INICIATIVA CON PROYECTO DE DECRETO QUE EXPIDE LA LEY GENERAL DEL SISTEMA NACIONAL DE SEGURIDAD DIGITAL.

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 buscando el pleno desarrollo de las personas usuarias en un ciberespacio seguro. Es fundamental que dicho sistema 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 TIC se refiere a aquellos recursos, herramientas y programas utilizados para procesar, administrar y compartir la información mediante computadoras, teléfonos móviles, televisores, reproductores portátiles de audio y video o consolas de juego. Hoy en día, su papel en la sociedad es muy importante, toda vez que de ellas dependen servicios como: correo electrónico, búsqueda de información, banca online, descarga de música y

video, comercio electrónico, etc.[1] 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.[2]

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 televisivos. Asimismo, difundir cualquier contenido por los medios mencionados, interactuar y formar parte integral de la

[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 2022. Disponible en: https://www.gob.mx/profeco/documentos/tecnologias-de-la-informacion-y-comunicacion-que-la-edad-no-sea-un-obstaculo?state=published

[2] (Constitución Política de los Estados Unidos Mexicanos, art. 6).

> Sociedad de la Información, sin importar condiciones sociales o económicas.[3]

A dichas **prerrogativas inherentes a los usuarios del mundo digital se les ha clasificado como Derechos de Cuarta Generación.[4] Estos revisten tanto derechos objetivos (degradación de derechos humanos por la evolución de la tecnología), como subjetivos (protección a los ciudadanos del mundo digital, comúnmente conocidos como cibernautas**).[5]

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.[6]

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

---

[3] CNDH. "DERECHO DE ACCESO Y USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN". CNDH (2015). Recuperado el 11 de octubre de 2022. Disponible en: http://appweb.cndh.org.mx/biblioteca/archivos/pdfs/foll_DerAccesoUsoTIC.pdf

[4] CESOP (2017). "Los derechos humanos de cuarta generación. Un acercamiento". Cámara de Diputados. Recuperado el 22 de octubre de 2022. Disponible en: http://www5.diputados.gob.mx/index.php/esl/content/download/91158/457163/file/CESOP-IL-72-14-DerHumaCuartaGeneracion-310817.pdf

[5] *Ibid.*

[6] *Ibid.*

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,[7] 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,[8] 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*.[9] 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, menciona que **se debe lograr que el internet funcione y evolucione de manera que sean cumplidos los derechos humanos.**[10]

---

[7] Barlow, JP (1996). "Declaración de Independencia del Ciberespacio" Uhu.es. Recuperado el 22 de octubre de 2022. Disponible en: http://www.uhu.es/ramon.correa/nn_tt_edusocial/documentos/docs/declaracion_independencia.pdf

[8] APC (2006). "Carta de Derechos en Internet de la Asociación para el Progreso de las Comunicaciones". Recuperado el 22 de octubre de 2022. Disponible en: https://www.apc.org/sites/default/files/APC_charter_ES_2.pdf

[9] 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 2022. Disponible en: https://derechoseninternet.com/docs/IRPC_Carta_Derechos_Humanos_Internet.pdf

[10] *Ibidem*.

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.[11]

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*,[12] 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 consecución del desarrollo en sus diversas formas, especialmente

[11] (Constitución Política de los Estados Unidos Mexicanos, art. 6, primer y segundo párrafos)

[12] 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 2022. Disponible en: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_38_L10.pdf

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***.[13] En ella, reafirmó lo dicho en la anterior resolución y **condenó las violaciones en contra de los derechos humanos de las personas al limitar su participación en las tecnologías**:

[13] 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 2022. Disponible en: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_32_L20.pdf

> 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**;[14]

De este modo, es pertinente mencionar que el Estado Mexicano es Estado Miembro de la ONU, aunado a que a lo largo de los años ha pugnado para garantizar los derechos humanos. Por lo que se puede cuestionar **cómo poner en marcha las solicitudes de la ONU, respecto de fomentar un entorno en línea propicio, seguro y favorable, así como garantizar la protección de los derechos humanos dentro y fuera de línea, cuando no existe ninguna norma mexicana que se encargue de esto.**

[14] *Ibid.*

Aunado a lo anterior, 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

La seguridad digital es uno de los desafíos clave para todos los Estados, ya que han crecido las TIC y la dependencia que tienen todos los países 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 previas fallidas

Reconociendo la importancia de la tecnología, el gobierno mexicano en turno 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.[15]

De este modo, señaló objetivos específicos y líneas de acción en materia de seguridad:

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	• Promover una política general de seguridad de la información que procure la preservación de la confidencialidad,

[15]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 2022. Disponible en: https://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021#gsc.tab=0

servicios tecnológicos institucionales y gubernamentales.	disponibilidad e integridad de la información resguardada por las Instituciones. • Promover la implementación de un Protocolo Homologado para la Gestión de Incidentes 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".[16] 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.[17]

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.[18]

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

[17] 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 2022. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/735044/Protocolo_Nacional_Homologado_de_Gestion_de_Incidentes_Ciberneticos.pdf

[18] 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

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.

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**.[19] **Se sustrajeron por lo menos 300 millones de pesos** de cinco instituciones bancarias.[20] 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**.[21] De este modo, en

Federación. Consultado el 24 de octubre del 2022. Disponible en: https://dof.gob.mx/nota_detalle.php?codigo=5628885&fecha=06/09/2021#gsc.tab=0

[19] 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 2022. Disponible en: https://www.banxico.org.mx/publicaciones-y-prensa/informes-trimestrales/recuadros/%7B86A498AE-5F8A-57CE-2C11-B5059AB9EB20%7D.pdf

[20] Forbes (2018). "Hackers roban al menos 300 mdp con ataque a bancos en México". Forbes México. Recuperado 10 de octubre de 2022. Disponible en: https://www.forbes.com.mx/hackers-roban-de-300-a-400-mdp-con-ataque-a-sistema-de-bancos/

[21] Riquelme, R. (2019). "El rescate por el hackeo a Pemex es el segundo mayor por ransomware". El Economista. Recuperado 10 de octubre de 2022. Disponible 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.[22]

- En 2020, la **Secretaría de Economía**, sufrió un ataque cibernético que impactó a los servidores[23] y afectó los trámites para la exportación.[24]

- En 2020 la **Secretaría de Trabajo y Previsión Social** fue *hackeada,* afectando a la plataforma de legitimación de contratos colectivos.[25]

- 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.[26]

- En 2021, la **Lotería Nacional y la Plataforma Nacional de Transparencia** sufrieron ciberataques, por medio del método conocido como *ramsonware* (un *software* con el que los cibercriminales secuestran

https://www.eleconomista.com.mx/empresas/El-rescate-por-el-hackeo-a-Pemex-es-el-segundo-mayor-por-ransomware-20191115-0035.html

[22] Badillo, D. (2021). "Flotan" en internet 180,000 archivos de Pemex sustraídos por hackers". El Economista. Recuperado 10 de octubre de 2022. Disponible en: https://www.eleconomista.com.mx/empresas/Flota-en-internet-informacion-sensible-de-Pemex-sustraida-por-hackers-20210216-0103.html

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

[24] 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 2022. Disponible en: https://www.eluniversal.com.mx/cartera/por-hackeo-economia-tramites-de-azucar-jitomate-y-llantas-seran-por-correo

[25] Excélsior (2020). "Incidente afecta la Secretaría del Trabajo". Excélsior. Recuperado 10 de octubre de 2022. Disponible en: https://www.excelsior.com.mx/nacional/incidente-afecta-la-secretaria-del-trabajo/1368850

[26] Armenta, MH (2020). "Hackean la página de la Condusef y la dejan fuera de servicio". Forbes México. Recuperado 10 de octubre de 2022. Disponible en: https://www.forbes.com.mx/hackean-la-pagina-de-internet-de-la-condusef/

datos a través de un cifrado de archivos que se libera pagando un rescate).[27]

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[28] 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**,[29] **transcripciones de intervenciones telefónicas, directorios y reportes sobre seguimiento a personas, como el Embajador de Estados Unidos en México**,[30] y el despliegue detallado de las fuerzas

