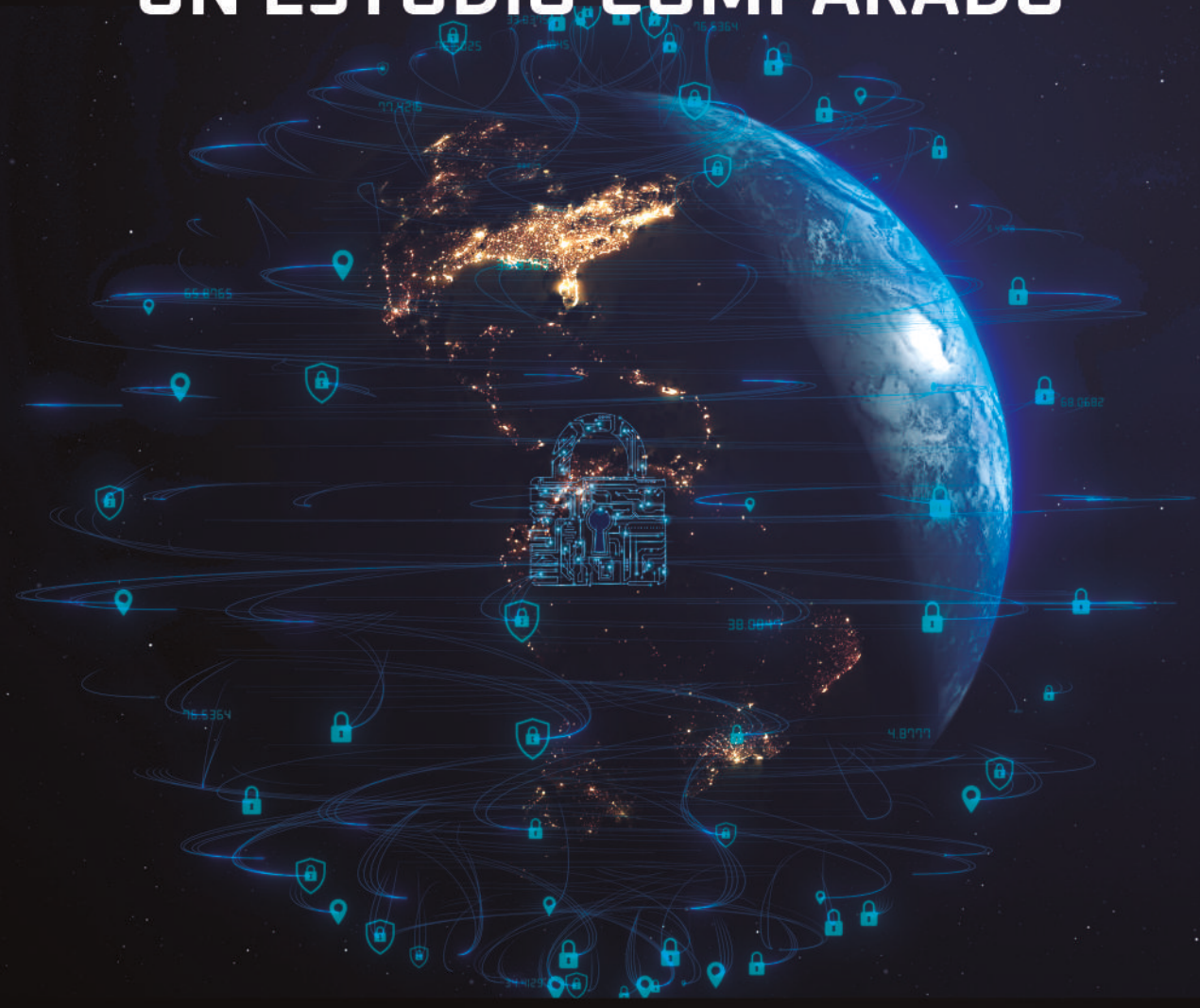
LA CIBERSEGURIDAD: UN ESTUDIO COMPARADO



CÁMARA DE DIPUTADOS
LXV LEGISLATURA

40 Aniversario Investigación Parlamentaria

CEDIP
CENTRO DE ESTUDIOS DE DERECHO E INVESTIGACIONES PARLAMENTARIAS

LA CIBERSEGURIDAD: UN ESTUDIO COMPARADO

LA CIBERSEGURIDAD: UN ESTUDIO COMPARADO

Centro de Estudios de Derecho e
Investigaciones Parlamentarias (CEDIP)
Cámara de Diputados LXV Legislatura

Diseño y formación de interiores:
Adolfo Pável Güemes Campos

Cuidado de la edición:
Noé Luis Ortiz

ISBN: 978-607-8877-19-5

Agosto de 2022

Mesa Directiva

Presidencia
Dip. Santiago Creel Miranda

Vicepresidencia
Dip. Karla Yuritzi Almazán Burgos
Dip. Noemí Berenice Luna Ayala
Dip. Marcela Guerra Castillo

Secretarías
Dip. Brenda Espinoza Lopez
Dip. Sarai Núñez Cerón
Dip. Fuensanta Guadalupe Guerrero Esquivel
Dip. María del Carmen Pinete Vargas
Dip. Magdalena del Socorro Núñez Monreal
Dip. Jessica Ortega de la Cruz
Dip. Olga Luz Espinosa Morales

Junta de Coordinación Política

Presidencia
Dip. Moisés Ignacio Mier Velazco

Integrantes
Dip. Jorge Romero Herrera
Dip. Rubén Ignacio Moreira Valdez
Dip. Carlos Alberto Puente Salas
Dip. Alberto Anaya Gutiérrez
Dip. Jorge Álvarez Máynez
Dip. Luis Angel Xariel Espinosa Cházaro

Director General del Centro de Estudios de Derecho e Investigaciones Parlamentarias
Juan Carlos Cervantes Gómez

Director de Estudios Jurídicos y coordinador de la investigación
Marcial Manuel Cruz Vázquez

Autores
Gustavo Eduardo Marín Hernández[1]
Irving Ilie Gómez Lara[2]

1 Investigador C del Centro de Estudios de Derecho e Investigaciones Parlamentarias de la Cámara de Diputados, maestro en Ciencia Política por el Centro de Investigación y Docencia Económicas.

2 Investigador A del Centro de Estudios de Derecho e Investigaciones Parlamentarias de la Cámara de Diputados, maestro en Estudios Latinoamericanos por la Universidad Nacional Autónoma de México.

ÍNDICE

PRÓLOGO

En el ámbito del derecho, un debate recurrente ha sido el de dilucidar si es la sociedad la que moldea al orden jurídico o si es este quien moldea a la colectividad. Sumado a lo anterior, esta discusión resulta compleja cuando se traslada al ámbito legislativo, ya que la génesis de cualquier ordenamiento jurídico siempre es acompañada por visiones normativas de carácter prescriptivo y descriptivo, lo que hace complicado definir las fronteras entre ambas esferas.

En el mundo contemporáneo, esta díada, que es constante en el quehacer legislativo, es más evidente cuando hacen su aparición tecnologías disruptivas que impactan significativamente en los diferentes campos de la actividad humana y la vida cotidiana.

Hoy en día resulta innegable que el tránsito que experimentamos de una economía basada en la sociedad industrial hacia una economía sustentada en el uso de la información conlleva sus propias expectativas promisorias, así como sus problemáticas específicas que habrán de ser sorteadas para maximizar el potencial humano que, como especie, es posible detonar a partir de la interacción que desarrollemos con el acceso y procesamiento exponencial de los datos que fluyen en el campo de lo digital.

Es justo, ante este escenario, que el Poder Legislativo debe aportar, si no todas las soluciones y respuestas, sí las alternativas para normar y atender gran parte de los fenómenos que surgen en la medida que se intensifica el uso de las Tecnologías de la Información.

Para dimensionar la importancia que ha tomado Internet y, con esta tecnología, la variedad de interacciones que se construyen a partir de su uso, es conveniente ubicar cómo se encuentra México en la actualidad. De acuerdo con un estudio realizado en 2021 por la Asociación Mexicana de Internet (AMI) sobre los hábitos de los usuarios en Internet, hasta el año 2020 existían 84.1 millones de internautas en nuestro país, lo que representa 72 por ciento de la población de 6 años o más.

Durante ese año, debido a la pandemia por COVID-19, los usuarios de Internet tuvieron el mayor crecimiento observado en los últimos 5 años. Al cierre de 2020 se contabilizaron 115 millones de teléfonos móviles inteligentes y, en promedio, los usuarios accedieron a sus redes 6.8 días a la semana. Así mismo, 7 de cada 10 internautas realizaron videollamadas durante el último año; 2 de cada 10 usuarios compraron

un producto publicitado en línea y 11 por ciento de la base total de internautas aumentaron su gasto en Internet durante dicho periodo.

Como es posible observar, la población de México cuenta en su mayoría con servicio de Internet. A su vez, el uso de esta tecnología permite el aprovechamiento de otras plataformas digitales que simplifican en gran medida las actividades habituales, ya que van desde la posibilidad de atender reuniones a distancia, comunicarnos mediante servicios de mensajería hasta lugares recónditos de nuestro planeta, o bien, realizar las compras cotidianas desde nuestro domicilio y efectuar operaciones bancarias sin importar la cantidad de que se trate.

Sin embargo, es importante destacar que, así como el Internet representa grandes beneficios para nuestra vida, también conlleva una serie de riesgos que bien vale la pena conocer para una adecuada prevención de los mismos.

El fenómeno de anonimidad que permite proteger la identidad de los usuarios en Internet, cuando es utilizado de forma dolosa, puede traer como consecuencia la vulneración de la esfera jurídica de otros usuarios. Tal es el caso de fenómenos como el *Grooming,* que está muy relacionado con delitos mayores como la pornografía infantil, la trata o el tráfico de personas; el *Phishing*, que se traduce en el fraude y la suplantación de identidades personales; la *Sextorsión,* que implica el chantaje para obtener contenidos o material sexual producidos por la misma víctima con base en amenazas; o el *Ciberbullying,* que se refiere al ciberacoso tal como lo conocemos.

Las figuras señaladas anteriormente impactan en la vida de todas aquellas personas que sufren la vulneración de su información en el ámbito digital y pueden derivar en muchos otros efectos negativos que minan la confianza en el uso de las Tecnologías de la Información. No obstante, sin restar importancia a la problemática de posibles riesgos que los particulares enfrentan, la seguridad digital es una cuestión trascendental para la vida de las instituciones que conforman el Estado mexicano, ya que el robo, el secuestro o la falsificación de la información implican un ataque flagrante al orden jurídico y a la sociedad en su conjunto.

Cabe señalar que se ha observado que el Estado mexicano carece de una ley especializada en materia de ciberseguridad, por lo que es menester fortalecer los mecanismos que ayuden a los particulares y las dependencias federales a prevenir los ciberataques y, en su caso, buscar el

amparo de la ley para contar con los medios respectivos para el fincamiento de responsabilidades.

