos, notas, etc**. Al respeto del espionaje que sufrió, Ramos Vázquez señala "Este espionaje no solamente nos expone a nosotros, expone a las víctimas, a las familias, a los abogados, a los periodistas**, nos exponen a todos por unas fuerzas armadas que están fuera de control**".[55]

- En 2022, dos integrantes del Centro de Prodh, **fueron espiados con el *malware* Pegasus**, debido a esto The Citizen Lab de la Universidad de

21 de agosto del 2023, en: https://r3d.mx/2023/03/07/estructura-secreta-del-ejercito-espio-con-pegasus-a-raymundo-ramos-con-pleno-conocimiento-del-secretario-de-la-defensa/

[53] Bergman, Ronen y Natalie Kitroeff (2023). "El espionaje del ejército mexicano genera temores de un 'Estado militar'". The Ney York Times. Consultado el 21 de agosto del 2023, en: https://www.nytimes.com/es/2023/03/07/espanol/espionaje-ejercito-pegasus-mexico.html

[54] Expansión Política (2022). "Software espía Pegasus se usó durante gobierno de AMLO, revela investigación". Expansión política. Consultado el 21 de agosto del 2023, en: https://politica.expansion.mx/mexico/2022/10/03/software-pegasus-se-uso-durante-gobierno-de-amlo-revela-investigacion

[55] Expansión Política (2022). "Software espía Pegasus se usó durante gobierno de AMLO, revela investigación". Expansión política. Consultado el 21 de agosto del 2023, en: https://politica.expansion.mx/mexico/2022/10/03/software-pegasus-se-uso-durante-gobierno-de-amlo-revela-investigacion

> Toronto analizó los dispositivos de Santiago Aguirre Espinosa, Director del Centro Prodh, y María Luisa Aguilar Rodríguez, coordinadora del Área Internacional, en dicho análisis se idéntico que ambas personas fueron espiadas utilizando el *malware* Pegasus.[56]

Debido a la alarmante situación de espionaje que vive la población mexicana la CIDH y su Relatoría Especial para la Libertad de Expresión (RELE), han manifestado su preocupación al respecto, manifestando lo siguiente:

> …**urgen al Estado mexicano** a redoblar sus esfuerzos en las investigaciones a periodistas y personas defensoras por el **uso ilegítimo del software de vigilancia Pegasus**…
> En los últimos años, la CIDH y la RELE **han conocido múltiples casos de espionaje a través de Pegasus en México.** Una investigación de Citizen Lab (Universidad de Toronto) de abril de 2023 **reveló que autoridades de la** Secretaría Nacional de Defensa (**SEDENA**) habrían **utilizado Pegasus para espiar** ilegalmente a dos integrantes de la organización "Centro de Derechos Humanos Miguel Agustín Pro Juárez" (Centro Prodh) entre junio y septiembre de 2022, lo cual podría estar vinculado con sus labores de defensa de graves violaciones a derechos humanos… **La lista de personas presuntamente afectadas por Pegasus** en los últimos años **incluye, entre otras, a periodistas, personas defensoras, un juez de la Corte Interamericana de Derechos Humanos y un integrante del Grupo Interdisciplinario de Expertos Independientes (GIEI) en el caso Ayotzinapa**.
> **Para la Comisión, este tipo de prácticas** no solo **vulnera el**

[56] R3D (2023). "Ejército Espía". Red en Defensa de los Derechos Digitales. Consultado el 21 de agosto del 2023, en: https://ejercitoespia.r3d.mx/

derecho a la privacidad consagrado en la Convención Americana, sino también tiene el potencial de **poner en riesgo la integridad de personas** periodistas y defensoras, a la vez que **incrementa la autocensura en la prensa y desincentiva las labores de defensa de derechos humanos.** El Estado tiene la obligación de garantizar el derecho a la vida privada mediante acciones positivas dirigidas a asegurar la protección de dicho derecho de las interferencias de autoridades públicas y de personas o instituciones privadas.

La CIDH y su RELE llaman al Estado mexicano a investigar de forma completa, exhaustiva e imparcial la adquisición y **el uso de Pegasus y sancionar a quienes resulten responsables**;…

Asimismo, **la CIDH y la RELE instan a garantizar la adopción de todas las medidas necesarias para respetar, proteger y garantizar el derecho a la privacidad y la libertad de expresión de la ciudadanía, el ejercicio del periodismo, la defensa de los derechos humanos y la participación pública.** Ello incluye el **deber** de las más altas **autoridades de rechazar** de manera clara, pública y contundente **cualquier tipo de injerencia ilegal a la privacidad de las personas por medio de la tecnología**.

Finalmente, de conformidad con pronunciamientos previos, la CIDH y su Relatoría Especial **urgen al Estado a** cesar inmediatamente cualquier acción destinada a la venta, la transferencia y el uso de tecnología de vigilancia hasta tanto se establezcan marcos normativos en línea con los derechos humanos y **a instruir a todos sus agentes a que se abstengan de utilizar el software Pegasus** de modo ilegal y que denuncien este tipo de instrucciones si viniesen de parte de sus superiores.[57]

[57]CIDH (2023). "CIDH manifiesta su preocupación por el aumento de casos sobre uso de Pegasus en México". OEA. Consultado el 21 de agosto del 2023, en:

Con esto la CIDH y la RELE reconocen diversos casos de espionaje a ciudadanos mexicanos, los cuales fueron autorizados por SEDENA, al tiempo que reconocen diversas violaciones a derechos, los cuales son:

- Vulnera el derecho a la privacidad.
- Pone en riesgo la integridad de las personas.
- Incrementa la autocensura.
- Desincentiva la labor de la defensa a los derechos humanos.

La CIDH y RELE recuerdan a las autoridades mexicanas que tienen el deber de rechazar cualquier tipo de interferencia o intromisión a la privacidad de las personas y les pide que forma urgente dejen de usar Pegasus. Las autoridades tienen la obligación de respetar las leyes, promover y proteger los derechos por lo tanto es inadmisible que en lugar de protegerlos los violenten y que abusen de su poder para espiar a las y los mexicanos.

SOLUCIÓN

La Mtra. Claudia Gamboa Montejano, Subdirectora de Análisis de Política Interior Servicios de Investigación y Análisis de la H. Cámara de Diputados en el informe sobre ciberseguridad señaló que "**No existe en México una entidad, órgano o institución que esté facultada para atender de manera exclusiva la ciberseguridad del Estado Mexicano**".[58]

Se debe de garantizar que exista Seguridad Digital para las personas usuarias de las TIC, que estas no sean espiadas y que sea una tarea prioritaria en la agenda gubernamental, por lo cual es imprescindible generar un Sistema de protección, que permita a las personas usar plenamente su derecho a las TIC y

https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2023/109.asp#:~:text=Por%20su%20parte%2C%20el%20Estado,ciudadanos%2C%20periodistas%20ni%20servidores%20p%C3%BAblicos

[58] Claudia Gamboa Montejano, Informe, SIAE.

que tenga como eje velar por la protección de los derechos humanos y garantice que estos no sean violentados, y que prohíba el espionaje a las y los mexicanos. Por tanto, la solución es crear el Sistema Nacional de Seguridad Digital mediante la Ley General del Sistema Nacional de Seguridad Digital.