[27] *Ibid*.
[28] 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 2022. Disponible en: https://www.nytimes.com/es/2022/10/06/espanol/mexico-sedena-guacamaya-hackeo.html
[29] BBC News Mundo. (2022). "Guacamaya Leaks: 5 revelaciones del hackeo masivo que sufrió el ejército de México". Recuperado 8 de octubre de 2022. Disponible en: https://www.bbc.com/mundo/noticias-america-latina-63167331
[30] Loret, C. (2022). "Loret Capítulo 96". Latin US. Recuperado 8 de octubre de 2022. Disponible en: https://latinus.us/2022/09/29/loret-capitulo-96/

armadas.[31] **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*.**[32]

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".[33] 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".[34]

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.**[35] Mientras que Adolfo Grego, especialista en investigación forense refiere que los hackers necesitaron por lo menos de tres días para copiar la información de la SEDENA, lo cual supone

[31] *Ibidem.*

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

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

[34] *Ibid.*

[35] *Ibid.*

inacción por parte de las autoridades.[36]

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*.[37]

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.[38] 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

[36] *Ibid.*
[37] 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 2022. Disponible en: https://www.forbes.com.mx/sedena-gasta-mas-de-340-mdp-en-ciberseguridad-y-aun-asi-la-hackean/
[38] (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.[39]

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.[40] Es inadmisible que esto siga ocurriendo.[41]

[39] Hackeo: Desde 2021 ASF reprobó a Sedena por deficiencias graves en ciberseguridad. Recuperado 9 de octubre de 2022, de https://m-x.com.mx/al-dia/hackeo-desde-2021-asf-reprobo-a-sedena-por-deficiencias-graves-en-ciberseguridad

[40] 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

[41] 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

SOLUCIÓN

Se debe de garantizar que exista seguridad digital para las personas usuarias de las TIC 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 que vele por sus derechos humanos.

Así, vale mencionar que 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 señalo.

> No existe en México una entidad, órgano o institución que esté facultada para atender de manera exclusiva la ciberseguridad del Estado Mexicano.[42]

Por tanto, la solución es crear el Sistema Nacional de Seguridad Digital mediante la Ley 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. 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.

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

[42] Claudia Gamboa Montejano, Informe, SIAE.

relación a los organismos de cobertura de ciber seguridad en el mundo, especificando su legislación, estructura y objetivo.

El Sistema estará facultado para:

- Establecer los instrumentos en materia de seguridad digital.
- Expedir políticas en materia de suministro, intercambio, sistematización y actualización de la información en materia de seguridad digital que generen los órganos de los tres niveles gobierno.
- Expedir recomendaciones a los órganos de los tres niveles de gobierno en materia de ciberseguridad, así como vigilar que estos cumplan las recomendaciones.

Dicho sistema no podría ser dependiente ni venir de la Secretaría de la Defensa Nacional. En primer lugar, porque la Secretaría no está preparada para cuidar de la seguridad digital de la población, y 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.[43]

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.

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

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.

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.

(…)

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.

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.

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;

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 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;

Resolución A/HRC/20/L.132

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;[44]

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

[44] ONU (2016). Resolución A/HRC/32/L.20, "Promoción protección y disfrute de los Derechos Humanos en Internet". Recuperado el 11 de octubre de 2022. Disponible en: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_32_L20.pdf

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.

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.

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 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

(...)

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 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.

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.

Con la intención de una mejor ilustración de la propuesta, se presenta a continuación.

LEY GENERAL DEL SISTEMA NACIONAL DE SEGURIDAD DIGITAL

TÍTULO PRIMERO

Disposiciones Preliminares

Artículo 1.- La presente Ley es reglamentaria del párrafo tercero del Artículo 6 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 entenderá por:

I. Ciberespacio: Un entorno digital global constituido por redes informáticas y de telecomunicaciones, en el que se comunican e interactúan las personas y permite el ejercicio de sus derechos y libertades como lo hacen en el mundo físico.
II. Consejo: Consejo de Secretariado Técnico,
III. Secretaría: Secretaría Técnica de Seguridad Digital;
IV. Sistema: El Sistema Nacional de Seguridad Digital; y
V. Ley: Ley General del Sistema Nacional de Seguridad Digital

Artículo 3.- La presente ley tiene como fin preservar la integridad y disponibilidad en el ciberespacio y unir a las diferentes instancias y órdenes de gobierno, salvaguardando los derechos humanos de las personas usuarias de los sistemas de información y comunicaciones cibernéticas.

Artículo 4.- La Seguridad Digital se rige por los principios de legalidad, responsabilidad 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.

Todas las autoridades competentes en materia de Seguridad Digital deberán apegarse a los principios de certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad.

TITULO SEGUNDO
Del Sistema Nacional de Seguridad Digital
CAPITULO I
De la organización del Sistema Nacional de Seguridad Digital

Artículo 5.- El Sistema Nacional de Seguridad Digital está constituido por un Consejo de Secretariado Técnico, el cual está conformado por:

I. Secretaría Técnica de Seguridad Digital;
II. Titular de la Secretaría de Gobernación;
I. Titular de la Comisión Nacional de Derechos Humanos;
II. Titular de la Fiscalía General de la Republica;
III. Titular Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;
IV. Titular del Consejo Nacional de Evaluación de la Política de Desarrollo Social;

V. Titular del Instituto Nacional Electoral;
VI. Titular del Instituto Nacional de Estadística y Geografía;
VII. Titular del Instituto Federal de Telecomunicaciones;
VIII. Titular de la Comisión Federal de Competencia Económica;
IX. Titular del del Banco de México;
X. Titular del Instituto para la Protección al Ahorro Bancario; y
XI. Titular de la Comisión Nacional Bancaria y de Valores.

CAPITULO II
Del Consejo de Secretariado Técnico.

Artículo 6- El Consejo de Secretariado Técnico tendrá las siguientes atribuciones:

I. Vigilar el cumplimiento de las recomendaciones que se emitan a los órganos de los tres niveles de gobierno en materia de seguridad digital. En caso de que estas incumplan el Consejo 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.
II. Podrá llevar a cabo grupos de trabajo con la sociedad civil y las cámaras empresariales, en las cuales participe el Instituto, para que escuchen las ideas y propuestas que tienen. Se tienen que hacer cuando sean solicitadas, y contar con toda la publicidad.
III. Recibir quejas de presuntas violaciones a la seguridad digital.

CAPÍTULO III
De la Secretaría Ejecutivo de Seguridad Digital.

Artículo 7.- La Secretaría Técnica de Seguridad Digital es el órgano operativo del Sistema y gozará de autonomía técnica, de gestión y contará con los recursos suficientes para sus funciones que anualmente se le asignarían en el Presupuesto de Egresos de la Federación.

La persona titular será nombrada y removida libremente por la Presidencia de la República cada cuatro años y 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 reconocida capacidad y probidad, así como contar con cinco años de experiencia en las áreas correspondientes a su función; y
V. No haber sido sentenciada por delito doloso o inhabilitada como servidora pública.

La Secretaría Técnica de Seguridad Digital tendrá la representación legal del organismo. Durante su encargo, no podrá tener ninguno otro empelo, cargo o comisión.