Por esta razón, la Comisión de Ciencia, Tecnología e Innovación de la Cámara de Diputados ha orientado parte de su actuar en el estudio de alternativas que fortalezcan la ciberseguridad en nuestro país, entendida ésta como la seguridad de las Tecnologías de la Información que comprende todas aquellas medidas diseñadas para combatir las amenazas contra los sistemas en red y las aplicaciones, ya sea que esas amenazas se originen dentro o fuera de una organización.[1]

Desde el seno de esta Comisión se ha desplegado un esfuerzo encomiable de parte de todos los actores estratégicos que intervienen en materia de ciberseguridad, los cuales trascienden el ámbito político y permean en el sector público, privado y social, y que al igual que las legisladoras y los legisladores de esta Comisión, también se preocupan porque México cuente con los elementos normativos que permitan hacer frente a tan serios problemas.

Como muestra del compromiso multilateral, el 25 de febrero de 2022 se constituyó la mesa de trabajo permanente en materia de ciberseguridad, la cual ha logrado construir un diálogo franco entre todos los actores estratégicos que en esta intervienen, abordando diversos temas que implican un análisis de la ciberseguridad desde sus diferentes enfoques, como son la seguridad nacional, la seguridad pública y la seguridad de los datos, así como aspectos financieros de la ciberseguridad, la coordinación internacional en la materia y el análisis legislativo de las iniciativas presentadas para atender este importante tema.

Siendo realistas, ante las áreas de oportunidad que, como país, tenemos en la seguridad de la información, bien vale la pena tener en cuenta que en México se han registrado varios desafortunados casos de ataque a las instituciones públicas, por mencionar algunos:

- Banco de México (abril de 2018).
- Petróleos Mexicanos (noviembre de 2019).
- Secretaría de Economía (febrero de 2020).
- Lotería Nacional (mayo de 2021).
- Secretaría de la Defensa Nacional (septiembre de 2022).

1 IBM, *¿Qué es la ciberseguridad?,* (3 de octubre de 2022), https://www.ibm.com/mx-es/topics/cybersecurity.

1. *Banco de México, 2018*

Una operación llevada a cabo con precisión a finales de abril de 2018, cuando varios de los mayores bancos de México detectaron transferencias no autorizadas. Se calcula que el monto osciló entre los 400 a 800 millones de pesos (entre US$21 y US$42 millones).

Se calcula que los hackers que atacaron el Banco de México, entre otras instituciones bancarias, estuvieron infiltrados dentro de las redes de estas instituciones hasta año y medio antes de ser detectados.

Tras la investigación forense se determinó que fue software de terceros que fueron adquiridos por los bancos los que sufrieron el ataque directamente, hubo controles que no se siguieron y existió una falta de supervisión por parte del Banco de México.

2. *PEMEX, 2019*

La empresa productiva del Estado fue víctima del ataque de *ransomware* (secuestro de datos) el 10 de noviembre de 2019 y los autores del hackeo demandaron un rescate de 568 bitcoins, el equivalente a 4.9 millones de dólares. Se estima que el 5% de los equipos de cómputo de la empresa productiva del Estado fueron infectados con el *malware* que encripta la información, para pedir rescate posteriormente.[2]

La agresión se le atribuyó a la banda de hackers *DoppelPaymer*. Según respuestas a solicitudes de información realizadas vía Ley de Transparencia, la empresa productiva identificó más de 176.3 millones de intentos de agresiones a sus sistemas, de enero de 2015 a agosto de 2020.

La Auditoría Superior de la Federación realizó la Auditoría de Cumplimiento a Tecnologías de Información y Comunicaciones: 2018-6-90T9N20-0449-2019, destacando que se comprobó que, en el rubro de ciberseguridad, los principales riesgos se desprenden de la carencia de controles, entre los que destaca la falta de un análisis de vulnerabilidades. Así pues, se recomendó que toda la infraestructura de PEMEX cumpla con los objetivos de la seguridad informática.[3]

2 MEZA, Nayeli y BUENDÍA, Eduardo, *PemexLeaks: el robo de información que la petrolera quiso ocultar*, (3 de octubre de 2022), https://oneamexico.org/pemex-leaks-el-robo-de-informacion-que-la-petrolera-quiso-ocultar.

3 AUDITORÍA SUPERIOR DE LA FEDERACIÓN, *Auditoría de Cumplimiento a Tecnologías de Información y Comunicaciones: 2018-6-90T9N20-0449-2019,* (3 de octubre de 2022), https://www.asf.gob.mx/Trans/Informes/ IR2018a/Documentos/Auditorias/2018_0449_a.pdf.

3. *Secretaría de Economía, 2020*

La Secretaría de Economía informó que, el 23 de febrero de 2020, sufrió un ataque cibernético en sus servidores. En el comunicado que publicó puede observarse lo siguiente:

> Ayer domingo, 23 de febrero a las 10:30 hrs., se detectó un ataque cibernético en algunos servidores de la Secretaría de Economía. Cabe destacar que la información sensible de la Secretaría y de sus usuarios no se vio comprometida. Sin embargo, como medida de precaución, la Dirección General de Tecnologías de la Información (DGTI) solicitó a los proveedores el aislamiento de todas las redes y servidores. La capacidad operativa será reestablecida de forma segura, paulatina y controlada.[4]

4. *Lotería Nacional, 2021*

En mayo de 2021, la Lotería Nacional (Lotenal) sufrió un ataque de *ransomware* a manos del grupo de hackers de origen ruso Avaddon. Los documentos que quedaron expuestos van desde información de pagos, pólizas, contratos, hasta bases de datos desde el 2009 hasta el 2021.[5]

Los operadores de Avaddon han hecho públicos 17 documentos que, presuntamente, extrajeron de los sistemas de Pronósticos Deportivos, dependencia gubernamental que se fusionó en 2019 con la Lotería Nacional, y amenazaron con ejecutar un ataque a la disponibilidad (DoS) en contra de la infraestructura de la institución.[6]

5. *SEDENA, 2022*

El último ciberataque que se encuentra documentado tuvo lugar durante el mes de septiembre de 2022. La revista Forbes México informó del hackeo a las bases de datos de la SEDENA y en su nota señaló lo siguiente:

---

4 GOBIERNO DE MÉXICO, *Alertas de seguridad informática,* (15 de mayo de 2022), https://www.gob.mx/se/prensa/controla-secretaria-de-economia-ataque-informati- co-235802.

5 REYES, Eréndira, *Ciberdelincuentes filtran documentos internos de la Lotería Nacional,* (3 de octubre de 2022), https://expansion.mx/tecnologia/2021/06/09/ciberdelincuentes-filtran-documentos-internos-de-la-loteria-nacional.

6 RIQUELME, Rodrigo, *Lotería Nacional confirma sustracción de información por delincuentes internacionales,* (3 de octubre de 2022), https://www.eleconomista.com.mx/politica/Loteria-Nacional-confir-ma-sustraccion-de-informacion-por-delincuentes-internacionales-20210601-0039.html.

> El hackeo de 6 terabytes de información clasificada, incluidos miles de correos electrónicos de la Secretaría de la Defensa Nacional (Sedena), ha dejado en evidencia la gran vulnerabilidad del gobierno de México y el país en general en temas de ciberseguridad derivada de una insuficiente inversión y planeación, advirtieron expertos.
>
> Este viernes, el presidente Andrés Manuel López Obrador confirmó una filtración masiva de documentos reservados de la Secretaría de la Defensa Nacional (Sedena) que, entre otras cosas, sacó a la luz partes médicos que dan detalles no revelados de los padecimientos coronarios del mandatario.[7]

La información que se extrajo de las bases de datos digitales de la Secretaría de la Defensa Nacional hace evidente el peligro que representan los ciberataques y el riesgo que implican en el contexto de la seguridad nacional.

De lo anterior, se puede advertir la necesidad de realizar las acciones pertinentes que tiendan a disminuir los riesgos de que, en el futuro, el Estado mexicano sea nuevamente víctima de un ciberataque.

Es por esta razón que, en mi carácter de presidente de la Comisión de Ciencia, Tecnología e Innovación, celebro la buena disposición del Centro de Estudios de Derecho e Investigaciones Parlamentarias de la Cámara de Diputados (CEDIP) que, a través de su titular, el doctor Juan Carlos Cervantes Gómez, y su equipo de investigadores, han aportado elementos adicionales para el estudio de las buenas prácticas en otras latitudes que también buscan la forma de combatir los ciberataques, resguardando el Estado de derecho y el respeto a los derechos humanos de todas las personas usuarias de las Tecnologías de la Información.

En la presente investigación, elaborada por los maestros Gustavo Eduardo Marín Hernández e Irving Ilie Gómez Lara, se puede contar con una aproximación sobre la ciberseguridad en términos conceptuales, así como la situación que guarda el marco jurídico mexicano en la materia. Así mismo, se cuenta con una comparativa muy interesante sobre cómo otros países han atendido este trascendente tema para la geopolítica internacional, siendo objeto de estudio Estados Unidos, Ar-

7 FORBES, *Hackeo masivo a Sedena evidencia vulnerabilidad de ciberseguridad; así fue el ataque,* (3 de octubre de 2022), https://www.forbes.com.mx/hackeo-masivo-a-sedena-evidencia-vulnerabilidad-de-ciberseguridad-asi-fue-el-ataque.

gentina, Brasil, Estonia y Singapur, los cuales atienden la ciberseguridad con similitudes y diferencias, tal como será posible dilucidar en la lectura de la investigación que nos ocupa.

Sea esta investigación un apoyo formal que permita, a todos los que intervenimos en la búsqueda de soluciones en materia de ciberseguridad, dilucidar los diferentes caminos que tenemos como país para dar respuesta a una necesidad inminente, construir un marco jurídico nacional que sea capaz de construir el andamiaje hacia el fortalecimiento institucional del Estado en materia de ciberseguridad.

Diputado Javier López Casarín
Presidente de la *Comisión de Ciencia, Tecnología e Innovación* de la LXV Legislatura de la Cámara de Diputados del Honorable Congreso de la Unión

Octubre de 2022

INTRODUCCIÓN

Nos encontramos en una era donde las comunicaciones y las operaciones económico-financieras se han expandido exponencialmente en el espacio cibernético-digital gracias a las tecnologías de la información y la comunicación (TIC). Esto implica un incremento en el número de personas usuarias, lo cual conlleva un aumento de riesgos, ataques y amenazas informáticas con formas y conductas cada vez más sofisticadas que aprovechan los avances y las vulnerabilidades tecnológicas. Algunos ejemplos son el robo de información y de identidad, fraudes y robos financieros, *phishing*, fuga de información sensible, secuestro de sistemas informáticos, entre otros. Esto resulta en una realidad cambiante que conviene ser entendida como un asunto de seguridad nacional y desde un enfoque donde los nuevos escenarios polemológicos (violencia cibernética, violencia cognitiva y guerras híbridas) se traduzcan en acciones legislativas.