SISTEMA NACIONAL DE SEGURIDAD CIBERNÉTICA

Actualmente, no existe una autoridad que se encargue exclusivamente de establecer una línea de acción con respecto a la Seguridad Digital de las personas, lo cual ha generado los ataques y violaciones a sus derechos a las TIC, entre ellos el espionaje. Por tanto, es urgente crear el Sistema Nacional de Seguridad Digital, el cual permita coordinación entre los diversos órganos gubernamentales con el fin de promover la seguridad y libertad de todas las personas usuarias de internet, garantizando sus derechos en el ciberespacio.

Cabe señalar que **la propuesta fue generada con base en el estudio del Centro de Estudios de Derecho e Investigaciones Parlamentarias** de la H. Cámara de Diputados, con expediente 354/2022, el cual elaboró una comparación con relación a los organismos de cobertura de ciber seguridad en el mundo, especificando su legislación, estructura y objetivo.

El Sistema estará facultado para coordinar y evaluar las acciones relativas a la política pública transversal de Seguridad Digital, así como establecer e implementar criterios y lineamientos en la materia para proteger los derechos digitales de todas las personas en el ciberespacio y proteger a todas las instituciones de la administración pública. Dicho Sistema estará conformado por el Consejo del Sistema Nacional de Seguridad Digital, la Secretaría del Consejo Nacional de Seguridad Digital y las Visitadoras Generales. Cabe aclarar que la Secretaria de la Defensa Nacional no forma parte de este Sistema. En primer lugar, porque la Secretaría no está preparada para cuidar de la

Seguridad Digital de la población, porque espió ilegalmente y por medio de las TIC a personas defensoras de los derechos humanos, periodistas, entre otros, y por qué se requiere de la independencia de acción y legitimidad para tomar acciones difíciles que promuevan la seguridad en el ciberespacio y permitan la protección de la información de la ciudadanía, permitiéndole hacer uso de su derecho a las TIC.[59]

Por lo tanto, y tomando en cuenta que los organismos constitucionalmente autónomos históricamente han sido los aliados de la ciudanía, es fundamental que, si bien exista una autoridad que se encargue exclusivamente de cuidar y velar por la Seguridad Digital de las y los mexicanos, dicha autoridad se encuentre apoyada y respaldada por los organismos constitucionalmente autónomos.

En cuanto al impacto presupuestal éste tendrá que ser cuantificado por el Centro para las Finanzas Públicas de la H. Cámara de Diputados, toda vez que se requiere una infraestructura institucional para dar base al Sistema Nacional de Seguridad Digital. Además de que esto ayudaría a cumplir con las solicitudes de diversas organizaciones internaciones como la Corte Interamericana de Derechos Humanos, al tiempo que ayudaría a cumplir las obligaciones voluntariamente asumidas en diversos constructos internacionales de los que el Estado Mexicano es parte.

Finalmente, se debe de tomar en cuenta que la estructura de este Sistema y la propuesta de Ley toman como base diversas leyes, como la Ley Federal de Transparencia y Acceso a la Información Pública, o la Ley General de Responsabilidades Administrativas, entre otras. Sin embargo, se redujeron los

[59] Loret, C. (2022). “Loret Capítulo 97”. Latin US. Recuperado 9 de octubre de 2023. Disponible en: https://latinus.us/2022/10/06/loret-capitulo-97/

tiempos de análisis y resolución de quejas, debido a que los medios tecnológicos mueven la información de forma mucho más rápida, por lo que las soluciones deben de responder a ello.

FUNDAMENTACIÓN

En el siguiente apartado, se describirá la fundamentación legal que da facultades para crear tal organismo, así como el respeto por los derechos humanos como una de las directrices de la propuesta.

Constitución Política de los Estados Unidos Mexicanos

> **Artículo 1o.** En los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece.
>
> Las normas relativas a los derechos humanos se interpretarán de conformidad con esta Constitución y con los tratados internacionales de la materia favoreciendo en todo tiempo a las personas la protección más amplia.
>
> Todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad.
>
> (…)
>
> **Artículo 6o.** La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los

términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.

Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión.

El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación

(…)

II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.

(…)

Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones

(…)

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

(…)

Las comunicaciones privadas son inviolables. (…)

Artículo 35. Son derechos de la ciudadanía:

I. Votar en las elecciones populares;

(…)

III. Asociarse individual y libremente para tomar parte en forma pacífica en los asuntos políticos del país;

(…)

VII. Iniciar leyes, en los términos y con los requisitos que señalen esta Constitución y la Ley del Congreso. El Instituto Nacional Electoral tendrá las facultades que en esta materia le otorgue la ley;

VIII. Votar en las consultas populares sobre temas de trascendencia nacional o regional, las que se sujetarán a lo siguiente:

(…)

4o. (…) El Instituto promoverá la participación de los ciudadanos en las consultas populares y será la única instancia a cargo de la difusión de las mismas.

(…)

IX. Participar en los procesos de revocación de mandato.[60]

Declaración Universal de los Derechos Humanos

Artículo 2. Toda persona tiene todos los derechos y libertades proclamados en esta Declaración, sin distinción alguna de raza, color, sexo, idioma, religión, opinión política o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición.

Artículo 3. Todo individuo tiene derecho a la vida, a la libertad y a la seguridad de su persona.

(…)

Artículo 12. Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

[60] (Constitución Política de los Estados Unidos Mexicanos, Artículo 1, Artículo 6, Artículo 16, Artículo 35)

(…)

Artículo 19. Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.

(…)

Artículo 21.

1. Toda persona tiene derecho a participar en el gobierno de su país, directamente o por medio de representantes libremente escogidos.

2. Toda persona tiene el derecho de acceso, en condiciones de igualdad, a las funciones públicas de su país.

3. La voluntad del pueblo es la base de la autoridad del poder público; esta voluntad se expresará mediante elecciones auténticas que habrán de celebrarse periódicamente, por sufragio universal e igual y por voto secreto u otro procedimiento equivalente que garantice la libertad del voto.[61]

Pacto Internacional de los Derechos Civiles y Políticos

Artículo 17.