Artículo 8.- La coordinación del Sistema estará a cargo de la Secretaría Técnica, correspondiéndole a ésta:

I. Representar legalmente al Consejo con facultades generales y especiales para actos de administración, dominio, pleitos y cobranzas, incluso las que requieran clausula especial conforme a la Ley aplicable;
II. Otorgar y revocar poderes a nombre del Consejo para actos de dominio, pleitos y cobranzas y para ser representado ante cualquier autoridad administrativa o judicial, ante los tribunales laborales o ante

particulares. Tratándose de actos de dominio sobre inmuebles destinados al Consejo o para otorgar poderes para dichos efectos, se requiere la autorización del órgano interno de control;

III. Dirigir y administrar los recursos humanos, financieros y materiales del Consejo;

IV. Participar en representación del Consejo en foros, reuniones, negociaciones, eventos, convenciones y congresos que se lleven a cabo con organismo nacionales, internacionales, gobiernos extranjeros, cuando se refieran a temas en el ámbito de competencia del Instituto, de conformidad con lo establecidos en la presente Ley o designar representantes para tales efectos;

V. Ejecutar y dar seguimiento a los acuerdos y resoluciones del Consejo del Secretariado Técnico;

VI. Impulsar mejoras para los instrumentos de información del Sistema;

VII. Expedir recomendaciones y resoluciones a los órganos de los tres niveles de gobierno en materia de Seguridad Digital;

VIII. Promover la efectiva coordinación de las instancias y dar seguimiento de las estrategias y acciones que para tal efecto se establezcan;

IX. Elaborar la Estrategia Nacional de Seguridad Digital, el Plan Anual de Trabajo y el Informe Anual de Labores, en colaboración con los titulares de los diferentes organismos;

X. Establecer en la Estrategia de Nacional de Seguridad Digital los instrumentos, programas y políticas públicas integrales, sistemáticas, continuas y evaluables, tendientes a cumplir los objetivos y fines de la Seguridad Digital;

XI. Presentará un Informe Anual de actividades y podrá ser llamada a asistir a reuniones de trabajo, conforme a los principios de transparencia y rendición de cuentas;

XII. Vigilar que los sujetos obligados en el ámbito federal cumplan con las

obligaciones de transparencia y poner a disposición del público, así como mantenerla actualizada, en los respectivos medios electrónicos, de acuerdo con sus facultades, atribuciones, funciones u objeto social, según corresponda; y

XIII. Las demás que se establezcan en otras disposiciones normativas y las que sean necesarias para el funcionamiento del Consejo de Secretariado Técnico y del Sistema.

CAPÍTULO IV
De las atribuciones de los integrantes del Consejo de Secretariado Técnico.

Artículo 10.- Como parte del Consejo de Secretariado Técnico, el Instituto Nacional de Estadística y Geografía, el Instituto Nacional Electoral, el Instituto Federal de Telecomunicaciones y el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, trabajarán en coordinación para:

I. Expedir recomendaciones a los órganos de los tres niveles de gobierno en materia de Seguridad Digital cuando ésta verse sobre las contramedidas de inteligencia técnica, para lo cual deberá llevar a cabo visitas de revisión y verificación a las autoridades correspondientes en términos de la Ley Federal del Procedimiento Administrativo. En caso de incumplimiento podrá emitir recomendaciones;

II. Aplicar la Estrategia Nacional de Seguridad Digital cuando ésta verse sobre la organización de la coordinación e interacción interdepartamental y el ejercicio de funciones especiales y de control de la Seguridad Digital del Estado Mexicano;

III. Coordinar y colaborar con la Fiscalía General de la República y de los Estados, para tener información veraz y oportuna sobre todos los procedimientos relacionados con los ciberdelitos; y

IV. Las demás que se establezcan en otras disposiciones normativas y las que sean necesarias para el funcionamiento del Consejo de Secretariado Técnico y del Sistema.

Artículo 11.- Como parte del Consejo de Secretariado Técnico, la Comisión Nacional de Derechos Humanos y el Consejo Nacional de Evaluación de la Política de Desarrollo Social, tendrán las siguientes facultades y obligaciones:

I. Sugerir programas que promuevan y fomenten la confianza en el ámbito digital a través de la formación en materia de Seguridad Digital;
II. Desarrollar la Seguridad Digital y la confianza digital de la ciudadanía, las academias y las redes de investigación;
III. Convocar a persona físicas o morales, a organizaciones de la sociedad civil y a instituciones educativas a mesas de diálogo, foros o grupos de trabajo, los cuales deberán ser públicos, en los que expongan conocimientos y experiencias para el cumplimiento de la seguridad cibernética; y
IV. Las demás que se establezcan en otras disposiciones normativas y las que sean necesarias para el funcionamiento del Consejo de Secretariado Técnico y del Sistema.

Artículo 12.- Como parte del Consejo de Secretariado Técnico, la Comisión Federal de Competencia Económica, el Banco de México, el Instituto para la Protección al Ahorro Bancario y la Comisión Nacional Bancaria y de Valores tendrán las siguientes facultades y obligaciones:

I. Trabajar por la seguridad de las y los usuarios en los diversos sectores económicos, privilegiando sus libertades y la protección de sus derechos humanos, con base en la Estrategia Nacional de Seguridad Digital, a la cual deberán de aportar en este tema particular;
II. Convocar a los diversos actores del sector económico a mesas de

diálogo, foros o grupos de trabajo, los cuales deberán ser públicos, en los que expongan conocimientos y experiencias para el cumplimiento de la seguridad cibernética; y

III. Las demás que se establezcan en otras disposiciones normativas y las que sean necesarias para el funcionamiento del Consejo de Secretariado Técnico y del Sistema.

TÍTULO TERCERO
Disposiciones Comunes a los integrantes del Sistema de Seguridad Digital
CAPÍTULO I
De las obligaciones y sanciones

Artículo 13.- Con el objeto de garantizar el cumplimiento de los principios constitucionales de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos, las personas integrantes del Sistema de Seguridad Digital se sujetarán a las siguientes obligaciones:

I. Conducirse siempre con dedicación y disciplina, así como con apego al orden jurídico y respeto a las garantías individuales y derechos humanos reconocidos en la Constitución Política de los Estados Unidos Mexicanos;

II. Cumplir sus funciones con absoluta imparcialidad y sin discriminación alguna;

III. Observar un trato respetuoso con todas las personas, debiendo abstenerse de todo acto arbitrario y de limitar indebidamente las acciones o manifestaciones que en ejercicio de sus derechos constitucionales y con carácter pacífico realice la población;

IV. Desempeñar sus funciones sin solicitar ni aceptar compensaciones, pagos o gratificaciones distintas a las previstas legalmente. En particular

se opondrán a cualquier acto de corrupción y, en caso de tener conocimiento de alguno, deberán denunciarlo; y

V. Las demás que establezcan las disposiciones legales aplicables.

TITULO CUARTO
Capítulo I
De la Estrategia Nacional de Seguridad Digital.
Sección I
Disposiciones Generales.

Artículo 14.- La Estrategia Nacional de Seguridad Digital es un instrumento por medio del cual se llevará a cabo la estrategia a seguir en el periodo establecido, reconociendo los retos y acciones a corto, mediano y largo plazo mediante la coordinación con las autoridades federales, estatales y locales, el sector social y el sector privado en materia de Seguridad Digital. Se elaborará y aprobará cada dos años. Tendrá que ser presentada y publicada en todos los medios de comunicación, así como en el portal del Consejo de Secretariado Técnico, la primera semana de enero de cada dos años.

Artículo 15.- La Estrategia Nacional de Seguridad Digital tendrá como propósito lograr el uso seguro del ciberespacio, impulsando una visión integradora cuya aplicación ayude a garantizar la Seguridad Digital y progreso por medio de la adecuada coordinación de las instituciones, organismos y dependencias de la administración pública federal, impulsando el máximo respeto a los derechos humanos.

Artículo 16.- La Estrategia Nacional de Seguridad Digital tendrá como ejes:

I. Garantizar que los sistemas de información y telecomunicaciones que utilice la administración pública posean un adecuado nivel de ciberseguridad.
II. Impulsar la ciberseguridad y resiliencia de los sistemas de información utilizados por el sector empresarial en general y los operadores de infraestructuras informáticas críticas.
III. Potenciar las capacidades de prevención, detección, reacción, defensa, análisis, recuperación, investigación y coordinación frente a las actividades de la delincuencia en el ciberespacio.
IV. Sensibilizar a la ciudadanía, profesionales, empresas y administraciones publicas de todos los riesgos derivados del ciberespacio.

La Secretaría de Gobernación será la encargada de coordinar los esfuerzos para lograr los ejes.

Artículo 17.- Para lograr garantizar que los sistemas de información y telecomunicaciones que utilizan todas las instituciones, órganos, empresas paraestatales y dependencias de la administración pública federal posean un adecuado nivel de seguridad, se llevaran a cabo las siguientes acciones:

Todas las instituciones, órganos, empresas paraestatales y dependencias de la administración pública federal se involucrarán en un proceso de mejora continua respecto de la protección de sus sistemas.

Los tres poderes están obligados a fungir como ejemplos en la gestión de la Seguridad Digital.