A través de las redes y tecnologías digitales, cada vez más personas, instituciones privadas y públicas tanto en México como en el mundo se han convertido en víctimas de ataques a sus derechos y patrimonios, lo que pone en riesgo la estabilidad del orden interno y externo de los Estados y de las relaciones internacionales. Se han observado algunas conductas que tienen al internet como objetivo de ataque, por ejemplo, cuando se *hackea* un sitio web oficial con fines expresivos, y otras que lo usan como medio para cometer delitos como robos, fraudes, trata de personas, tráfico de armas o narcóticos, entre muchas otras actividades ilícitas.

Los efectos nocivos de las vulnerabilidades cibernéticas son múltiples y de naturaleza variada. Por ejemplo, en la Estrategia Nacional de Ciberseguridad de 2017 del Gobierno de México, se estipuló que los *riesgos y amenazas en el ciberespacio pueden constituir un posible ataque a la dignidad humana, a la integridad de las personas, a la credibilidad, reputación y patrimonio de las empresas y las instituciones públicas; así como afectaciones a la seguridad pública o incluso la seguridad nacional*.[1]

No obstante, las conductas relacionadas a la cibercriminalidad aún no han sido tipificadas suficientemente en la legislación penal mexi-

1 GOBIERNO DE MÉXICO, *Estrategia Nacional de Ciberseguridad*, México, 2017, p. 3, https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf.

cana, tales como el robo de identidad o el *grooming* (acoso sexual a menores por medio de redes sociales o plataformas digitales). Además, debido a que los ataques pueden tener un origen transnacional, la identificación y sanción de las personas infractoras se vuelve improbable e ineficaz. Una de las posibles causas es la ausencia de un marco jurídico actualizado que facilite perseguir y evitar estos actos ilícitos que afectan derechos patrimoniales, personales y digitales.

Por lo anterior, el Poder Legislativo puede contribuir a evitar el impacto pernicioso de los ciberataques en la sociedad e instituciones mexicanas. Por ello, esta obra tiene por objetivo elaborar un mapa de ruta consecuente y útil acerca de las formas en que la ciberseguridad puede entenderse como fenómeno de análisis, al tiempo que se construyen vectores de comprensión de sus problemáticas.

Es decir, se busca proveer, a partir del entendimiento de la realidad mundial, táctica y nacional, así como del análisis de los marcos normativos de otros países, a las y los legisladores de información situacional, analítica, estratégica y jurídica. Esto con el fin de colaborar en el diseño de una normativa sobre ciberseguridad adecuada al contexto mexicano y a los tiempos actuales, que proteja los derechos humanos de todas las personas y la estabilidad de las instituciones.

Para lograrlo, se ha elaborado un marco conceptual, así como un diagnóstico de los antecedentes y del orden jurídico vigente sobre ciberseguridad en México. Posteriormente, se analizan algunos órdenes jurídicos extranjeros que han adoptado protocolos para prevenir riesgos, han definido tipos penales específicos y han creado organismos nacionales en materia de seguridad cibernética, entre otras medidas.

El hecho de que la ciberseguridad sea un fenómeno cambiante, complejo y transversal a la realidad social e individual, significa que se trata de un asunto de alto interés para cualquier Estado. Por ello, se ha seguido un enfoque y análisis multifactorial con base en la siguiente hipótesis: si el Estado mexicano contara con una regulación moderna sobre ciberseguridad, que atienda el problema multidimensionalmente y se encuentre tanto a la altura del contexto social como de los avances tecnológicos actuales, se podrían contrarrestar eficazmente los efectos negativos de los ataques cibernéticos a instituciones públicas, privadas y a la sociedad en general.

Debido al carácter transversal de los fenómenos cibernéticos, los hallazgos de esta investigación podrían justificar la conveniencia de ejercer mecanismos de control por parte de la Cámara de Diputados sobre otros poderes del Estado y, por supuesto, la función legislativa para actualizar el marco normativo.

La justificación de esta obra tiene un doble carácter. Primero, fáctico, porque atiende un problema que aqueja a personas e instituciones tanto públicas como privadas, siendo que *el riesgo de ciberataques suscita preocupación en varios ámbitos, entre ellos: pérdida de datos, costos, daños a la organización y la reputación ante la visión de sus clientes y socios*.[2] Segundo, jurídico, debido a la necesidad de un marco normativo actualizado que establezca los procedimientos y las autoridades especializados en este fenómeno nacional, internacional y transnacional.

Respecto a la justificación jurídica, diversas iniciativas sobre ciberseguridad y ciberdelincuencia se han presentado en el Congreso de la Unión durante los últimos años. Sin embargo, ninguna ha concluido su proceso legislativo. Por tal motivo, este libro representa un insumo de información oportuna y de calidad para analizar esas iniciativas y elaborar nuevas propuestas legislativas, lo que podría resultar en un marco normativo eficaz que facilite contrarrestar los efectos de los ataques cibernéticos y construir capacidades de investigación y desarrollo en la materia.

En general, la base metodológica aquí seguida se caracteriza por ser una perspectiva interdisciplinaria con un horizonte conceptual dirigido hacia el problema de la ciberseguridad y su vínculo con las actividades legislativas, entendiendo que el problema y el objeto de estudio son cuestiones estratégicas. Por ello, su construcción multidimensional basada en evidencia empírica en *pro* de convertirse en propuesta legislativa conecta los eslabones del ordenamiento internacional con factores económicos, sociológicos y epistemológicos para esclarecer las líneas de tensión existentes entre la realidad multifactorial y la *episteme* jurídica. Por esta razón, la sistematización documental del *nomotopo*[3] es lo que guía y construye este análisis.

---

2 ASOCIACIÓN MEXICANA DE CIBERSEGURIDAD (AMECI), *Ciberseguridad y protección de datos en México,* (26 de abril de 2022), https://www.ameci.org.

3 *Grosso modo*, el *nomotopo* se refiere a aquello que Hegel denominó como espíritu objetivo, es decir, el campo de acción donde opera la arquitectura normativa de la autoridad que pre-ordena a los individuos y se transmite de generación en generación. SLOTERDIJK, Peter, *Esferas III. Esferología plural*, Madrid, Siruela, 2009, pp. 357-374.

En particular, se emplea el método hermenéutico para analizar disposiciones normativas vigentes e iniciativas legislativas en materia de ciberseguridad, así como el sistemático y el comparado para estudiar conjuntos normativos de otros países e identificar sus principales semejanzas y diferencias, con la intención de adaptarlas a la legislación y prácticas mexicanas.

Finalmente, los autores agradecen los valiosos aportes de las y los participantes de las mesas de trabajo sobre ciberseguridad organizadas por la Comisión de Ciencia, Tecnología e Innovación de la LXV Legislatura de la H. Cámara de Diputados, presidida por el diputado Javier Joaquín López Casarín, al Dr. Marcial Manuel Cruz Vázquez por sus atinados comentarios, y al Lic. Edgar Esteban Téllez Alonso por colaborar en la recopilación de información.

CAPÍTULO PRIMERO
ANTECEDENTES DE LA CIBERSEGURIDAD EN MÉXICO

I. CONTEXTO DE LA CIBERSEGURIDAD EN MÉXICO

Antes de desarrollar el presente capítulo, se debe señalar que el estudio del caso mexicano requiere un capítulo propio, pues se usará como caso de contraste frente a los demás países estudiados. Esto debido a que se busca argumentar la necesidad de reformar la normativa vigente o emitir nueva, especialmente algunas leyes, cuestión que cae en el ámbito competencial del Congreso de la Unión en general, y de la Cámara de Diputados en particular.

Pese a que la digitalización abarca cada vez más ámbitos de la realidad, el Estado y la sociedad mexicanos muestran cierto rezago técnico y jurídico respecto a la seguridad de las TIC en comparación con otras naciones vanguardistas en el desarrollo tecnológico.

En 2020, el 78.3% de la población urbana era usuaria del servicio de internet, mientras que la rural era del 50.4%. Los tres principales medios empleados fueron el celular inteligente (*smartphone*) con 96%, la computadora portátil con 33.7% y el televisor con acceso a internet (22.2%). Las principales actividades realizadas por los usuarios fueron la comunicación (93.8%), la búsqueda de información (91%) y el acceso a redes sociales (89%).[4]

A pesar del uso prevalente, la dimensión de la ciberseguridad a nivel jurídico, político, económico, social, securitario y educativo es sumamente difusa. Fue hasta la última década del siglo XX que el Estado mexicano comenzó a incursionar en la digitalización, momento en el que la importancia de la ciberseguridad se volvió explícita.[5]

Durante la pandemia por COVID-19, México fue uno de los países latinoamericanos que más se vio afectado por ciberataques.[6] En 2021,

4 INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA, *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2020* [base de datos], México, junio de 2021, https://www.inegi.org.mx/programas/dutih/2020. La información y los datos presentados en esta obra corresponden al segundo trimestre de 2022, es decir, hasta junio de 2022.

5 Véase GUEL, Juan Carlos, *Panorama de la ciberseguridad en México*, Conferencia en ANUIES-TIC, Universidad Autónoma de Nuevo León, 2019, https://www.youtube.com/watch?v=lh5tOnc1or4&ab_channel=Comit%C3%A9ANUIES-TIC.

6 *Cfr*. GUARNEROS OLMOS, Fernando, *En un trimestre, México registró 80,000 millones de intentos de ciberataques*,

Brasil lideró *la región con más de 1,390 intentos de infección por minuto, seguido de México (299 por minuto)*.[7] Por poner un caso concreto, en junio de 2021 el portal de la Lotería Nacional sufrió un ciberataque mediante el cual fue sustraída información.[8]

Poco antes, en abril de 2018, fue realizado uno de los más grandes ciberataques a instituciones bancarias, teniendo como resultado pérdidas millonarias para nuestro país.[9] Dentro del conjunto de casos referentes a las intrusiones cibernéticas, destaca el espionaje realizado con el *software Pegasus* de la firma israelí NSO Group en contra de periodistas, activistas y funcionarios públicos, lo que evidenció la injerencia del Gobierno mexicano en este tipo de actividades.[10]

También algunas instituciones gubernamentales han sido blancos de ciberataques, tales como Petróleos Mexicanos (PEMEX), la Secretaría de Economía, el Instituto Nacional de Migración (INM), el Banco de México (BANXICO), el Servicio de Administración Tributaria (SAT), entre otras.[11]

Debido a estos ataques, se han creado Centros de Respuesta a Incidentes Informáticos (CERT) públicos y privados, tales como CERT-MX de la Guardia Nacional, UNAM CERT para resguardar la red de la universidad nacional, CERT NETRIX para las empresas, organizaciones y gobierno, entre otros.[12]

Expansión, 11 de mayo de 2022, https://expansion.mx/tecnologia/2022/05/11/en-un-trimestre-mexico-registro-80-000-millones-de-intentos-de-ciberataques; RIQUELME, Rodrigo, *Tres de cada cuatro empresas mexicanas fueron víctimas de ransomware: Sophos*, El Economista, 11 de mayo de 2022, https://www.eleconomista.com.mx/tecnologia/Tres-de-cada-cuatro-empresas-mexicanas-fueron-victimas-de-ransomware-Sophos-20220511-0060.html; GÓMEZ FLORES, Laura, *México, segundo lugar mundial en ciberataques: FEM*, La Jornada, 4 de octubre de 2021, https://www.jornada.com.mx/notas/2021/10/04/sociedad/mexico-segundo-lugar-mundial-en-ciberataques-fem; FORBES, *México, primer lugar en ciberataques en Latinoamérica*, 30 de noviembre de 2021, https://www.forbes.com.mx/negocios-mexico-primer-lugar-en-ciberataques-en-latinoamerica.