1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

(…)

Artículo 19.

[61] (Declaración Universal de los Derechos Humano, Artículo 2, Artículo 3, Artículo 12, Artículo 19, Artículo 21)

1. Nadie podrá ser molestado a causa de sus opiniones.

2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

Artículo 20.

1. Toda propaganda en favor de la guerra estará prohibida por la ley.

2. Toda apología del odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia estará prohibida por la ley.

(…)

Artículo 25.

Todos los ciudadanos gozarán, sin ninguna de la distinciones mencionadas en el Artículo 2, y sin restricciones indebidas, de los siguientes derechos y oportunidades:

a) Participar en la dirección de los asuntos públicos, directamente o por medio de representantes libremente elegidos;[62]

Resolución A/HRC/20/L.132, Promoción, protección y disfrute de los derechos humanos en Internet

Considerando la importancia fundamental del compromiso estatal con todas las partes interesadas (…) en la promoción y protección en línea de los derechos humanos y las libertades fundamentales,

1. Afirma que los mismos derechos que tienen fuera de línea las personas también deben protegerse en línea, en particular la libertad de expresión, lo que es aplicable independientemente de las fronteras

[62] (Pacto Internacional de los Derechos Civiles y Políticos, Artículo 17, Artículo 19, Artículo 20, Artículo 25)

y por conducto de cualquier medio de su propia elección, de conformidad con el artículo 19 de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos;

2. Reconoce la naturaleza global y abierta de Internet como fuerza motriz de la aceleración de los progresos en la consecución del desarrollo en sus diversas formas, especialmente el logro de los Objetivos de Desarrollo Sostenible;

(…)

5. Exhorta a todos los Estados a cerrar las brechas digitales, especialmente la existente entre los géneros, y a aumentar el uso de la tecnología de la información y las comunicaciones, para promover el pleno disfrute de los derechos humanos para todos, en particular:

a) Fomentando un entorno en línea propicio, seguro y favorable a la participación de todos

(…)

d) Aplicando un enfoque integral basado en los derechos humanos en el suministro y la ampliación del acceso a la tecnología de la información y las comunicaciones, y promoviendo, en consulta con todos los sectores de la sociedad, especialmente las empresas comerciales y los actores de la sociedad civil, políticas y directrices en materia de tecnología de la información y las comunicaciones que otorguen una atención específica a las consideraciones de género;

6. Exhorta a los Estados a garantizar recursos eficaces en los casos de violaciones de los derechos humanos, en particular las relacionadas con Internet, de conformidad con sus obligaciones internacionales;

(…)

9. Condena inequívocamente todos los abusos y violaciones de los derechos humanos, como torturas, ejecuciones extrajudiciales,

desapariciones forzadas y detenciones arbitrarias, así como la expulsión, intimidación y hostigamiento y la violencia de género cometida contra las personas por ejercer sus derechos humanos y libertades fundamentales en Internet, y exhorta a todos los Estados a que garanticen la rendición de cuentas a este respecto;

10. Condena inequívocamente las medidas cuyo objetivo deliberado es impedir u obstaculizar el acceso o la divulgación de información en línea, vulnerando el derecho internacional de los derechos humanos, y exhorta a todos los Estados a que se abstengan de adoptar estas medidas, o cesen de aplicarlas;

11. Destaca la importancia de luchar contra la apología del odio, que constituye una incitación a la discriminación y la violencia en Internet, entre otras cosas fomentando la tolerancia y el diálogo;

12. Exhorta a todos los Estados a que consideren la posibilidad de formular, mediante procesos transparentes e inclusivos con la participación de todos los interesados, y adoptar políticas públicas nacionales relativas a Internet que tengan como objetivo básico el acceso y disfrute universal de los derechos humanos;[63]

Objetivos de Desarrollo Sostenible

Objetivo 16: Promover sociedades justas, pacíficas e inclusivas.

Metas.

16.6 Crear a todos los niveles instituciones eficaces y transparentes que rindan cuentas

16.7 Garantizar la adopción en todos los niveles de decisiones inclusivas, participativas y representativas que respondan a las necesidades.

16.10 Garantizar el acceso público a la información y proteger las

[63] ONU (2016). Resolución A/HRC/32/L.20, "Promoción protección y disfrute de los Derechos Humanos en Internet". ONU. Recuperado el 11 de octubre de 2023. Disponible en: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_32_L20.pdf

libertades fundamentales, de conformidad con las leyes nacionales y los acuerdos internacionales [64]

Carta de Derechos en Internet de la Asociación para el Progreso de las Comunicaciones

2.2 Derecho a estar libre de censura Internet debe estar protegida contra todo intento de silenciar las voces críticas y de censurar contenidos o debates sociales y políticos.

2.3 Derecho a participar en manifestaciones en línea. Las organizaciones, comunidades e individuos deben tener libertad para usar internet con el pro- pósito de organizar manifestaciones y participar en ellas.

3.1 Derecho a tener acceso al conocimiento El acceso al conocimiento y a un fondo comunal y saludable de conocimiento difundidos es la base del desarrollo humano sustentable. Dado que internet permite el intercambio de conocimientos y la creación colaborativa de conocimiento a una escala sin precedentes, debería ser el foco de la comunidad del desarrollo.

3.2 Derecho a la libertad de información Los gobiernos nacionales y loca- les, así como las organizaciones internacionales públicas, deben garantizar la transparencia y la responsabilidad poniendo a disposición la información relevante para la opinión pública. Deben asegurarse de que dicha información se difunda en línea mediante el uso de formatos compatibles y abiertos, y de que la misma sea accesible incluso si se usan computadores más antiguos y conexiones lentas a internet.

[64] ONU (2015). "Objetivos de Desarrollo Sostenible". ONU. Recuperado el 11 de octubre de 2023. Disponible en: https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

3.3 Derecho al acceso a la información financiada por fondos públicos

Toda la información que se produce con el apoyo de fondos públicos, incluso las investigaciones científicas y sociales, deben ser accesibles en forma gratuita para todos y todas.[65]

Carta de Derechos Humanos y Principios para Internet

2. No discriminación en el acceso, uso y gestión de Internet

(…)

3. Libertad y seguridad en Internet

(…)

Todas las medidas de seguridad deben estar en consonancia con el derecho y las normas internacionales y los derechos humanos. Esto significa que las medidas de seguridad serán ilegales en la medida en que restrinjan otro derecho humano (por ejemplo, el derecho a la intimidad o el derecho a la libertad de expresión), excepto en circunstancias excepcionales. Todas las restricciones deben estar definidas de forma precisa. Todas las restricciones deben ser las mínimas necesarias para satisfacer una necesidad real que se reconoce como legal en el derecho internacional, y proporcionadas a esa necesidad. Las restricciones también deben cumplir con criterios adicionales que son específicos de cada derecho. No se permiten restricciones fuera de estos límites estrictos.