TÍTULO QUINTO
De la participación de la comunidad
CAPÍTULO
De los Servicios de Atención a la Población
SECCIÓN I
De los procedimientos

Artículo 18.- Las personas integrantes del Sistema deberán garantizar las medidas y condiciones de accesibilidad para que toda persona goce de seguridad digital. En caso de violaciones a la seguridad digital la o las víctimas de dicha violación podrán presentar quejas que serán procesadas por la Secretaría, la cual hará las recomendaciones pertinentes al organismo de gobierno que haya violentado la seguridad digital.

Artículo 19.- Cualquier persona podrá presentar quejas sobre presuntas violaciones a la seguridad digital y acudir ante la Secretaría para presentar, ya sea directamente o por medio de un representante.
Cuando las personas interesadas estén privadas de su libertad o se desconozca su paradero, los hechos se podrán denunciar por sus parientes o vecinos, inclusive siendo menores de edad.
Las quejas también podrán presentarse oralmente, cuando las personas comparecientes no puedan escribir o sean menores de edad. Tratándose de personas que no hablen o entiendan correctamente el idioma español, o de aquellas pertenecientes a los pueblos o comunidades indígenas que así lo requieran o personas con discapacidad auditiva, se les proporcionará gratuitamente un traductor o intérprete que tenga conocimiento de su lengua y cultura, o en su caso intérprete de lengua de señas mexicanas.
Las organizaciones no gubernamentales legalmente constituidas podrán acudir ante la Secretaría para quejarse sobre violaciones a la seguridad digital

respecto de personas que, por sus condiciones físicas, mentales, socioeconómicas y culturales, no tengan la capacidad efectiva de presentar quejas de manera directa.

Artículo 20.- La Secretaría 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 la Secretaría orientará y apoyará a las personas comparecientes sobre el contenido de su queja.

Artículo 21.- La instancia respectiva deberá presentarse de forma oral, por escrito o por lenguaje de señas y podrá formularse por cualquier medio de comunicación eléctrica, electrónica o telefónica y a través de mecanismos accesibles para personas con discapacidad. No se admitirán comunicaciones anónimas, por lo que toda queja deberá ratificarse dentro de los tres días siguientes a su presentación, si la persona quejosa no se identifica y la suscribe en un primer momento.

Artículo 22.- La Secretaría designará personal de guardia para recibir y atender las quejas urgentes a cualquier hora y en cualquier día que sea necesario.

Artículo 23.- En el supuesto de que las personas quejosas no puedan identificar a las autoridades o servidores públicos, cuyos actos u omisiones consideren haber violentado su seguridad digital, la instancia será admitida, si procede, bajo la condición de que se logre dicha identificación en la investigación posterior de los hechos.

Artículo 24.- La formulación de quejas, así como las resoluciones y recomendaciones que emita la Secretaría, no afectarán el ejercicio de otros derechos y medios de defensa que puedan corresponder a los afectados

conforme a las leyes, y no suspenderán ni interrumpirán sus plazos preclusivos, de prescripción o caducidad. Esta circunstancia deberá señalarse a las personas interesadas en el acuerdo de admisión de la instancia.

Artículo 25.- Cuando la instancia sea inadmisible por ser manifiestamente improcedente o infundada, será rechazada de inmediato. Cuando no corresponda de manera ostensible a la competencia de la Secretaría, se deberá proporcionar orientación a la persona quejosa, a fin de que acuda a la autoridad o servidores públicos a quienes corresponda conocer o resolver el asunto.

Artículo 26.- Una vez admitida la instancia, deberá ponerse en conocimiento de las autoridades señaladas como responsables, utilizando en casos de urgencia cualquier medio de comunicación electrónica. En la misma comunicación se solicitará a dichas autoridades o servidores públicos 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 naturales y por los medios que sean convenientes, de acuerdo con el caso. En las situaciones que a juicio de la Secretaría se consideren urgentes, dicho plazo podrá ser reducido.

Artículo 27.- Cuando para la resolución de un asunto se requiera una investigación, se involucrarán las personas Visitadoras Generales, quienes tendrán las siguientes facultades:

I. Pedir a las autoridades o servidores públicos a los que se imputen violaciones de seguridad digital, la presentación de informes o documentación adicionales;
II. Solicitar de otras autoridades, servidores públicos o particulares todo género de documentos e informes;

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;
V. Efectuar todas las demás acciones que conforme a derecho juzgue convenientes para el mejor conocimiento del asunto.

Estas personas serán nombradas por la Secretaría Técnica tras su nombramiento como Secretaría Técnica, por lo que durarán en el cargo el mismo tiempo. Para el nombramiento, seguirán los mismos requisitos enunciados en el Artículo 8 de la presente Ley.

Artículo 28.- La Secretaría y los Visitadores Generales no podrán ser detenidos ni sujetos a responsabilidad civil, penal o administrativa, por las opiniones y recomendaciones que formulen.

Artículo 29.- Desde el momento en que se admita la queja, la Secretaría o los Visitadores Generales y, en su caso, el personal técnico y profesional, se pondrán en contacto inmediato con la autoridad señalada como responsable de la presunta violación de seguridad digital para intentar lograr una conciliación entre los intereses de las partes involucradas, a fin de lograr una solución inmediata del conflicto. De lograrse una solución satisfactoria o el allanamiento de la o de las personas responsables, la Secretaría lo hará constatar así y ordenará el archivo del expediente, el cual podrá reabrirse cuando las personas quejosas o denunciantes expresen a la Secretaría que no se ha cumplido con el compromiso en un plazo de 90 días. Para estos efectos, la Secretaría en el término de setenta y dos horas dictará el acuerdo correspondiente, y en su caso, proveerá las acciones y determinaciones conducentes.

Artículo 30.- Si de la presentación de la queja no se deducen los elementos que permitan la intervención de la Secretaría, ésta requerirá por escrito a la persona quejosa para que la aclare, de tratarse de una persona que no pueda leer, se le comunicará por el medio más conveniente. Si después de dos requerimientos la quejosa no contesta, se enviará la queja al archivo por falta de interés de la persona quejosa.

Artículo 31.- Las pruebas que se presenten, tanto por las personas interesadas como por las autoridades o servidores públicos a quienes se imputen las violaciones, 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 32.- Las conclusiones del expediente, que serán la base de las recomendaciones, estarán fundamentadas exclusivamente en la documentación y pruebas que obren en el propio expediente.

SECCIÓN II
De los Acuerdos y Recomendaciones

Artículo 33.- La Secretaría podrá dictar acuerdos de trámite, que serán obligatorios para las autoridades y servidores públicos para que comparezcan o aporten información o documentación.

Artículo 34.- Concluida la investigación, la persona Visitadora General formulará, en su caso, un proyecto de Recomendación o Acuerdo de no responsabilidad en el cual se analizarán los hechos, los argumentos y pruebas, así como los elementos de convicción y las diligencias practicadas, a fin de

determinar si las autoridades o servidores han violado o no la seguridad digitar de las personas afectadas, al haber incurrido en actos y omisiones ilegales, irrazonables, injustas, inadecuadas, o erróneas, o hubiesen dejado sin respuesta las solicitudes presentadas por las personas interesadas durante un período que exceda notoriamente los plazos fijados por las leyes. En el proyecto de Recomendación, se señalarán las medidas recomendadas para la efectiva restitución de las personas afectadas en su seguridad, y si procede en su caso, para la reparación de los daños y perjuicios que se hubiesen ocasionado.

Artículo 35.- Las recomendaciones y acuerdos serán públicos y no tendrá carácter imperativo para la autoridad o servidor público a los cuales se dirigirá y, en consecuencia, no podrá por sí misma anular, modificar o dejar sin efecto las resoluciones o actos contra los cuales se hubiese presentado la queja o denuncia. En todo caso, una vez recibida, la autoridad o servidor público de que se trate informará, dentro de los quince días hábiles siguientes a su notificación, si acepta dicha Recomendación. Entregará, en su caso, en otros quince 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. Cuando las recomendaciones emitidas no sean aceptadas o cumplidas, se procederá conforme a lo siguiente:

La autoridad o servidor público de que se trate deberá fundar, motivar y hacer pública su negativa.