7 DIAZGRANADOS, Hernán, *Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021*, Kaspersky Daily, 31 de agosto de 2021, https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021.

8 FORBES STAFF, *Lotería Nacional confirma que sí sufrió un ciberataque*, Forbes, 1 de junio de 2021, https://www.forbes.com.mx/loteria-nacional-confirma-que-si-sufrio-un-ciberataque.

9 BBC MUNDO, *México: el ciberataque "sin precedentes" a los bancos del país que causó pérdidas millonarias*, 15 de mayo de 2018, https://www.bbc.com/mundo/noticias-america-latina-44130887.

10 SANTOS CID, Alejandro, *El espionaje del 'caso Pegasus' en México se cobra su primer detenido*, El País, 8 de noviembre de 2021, https://elpais.com/mexico/2021-11-09/el-espionaje-del-caso-pegasus-en-mexico-se-cobra-su-primer-detenido.html.

11 LANDEROS, Emma, *México: ciberataques a las dependencias de gobierno*, Newsweek, 21 de julio de 2021, https://newsweekespanol.com/2021/07/mexico-ciberataques-dependencias-gobierno.

12 CSIRTS EN MÉXICO, *Lista de centros de respuesta ante incidentes informáticos*, (19 de mayo de 2022), https://csirt.com.mx.

Por su parte, la Auditoría Superior de la Federación (ASF) ha llevado a cabo auditorías de cumplimiento para supervisar la seguridad de los sistemas informáticos. Por ejemplo, en 2020 identificó deficiencias en la administración y operación de los controles de ciberseguridad para la infraestructura de *hardware* y *software* de la Secretaría de Hacienda y Crédito Público (SHCP), y que no contaba con un Análisis de Impacto al Negocio (BIA, por sus siglas en inglés).[13] Igualmente, reveló que la Secretaría de la Defensa Nacional (SEDENA) presentó brechas en ciberseguridad, tales como la carencia de controles contra *malware* para correos electrónicos y navegador web, y para la recuperación de datos, así como la ausencia de un procedimiento de respuesta a incidentes cibernéticos.[14]

En el aspecto educativo, el Instituto Federal de Telecomunicaciones (IFT) ha desarrollado un portal con información sobre ciberseguridad para niñas, niños, adolescentes, padres de familia, mujeres y empresas.[15] Por su parte, la Secretaría de Infraestructura, Comunicaciones y Transportes (SICT) elaboró una guía de ciberseguridad para que sus trabajadores pudieran realizar sus labores a distancia de manera segura mediante los dispositivos personales.[16]

A pesar de la insuficiencia del marco jurídico actual, el Estado mexicano cuenta con algunos órganos encargados de prevenir, investigar, y reaccionar ante ciberataques. Por ejemplo, la Guardia Nacional realiza investigaciones cibernéticas a través del Centro de Respuesta a Incidentes Cibernéticos dependiente de la Dirección General Científica, cuya misión consiste en brindar servicios de apoyo y respuesta a incidentes cibernéticos que afectan a las instituciones con infraestructuras de información críticas, entre los cuales se incluye la identificación de amenazas y *modus operandi* de la ciberdelincuencia para alertar a la ciudadanía mediante la gestión de incidentes.

---

13 AUDITORÍA SUPERIOR DE LA FEDERACIÓN, *Auditoría de TIC a la Secretaría de Hacienda y Crédito Público*: *2019-0-06100-20-0015-2020*, México, 2020, http://www.asf.gob.mx/Trans/Informes/IR2019b/Documentos/Auditorias/2019_0015_a.pdf.

14 RÍOS, Ailyn, *Reprueba Sedena en ciberseguridad*, Reforma, Ciudad de México, 26 de febrero de 2022, https://www.reforma.com/reprueba-sedena-en-ciberseguridad.

15 INSTITUTO FEDERAL DE TELECOMUNICACIONES, *Ciberseguridad*, (8 de mayo de 2022), https://ciberseguridad.ift.org.mx.

16 SECRETARÍA DE COMUNICACIONES Y TRANSPORTES, *Guía de Ciberseguridad para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo al teletrabajo*, (8 de mayo de 2022), https://www.gob.mx/cms/uploads/attachment/file/555226/Gui_a_de_Ciberseguridad_SCT_VF.pdf.

Además, dicho centro funge como el único punto de contacto y coordinación dentro y fuera del territorio nacional que realiza investigación forense digital y análisis técnico policial en apoyo a la Fiscalía General de la República (FGR).[17] Aunado a ello, ha desarrollado un *Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos*,[18] que busca gestionar de forma coordinada los incidentes cibernéticos de mayor criticidad e impacto en activos esenciales de información mediante la aplicación de procedimientos y mejores prácticas para contener y mitigar las ciberamenazas, para así mantener los riesgos en niveles aceptables. También ha elaborado guías de ciberseguridad como el *Manual Básico de Ciberseguridad para la Micro, Pequeña y Mediana Empresa*,[19] un boletín de vulnerabilidades informáticas, aunque no siempre se encuentra actualizado, y emite alertas de seguridad informática.[20]

Por su parte, la Secretaría de Seguridad y Protección Ciudadana (SSPC) ha implementado los operativos *Ciberguardián* y *Salvación* para la prevención y combate de los ciberdelitos, mediante los cuales se ha puesto énfasis en los casos de trata de personas y pornografía infantil. Así, ha atendido 20,213 reportes ciudadanos en materia de ciberseguridad, gestionado la desactivación de 5,775 sitios *web* apócrifos que usurpaban la identidad de diversas instituciones, y difundido la Guía de Ciberseguridad o *CiberGuía*, que es un material informativo dirigido a la ciudadanía con el objetivo de prevenir ciberdelitos.[21]

A nivel estatal, y a partir del Modelo Homologado de Unidades de Policía Cibernética, diversas secretarías de seguridad, así como algunas fiscalías, cuentan con unidades de policía o de investigación cibernética, respectivamente.[22] No obstante, su operatividad y efectividad son varia-

17 GOBIERNO DE MÉXICO, *CERT-MX*, (15 de mayo de 2022), https://www.gob.mx/gncertmx?tab=%C2%BFQu%C3%A9%20es%20CERT-MX.

18 PRESIDENCIA DE LA REPÚBLICA *et al*., *Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos*, México, octubre 2021, https://www.gob.mx/gncertmx/documentos/94081.

19 CERT-MX, *Manual Básico de Ciberseguridad para la Micro, Pequeña y Mediana Empresa*, México, Guardia Nacional, 2018, https://www.gob.mx/cms/uploads/attachment/file/682364/MANUAL_B_SICO_CIBERSEGURIDAD_MIPYMES_2021_11_18.pdf.

20 GOBIERNO DE MÉXICO, *Alertas de seguridad informática*, (15 de mayo de 2022), https://www.gob.mx/gncertmx?tab=alertas.

21 SECRETARÍA DE SEGURIDAD Y PROTECCIÓN CIUDADANA, *Tercer informe de la Estrategia Nacional de Seguridad Pública*, México, abril 2022, pp. 161-163, https://seguridad.sspc.gob.mx/uploads/documentos/146/3er-inensp.pdf.

22 INSTITUTO FEDERAL DE TELECOMUNICACIONES, *Ciberseguridad, Reporte ciudadano*, (15 de mayo de 2022), https://ciberseguridad.ift.org.mx/reporte_ciudadano.php.

bles y dependen tanto del desarrollo del marco jurídico que regula su actuación, como de los recursos y capacidades institucionales disponibles.

En el ámbito castrense, la Unidad de Ciberseguridad de la Secretaría de Marina elaboró la Estrategia Institucional para el Ciberespacio 2021-2024,[23] el Glosario de Términos SEDENA-MARINA en Materia de Seguridad en el Ciberespacio[24] y una Cartilla de Ciberseguridad para los funcionarios de la propia dependencia.[25]

Por su parte, la Cámara de Diputados del Congreso de la Unión adoptó durante la pandemia de COVID-19 el *Reglamento que la Cámara de Diputados aplicará durante las situaciones de emergencia y la contingencia sanitaria en las sesiones ordinarias y extraordinarias durante la LXV Legislatura*, el cual prevé la adopción de medidas de ciberseguridad para el uso de la plataforma digital que los diputados y las diputadas utilizan para asistir y votar de manera telemática.

A pesar de la atención que han prestado los sectores público y privado para atender el problema, *una de las razones que hace a México un blanco para los ataques cibernéticos es la falta de un marco regulatorio sólido e innovador*.[26] De acuerdo con el Banco Interamericano de Desarrollo, nuestro país no cuenta con una ley dedicada al delito cibernético, y aunque el Código Penal Federal prevé el delito informático, *las disposiciones son limitadas y dejan varias lagunas, lo que dificulta la lucha contra el cibercrimen*.[27] Lo anterior evidencia la necesidad de actualizar el marco regulatorio para contribuir a contrarrestar sus efectos nocivos.

Por lo anterior, el Poder Ejecutivo federal publicó en 2017 la Estrategia Nacional de Ciberseguridad (ENC), documento donde se plasmó la visión del Estado mexicano sobre este tema. La cuestión es que, debido al cambio de gobierno, ha dejado de ser aplicable. Sin embargo, allí se da cuenta de que, para crear un diseño, planeación y despliegue institucional que combata efectivamente a la ciberdelincuencia, es menester especificar las

23 SECRETARÍA DE MARINA, *Estrategia Institucional para el Ciberespacio 2021-2024*, México, 2021, https://www.gob.mx/cms/uploads/attachment/file/661788/Estrategia_Institucional_Ciberespacio_SM.pdf.

24 GOBIERNO DE MÉXICO *et al*., *Glosario de Términos SEDENA - MARINA en Materia de Seguridad en el Ciberespacio*, México, junio 2021, https://www.gob.mx/cms/uploads/attachment/file/661790/Glosario_de_Terminos_SD-_SM_compressed.pdf.

25 SECRETARÍA DE MARINA, *Cartilla de Ciberseguridad de la Secretaría de Marina*, México, 2021, https://www.gob.mx/cms/uploads/attachment/file/677122/Cartilla_Ciberseguridad_final_111021.pdf.

26 METABASE Q, *El Estado de la Ciberseguridad en México*, 2021, p. 7.

27 BANCO INTERAMERICANO DE DESARROLLO, *Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte Ciberseguridad 2020*, 2021, p. 125.

dimensiones, los tipos de riesgos y amenazas cibernéticas, los mecanismos de cooperación internacional para cerrar brechas de vulnerabilidad en el ciberespacio, capacitar personal especializado y generar colaboraciones interinstitucionales con los diversos sectores de la sociedad, todo ello bajo la orientación, guía y supervisión de un ente institucional que coordine las actividades mediante planes, programas y protocolos.