En Internet, el derecho a la vida, la libertad y la seguridad incluyen:

a) Protección contra todas las formas de la delincuencia

Todo el mundo debe ser protegido contra toda forma de delito cometido en o mediante Internet, incluyendo el acoso, el ciber-acoso, el tráfico de personas y el uso indebido de datos o de la

[65] Asociación para el Progreso de las Comunicaciones (2006). "Carta de APC sobre los Derechos en Internet". Asociación para el Progreso de las Comunicaciones. Recuperado el 11 de octubre de 2023. Disponible en: https://www.apc.org/sites/default/files/APC_charter_ES_2.pdf

identidad digital.

b) Seguridad de Internet

Toda persona tiene derecho a disfrutar de conexiones seguras y en Internet. Esto incluye protección de servicios y protocolos que podrían poner en peligro el adecuado funcionamiento del internet como virus, códigos maliciosos, y phishing.

5. Libertad de expresión e información en Internet

(…)

La libertad de expresión **es esencial en cualquier sociedad para disfrutar otros derechos humanos** y bienes sociales como la democracia y el desarrollo humano.

En Internet, el derecho a la libertad de opinión y de expresión comprende:

a) La libertad de protesta en línea

(…)

b) La libertad ante la censura

(…)

c) Derecho a la información

(…)

d) La libertad de los medios de comunicación

(…)

e) Libertad frente al discurso de odio

(…)

8. Privacidad en Internet

(…)

Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

En Internet el derecho a la privacidad incluye:

a) La legislación nacional sobre la privacidad

Los Estados deben establecer, implementar y hacer cumplir marcos legales integrales para proteger la privacidad y los datos personales de los ciudadanos. Éstos deben estar en consonancia con las normas internacionales de derechos humanos y la protección de los consumidores, y deben incluir la protección contra violaciones de privacidad por parte del Estado y de las empresas privadas.

b) Políticas de configuración de la privacidad

(…)

c) Normas de confidencialidad e integridad de los sistemas TIC

El derecho a la privacidad debe ser protegido por las normas de confidencialidad e integridad de los sistemas de TIC, proporcionando protección contra el acceso a los sistemas de TIC sin su consentimiento.

d) Protección de la personalidad virtual

(…)

e) Derecho al anonimato y a utilizar cifrado

Toda persona tiene derecho a comunicarse de forma anónima en Internet.

Toda persona tiene derecho a utilizar la tecnología de encriptación para garantizar una comunicación segura, privada y anónima.

f) La libertad ante la vigilancia

Todo el mundo tiene la libertad de comunicarse sin la vigilancia o interceptación arbitraria (incluyendo el seguimiento del comportamiento, de perfiles y del acecho cibernético), o la amenaza de vigilancia o interceptación (…)

g) La libertad ante la difamación

Nadie puede ser objeto de ataques ilegales a su honra y reputación en Internet. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques. Sin embargo, la protección de la reputación no debe utilizarse como excusa para restringir la libertad de expresión legítima.

9. Protección de los datos digitales

(…)

Toda persona tiene derecho a la protección de sus datos personales.

En Internet, el derecho a la protección de datos personales incluye:

a) Protección de datos personales

(…)

b) Obligaciones de los colectores de datos

(…)

c) Normas mínimas sobre el uso de datos personales

(…)

d) Monitorización de la protección de datos

(…)

15. Participación online en los asuntos públicos

En Internet el derecho a participar en el gobierno de su país incluye:

a) Derecho a la igualdad de acceso a los servicios electrónicos

(…)

b) Derecho a participar en el gobierno electrónico

(…) [66]

Carta de Derechos de la Persona, Entorno Digital

4. Derecho a la neutralidad de Internet.

4.5. Las personas usuarias tendrán derecho a acceder a la

[66] ONU (2015). "Carta de Derechos Humanos y Principios para internet". ONU. Recuperado el 11 de octubre de 2023. Disponible en: https://www.palermo.edu/cele/pdf/Carta-de-Derechos-Humanos-y-Principios-para-Internet-en-Espanol.pdf

información y contenidos, así como a distribuirlos, usar y suministrar aplicaciones y servicios y utilizar los equipos terminales de su elección, con independencia de la ubicación del usuario final o del proveedor o de la ubicación, origen o destino de la información, contenido, aplicación o servicio, a través de su servicio de acceso a Internet.

1. Derecho a la identidad.

3. Derecho de la persona a no ser localizada y perfilada.

3.1. La navegación en plataformas digitales debe estar libre de sistemas de geolocalización o de algoritmos cuya función sea la creación de perfiles de las personas usuarias, que tengan por objetivo conocer sus gustos y preferencias.

3.2. Únicamente podrán ser usados sistemas de geolocalización y perfilamiento cuando, por mandamiento legal, sean necesarios para la realización de determinados trámites, sean públicos o privados, siempre y cuando se le informe a las personas usuarias dicha situación y la finalidad de la misma.

5. Derecho a la imagen digital

5.1. Toda persona tiene derecho a decidir sobre el uso de su propia imagen digital, sobre las representaciones o manifestaciones gráficas de la misma y los usos o finalidades que se pretenda dar.[67]

Anexo 12-C Tecnología de la Información y de la Comunicación del T-MEC

El tratado celebrado entre México, Estados Unidos y Canadá (T-MEC), el cual si bien no se enfoca de forma específica al derecho humano al acceso y uso de las TIC, sí lo hace respecto de la implementación de dichas tecnologías de

[67] INAI (2022). "Carta de los Derechos de la Persona, Entorno Digital". INAI. Recuperado el 11 de octubre de 2023. Disponible en: https://www.infocdmx.org.mx/doctos/2022/Carta_DDigitales.pdf

forma homóloga a través de diversas disposiciones que establecen obligaciones a cargo de los Estados parte consistentes en la cooperación e intercambio tecnológico entre ellos.

Artículo 12.C.5: Equipo Terminal

(…)

2. Cada Parte asegurará que sus reglamentos técnicos, normas y procedimientos de evaluación de la conformidad relacionados con la conexión del equipo terminal a las redes públicas de telecomunicaciones, incluidas aquellas medidas relativas al uso de equipos de prueba y medición para los procedimientos de evaluación de la conformidad, sean adoptados o mantenidos solo en la medida necesaria para:

(a) prevenir daño a las redes públicas de telecomunicaciones;

(b) prevenir la degradación de los servicios públicos de telecomunicaciones;

(…)

(e) garantizar la seguridad y el acceso a redes o servicios públicos de telecomunicaciones, incluso para las personas con discapacidad auditiva u otras personas con discapacidad.