Las autoridades o servidores públicos, a quienes se les hubiese notificado la insuficiencia de la fundamentación y motivación de la negativa, informarán dentro de los quince días hábiles siguientes a la notificación del escrito referido en el inciso que antecede, si persisten o no en la posición de no aceptar o no cumplir la recomendación.

Artículo 36.- En el informe que deberán rendir las autoridades señaladas como responsables contra las cuales se interponga queja se deberá hacer constar los antecedentes del asunto, los fundamentos y motivaciones de los actos u omisiones impugnados, la compensación pertinente a las personas afectadas, una garantía de no repetición, así como los elementos de información necesarios para la documentación del asunto.
La falta de rendición del informe o de la documentación que lo apoye, así como el retraso injustificado en su presentación, tendrá el efecto de que en relación con el trámite de la queja se tengan por ciertos los hechos materia de la misma, los cuales serán presentados ante la Fiscalía General de la República para tomar las acciones pertinentes.

Artículo 37.- No procederá ningún recurso en contra de las Recomendaciones, acuerdos o resoluciones definitivas.

Artículo 38.- El Visitador General no estará obligada a entregar ninguna de sus pruebas a la autoridad a la cual dirigió una Recomendación o a algún particular. Si dichas pruebas le son solicitadas, resolverá si son de entregarse o no, excepto en los casos en que la persona quejosa o sus familiares en línea ascendente o descendente en cualquier grado o colaterales hasta el segundo grado, ofrezcan como medio de convicción en un procedimiento jurisdiccional, las pruebas o constancias que integraron la queja ventilada.

Artículo 39.- 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.

TÍTULO SEXTO
De las intervenciones de las Comunicaciones
CAPÍTULO I
Disposiciones Generales

Artículo 40.- Los entes públicos tienen la responsabilidad de actuar respetando en todo momento los derechos de seguridad digital de las personas físicas o morales, siendo estos confidencialidad, integridad y disponibilidad de la información. El Estado Mexicano no podrá en ningún momento y bajo ninguna circunstancia violar los derechos de seguridad digital.
Todas las medidas de intervención de las comunicaciones deben ser necesarias y proporcionales, solo podrán efectuarse si no existe otra alternativa menos lesiva del derecho para conseguir el objeto legítimo y proporcional. En caso de que dicha medida sea exagerada y desmedida será ilegal y violatoria, aunque se tenga autorización judicial, y podrá ser denunciada mediante una queja con la Secretaría Técnica del Sistema.

Artículo 41.- Se prohíbe la intervención de comunicaciones privadas cuando se trate de cuestiones de carácter electoral, fiscal, mercantil, civil, laboral, administrativo o periodístico, así como en el caso de las comunicaciones de la persona detenida con su defensor.

Artículo 42.- La autoridad judicial que autorice la vigilancia o intervención de las comunicaciones tiene las siguientes obligaciones:

I. Ponderar, de manera previa y continua, la legitimidad de cualquier medida de vigilancia encubierta y su estricto apego a la ley y a los principios de finalidad legítima, idoneidad, necesidad y proporcionalidad;
II. Evitar o remediar los riesgos de abuso que la naturaleza secreta de la

vigilancia irremediablemente produce; y

III. Las demás que se establezcan en otras disposiciones normativa

En caso de que la autoridad judicial falte a sus obligaciones, será separada de su encargo e inhabilitada para desempeñar funciones, empleos, cargos o comisiones de cualquier naturaleza en el servicio público por un lapso de diez años.

Artículo 43.- La Secretaría tiene la obligación publicar anualmente un informe en el que especifique el número de solicitudes aprobadas y rechazadas, una desagregación de las solicitudes sobre la vigilancia o intervención de las comunicaciones por proveedor de servicios y por investigación y propósito.

Artículo 44.- El Consejo tiene la obligación de divulgar en todos los medios de comunicación la información sobre los programas de vigilancia de comunicaciones privadas, su alcance y técnicas; los requerimientos a empresas para colaborar con medidas de vigilancia; las resoluciones de autoridades judiciales autorizando o negando las solicitudes de autoridades; los órganos encargados de implementar y supervisar dichos programas; y los procedimientos de autorización, de selección de objetivos y de manejo de datos. Esto lo hará en colaboración con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos.

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos tiene la obligación de fiscalizar de forma permanente y sin restricciones las medidas de vigilancia gubernamental.

TÍTULO SEPTIMO
Disposiciones Generales

Artículo 45.- Para lograr potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades criminales.

1. La actuación policiaca y judicial del Estado en materia de Seguridad Digital deberá adecuase a los patrones de conducta y a las modalidades delictivas de los delincuentes en el ciberespacio de lo cual se encargará la Fiscalía General de la Republica.

La Dirección de Prevención y Atención a Riesgos se encargará de lograr este objetivo.

Artículo 46.- Para lograr sensibilizar a la ciudadanía, profesionales, empresas y agentes de la Administración Pública Federal de los riesgos del ciberespacio, se llevarán a cabo las siguientes acciones:

1. Las empresas públicas y privadas serán responsables de la seguridad de sus sistemas, la protección de la información de sus clientes, proveedores y la confiabilidad de los servicios que prestan.
2. Se promoverá una sólida 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
3. Todas las personas usuarias de internet deberán ser sensibilizadas 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
Disposiciones Generales

Artículo 47.- Los integrantes del Sistema vigilaran el cumplimiento de las recomendaciones que se emitan a los órganos de los tres niveles de gobierno en materia de Seguridad Digital.
En caso de que éstas 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.

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
TÍTULO PRIMERO
Disposiciones Preliminares

Artículo 1.- La presente Ley es reglamentaria del párrafo tercero del Artículo 6, 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 entenderá por:

I. Ciberespacio: Un entorno digital global constituido por redes informáticas y de telecomunicaciones, en el que se comunican e interactúan las personas y permite el ejercicio de sus derechos y libertades como lo hacen en el mundo físico.
II. Consejo: Consejo de Secretariado Técnico,
III. Secretaría: Secretaría Técnica de Seguridad Digital;
IV. Sistema: El Sistema Nacional de Seguridad Digital; y
V. Ley: Ley General del Sistema Nacional de Seguridad Digital

Artículo 3.- La presente ley tiene como fin preservar la integridad y disponibilidad en el ciberespacio y unir a las diferentes instancias y órdenes de gobierno, salvaguardando los derechos humanos de las personas usuarias de los sistemas de información y comunicaciones cibernéticas.

Artículo 4.- La Seguridad Digital se rige por los principios de legalidad, responsabilidad 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.

Todas las autoridades competentes en materia de Seguridad Digital deberán apegarse a los principios de certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad.

TITULO SEGUNDO
Del Sistema Nacional de Seguridad Digital.
CAPITULO I
De la organización del Sistema Nacional de Seguridad Digital.

Artículo 5.- El Sistema Nacional de Seguridad Digital está constituido por un Consejo de Secretariado Técnico, el cual está conformado por:

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

CAPITULO II
Del Consejo de Secretariado Técnico.

Artículo 6- El Consejo de Secretariado Técnico tendrá las siguientes atribuciones:

I. Vigilar el cumplimiento de las recomendaciones que se emitan a los órganos de los tres niveles de gobierno en materia de seguridad digital. En caso de que estas incumplan el Consejo 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.

II. Podrá llevar a cabo grupos de trabajo con la sociedad civil y las cámaras empresariales, en las cuales participe el Instituto, para que escuchen las ideas y propuestas que tienen. Se tienen que hacer cuando sean solicitadas, y contar con toda la publicidad.

III. Recibir quejas de presuntas violaciones a la seguridad digital.

CAPÍTULO III
De la Secretaría Ejecutivo de Seguridad Digital.

Artículo 7.- La Secretaría Técnica de Seguridad Digital es el órgano operativo del Sistema y gozará de autonomía técnica, de gestión y contará con los recursos suficientes para sus funciones que anualmente se le asignarían en el Presupuesto de Egresos de la Federación.

La persona titular será nombrada y removida libremente por la Presidencia de la República cada cuatro años y 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 reconocida capacidad y probidad, así como contar con cinco años de experiencia en las áreas correspondientes a su función; y
V. No haber sido sentenciada por delito doloso o inhabilitada como servidora pública.