Por todo lo anterior, la ENC tiene como objetivo general *identificar y establecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano*.[28] También cuenta con cinco objetivos estratégicos, tres principios rectores y ocho ejes transversales,[29] articulados desde un abordaje integral, colaborativo, holístico y transversal.

En el documento se señala la relación de cooperación que guarda el Estado mexicano con organismos internacionales,[30] así como los esfuerzos de estos últimos para categorizar, especificar, analizar y construir alternativas de solución respecto de la ciberdelincuencia y los problemas existentes o que pueden suscitarse en el ciberespacio. Esta cooperación permite establecer las rutas que han seguido otras naciones, conocer los problemas a los que se han enfrentado y las mejores prácticas internacionales.

La ENC destaca la necesidad de contar con una agencia de ciberseguridad nacional coordinadora, la importancia de redefinir el marco jurídico para la ciberseguridad que armonice las legislaciones federales y estatales, de manera que se garantice la protección de datos personales y se estimule el intercambio de información; el imperativo de proteger las infraestructuras críticas; el fortalecimiento de una ciberresiliencia bajo un enfoque de gestión de riesgo, y el desarrollo de habilidades y competencias para el nuevo ecosistema digital.[31]

28 GOBIERNO DE MÉXICO, *Estrategia Nacional de Ciberseguridad... cit.*, p. 16.

29 Objetivos estratégicos: sociedad y derechos, economía e innovación, instituciones públicas, seguridad pública y seguridad nacional. Principios rectores: perspectiva de derechos humanos, enfoque basado en gestión de riesgos, colaboración multidisciplinaria y de múltiples actores. Ejes transversales: cultura de ciberseguridad, desarrollo de capacidades, coordinación y colaboración, investigación, desarrollo e innovación TIC, estándares y criterios técnicos, infraestructuras críticas, marco jurídico y autorregulación, medición y seguimiento. *Ibidem,* p. 5.

30 Donde destaca la Organización de las Naciones Unidas, la Organización de Estados Americanos, el Foro Económico Mundial o la Alianza del Pacífico, entre muchos otros.

31 GOBIERNO DE MÉXICO, *Estrategia Nacional de Ciberseguridad... cit.*, p. 14.

Los objetivos definidos se traducen en acciones que desde el Poder Legislativo es menester realizar. En la esfera social y económica, lo que se busca es que los ciudadanos puedan realizar sus actividades digitales con total libertad y responsabilidad, en un entorno de respeto de los derechos humanos, la vida privada y la protección de datos personales; que se protejan los sectores productivos, se promueva el desarrollo y la innovación tecnológica, y se impulse al sector industrial de ciberseguridad.

Asimismo, se debe proteger la información y los sistemas informáticos de las instituciones públicas para garantizar su óptimo funcionamiento. En términos de seguridad pública, se pretende *incrementar las capacidades para la prevención e investigación de conductas delictivas en el ciberespacio que afectan a las personas y su patrimonio,* y en lo referente a la seguridad nacional lo que se busca es desarrollar *capacidades para prevenir riesgos y amenazas en el ciberespacio que puedan alterar la independencia, integridad y soberanía nacional, afectando el desarrollo y los intereses nacionales*.[32]

Ahora bien, dentro de los nueve objetivos postulados en la Estrategia Digital Nacional derivada del Plan Nacional de Desarrollo 2019-2024, un pilar primordial es la promoción de las TIC para colaborar y compartir recursos interinstitucionalmente, intercambiar información y conocimientos, impulsar la transparencia y el seguimiento en la asignación de recursos públicos, homologar protocolos, fortalecer la seguridad informática y la coordinación entre las autoridades e instituciones tanto públicas como privadas, además de apoyar en la definición e implementación de los programas y proyectos prioritarios.[33] Finalmente, si bien los ciberataques y los ciberdelitos han estado presentes desde hace más de una década en México, durante la pandemia de COVID-19 se incrementaron exponencialmente. De ahí que diversos grupos parlamentarios de las LXIV y LXV Legislaturas del Congreso de la Unión incorporaran este problema público en sus agendas legislativas. En consecuencia, diversas iniciativas sobre la ciberseguridad y protección de sistemas informáticos fueron presentadas. Sin embargo, ninguna se ha convertido en derecho vigente.

32 *Ibidem*, p. 18.

33 PRESIDENCIA DE LA REPÚBLICA, *Acuerdo por el que se expide la Estrategia Digital Nacional 2021-2024*, Diario Oficial de la Federación, 6 de septiembre de 2021, https://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021.

II. INICIATIVAS SOBRE CIBERSEGURIDAD PRESENTADAS EN LAS LXIV Y LXV LEGISLATURAS DEL CONGRESO DE LA UNIÓN

Al momento de concluir esta investigación, se han presentado 14 iniciativas,[34] siete en la Cámara de Diputados y el resto en el Senado de la República. Dos de ellas proponían reformar el artículo 73 constitucional; seis, modificar varios ordenamientos (Código Penal Federal, Ley General del Sistema Nacional de Seguridad Pública, Ley de Seguridad Nacional, Ley Federal de Austeridad Republicana, Ley de la Fiscalía General de la República); otra, elaborar una nueva ley; tres plantearon reformar y expedir nuevos ordenamientos (como una ley general de ciberseguridad o de seguridad informática), y dos más, conmemorar un día y un mes nacional de la ciberseguridad. Cabe mencionar que estas últimas dos han sido las únicas dictaminadas.

En síntesis, el conjunto de aquellas propuestas ha planteado facultar constitucionalmente al Congreso de la Unión para legislar en la materia, tipificar penalmente algunas conductas, crear órganos como la Agencia Nacional de Ciberseguridad, la Comisión Nacional de Ciberseguridad en el marco del Sistema Nacional de Seguridad Pública, una fiscalía especializada en materia de ciberseguridad y una Universidad de Tecnologías de la Información, Comunicaciones e Innovación. Dichos planteamientos coadyuvarían a establecer las bases de coordinación para que las autoridades competentes en todos los órdenes de gobierno puedan hacer frente a los ciberataques y reponerse de ellos, evitando así situaciones que pudieran resultar catastróficas para la nación.

Algunos planteamientos comunes que se desprenden de estas propuestas son: a) crear un organismo coordinador, b) formular una estrategia nacional de ciberseguridad, c) tipificar algunos delitos cibernéticos, d) considerar los ciberataques como afectaciones a la seguridad nacional y e) fomentar la educación para navegar de manera segura en internet.[35] A continuación se presenta un cuadro que resume las iniciativas.

34 Algunas iniciativas relativas a la materia de ciberseguridad fueron presentadas antes de que la LXIV legislatura del Congreso de la Unión entrara en funciones. No obstante, en el presente estudio solo se consideran las presentadas durante esta y la LXV legislatura.

35 *Cfr*. METABASE Q, *Comparativo de Iniciativas en Ciberseguridad*, México, 2020, https://www.metabaseq.com/recursos/comparativo-vinculacion-instutucional.

Tabla 1. Iniciativas sobre ciberseguridad presentadas durante las legislaturas LXIV y LXV del Congreso de la Unión

	Iniciativa y fecha de presentación	Objeto	Iniciante	Estatus
1	Iniciativa con proyecto de decreto que declara el mes de octubre como *El Mes Nacional de la Ciberseguridad*. 23 de octubre de 2018	• Declarar el mes de octubre de cada año como el *Mes Nacional de la Ciberseguridad*.	Sen. Alejandra Lagunes Soto Ruíz	Pendiente en comisión(es) de cámara revisora 5 de noviembre de 2019
2	Iniciativa con Proyecto de decreto por el que se adiciona la fracción XIV al artículo 5 de la Ley de Seguridad Nacional. 4 de noviembre de 2018	• Establecer que son amenazas a la seguridad nacional los actos que vulneren la ciberseguridad y que lesionen a los habitantes y a las instituciones.	Sen. José Ramón Enríquez Herrera	Pendiente en comisión(es) de cámara de origen
3	Iniciativa con proyecto de decreto por el que se reforman y derogan diversas disposiciones del Título Noveno, Libro Segundo del Código Penal Federal y se expide la Ley de Seguridad Informática. 27 de marzo de 2019	• Reformar y derogar disposiciones del Código Penal Federal relativas a ciberdelitos o delitos cometidos por medio de sistemas informáticos. • Crear una ley especializada en materia de ciberdelitos. • Establecer las bases de integración y acción para preservar la seguridad informática nacional.	Sen. Jesús Lucía Trasviña Waldenrath	Pendiente en comisión(es) de cámara de origen
4	Iniciativa con aval del grupo parlamentario que contiene el proyecto de decreto que reforma y adiciona diversas disposiciones del Código Penal Federal, de la Ley General del Sistema Nacional de Seguridad Pública, de la Ley de Seguridad Nacional; y expide la Ley General de Ciberseguridad. 2 de septiembre de 2019	• Establecer las bases de integración y acción coordinada de las instituciones y autoridades encargadas de preservar la ciberseguridad en las instituciones del Estado y la sociedad.	Sen. Miguel Ángel Mancera Espinosa	Pendiente en comisión(es) de cámara de origen
5	Iniciativa que reforma el artículo 73 de la Constitución Política de los Estados Unidos Mexicanos. 29 de octubre de 2019	• Facultar al Congreso de la Unión para legislar en materia de ciberseguridad.	Dip. Javier Salinas Narváez	Pendiente en comisión(es) de cámara de origen

	Iniciativa y fecha de presentación	Objeto	Iniciante	Estatus
6	Iniciativa que adiciona los artículos 5° y 6° de la Ley de Seguridad Nacional. 8 de enero de 2020	• Establecer mecanismos legales en materia de ciberseguridad como parte de la Estrategia Digital Nacional.	Dip. María Eugenia Hernández Pérez	Pendiente en comisión(es) de cámara de origen
7	Iniciativa con proyecto de decreto que declara el 23 de noviembre de cada año como *Día Nacional de la Ciberseguridad*. 12 de agosto de 2020	• Declarar el 23 de noviembre de cada año, como *Día Nacional de la Ciberseguridad*.	Dip. María Eugenia Hernández Pérez	Pendiente en comisión(es) de cámara de origen
8	Iniciativa con proyecto de decreto por el que se expide la Ley que crea la Universidad de Tecnologías de la Información, Comunicaciones e Innovación. 12 de agosto de 2020	• Crear el marco regulatorio para la universidad encargada de impartir educación superior a nivel licenciatura, especialidad, maestría, doctorado y opciones terminales, en materia de desarrollo tecnológico e innovación en el país, como organismo público con personalidad jurídica, patrimonio propio, autonomía técnica y de gestión.	Dip. Carlos Iván Ayala Bobadilla	Pendiente en comisión(es) de cámara de origen
9	Iniciativa que reforma el artículo 16 de la Ley Federal de Austeridad Republicana. 2 de marzo de 2021	• Establecer el principio de austeridad en la adquisición y arrendamiento de equipo y servicios de cómputo que se usan para garantizar la operación de programas sociales y labores de ciberseguridad.	Dip. José Salvador Rosas Quintanilla	Pendiente en comisión(es) de cámara de origen
10	Iniciativa con proyecto de decreto por el que se reforman y adicionan diversas disposiciones del Código Penal Federal, en materia de delitos cibernéticos. 25 de marzo de 2021	• Prevenir y sancionar los delitos cibernéticos.	Sen. Gustavo Enrique Madero Muñoz	Pendiente en comisión(es) de cámara de origen
11	Iniciativa con Proyecto de Decreto por el que se expide la Ley General de Ciberseguridad y se derogan diversas disposiciones del Código Penal Federal. 6 de abril de 2021	• Regular la integración, organización y funcionamiento de la Comisión Nacional de Ciberseguridad y de la Agencia Nacional de Ciberseguridad.	Sen. Jesús Lucía Trasviña Waldenrath	Pendiente en comisión(es) de cámara de origen