3. Cada Parte garantizará que los puntos de terminación de la red para sus redes de telecomunicaciones públicas se establezcan sobre bases razonables y transparentes.[68]

OBJETIVO DE LA INICIATIVA

La presente iniciativa por la que se expide la Ley General del Sistema Nacional de Seguridad Digital tiene como objeto crear el Sistema Nacional de Seguridad Digital.

[68] Gobierno de México (2020) "CAPÍTULO 12 ANEXOS SECTORIALES". Gobierno de México. Recuperado el 11 de octubre de 2023. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/465794/12ESPAnexosSectoriales.pdf

En virtud de lo anteriormente expuesto, se somete a la consideración del Pleno la siguiente iniciativa con proyecto de:

DECRETO

POR EL QUE SE EXPIDE LA LEY GENERAL DEL SISTEMA NACIONAL DE SEGURIDAD DIGITAL.

UNICO. Se expide la Ley General del Sistema Nacional de Seguridad Digital.

LEY GENERAL DEL SISTEMA NACIONAL DE SEGURIDAD DIGITAL
CAPÍTULO I

DISPOSICIONES PRELIMINARES

Artículo 1.- La presente Ley es reglamentaria del párrafo tercero del artículo 6, y del segundo y doceavo del Artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. Es de orden público y de observancia general en todo el territorio nacional.

Artículo 2.- Para los efectos de la presente Ley, se entiende por:

I. Brecha de seguridad: Es cualquier vulnerabilidad en los sistemas de seguridad de un ente que permite que se produzca acceso no autorizado o se comprometa la información confidencial existente en los sistemas informáticos y de telecomunicaciones;
II. Ciberespacio: Un entorno digital global constituido por redes informáticas y de telecomunicaciones, en el que se comunican e interactúan con todo tipo de finalidad las personas, en ejercicio de sus derechos y libertades;

III. Consejo: Consejo del Sistema Nacional de Seguridad Digital;
IV. Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento;
V. Phishing: Es la práctica de engañar, presionar o manipular a las personas para que envíen información o activos a personas indebidas, haciéndose pasar o no por instituciones o personas físicas en las que la víctima confía.
VI. Secretaría: Secretaría del Consejo Nacional de Seguridad Digital;
VII. Sistema Nacional: El Sistema Nacional de Seguridad Digital;
VIII. Ley: Ley General del Sistema Nacional de Seguridad Digital; y
IX. Vigilar: Observar y controlar las actividades del Estado para confirmar que se ajusten a los principios de legalidad, definitividad, imparcialidad y confiabilidad.

Artículo 3.- El objeto de esta Ley es:

I. Reconocer y garantizar los derechos digitales de todas las personas en el ciberespacio;
II. Instaurar el Sistema Nacional de Seguridad Digital;
III. Establecer Estrategia Nacional de Seguridad Digital; y
IV. Proteger los derechos humanos de las personas usuarias de los sistemas de información y comunicaciones cibernéticas.

CAPÍTULO II

DISPOSICIONES GENERALES

Artículo 4.- La Ley se rige por los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos reconocidos en

la Constitución Política de los Estados Unidos Mexicanos y en los tratados internacionales de los que el Estado Mexicano es parte, así como las garantías individuales y sociales.

Artículo 5.- A falta de disposición expresa en esta ley o en los tratados internacionales, se aplicarán:

I. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
II. Ley General de Transparencia y Acceso a la Información Pública;
III. Ley Federal de Protección de Datos Personales en Posesión de los Particulares;
IV. Ley Federal de Transparencia y Acceso a la Información Pública;
V. Ley Federal contra la Delincuencia Organizada;
VI. Ley Federal de Telecomunicaciones y Radiodifusión;
VII. Ley de Seguridad Nacional;
VIII. Código Nacional de Procedimientos Penales; y
IX. Las disposiciones de la legislación común.

Artículo 6.- Para efectos de la presente Ley son derechos digitales, los siguientes:

I. A un entorno en línea propicio y seguro;
II. A la identidad digital;
III. A la no discriminación para el acceso e interacción en los servicios de tecnologías de la información y comunicación, y en los medios digitales;
IV. A la libertad de expresión en los medios digitales;
V. Al acceso a la información en los medios digitales;
VI. A la protección de sus datos en el entorno digital y a la privacidad digital;
VII. A la libertad de reunión y asociación en línea;
VIII. A la defensa de su integridad en medios digitales;

IX. A estar protegido del espionaje por medio de las tecnologías de la información y medios digitales.
X. A estar protegido de localización o perfilado por medios digitales sin consentimiento, salvo por orden de autoridad judicial o por sentencia judicial firme.
XI. A decidir sobre el uso de la imagen digital propia, sobre las representaciones o manifestaciones gráficas de la misma, así como los usos o finalidades que se pretenda dar a esta.
XII. A recibir educación y cultura por medio de las tecnologías de la información y medios digitales; y
XIII. A ser protegido de ataques cibernéticos en cualquier medio digital; y
XIV. Las demás que se establezcan en otras disposiciones normativas.

Artículo 7.- Las y los servidores públicos que incurran en falta administrativa no grave cuyos actos u omisiones cumplan o transgredan las obligaciones siguientes:

I. Proteger los derechos digitales establecidos en esta Ley;
II. Tomar las medidas de seguridad técnicas necesarias para la protección de la Seguridad Digital de sus órganos de gobierno;
III. Notificar al Consejo en caso de brecha de seguridad a su infraestructura de tecnologías de la información y la comunicación;
IV. Cooperar con las autoridades competentes en caso de investigación sobre una brecha de seguridad; y
V. Tomar medidas de seguridad para proteger los órganos públicos y los derechos digitales de las y los usuarios.

La Secretaria dará vista a las autoridades administrativas competentes para que estas determinen las responsabilidades administrativas, que en su caso proceden en los términos de la legislación aplicable.

Artículo 8.- Las medidas de seguridad técnicas que deben tomar todos los órganos de los tres órdenes de gobierno son:

I. Aplicar políticas de contraseñas;
II. Aplicar políticas de uso de dispositivos móviles;
III. Aplicar políticas de acceso a los sistemas;
IV. Formar a las y los empleados en materia de Seguridad Digital;
V. Implementar soluciones de seguridad, como firewalls, antivirus y antispam;
VI. Realizar auditorías de Seguridad Digital periódicas; y
VII. Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.

Artículo 9.- Toda organización que brinde servicios de infraestructura de las tecnologías de la información y comunicación, dentro del territorio nacional, así como de contenido digital, debe aplicar programas de Seguridad Digital para proteger de riesgos la confidencialidad e integridad de la información de datos personales de los usuarios, y no divulgarla, venderla, compartirla o hacer mal uso de ella.