La Secretaría Técnica de Seguridad Digital tendrá la representación legal del organismo. Durante su encargo, no podrá tener ninguno otro empelo, cargo o comisión.

Artículo 8.- La coordinación del Sistema estará a cargo de la Secretaría Técnica, correspondiéndole a ésta:

I. Representar legalmente al Consejo con facultades generales y especiales para actos de administración, dominio, pleitos y cobranzas, incluso las que requieran clausula especial conforme a la Ley aplicable;
II. Otorgar y revocar poderes a nombre del Consejo para actos de dominio, pleitos y cobranzas y para ser representado ante cualquier autoridad administrativa o judicial, ante los tribunales laborales o ante particulares. Tratándose de actos de dominio sobre inmuebles destinados al Consejo o para otorgar poderes para dichos efectos, se requiere la autorización del órgano interno de control;
III. Dirigir y administrar los recursos humanos, financieros y materiales del Consejo;
IV. Participar en representación del Consejo en foros, reuniones, negociaciones, eventos, convenciones y congresos que se lleven a cabo con organismo nacionales, internacionales, gobiernos extranjeros, cuando se refieran a temas en el ámbito de competencia del Instituto, de conformidad con lo establecidos en la presente Ley o designar representantes para tales efectos;

V. Ejecutar y dar seguimiento a los acuerdos y resoluciones del Consejo del Secretariado Técnico;
VI. Impulsar mejoras para los instrumentos de información del Sistema;
VII. Expedir recomendaciones y resoluciones a los órganos de los tres niveles de gobierno en materia de Seguridad Digital;
VIII. Promover la efectiva coordinación de las instancias y dar seguimiento de las estrategias y acciones que para tal efecto se establezcan;
IX. Elaborar la Estrategia Nacional de Seguridad Digital, el Plan Anual de Trabajo y el Informe Anual de Labores, en colaboración con los titulares de los diferentes organismos;
X. Establecer en la Estrategia de Nacional de Seguridad Digital los instrumentos, programas y políticas públicas integrales, sistemáticas, continuas y evaluables, tendientes a cumplir los objetivos y fines de la Seguridad Digital;
XI. Presentará un Informe Anual de actividades y podrá ser llamada a asistir a reuniones de trabajo, conforme a los principios de transparencia y rendición de cuentas;
XII. Vigilar que los sujetos obligados en el ámbito federal cumplan con las obligaciones de transparencia y poner a disposición del público, así como mantenerla actualizada, en los respectivos medios electrónicos, de acuerdo con sus facultades, atribuciones, funciones u objeto social, según corresponda; y
XIII. Las demás que se establezcan en otras disposiciones normativas y las que sean necesarias para el funcionamiento del Consejo de Secretariado Técnico y del Sistema.

CAPÍTULO IV
De las atribuciones de los integrantes del Consejo de Secretariado Técnico.

Artículo 10.- Como parte del Consejo de Secretariado Técnico, el Instituto Nacional de Estadística y Geografía, el Instituto Nacional Electoral, el Instituto Federal de Telecomunicaciones y el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, trabajarán en coordinación para:

I. Expedir recomendaciones a los órganos de los tres niveles de gobierno en materia de Seguridad Digital cuando ésta verse sobre las contramedidas de inteligencia técnica, para lo cual deberá llevar a cabo visitas de revisión y verificación a las autoridades correspondientes en términos de la Ley Federal del Procedimiento Administrativo. En caso de incumplimiento podrá emitir recomendaciones;
II. Aplicar la Estrategia Nacional de Seguridad Digital cuando ésta verse sobre la organización de la coordinación e interacción interdepartamental y el ejercicio de funciones especiales y de control de la Seguridad Digital del Estado Mexicano;
III. Coordinar y colaborar con la Fiscalía General de la República y de los Estados, para tener información veraz y oportuna sobre todos los procedimientos relacionados con los ciberdelitos; y
IV. Las demás que se establezcan en otras disposiciones normativas y las que sean necesarias para el funcionamiento del Consejo de Secretariado Técnico y del Sistema.

Artículo 11.- Como parte del Consejo de Secretariado Técnico, la Comisión Nacional de Derechos Humanos y el Consejo Nacional de Evaluación de la Política de Desarrollo Social, tendrán las siguientes facultades y obligaciones:

I. Sugerir programas que promuevan y fomenten la confianza en el ámbito digital a través de la formación en materia de Seguridad Digital;
II. Desarrollar la Seguridad Digital y la confianza digital de la ciudadanía, las academias y las redes de investigación;
III. Convocar a persona físicas o morales, a organizaciones de la sociedad civil y a instituciones educativas a mesas de diálogo, foros o grupos de trabajo, los cuales deberán ser públicos, en los que expongan conocimientos y experiencias para el cumplimiento de la seguridad cibernética; y
IV. Las demás que se establezcan en otras disposiciones normativas y las que sean necesarias para el funcionamiento del Consejo de Secretariado Técnico y del Sistema.

Artículo 12.- Como parte del Consejo de Secretariado Técnico, la Comisión Federal de Competencia Económica, el Banco de México, el Instituto para la Protección al Ahorro Bancario y la Comisión Nacional Bancaria y de Valores tendrán las siguientes facultades y obligaciones:

I. Trabajar por la seguridad de las y los usuarios en los diversos sectores económicos, privilegiando sus libertades y la protección de sus derechos humanos, con base en la Estrategia Nacional de Seguridad Digital, a la cual deberán de aportar en este tema particular;
II. Convocar a los diversos actores del sector económico a mesas de diálogo, foros o grupos de trabajo, los cuales deberán ser públicos, en los que expongan conocimientos y experiencias para el cumplimiento de la seguridad cibernética; y

III. Las demás que se establezcan en otras disposiciones normativas y las que sean necesarias para el funcionamiento del Consejo de Secretariado Técnico y del Sistema.

TÍTULO TERCERO
Disposiciones Comunes a los integrantes del Sistema de Seguridad Digital.
CAPÍTULO I
De las obligaciones y sanciones.

Artículo 13.- Con el objeto de garantizar el cumplimiento de los principios constitucionales de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos, las personas integrantes del Sistema de Seguridad Digital se sujetarán a las siguientes obligaciones:

I. Conducirse siempre con dedicación y disciplina, así como con apego al orden jurídico y respeto a las garantías individuales y derechos humanos reconocidos en la Constitución Política de los Estados Unidos Mexicanos;
II. Cumplir sus funciones con absoluta imparcialidad y sin discriminación alguna;
III. Observar un trato respetuoso con todas las personas, debiendo abstenerse de todo acto arbitrario y de limitar indebidamente las acciones o manifestaciones que en ejercicio de sus derechos constitucionales y con carácter pacífico realice la población;
IV. Desempeñar sus funciones sin solicitar ni aceptar compensaciones, pagos o gratificaciones distintas a las previstas legalmente. En particular se opondrán a cualquier acto de corrupción y, en caso de tener conocimiento de alguno, deberán denunciarlo; y
V. Las demás que establezcan las disposiciones legales aplicables.

TITULO CUARTO
Capítulo I
De la Estrategia Nacional de Seguridad Digital.
Sección I
Disposiciones Generales.

Artículo 14.- La Estrategia Nacional de Seguridad Digital es un instrumento por medio del cual se llevará a cabo la estrategia a seguir en el periodo establecido, reconociendo los retos y acciones a corto, mediano y largo plazo mediante la coordinación con las autoridades federales, estatales y locales, el sector social y el sector privado en materia de Seguridad Digital. Se elaborará y aprobará cada dos años. Tendrá que ser presentada y publicada en todos los medios de comunicación, así como en el portal del Consejo de Secretariado Técnico, la primera semana de enero de cada dos años.

Artículo 15.- La Estrategia Nacional de Seguridad Digital tendrá como propósito lograr el uso seguro del ciberespacio, impulsando una visión integradora cuya aplicación ayude a garantizar la Seguridad Digital y progreso por medio de la adecuada coordinación de las instituciones, organismos y dependencias de la administración pública federal, impulsando el máximo respeto a los derechos humanos.