	Iniciativa y fecha de presentación	Objeto	Iniciante	Estatus
12	Iniciativa con proyecto de decreto por el que se adiciona la fracción XXI-II Ter del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, en materia de ciberdelincuencia. 23 de septiembre de 2021	• Facultar al Congreso de la Unión para expedir las normas de carácter general en materia de ciberdelincuencia y cibercrimen, que contengan mecanismos de coordinación entre autoridades de los tres órdenes de gobierno y el diseño de una estrategia nacional de inteligencia cibernética y policial.	Dip. Juanita Guerra Mena	Pendiente en comisión(es) de cámara de origen
13	Que reforma diversos artículos de la Ley General del Sistema Nacional de Seguridad Pública. 14 de octubre de 2021	• Regular la integración, organización y funcionamiento de la Comisión Nacional de Ciberseguridad. • Definir que los órganos de ciberseguridad son la Comisión Nacional de Ciberseguridad (CNC) y las instituciones de la federación, entidades federativas y municipios que realicen funciones de ciberseguridad. • Establecer que la Comisión Nacional de Ciberseguridad estará integrada por la o el titular de la SSPC, SEDENA, SEMAR, SEGOB, SRE, SCT, SENER, SHCP, SE, SEP, FGR, y las y los gobernadores de los estados. • Señalar que la CNC planteará la Estrategia Nacional de Ciberseguridad y el Programa Nacional de Ciberseguridad procurando su ejecución y evaluación anual.	Sen. Jesús Lucía Trasviña Waldenrath	Pendiente en comisión(es) de Cámara de origen
14	Iniciativa con proyecto de decreto por el que se reforman los artículos 11 y 13 de la Ley de la Fiscalía General de la República. 2 de diciembre de 2021	• Propone señalar que: 1) la FGR contará con la fiscalía especializada en materia de ciberseguridad, y 2) esta podrá investigar y perseguir los delitos de competencia federal en el que los medios electrónicos y tecnológicos constituyan o representen un medio de comisión relevante y trascendente, a excepción de delincuencia organizada.	Dip. Lidia García Anaya	Pendiente en comisión(es) de Cámara de origen

Fuentes: AGUIRRE QUEZADA, Juan Pablo, *Ciberseguridad, desafío para México y trabajo legislativo*, Cuaderno de investigación núm. 87, Senado de la República, Instituto Belisario Domínguez, marzo 2022, pp. 10-15 y SECRETARÍA DE GOBERNACIÓN, *Sistema de Información Legislativa (SIL)*, (30 de abril de 2022), http://sil.gobernacion.gob.mx.

III. CONCLUSIONES SOBRE LOS ANTECEDENTES DE LA CIBERSEGURIDAD EN MÉXICO

Si bien el Estado mexicano cuenta con algunos elementos necesarios para hacer frente a los ataques y amenazas a través de medios y tecnologías digitales, tales como ordenamientos jurídico-administrativos y equipos de respuesta públicos y privados, no es menos cierto que también podría inspirarse en algunas naciones vanguardistas en el desarrollo tecnológico y jurídico sobre ciberseguridad, debido a que la digitalización forma parte de diversos ámbitos tanto de la vida pública como privada, y algunos de estos han sido cada vez más afectados por ciberataques y delitos informáticos, ya sean dirigidos contra instituciones públicas, organizaciones privadas y personas físicas.

Durante la pandemia por COVID-19, México fue uno de los países latinoamericanos que más se vio afectado por ciberataques. Como reacción, se han creado centros de respuesta ante incidentes informáticos (CERT) públicos y privados, lo que indica que el Estado mexicano cuenta con algunos organismos responsables de atender este tipo de actividades. Inclusive, la Estrategia Digital Nacional derivada del Plan Nacional de Desarrollo 2019-2024 contempla fortalecer la seguridad informática.

A pesar de la atención que los sectores público y privado han prestado para atender el problema, se requiere un marco regulatorio sólido e innovador que coordine y faculte a diversas autoridades de todos los niveles de gobierno para que, en el ámbito de sus competencias, ordenen lo referente a la ciberseguridad.

Además, para un efectivo diseño, planeación y ejecución institucional que combata a la ciberdelincuencia, sería necesaria una estrategia nacional de ciberseguridad y un ente institucional que coordine las actividades de todos los actores involucrados.

La falta de regulación ha sido un área de oportunidad de gran importancia que el Congreso federal ha detectado en reiteradas ocasiones, tal como lo evidencia el hecho de que diversos grupos parlamentarios de las LXIV y LXV legislaturas del Congreso de la Unión incorporaran este problema público en sus respectivas agendas legislativas. De ahí derivaron varias iniciativas que han propuesto, entre otras medidas, crear un organismo coordinador, tipificar algunos delitos cibernéticos, considerar a los ciberataques como afectaciones a la seguridad nacional y

fomentar la educación para una navegación segura, aunque ninguna se ha convertido en derecho vigente hasta este momento.

Ahora bien, para desarrollar propuestas normativas, es conveniente que el órgano creador de la norma considere los conceptos y definiciones esenciales en materia de ciberseguridad. Por ello, en el siguiente capítulo se hace un breve recuento teórico y conceptual sobre la ciberseguridad y los conceptos relacionados.

CAPÍTULO SEGUNDO
MARCO TEÓRICO Y CONCEPTUAL DE LA CIBERSEGURIDAD

I. INTRODUCCIÓN

El fenómeno que envuelve el concepto de ciberseguridad ha sido abordado en múltiples foros y por diversos actores.[36] Sin embargo, es conveniente señalar que la falta de un marco jurídico unificado con responsabilidades precisas y modos claros de actuación por parte de las instituciones mexicanas es una situación que requiere un tratamiento urgente. Lo anterior se justifica por la exponencial velocidad de transformación y reorientación de los parámetros de la realidad derivadas de las innovaciones en las TIC.

De ahí que sea menester trazar las líneas centrales de entendimiento y la base conceptual desde una perspectiva geopolítica y geoestratégica que aclaren lo que es la ciberseguridad, su rumbo, su orientación y los futuros escenarios posibles para el Estado mexicano y para la región latinoamericana.

Uno de los elementos imprescindibles es el relativo a los escenarios polemológicos cibernéticos, es decir, todo aquello relativo a la ciberguerra. Mediante ellos se concibe la defensa de los intereses nacionales, lo que posibilita la construcción de una doctrina que asegure la estabilidad institucional y social, la creación de diagnósticos especializados, la identificación de necesidades, así como el procesamiento y la elaboración de marcos jurídicos adecuados que, abordados desde una visión amplia de la totalidad, devengan en acciones estatales racionales y fundamentadas.

Esta particular forma de proceder propia de la geopolítica y de la geoestrategia puede orientar las transformaciones necesarias en las instituciones del Estado mexicano para hacer frente a las nuevas formas de beligerancia. Estas suponen el dominio psíquico de las mentes y las emociones, lo que constituye uno de sus objetivos fundamentales. También lo es la conquista de los procesos cognitivos y los espacios virtuales en donde se ejecutan acciones que dan forma a la realidad, pues se trata

36 Por ejemplo, la Secretaría de la Defensa Nacional, la Secretaría de Infraestructura, Comunicaciones y Transportes, la Secretaría de Marina, el Instituto Federal de Telecomunicaciones, entre otros.

de espacios digitales donde sucede cada vez más lo político, lo económico, lo financiero, lo judicial, lo comunicacional, lo social, lo cultural, etc. Esta espacialidad digital es uno de los frentes esenciales aún vacíos donde es menester legislar para garantizar la seguridad tanto de las personas físicas y jurídicas, así como del Estado mexicano en general.

Por lo tanto, perfilar los elementos esenciales de las transformaciones institucionales y sociales que podrán devenir en acciones legislativas requiere definir y poner en operación categorías científicas y analíticas que describan y expliquen los fenómenos ciberdigitales, comprendiendo que la ciberseguridad (protección de los ciudadanos) y la ciberdefensa (salvaguarda de las instituciones estatales) constituyen uno de los dos rostros de la moneda. Su otra faz, entonces, está comprendida por las diferentes formas de violencia organizada que ejecutan tanto la delincuencia transnacional y el crimen organizado como cualquier otro ente o individuo antagónico a los intereses nacionales, sea o no estatal.

Por ejemplo, en la Estrategia Institucional para el Ciberespacio 2021-2024,[37] la Secretaría de Marina (SEMAR) estableció algunos de los parámetros centrales del marco conceptual en materia de ciberseguridad como función estatal. Si bien constituye una comprensión castrense de las amenazas –reales y probables– que pueden atentar en contra de la integridad, la estabilidad y la permanencia del Estado mexicano, también contribuye a la edificación de un pensamiento estratégico y un marco legislativo para el sector civil nacional respecto a los mecanismos de seguridad en el ciberespacio.

Entonces, cabría preguntar lo siguiente: ¿qué se entiende por ciberseguridad, ciberguerra, cibercrimen y demás conceptos relacionados? ¿Cuáles son las amenazas en el ciberespacio? ¿Qué es un ciberataque? ¿Puede tipificarse como tal a las acciones ejecutadas en un entorno de guerra cibernética, ciberterrorismo o de protesta civil o, por el contrario, habría gradientes de diferenciación y, por ende, de tipificación conceptual y jurídica?

37 SECRETARÍA DE MARINA, *Estrategia Institucional... cit.*

II. APROXIMACIONES CATEGORIALES

El concepto de *ciberespacio* puede definirse como el *espacio inmaterial producido por el conjunto de relaciones sociales que se establecen mediante redes de telecomunicaciones e informáticas interconectadas (internet)*.[38] Se conforma por todas las estructuras de redes informáticas a nivel mundial que conectan y controlan diversos sistemas no limitados al internet comercial, que sería solamente una red de redes abierta entre muchas otras, ya que también incluyen otras redes de ordenadores como las transaccionales (envío y recepción de datos sobre flujos de dinero), operaciones financieras, tarjetas de crédito, sistemas de control para la interconexión de máquinas y también la llamada *Internet de las Cosas* (*Internet of Things*, o IoT).[39]

La palabra *ciberespacio* se compone del prefijo derivado de la voz *cibernética*, la cual tiene su raíz en la voz griega *kybernetike* que, en términos generales, puede entenderse como *el arte de gobernar*. Pero en su acepción contemporánea se define como el *estudio de los procesos de control y de comunicación en los seres vivos y las máquinas*.[40] El término *ciberespacio* fue creado en 1984 por el novelista William Gibson[41] y teorizado en 1998 por Rob Kitchin[42] a partir del surgimiento del protocolo universal *World Wide Web* y los primeros portales de navegación de la *Netscape* a lo largo de los noventa del siglo anterior, y su uso se extendió desde entonces a casi la totalidad de países desarrollados y en vías de desarrollo por medio de múltiples tecnologías como servidores, computadoras, teléfonos móviles e inteligentes, electrodomésticos, automóviles, aeronaves y, en general, casi cualquier aparato o dispositivo de uso cotidiano.