CAPÍTULO III

DISPOSICIONES ORGANICAS

Sección I

Del Sistema Nacional de Seguridad Digital

Artículo 10. -El Sistema Nacional de Seguridad Digital tiene como función coordinar y evaluar las acciones relativas a la política pública transversal de Seguridad Digital, así como establecer e implementar criterios y lineamientos en la materia para proteger los derechos digitales de todas las personas en el

ciberespacio y proteger a todas las instituciones del Estado Mexicano en materia de Seguridad Digital.

Artículo 11.- El Sistema Nacional está conformado por el Consejo, la Secretaría y las personas Visitadoras Generales.

El órgano de decisión del Sistema Nacional es el Consejo y está conformado por:

I. Titular de la Secretaría de Gobernación, quien preside el Consejo;
II. Titular de la Comisión Nacional de Derechos Humanos;
III. Titular de la Fiscalía General de la República;
IV. Titular del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;
V. Titular del Consejo Nacional de Evaluación de la Política de Desarrollo Social;
VI. Titular del Instituto Nacional Electoral;
VII. Titular del Instituto Nacional de Estadística y Geografía;
VIII. Titular del Instituto Federal de Telecomunicaciones;
IX. Titular de la Comisión Federal de Competencia Económica;
X. Titular del Banco de México;
XI. Titular del Instituto para la Protección al Ahorro Bancario; y
XII. Titular de la Comisión Nacional Bancaria y de Valores.

El Consejo funcionará en Pleno que se reunirá de manera ordinaria la primera semana de febrero, la primera semana de mayo, la primera semana de agosto y la primera semana de diciembre, pudiéndose reunir de manera extraordinaria las veces que sea necesario a convocatoria de su Presidencia, la cual integrará y socializará la agenda de los asuntos a tratar mediante la Secretaría del Consejo del Sistema Nacional de Seguridad Digital. El quórum para las reuniones del Consejo se integrará con la mitad más uno de sus integrantes.

Artículo 12.- El Consejo tendrá las siguientes atribuciones:

I. Aprobar acuerdos, los cuales se tomarán por la mayoría de los integrantes presentes del Consejo. Los miembros del Consejo podrán formular propuestas de acuerdos que permitan el mejor funcionamiento del Sistema;

II. Aprobar, aplicar y coordinar la Estrategia Nacional de Seguridad Digital;

III. Emitir los criterios y las bases generales de Seguridad Digital para la protección de información que generen y administren las dependencias y entidades de la administración pública Federal, los cuales serán de observancia obligatoria para estas;

IV. Aprobar el proyecto del Presupuesto Anual de Egresos del Sistema Nacional de Seguridad Digital que le someta su Presidencia, observando los criterios generales de política económica a que se refiere la Ley Federal de Presupuesto y Responsabilidad Hacendaria;

V. Aprobar anualmente la opinión sobre las previsiones y montos que el Presupuesto de Presupuesto de Egresos de la Federación debe destinar en materia de Seguridad Digital;

VI. Coordinar y supervisar a las empresas que proveen servicios digitales a órganos de los tres órdenes de gobierno y órganos constitucionalmente autónomos en materia de Seguridad Digital, en la provisión de los mismos servicios;

VII. Incentivar el desarrollo de la Seguridad Digital por medio de programas que fomenten la confianza y promuevan la información sobre Seguridad Digital;

VIII. Vigilar el cumplimiento de las recomendaciones que se emitan a los órganos de los tres órdenes de gobierno en materia de Seguridad Digital y vigilar el cumplimiento de estas;

IX. Recibir propuestas de los sectores académico, económico y social, tendientes a garantizar la Seguridad Digital y los derechos de las personas usuarias digitales;

X. Convocar a foros públicos a los sectores académico, económico y social en materia de Seguridad Digital;
XI. Participar en el ámbito internacional mediante acuerdos de cooperación con las instituciones pertinentes y los actores relevantes, así como la participación en foros y espacios de aprendizaje y actualización bajo los estándares internacionales; y
XII. Las demás que se establezcan en otras disposiciones normativas y las que sean necesarias para el funcionamiento del Consejo.

Artículo 13.- La Secretaría del Consejo del Sistema Nacional de Seguridad Digital es el órgano administrativo que responderá al Consejo, gozará de autonomía técnica, así como de gestión, contará con los recursos suficientes para sus funciones y tendrá las siguientes facultades:

I. Elaborar cada dos años el anteproyecto de la Estrategia Nacional de Seguridad Digital, que será propuesto al Consejo por medio de su Presidencia para su aprobación;
II. Elaborar anualmente el anteproyecto del Presupuesto Anual de Egresos del Consejo, que será aprobado por la Presidencia y presentado al Consejo por la misma;
III. Remitir al titular del Ejecutivo Federal el proyecto de Presupuesto Anual de Egresos del Consejo aprobado por el Consejo en forma de opinión para su inclusión en el proyecto de Presupuesto de Egresos de la Federación;
IV. Ejercer los recursos financieros asignados en el Presupuesto de Egresos de la Federación;
V. Recibir quejas sobre riesgos o presuntas violaciones a la Seguridad Digital de los órganos de los tres órdenes de gobierno;
VI. Emitir recomendaciones a los órganos de los tres órdenes de gobierno y organismos públicos descentralizados en materia de Seguridad Digital y

vigilar el cumplimiento de estas;

VII. Dictar acuerdos de trámite, que serán obligatorios para las autoridades y servidores públicos para que comparezcan o aporten información o documentación; y

VIII. Las demás que se establezcan en otras disposiciones normativas y las que sean necesarias para el funcionamiento de la Secretaría.

La Secretaria tendrá un lugar en todas las reuniones del Consejo, con derecho al uso de la voz y sin derecho a voto. Tampoco será tomado en cuenta para el conteo del quórum.

Artículo 14.- La persona titular de la Secretaría será nombrada por la Presidencia de la República cada cuatro años, quien la podrá remover libremente. Para ser nombrada deberá cumplir con los siguientes requisitos:

I. Tener ciudadanía mexicana por nacimiento;

II. Pleno goce de sus derechos civiles y políticos;

III. Contar con título profesional de nivel licenciatura debidamente registrado;

IV. Tener mínimo cinco años de experiencia en el ámbito de la Seguridad Digital las áreas correspondientes a su función; y

V. No haber sido sentenciado por delito doloso o inhabilitado como servidor público.

Durante su compromiso, la persona titular de la Secretaría no podrá tener ninguno otro empelo, cargo o comisión.