Artículo 16.- La Estrategia Nacional de Seguridad Digital tendrá como ejes:

I. Garantizar que los sistemas de información y telecomunicaciones que utilice la administración pública posean un adecuado nivel de ciberseguridad.
II. Impulsar la ciberseguridad y resiliencia de los sistemas de información utilizados por el sector empresarial en general y los operadores de infraestructuras informáticas críticas.

III. Potenciar las capacidades de prevención, detección, reacción, defensa, análisis, recuperación, investigación y coordinación frente a las actividades de la delincuencia en el ciberespacio.
IV. Sensibilizar a la ciudadanía, profesionales, empresas y administraciones publicas de todos los riesgos derivados del ciberespacio.

La Secretaría de Gobernación será la encargada de coordinar los esfuerzos para lograr los ejes.

Artículo 17.- Para lograr garantizar que los sistemas de información y telecomunicaciones que utilizan todas las instituciones, órganos, empresas paraestatales y dependencias de la administración pública federal posean un adecuado nivel de seguridad, se llevaran a cabo las siguientes acciones:
Todas las instituciones, órganos, empresas paraestatales y dependencias de la administración pública federal se involucrarán en un proceso de mejora continua respecto de la protección de sus sistemas.
Los tres poderes están obligados a fungir como ejemplos en la gestión de la Seguridad Digital.

TÍTULO QUINTO
De la participación de la comunidad.
CAPÍTULO
De los Servicios de Atención a la Población.
SECCIÓN I
De los procedimientos.

Artículo 18.- Las personas integrantes del Sistema deberán garantizar las medidas y condiciones de accesibilidad para que toda persona goce de seguridad digital. En caso de violaciones a la seguridad digital la o las víctimas de dicha violación podrán presentar quejas que serán procesadas por la

Secretaría, la cual hará las recomendaciones pertinentes al organismo de gobierno que haya violentado la seguridad digital.

Artículo 19.- Cualquier persona podrá presentar quejas sobre presuntas violaciones a la seguridad digital y acudir ante la Secretaría para presentar, ya sea directamente o por medio de un representante.

Cuando las personas interesadas estén privadas de su libertad o se desconozca su paradero, los hechos se podrán denunciar por sus parientes o vecinos, inclusive siendo menores de edad.

Las quejas también podrán presentarse oralmente, cuando las personas comparecientes no puedan escribir o sean menores de edad. Tratándose de personas que no hablen o entiendan correctamente el idioma español, o de aquellas pertenecientes a los pueblos o comunidades indígenas que así lo requieran o personas con discapacidad auditiva, se les proporcionará gratuitamente un traductor o intérprete que tenga conocimiento de su lengua y cultura, o en su caso intérprete de lengua de señas mexicanas.

Las organizaciones no gubernamentales legalmente constituidas podrán acudir ante la Secretaría para quejarse sobre violaciones a la seguridad digital respecto de personas que, por sus condiciones físicas, mentales, socioeconómicas y culturales, no tengan la capacidad efectiva de presentar quejas de manera directa.

Artículo 20.- La Secretaría 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 la Secretaría orientará y apoyará a las personas comparecientes sobre el contenido de su queja.

Artículo 21.- La instancia respectiva deberá presentarse de forma oral, por escrito o por lenguaje de señas y podrá formularse por cualquier medio de comunicación eléctrica, electrónica o telefónica y a través de mecanismos accesibles para personas con discapacidad. No se admitirán comunicaciones anónimas, por lo que toda queja deberá ratificarse dentro de los tres días siguientes a su presentación, si la persona quejosa no se identifica y la suscribe en un primer momento.

Artículo 22.- La Secretaría designará personal de guardia para recibir y atender las quejas urgentes a cualquier hora y en cualquier día que sea necesario.

Artículo 23.- En el supuesto de que las personas quejosas no puedan identificar a las autoridades o servidores públicos, cuyos actos u omisiones consideren haber violentado su seguridad digital, la instancia será admitida, si procede, bajo la condición de que se logre dicha identificación en la investigación posterior de los hechos.

Artículo 24.- La formulación de quejas, así como las resoluciones y recomendaciones que emita la Secretaría, no afectarán el ejercicio de otros derechos y medios de defensa que puedan corresponder a los afectados conforme a las leyes, y no suspenderán ni interrumpirán sus plazos preclusivos, de prescripción o caducidad. Esta circunstancia deberá señalarse a las personas interesadas en el acuerdo de admisión de la instancia.

Artículo 25.- Cuando la instancia sea inadmisible por ser manifiestamente improcedente o infundada, será rechazada de inmediato. Cuando no corresponda de manera ostensible a la competencia de la Secretaría, se deberá proporcionar orientación a la persona quejosa, a fin de que acuda a la autoridad o servidores públicos a quienes corresponda conocer o resolver el asunto.

Artículo 26.- Una vez admitida la instancia, deberá ponerse en conocimiento de las autoridades señaladas como responsables, utilizando en casos de urgencia cualquier medio de comunicación electrónica. En la misma comunicación se solicitará a dichas autoridades o servidores públicos 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 naturales y por los medios que sean convenientes, de acuerdo con el caso. En las situaciones que a juicio de la Secretaría se consideren urgentes, dicho plazo podrá ser reducido.

Artículo 27.- Cuando para la resolución de un asunto se requiera una investigación, se involucrarán las personas Visitadoras Generales, quienes tendrán las siguientes facultades:

VI. Pedir a las autoridades o servidores públicos a los que se imputen violaciones de seguridad digital, la presentación de informes o documentación adicionales;

VII. Solicitar de otras autoridades, servidores públicos o particulares todo género de documentos e informes;

VIII. Practicar visitas e inspecciones, ya sea personalmente o por medio del personal técnico o profesional bajo su dirección en términos de ley;

IX. Citar a las personas que deban comparecer como peritos o testigos;

X. Efectuar todas las demás acciones que conforme a derecho juzgue convenientes para el mejor conocimiento del asunto.

Estas personas serán nombradas por la Secretaría Técnica tras su nombramiento como Secretaría Técnica, por lo que durarán en el cargo el mismo tiempo. Para el nombramiento, seguirán los mismos requisitos enunciados en el Artículo 8 de la presente Ley.

Artículo 28.- La Secretaría y los Visitadores Generales no podrán ser detenidos ni sujetos a responsabilidad civil, penal o administrativa, por las opiniones y recomendaciones que formulen.

Artículo 29.- Desde el momento en que se admita la queja, la Secretaría o los Visitadores Generales y, en su caso, el personal técnico y profesional, se pondrán en contacto inmediato con la autoridad señalada como responsable de la presunta violación de seguridad digital para intentar lograr una conciliación entre los intereses de las partes involucradas, a fin de lograr una solución inmediata del conflicto. De lograrse una solución satisfactoria o el allanamiento de la o de las personas responsables, la Secretaría lo hará constatar así y ordenará el archivo del expediente, el cual podrá reabrirse cuando las personas quejosas o denunciantes expresen a la Secretaría que no se ha cumplido con el compromiso en un plazo de 90 días. Para estos efectos, la Secretaría en el término de setenta y dos horas dictará el acuerdo correspondiente, y en su caso, proveerá las acciones y determinaciones conducentes.

Artículo 30.- Si de la presentación de la queja no se deducen los elementos que permitan la intervención de la Secretaría, ésta requerirá por escrito a la persona quejosa para que la aclare, de tratarse de una persona que no pueda leer, se le comunicará por el medio más conveniente. Si después de dos requerimientos la quejosa no contesta, se enviará la queja al archivo por falta de interés de la persona quejosa.

Artículo 31.- Las pruebas que se presenten, tanto por las personas interesadas como por las autoridades o servidores públicos a quienes se imputen las violaciones, 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 32.- Las conclusiones del expediente, que serán la base de las recomendaciones, estarán fundamentadas exclusivamente en la documentación y pruebas que obren en el propio expediente.

SECCIÓN II
De los Acuerdos y Recomendaciones.

Artículo 33.- La Secretaría podrá dictar acuerdos de trámite, que serán obligatorios para las autoridades y servidores públicos para que comparezcan o aporten información o documentación.