Ligado a este concepto se encuentra el de *ciberguerra* o *guerra cibernética*, la cual se refiere a las operaciones militares ejecutadas en y a través de las redes informáticas con el fin de infiltrarse para obtener información, espiar, controlar los sistemas de misiles, planificar

38 HUISSOUD, Jean-Marc y GAUCHON, Pascal (coords.), *Las 100 palabras de la geopolítica*, Madrid, Akal, 2013, p. 101.

39 *Cfr.* CLARKE, Richard A. y KNAKE, Robert K., *Guerra en la red. Los nuevos campos de batalla*, Barcelona, Ariel, pp. 103 y 104.

40 *Idem*.

41 GIBSON, William, *Neuromancer,* Electronic Edition, Nueva York, The Ace Publishing Group, 2003, p. 53.

42 KITCHIN, Rob, *Cyberspace: The World in the Wires*, USA, Wiley, 1998.

operaciones castrenses, gestionar abastecimientos para los elementos militares y hasta la destrucción física de infraestructuras y recursos enemigos.[43] Se trata, pues, de acciones militares realizadas en el ciberespacio no solo contra infraestructuras informáticas y sistemas electrónicos militares, sino también civiles, en especial aquellas que se consideran estratégicas o críticas (plantas eléctricas, bancos, sistemas financieros, sitios *web* gubernamentales, empresariales, académicos, redes de computadoras corporativas, sistemas de transporte, entre muchas otras).

Esta particular forma de guerra es sumamente compleja. Además de ejecutarse por medio de *hackeos*, infecciones e infiltraciones en sistemas para sustraer información, controlarlos, sabotearlos o incluso destruirlos, su espectro operativo se puede conjugar con otras formas bélicas, por lo que en algunas doctrinas militares como la estadounidense se han articulado en un solo comando.[44]

Los pilares operativos en los que se lleva a cabo la ciberguerra se basan en tres formas de guerra dependiendo de la dimensión en la que se despliegue, a saber: cibernética, electromagnética y de información, aunque normalmente se manifiestan de modo fusionado. Además, puede abarcar diversos ámbitos polemológicos como la guerra psicológica, de propaganda, política, económica, espacial, etc.[45]

La *guerra electrónica* (ahora ampliada y fusionada como guerra electromagnética) se puede definir como:

> [E]l conjunto de actividades desarrolladas en el ámbito militar, dentro de los espectros de radiaciones electromagnéticas y acústicas, con el propósito de determinar y explorar la presencia de actividad enemiga en esos espectros, neutralizar y reducir el empleo de la energía irradiada por el enemigo y asegurar el empleo de la energía irradiada por los medios propios. Comprende una serie de acciones militares que implican el uso de la energía electromagnética para determinar, explotar, reducir o prevenir

43 BARRIOS, Miguel Ángel (dir.), *Diccionario latinoamericano de seguridad y geopolítica,* Buenos Aires, Editorial Biblos, 2009, p. 216.

44 Este es el caso del *U.S. Army Cyber Command que integra y conduce operaciones en el ciberespacio, guerra electromagnética y operaciones de información* con base en cinco principios doctrinarios: operar, defender, atacar, influenciar e informar. Véase UNITED STATES GOVERNMENT, *U.S. Army Cyber Command*, (5 de mayo de 2022), https://www.arcyber.army.mil.

45 Véase SOHR, Raúl, *Las guerras que nos esperan*, Chile, Ediciones B, 2000, pp. 261-264.

el empleo hostil del espectro electromagnético manteniendo su utilización por parte de fuerzas propias o amigas.[46]

Las tres actividades principales de la guerra electromagnética son:

1) Apoyo a las medidas electrónicas: búsqueda, interceptación, localización, análisis y registro de emisiones electrónicas para apoyar las acciones de contramedidas y contra-contramedidas electrónicas.
2) Contramedidas electrónicas: orientadas a impedir o reducir *el uso del efecto electromagnético por parte del enemigo* mediante acciones que pueden dividirse en:

    i. *Jamming*: radiación deliberada, reirradiación o reflexión de energía electromagnética utilizada con el fin de reducir o anular el uso de aparatos electrónicos de localización,
    ii. Engaño o decepción: se refiere a *la radiación deliberada, reirradiación alteración, absorción o reflexión de energía electromagnética utilizada con el fin de engañar a un operador en la interpretación o el uso de las informaciones recibidas de aparatos electrónicos*, es decir, se engaña tanto al operador como al aparato.[47]

A su vez, ambas acciones se clasifican en dos tipos: activo (transmisión de energía electromagnética hacia un sistema de transmisión electrónico) y pasivo (reflejado, refiriéndose a *sistemas de contramedidas electrónicas que no irradian, pero reflejan la señal recibida contra la fuente que la emite, o sea, radares, sistemas y aparatos de comunicaciones, misiles guiados, sistemas de navegación como el GPS e identificadores amigo-enemigo*).[48]

3) Contra-contramedidas electrónicas: son acciones para asegurar la utilización eficaz del espectro electromagnético. Se clasifican en:

    i. Equipos especiales para mejorar la búsqueda de los radares y el control de tiro.

46 BARRIOS, Miguel Ángel, *Diccionario latinoamericano… cit.*, pp. 218 y 219.
47 *Ibidem*, p. 219. Véase también SOHR, R., *Las guerras… cit.,* pp. 237-239.
48 *Idem.*

ii. Tácticas particulares para mejorar la eficiencia operativa de los radares en ambientes de contramedidas electromagnéticas.[49]

Por su parte, la *ciberdefensa* se refiere a las acciones que ejecutan los Estados con objeto de ampliar sus espacios de defensa ante las amenazas latentes que implican la interconectividad entre diferentes actores tanto estatales como no estatales.[50] Esta definición asume la incorporación de la información, las redes donde circula y el espacio virtual de operatividad, además de los tradicionales espacios terrestres, aéreos, marítimos y ultraterrestres, lo que ha generado que mantengan una importancia estratégica al nivel de la defensa energética o defensa militar convencional.

Así, pues, la ciberdefensa:

> ... tiene como misión proteger la infraestructura crítica de las naciones, especialmente las infraestructuras críticas de la información, del comercio electrónico, las acciones que realiza el gobierno *online*, la identidad digital y la de los ciudadanos, las empresas y el gobierno, los derechos y garantías de los usuarios de internet, los sistemas de información y telecomunicaciones.[51]

Asimismo, el *cibercrimen* y el *ciberterrorismo* son consustanciales a la ciberdefensa, entendiendo por el primero los delitos que violan la seguridad de internet (y cualquier red dentro del espacio de información) mediante el uso de *softwares* maliciosos denominados *malwares* para el desarrollo de actividades criminales.[52] Estas violaciones a la confianza de los usuarios de computadoras y de redes de información (sustracción de datos, robo de dinero y tarjetas de crédito, estafas, fraudes bancarios, etc.) pueden masificarse y crear carreras para el desarrollo de sistemas de armas tecnológicas o posibilitar diversos tipos de ataques a cualquier computadora que se encuentre operando en línea, de forma independiente al éxito de los mismos.

El *ciberterrorismo* se refiere al uso violento que se le da a la tecnología en las prácticas delincuenciales de los cibercriminales. Se trata de ataques,

49 *Idem*.

50 BARRIOS, Miguel Ángel, *Diccionario latinoamericano... cit.,* p. 104.

51 *Idem.*

52 *Idem.*

premeditados o no, que tienen como objetivo la creación de pánico e intimidar, presionar y afectar las infraestructuras críticas de los Estados. Con esto se busca encontrar y dañar los espacios de información estatales explotando sus *cibervulnerabilidades*, por ejemplo, en aquellas áreas vinculadas con la infraestructura hídrica (presas, plantas potabilizadoras, redes de suministro, etc.), eléctrica (sistemas de generación, transmisión, comercialización, etc.), del transporte aéreo (sistemas de navegación satelital, torres de control, etc.) o del sector energético (plantas eléctricas, nucleares, ductos y refinerías de hidrocarburos y gas, etc.). En resumen, se trata de acciones para crear el mayor daño posible a un Estado, región o sociedad inutilizando sus sistemas vitales o inhabilitándolos temporalmente, siendo escasa la visibilidad del perpetrador que actúa en escenarios intangibles.

III. GEOPOLÍTICA DE LA CIBERSEGURIDAD

Recuperando lo dicho previamente, la ciberseguridad puede entenderse como un subconjunto de la ciberguerra que busca dominar o dañar datos e información digital, sistemas de comunicación, redes informáticas y hasta el pensamiento individual y colectivo. Puede resultar en averías o en el control del sistema económico y financiero nacional, la infraestructura estratégica, las capacidades de respuesta militar y de seguridad ciudadana, de información y comunicación estatales, además de los procesos psico-cognitivos de las poblaciones para así desestructurar las capacidades de respuesta e implementar otras modalidades de guerra.

Esto significa que la ciberseguridad se comprende como las operaciones conducidas en el ciberespacio y en la dimensión electromagnética e informacional, acciones que pueden ser realizadas por Estados, organizaciones internacionales o grupos e individuos subversivos con el objetivo de atacar y dañar los sistemas computacionales y las redes de información de otra nación.[53] Esta forma de ataque es altamente compleja en cuanto que los límites de separación con otras formas de acción beligerante son altamente permeables. Por ello, la ciberseguridad está íntimamente vinculada a las estrategias en el espacio exterior donde los dispositivos satelitales son uno de los pilares infraestructurales de las redes de comunicación.

53 Véase UNITED STATES GOVERNMENT, *op. cit.*, así como RAND CORPORATION, *Sitio web oficial*, https://www.rand.org/topics/cyber-warfare.html?content-type=research&page=2.