Artículo 15.- La Secretaría, para el ejercicio de sus facultades, estará integrada por:

I. Dirección Técnica, Gubernamental e Intersectorial;

II. Dirección de Prevención y Atención de Riesgos;

III. Dirección de Cultura de Seguridad Digital y Atención Ciudadana; y

IV. Dirección de Ciberdefensa.

Artículo 16.- Las personas Visitadoras Generales son dependientes del Consejo, se encargan de investigar las quejas, son nombradas por la Secretaría y durarán en el cargo cuatro años. El Consejo tiene libertad para decidir por acuerdo el número de personas Visitadoras Generales.

Artículo 17.- La Secretaría y las personas Visitadoras Generales no podrán ser detenidos ni sujetos a responsabilidad civil, penal o administrativa, por las opiniones y recomendaciones que formulen.

Sección II

De la Estrategia Nacional de Seguridad Digital

Artículo 18.- La Estrategia Nacional de Seguridad Digital es un instrumento de coordinación de la administración pública y de los sectores económico, académico y social, que tiene como objetivo garantizar la Seguridad Digital y los derechos digitales en el marco del máximo respeto a los derechos humanos.

La Secretaría es la encargada de elaborar cada dos años el anteproyecto de la Estrategia Nacional de Seguridad Digital, que debe contener los retos y acciones a corto, mediano y largo plazo. Dicho anteproyecto será propuesto al Consejo por medio de la Presidencia para su aprobación. Una vez aprobada la Estrategia Nacional de Seguridad Digital será publicada en todos los medios de comunicación, así como en el portal digital del Consejo, la primera semana de enero de cada dos años.

Artículo 19.- La Estrategia Nacional de Seguridad Digital tiene como ejes rectores:

I. Garantizar que los sistemas de información y telecomunicaciones que utilice la administración pública en los tres órdenes de gobierno posean un adecuado nivel de Seguridad Digital;
II. Impulsar la Seguridad Digital y resiliencia de los sistemas de información utilizados por el sector económico, académico, social y los operadores de infraestructuras informáticas críticas;
III. Potenciar las capacidades de prevención, investigación, reacción y coordinación frente a las actividades de la delincuencia en el ciberespacio; y
IV. Sensibilizar a la ciudadanía, profesionales, empresas y al sector público de los riesgos existentes en el ciberespacio.

La Presidencia del Consejo es la encargada de coordinar los esfuerzos para el cumplimiento de los ejes antes mencionados.

Artículo 20.- Para garantizar que los sistemas de información y telecomunicaciones que utilizan todas las instituciones, órganos, empresas paraestatales y dependencias de la administración pública de sus tres órdenes de gobierno posean un adecuado nivel de seguridad, se llevaran a cabo las siguientes acciones:

I. Implementar la Estrategia Nacional de Seguridad Digital siendo coordinados por el Consejo;
II. Atender todas las recomendaciones que emita la Secretaría; y
III. Llevar un proceso de mejora continua respecto de la protección de sus sistemas de Seguridad Digital.

Artículo 21.- Las acciones para promover la responsabilidad en el ciberespacio, por parte de las instituciones, órganos, empresas paraestatales y dependencias de la administración pública de sus tres órdenes de gobierno serán las siguientes:

Para sensibilizar a la ciudadanía, profesionales, empresas y sector público de los tres órdenes de gobierno, sobre los riesgos del ciberespacio, se llevarán a cabo las siguientes acciones:

I. Asumir la responsabilidad de las empresas públicas y privadas de la seguridad de sus sistemas, la protección de la información de sus clientes, proveedores y la confiabilidad de los servicios que prestan;

II. Promover una cultura de la Seguridad Digital que proporcione a todos los sectores la conciencia y la confianza necesarias para maximizar los beneficios de la sociedad de la información y reducir al mínimo su exposición a los riesgos del ciberespacio mediante la adopción de medidas razonables que garanticen la protección de sus Datos, así como la conexión segura de sus sistemas y equipos; y

III. Fomentar que todas las personas usuarias de internet tengan acceso a información respecto de los riesgos que entraña el ciberespacio, así como el conocimiento de las herramientas para la protección de su información, sistemas y servicios.

CAPÍTULO IV

DISPOSICIONES PROCEDIMENTALES

Sección I

De la Queja

Artículo 22.- Cualquier persona física o moral podrá quejarse ante la Secretaría por violaciones a los derechos digitales.

No se admitirán quejas presentadas de forma anónima.

Las quejas serán procesadas por la Secretaría, la cual hará las recomendaciones pertinentes al organismo gubernamental o privado que haya violentado los derechos digitales.

Artículo 23.- El procedimiento de la queja se integra por las siguientes etapas:

I. Presentación de la queja ante la Secretaría;
II. Admisión y apertura del expediente.
Independientemente del modo en que se presente la queja, todos los expedientes deberán integrarse electrónicamente;
III. Solicitud por parte de la Secretaría de un informe de la autoridad señalada como responsable;
IV. Etapa de investigación efectuada por la Secretaría a través de las personas Visitadoras Generales; y
V. Resolución de la queja. De encontrarse que se efectuaron violaciones se levantara una recomendación a las autoridades responsables.

Artículo 24.- La queja deberá cumplir, al menos, los siguientes requisitos:

I. El nombre de la autoridad responsable de las violaciones. En el supuesto de que el quejoso no pueda identificar a las autoridades responsables cuyos actos u omisiones consideren haber violentado sus derechos digitales, la queja será admitida, bajo la condición de que se logre dicha identificación en la investigación posterior de los hechos;
II. La descripción clara y precisa de los hechos y las violaciones a sus derechos digitales;
III. Los medios de prueba que el quejoso estime necesarios para respaldar su queja;
IV. El domicilio o la dirección de correo electrónico del quejoso para recibir notificaciones; y

V. El nombre del quejoso.

Artículo 25.- La denuncia podrá presentarse de la forma siguiente:

I. Por medio electrónico, de forma escrita:
   a. A través del portal digital del Consejo, presentándose en el apartado de queja; y
II. Por escrito presentado físicamente, ante la Oficialía de Partes Común.

Artículo 26.- La Secretaría por medio de la Oficialía de Partes Común deberá poner a disposición de las personas reclamantes formularios que faciliten el trámite y en todos los casos ejercerá la suplencia en la deficiencia de la queja, para lo cual Secretaría pondrá a un asesor jurídico que orientará y apoyará a las personas comparecientes sobre el contenido de su queja.
Una vez recibida la queja se emitirá acuse de recibo físico o electrónico, en el que se conste la fecha y hora de presentación.

Artículo 27.- La Secretaría resolverá sobre la admisión de la denuncia, dentro de las veinticuatro horas siguientes a su recepción.