Artículo 34.- Concluida la investigación, la persona Visitadora General formulará, en su caso, un proyecto de Recomendación o Acuerdo de no responsabilidad en el cual se analizarán los hechos, los argumentos y pruebas, así como los elementos de convicción y las diligencias practicadas, a fin de determinar si las autoridades o servidores han violado o no la seguridad digitar de las personas afectadas, al haber incurrido en actos y omisiones ilegales, irrazonables, injustas, inadecuadas, o erróneas, o hubiesen dejado sin respuesta las solicitudes presentadas por las personas interesadas durante un período que exceda notoriamente los plazos fijados por las leyes. En el proyecto de Recomendación, se señalarán las medidas recomendadas para la efectiva restitución de las personas afectadas en su seguridad, y si procede en su caso, para la reparación de los daños y perjuicios que se hubiesen ocasionado.

Artículo 35.- Las recomendaciones y acuerdos serán públicos y no tendrá carácter imperativo para la autoridad o servidor público a los cuales se dirigirá y, en consecuencia, no podrá por sí misma anular, modificar o dejar sin efecto las resoluciones o actos contra los cuales se hubiese presentado la queja o denuncia. En todo caso, una vez recibida, la autoridad o servidor público de que se trate informará, dentro de los quince días hábiles siguientes a su notificación, si acepta dicha Recomendación. Entregará, en su caso, en otros quince 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. Cuando las recomendaciones emitidas no sean aceptadas o cumplidas, se procederá conforme a lo siguiente:
La autoridad o servidor público de que se trate deberá fundar, motivar y hacer pública su negativa.
Las autoridades o servidores públicos, a quienes se les hubiese notificado la insuficiencia de la fundamentación y motivación de la negativa, informarán dentro de los quince días hábiles siguientes a la notificación del escrito referido en el inciso que antecede, si persisten o no en la posición de no aceptar o no cumplir la recomendación.

Artículo 36.- En el informe que deberán rendir las autoridades señaladas como responsables contra las cuales se interponga queja se deberá hacer constar los antecedentes del asunto, los fundamentos y motivaciones de los actos u omisiones impugnados, la compensación pertinente a las personas afectadas, una garantía de no repetición, así como los elementos de información necesarios para la documentación del asunto.
La falta de rendición del informe o de la documentación que lo apoye, así como el retraso injustificado en su presentación, tendrá el efecto de que en relación con el trámite de la queja se tengan por ciertos los hechos materia de la misma, los cuales serán presentados ante la Fiscalía General de la República para

tomar las acciones pertinentes.

Artículo 37.- No procederá ningún recurso en contra de las Recomendaciones, acuerdos o resoluciones definitivas.

Artículo 38.- El Visitador General no estará obligada a entregar ninguna de sus pruebas a la autoridad a la cual dirigió una Recomendación o a algún particular. Si dichas pruebas le son solicitadas, resolverá si son de entregarse o no, excepto en los casos en que la persona quejosa o sus familiares en línea ascendente o descendente en cualquier grado o colaterales hasta el segundo grado, ofrezcan como medio de convicción en un procedimiento jurisdiccional, las pruebas o constancias que integraron la queja ventilada.

Artículo 39.- 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.

TÍTULO SEXTO
De las intervenciones de las Comunicaciones
CAPÍTULO I
Disposiciones Generales

Artículo 40.- Los entes públicos tienen la responsabilidad de actuar respetando en todo momento los derechos de seguridad digital de las personas físicas o morales, siendo estos confidencialidad, integridad y disponibilidad de la información. El Estado Mexicano no podrá en ningún momento y bajo ninguna circunstancia violar los derechos de seguridad digital.

Todas las medidas de intervención de las comunicaciones deben ser necesarias y proporcionales, solo podrán efectuarse si no existe otra alternativa menos

lesiva del derecho para conseguir el objeto legítimo y proporcional. En caso de que dicha medida sea exagerada y desmedida será ilegal y violatoria, aunque se tenga autorización judicial, y podrá ser denunciada mediante una queja con la Secretaría Técnica del Sistema.

Artículo 41.- Se prohíbe la intervención de comunicaciones privadas cuando se trate de cuestiones de carácter electoral, fiscal, mercantil, civil, laboral, administrativo o periodístico, así como en el caso de las comunicaciones de la persona detenida con su defensor.

Artículo 42.- La autoridad judicial que autorice la vigilancia o intervención de las comunicaciones tiene las siguientes obligaciones:

I. Ponderar, de manera previa y continua, la legitimidad de cualquier medida de vigilancia encubierta y su estricto apego a la ley y a los principios de finalidad legítima, idoneidad, necesidad y proporcionalidad;
II. Evitar o remediar los riesgos de abuso que la naturaleza secreta de la vigilancia irremediablemente produce; y
III. Las demás que se establezcan en otras disposiciones normativa.

En caso de que la autoridad judicial falte a sus obligaciones, será separada de su encargo e inhabilitada para desempeñar funciones, empleos, cargos o comisiones de cualquier naturaleza en el servicio público por un lapso de diez años.

Artículo 43.- La Secretaría tiene la obligación publicar anualmente un informe en el que especifique el número de solicitudes aprobadas y rechazadas, una desagregación de las solicitudes sobre la vigilancia o intervención de las comunicaciones por proveedor de servicios y por investigación y propósito.

Artículo 44.- El Consejo tiene la obligación de divulgar en todos los medios de comunicación la información sobre los programas de vigilancia de comunicaciones privadas, su alcance y técnicas; los requerimientos a empresas para colaborar con medidas de vigilancia; las resoluciones de autoridades judiciales autorizando o negando las solicitudes de autoridades; los órganos encargados de implementar y supervisar dichos programas; y los procedimientos de autorización, de selección de objetivos y de manejo de datos. Esto lo hará en colaboración con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos.

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos tiene la obligación de fiscalizar de forma permanente y sin restricciones las medidas de vigilancia gubernamental.

.

TÍTULO SEPTIMO
Disposiciones Generales

Artículo 45.- Para lograr potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades criminales.

2. La actuación policiaca y judicial del Estado en materia de Seguridad Digital deberá adecuase a los patrones de conducta y a las modalidades delictivas de los delincuentes en el ciberespacio de lo cual se encargará la Fiscalía General de la Republica.

La Dirección de Prevención y Atención a Riesgos se encargará de lograr este objetivo.

Artículo 46.- Para lograr sensibilizar a la ciudadanía, profesionales, empresas y agentes de la Administración Pública Federal de los riesgos del ciberespacio, se llevarán a cabo las siguientes acciones:

4. Las empresas públicas y privadas serán responsables de la seguridad de sus sistemas, la protección de la información de sus clientes, proveedores y la confiabilidad de los servicios que prestan.
5. Se promoverá una sólida 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
6. Todas las personas usuarias de internet deberán ser sensibilizadas 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
Disposiciones Generales

Artículo 47.- Los integrantes del Sistema vigilaran el cumplimiento de las recomendaciones que se emitan a los órganos de los tres niveles de gobierno en materia de Seguridad Digital.

En caso de que éstas 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.

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 Técnica de Seguridad Digital, 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 1 de febrero de 2023.

Cámara de Diputados del Honorable Congreso de la Unión, LXV Legislatura

Junta de Coordinación Política

Diputados: Moisés Ignacio Mier Velasco, presidente; Jorge Romero Herrera, PAN; Rubén Ignacio Moreira Valdez, PRI; Carlos Alberto Puente Salas, PVEM; Alberto Anaya Gutiérrez, PT; Jorge Álvarez Máynez, MOVIMIENTO CIUDADANO; Luis Ángel Xariel Espinosa Cházaro, PRD.

Mesa Directiva

Diputados: Santiago Creel Miranda, presidente; vicepresidentes, Karla Yuritzi Almazán Burgos, MORENA; Nohemí Berenice Luna Ayala, PAN; Marcela Guerra Castillo, PRI; secretarios, Brenda Espinoza López, MORENA; Saraí Núñez Cerón, PAN; Fuensanta Guadalupe Guerrero Esquivel, PRI; María del Carmen Pinete Vargas, PVEM; Magdalena del Socorro Núñez Monreal, PT; Jessica María Guadalupe Ortega de la Cruz, MOVIMIENTO CIUDADANO; Olga Luz Espinosa Morales, PRD.

Secretaría General

Secretaría de Servicios Parlamentarios

Gaceta Parlamentaria de la Cámara de Diputados

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

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