Artículo 28.- Una vez admitida la queja, la Secretaría podrá prevenir al quejoso, para que en el plazo de veinticuatro horas subsane lo siguiente:

I. En su caso, exhiba ante el Consejo los documentos con los que acredite la personalidad del representante de una persona física o moral, en caso de aplicar; o
II. Aclare o precise alguno de los requisitos o motivos de la queja.

En el caso de que no se desahogue la prevención en el periodo establecido para tal efecto en este artículo, deberá desecharse la queja, dejando a salvo los derechos del quejoso para volver a presentar la misma.

Artículo 29. La Secretaría podrá determinar la improcedencia de la queja cuando:

I. Esta hubiera sido objeto de una queja anterior que ya fue resuelta; o
II. Si la queja no versa sobre presuntas violaciones a los derechos digitales.

La Secretaría dictará un acuerdo de desechamiento de la queja y, en su caso, dejará a salvo los derechos del promovente para que los haga valer por la vía y forma correspondientes.

Artículo 30.- Una vez admitida la queja, la Secretaría deberá hacer del conocimiento de las autoridades señaladas como responsables de la queja puesta en su contra, utilizando en casos de urgencia cualquier medio de comunicación electrónica. En la misma comunicación se solicitará a dichas autoridades que rindan un informe sobre los actos, omisiones o resoluciones que se les atribuyan en la queja, el cual deberán presentar dentro de un plazo máximo de quince días hábiles y por los medios que sean convenientes, de acuerdo con el caso.

Artículo 31.- Para la etapa de investigación las personas Visitadoras Generales tendrán las siguientes facultades:

I. Pedir a las autoridades a los que se imputen violaciones de Seguridad Digital, la presentación de informes o documentación adicionales ya sea escritos o en forma digital;
II. Solicitar de otras autoridades, servidores públicos o particulares todo género de documentos e informes en formato escrito o digital;
III. Practicar visitas e inspecciones, ya sea personalmente o por medio del personal técnico o profesional bajo su dirección en términos de ley;
IV. Citar a las personas que deban comparecer como peritos o testigos; y
V. Efectuar todas las demás acciones que conforme a derecho juzgue convenientes para el mejor conocimiento del asunto.

Artículo 32.- Las pruebas que se presenten, tanto por las personas interesadas como por las autoridades responsables, o bien que la Secretaría requiera y recabe de oficio, serán valoradas en su conjunto por la persona Visitadora General, de acuerdo con los principios de la lógica y de la experiencia, y en su caso, de la legalidad, a fin de que puedan producir convicción sobre los hechos en materia de la queja.

Artículo 33.- Concluida la investigación, la persona Visitadora General analizará los hechos, los argumentos y las pruebas, a fin de determinar si las autoridades han violado o no los derechos digitales de las personas afectadas y formulará:

a) Proyecto de Acuerdo de no responsabilidad; o
b) Proyecto de Recomendación, especificando las medidas recomendadas para la efectiva restitución de las personas afectadas en sus derechos digitales y, si procede en su caso, para la reparación de los daños y perjuicios que se hubiesen ocasionado.

Artículo 34.- La Secretaría dictará la resolución del expediente la cual debe estar fundada y motivada. Dependiendo el caso dictará:

a) Acuerdo de no responsabilidad; o
b) Recomendación.

La Secretaría deberá notificar la resolución a la persona quejosa y a las autoridades responsables dentro de las veinticuatro horas siguientes a su emisión, también dará vista las autoridades competentes para que estas determinen las responsabilidades penales y administrativas, que en su caso proceden en los términos de la legislación aplicable.

Las resoluciones que emita la Secretaría son definitivas e inatacables.

Sección II

De las Recomendaciones

Artículo 35.- Las Recomendaciones son inatacables y deben ser publicadas en el portal digital del Consejo y en todos los medios de comunicación a su alcance.

Artículo 36.- Una vez recibida, la autoridad responsable informará dentro de los quince días hábiles siguientes a su notificación si acepta dicha Recomendación. Entregará, en su caso, en otros siete días adicionales, las pruebas correspondientes de que ha cumplido con la Recomendación. Dicho plazo podrá ser ampliado cuando la naturaleza de la Recomendación así lo amerite.

Artículo 37.- Cuando las Recomendaciones emitidas no sean aceptadas, la autoridad responsable deberá en plazo de tres días hábiles, presentar un escrito de forma física y virtual a la Secretaría. En dicho escrito debe fundar, motivar y hacer pública su negativa a la recomendación.

Artículo 38.- Las Recomendaciones y los Acuerdos de no responsabilidad se referirán a casos concretos. Las autoridades no podrán aplicarlos a otros casos por analogía o mayoría de razón.

Artículo 39.- Las y los integrantes del Consejo vigilarán el cumplimiento de las Recomendaciones que se emitan a los órganos de los tres órdenes de gobierno en materia de Seguridad Digital.
En caso de que incumplan, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales deberá publicar un comunicado en el que especifique la institución que no cumplió con las recomendaciones y un informe en el que especifique las medidas o acciones que incumplió,

incluyendo los datos de las autoridades responsables. Dichos escritos también serán publicados en el portal digital del Consejo.

Artículo 40.- Cualquier intervención a las comunicaciones se efectuará en términos del Código Nacional de Procedimientos Penales, de la Ley de Seguridad Nacional y de la Ley Federal contra la Delincuencia Organizada. Una vez concluido el proceso judicial por el que se efectuó la intervención, las autoridades de procuración y participación de justicia están obligadas a hacer público un informe en el que especifique la persona que tuvo intervenidas sus comunicaciones, motivo y periodo en el que se llevo a cabo la intervención. Dicho informe también será publicado en el portal digital del Consejo.

TRANSITORIOS

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

SEGUNDO. La designación de la persona titular de la Secretaría deberá realizarse dentro de los 30 días siguientes a la entrada en vigor del presente decreto.

TERCERO. La designación del Consejo deberá realizarse dentro de los 60 días siguientes a la publicación de la Ley.

CUARTO. La Secretaría someterá a la aprobación del Consejo el proyecto del Estatuto Orgánico dentro de los 120 días siguientes a su nombramiento.

QUINTO. Una vez designada la persona titular de la Secretaría, la Secretaría de Hacienda y Crédito Público proveerá, con sujeción a las previsiones que para tal efecto estén contenidas en el Presupuesto de Egresos de la Federación, los recursos necesarios para iniciar las actividades del Instituto.

ATENTAMENTE

Dip. Salvador Caro Cabrera.
Grupo Parlamentario de Movimiento Ciudadano.
Cámara de Diputados.
LXV Legislatura
Dado en el Palacio Legislativo de San Lázaro, a 05 de diciembre de 2023.