De la misma manera, se relaciona con formas de ataque psicológico y batallas cognitivas, pues al ser la información el medio y el objetivo de las operaciones de violencia cibernética, surge la posibilidad de manipular a poblaciones enteras a partir de la información que reciben, de orientar la opinión pública con noticias falsas (*fake news*), mala información y desinformación que transforman la percepción de la realidad. Estas formas de guerra híbridas se han expandido vertiginosamente a raíz de que el ciberespacio se convirtió en el lugar por excelencia para la comunicación y el intercambio de ideas e información.[54]

A través de su Oficina de Lucha contra el Terrorismo, la ONU ha señalado que el uso indebido de las TIC por parte de terroristas ha cobrado especial relevancia en el contexto de la masificación de dichas tecnologías a nivel mundial. Sin embargo, lo más preocupante (de ahí que sea la oficina contra el terrorismo quien encabece los trabajos de ciberseguridad) son los posibles ataques contra instalaciones de infraestructura vital. Por ello, esta organización ha categorizado las actividades terroristas en línea de la siguiente manera:

a) Ciberataques
b) Propagación de los contenidos terroristas en línea
c) Comunicaciones entre terroristas en internet
d) Financiamiento al terrorismo digital.[55]

Estas categorías surgen a partir de un enfoque orientado por un organismo internacional y es así porque una de sus principales motivaciones es la de crear acuerdos y mecanismos de coordinación para la búsqueda de la paz mundial. De ahí que el concepto de ciberseguridad se comprenda metodológicamente (en el marco de la ONU y del derecho internacional) a partir de acciones de entidades no-estatales, evitando con ello definir el concepto de ciberguerra que sería el conflicto entre

54 *Cfr*. JANCZEWSKI, Lech J. y COLARIK, Andrew M., *Cyber Warfare and Cyber Terrorism*, Nueva York, Hershey, 2008; CZOSSECK, C. y GEERS, K. (eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare*, Cryptology and Information Security Series, vol. 3, 2009; CARR, Jeffrey, *Inside Cyber Warfare*, 2ª ed., EE. UU., O'Reilly, 2011; ERBSCHLOE, Michael, *Information Warfare. How to Survive Cyber Attacks*, EE. UU., Osborne/McGraw-Hill, 2001; SHAKARIAN, Paulo *et al*., *Introduction to Cyber Warfare. A multidisciplinary Approach*, EE. UU., Syngress, 2013; ANDRESS, Jason y WINTERFELD, Steve, *Cyber Warfare. Techniques, TacTIC and Tools for Security Practitioners*, EE. UU., Syngress, 2011.

55 CONSEJO DE SEGURIDAD DE LA ORGANIZACIÓN DE LAS NACIONES UNIDAS, *Resolución 2341 (2017)*, aprobada en su 7882a sesión celebrada el 13 de febrero de 2017, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/038/62/PDF/N1703862.pdf?OpenElement.

dos o más Estados en el ciberespacio, siguiendo la definición convencional de guerra acorde con el *ius belli*, o el derecho de la guerra.

Sin embargo, el propio Secretario General de la ONU declaró que [y]*a existen episodios de guerra cibernética entre Estados. Y lo peor es que no hay un esquema reglamentario para este tipo de guerra, no está claro si ahí se aplica la Convención de Ginebra o el Derecho Internacional pueden aplicarse en estos casos*.[56] Pero también ha advertido que no existe un marco regulatorio concreto a nivel internacional, por lo que *estamos totalmente desprotegidos de mecanismos regulatorios que garanticen que ese nuevo tipo de guerra obedezca a aquel progresivo desarrollo de leyes de guerra*.[57]

En otras palabras, no existe un marco regulatorio que caracterice específicamente a la ciberguerra, ni tampoco son claras las reglas que han de aplicarse a este fenómeno con base en el *ius in bello* establecido en la Convención de Ginebra y sus Protocolos adicionales, los principios del derecho internacional o el Estatuto de Roma de la Corte Penal Internacional.[58] Lo que sí existe es el reconocimiento fáctico de ciberataques contra objetivos vitales e infraestructuras civiles, gubernamentales y militares por parte de Estados, constituyendo de una u otra manera, dependiendo de las diferentes doctrinas militares de los Estados, acciones de ciberguerra y, por consecuencia, acciones de beligerancia interestatal que podrían devenir en una legítima declaración de guerra.

Por ejemplo, el Comando de Ciberguerra de EE. UU. ha señalado que se encuentran involucrados en escenarios de competencia en el largo plazo contra Rusia y China.[59] Ambos países han desarrollado estrategias que representan diversos riesgos para Washington, pues erosionan sus capacidades económicas, persisten acciones de espionaje cibernético

56 DEL BARRIO, Javier Martín, *El Secretario General de la ONU dice que hay "ciberguerra entre Estados"*, El País, España, 19 de febrero de 2018, (10 de mayo de 2022), https://elpais.com/internacional/2018/02/19/actualidad/1519058033_483850.html.

57 *Idem*.

58 El Estatuto de Roma de la Corte Penal Internacional señala en el artículo 8, Crímenes de Guerra, que *1. La Corte tendrá competencia respecto de los crímenes de guerra en particular cuando se cometan como parte de un plan o política o como parte de la comisión en gran escala de tales crímenes. 2. A los efectos del presente Estatuto, se entiende por "crímenes de guerra": ... iii) El hecho de causar deliberadamente grandes sufrimientos o de atentar gravemente contra la integridad física o la salud; iv) La destrucción y la apropiación de bienes, no justificadas por necesidades militares, y efectuadas a gran escala, ilícita y arbitrariamente...* CORTE PENAL INTERNACIONAL, *Estatuto de Roma*, (11 de mayo de 2022), https://www.un.org/spanish/law/icc/statute/spanish/rome_statute(s).pdf.

59 Comando que aglutina estratégica, táctica y doctrinalmente a cuatro ramas de las fuerzas armadas de los Estados Unidos (https://www.cybercom.mil): *U.S. Army Cyber Command*, https://www.arcyber.army.mil/; *Fleet Cyber Command* (*10th Fleet*); *Sixteenth Air Force* (*Air Force Cyber*) https://www.16af.af.mil/; y *Marine Corps Forces Cyberspace Command*, https://www.marforcyber.marines.mil.

para la obtención de información sensible tanto gubernamental como del sector privado estadounidense y ejecutan operaciones de información en su población para generar polarización y así desestabilizar sus procesos democráticos a partir de la fragmentación social.[60]

Todo lo anterior es comprendido por el Comando de Ciberguerra no únicamente en términos de ciberseguridad, sino como la suma de acciones que se conjugan en un espectro multidimensional de operatividad que pretende evitar la consecución de sus planes e intereses. Por lo tanto, durante las fases operativas en los diversos campos de acción se deberán desplegar de manera efectiva y en términos de inteligencia múltiple acciones de *vigilancia y reconocimiento, guerra cibernética, guerra electrónica y capacidades de operaciones de información a lo largo de la continuidad del conflicto*,[61] lo que significa que las ramas de las fuerzas armadas han de actuar de manera rápida, letal y completamente coordinada tanto en la competencia (económica, financiera, comercial, tecnológica, política, diplomática y demás formas de guerra no convencional) como en la guerra *stricto sensu*, para que se reconozca *el papel de la información en la creación de dilemas para los adversarios en competencia y, si es necesario, en conflictos futuros*.[62]

Los escenarios de ciberguerra son muy claros para este Comando Conjunto. En sus propias palabras:

> Durante tiempos de guerra, las fuerzas cibernéticas de EE. UU. estarán preparadas para operar junto con nuestras fuerzas aéreas, terrestres, marítimas y fuerzas espaciales, para apuntar a las debilidades del adversario, compensar las fortalezas del adversario y amplificar la efectividad de otros elementos de la Fuerza Conjunta. [...] El Departamento explotará esta dependencia para obtener una ventaja militar. La Fuerza Conjunta empleará medidas ofensivas con capacidades cibernéticas y conceptos innovadores que permiten el uso de las operaciones del ciberespacio en todo el espectro completo del conflicto.[63]

60 UNITED STATES DEPARTMENT OF DEFENSE, *Cyber Strategy 2018*, (11 de mayo de 2022), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

61 UNITED STATES GOVERNMENT, *Sixteenth Air Force (Air Force Cyber)*, (16 de mayo de 2022), https://www.16af.af.mil.

62 *Idem*.

63 UNITED STATES DEPARTMENT OF DEFENSE, *Cyber Strategy 2018... cit.*, pp. 1-2. La traducción es de los autores.

Como se puede observar, la ciberdefensa se transforma en ciberguerra cuando la dinámica del conflicto afecta las capacidades para garantizar que los propios intereses no sean socavados en una lógica de dominación de espectro completo.[64] Cuando la guerra ha traspasado los límites que la acotaban como una actividad específica, en lugares bien definidos y entre combatientes claramente identificados, la existencia o inexistencia de regulaciones se torna irrelevante y facilita el proceso de que las acciones de guerra convencional se articulen con operaciones y tácticas cibernéticas, cognitivas, psicológicas, comunicacionales, propagandísticas, diplomáticas, económico-financieras, socioculturales y demás formas de guerra no convencional.

La guerra cognitiva, que es una de las tantas facetas en las que se ejecutan las guerras híbridas por medio del control de las emociones y de los pensamientos, de sus contenidos y de sus interpretaciones, en gran medida transmitidos por medios digitales, representa un caso en el que se evidencia la hibridación entre múltiples formas de guerra desplegadas en modalidades multinivel, las cuales persiguen objetivos diversos, pero acoplados y entremezclados estratégicamente a partir del poder nacional con el fin de propiciar acciones y fenómenos desestabilizadores en individuos y grupos poblacionales. Se trata de una reorientación de sus *psiques* a partir de procesos psicoprofilácticos que, en un efecto dominó, conlleven finalmente al colapso completo de un Estado o de una región desde su interior y sin la necesidad de realizar ningún tipo de acción militar desde el exterior, deslindando de toda responsabilidad al actor ejecutante.

Desde el espacio de entendimiento de la sociología del conocimiento,[65] el enfoque orientado a la profilaxis psicológica pretende encontrar los elementos patológicos, disfuncionales o anómalos de los individuos o de grupos sociales a fin de desplegar sobre ellos acciones concretas de espasticidad muscular (principalmente sobre el cerebro) para incidir y eliminar en el comportamiento individual y social mecanismos conductuales que reduzcan la estabilidad y eventualmente se genere desorganización social, situaciones de caos, polarización poblacional y el eventual desmoronamiento del orden interno del Estado o región sobre los que se

64 La idea de la dominación de espectro completo como parte de la doctrina militar estadounidense durante las décadas de 1990 y los 2000 fue analizada por F. WILLIAM ENGDAHL en su obra *Full Spectrum Dominance: Totalitarian Democracy in the New World Order,* Massachusetts, Third Millennium Press, 2009.

65 MILLS, Charles Wright, *Poder, Política, Pueblo*, México, Fondo de Cultura Económica, 1973.

ejerce este tipo de guerras hipercomplejas. Con el objetivo de eliminar o modificar la percepción de la realidad a través de impulsos psicológicos y orientarla hacia la aceptación de un estado de realidad impuesto, la plasticidad beligerante del atacante hace de este proceso el rasgo de carácter más conveniente para quien aplica dicha violencia cognitiva.

Si bien la guerra psicológica encuentra su etiología en los fenómenos religiosos de control social a través del dominio de las almas y de los actos de fe, y posteriormente retomando los conocimientos de la neuropsicofarmacología, la psicopatología (en particular de la esquizofrenia)[66] y la parapsicología,[67] se ha perfeccionado en sus alcances, objetivos y en sus vectores de transmisión. Así pues, el desarrollo de la guerra que se despliega en la dimensión psíquico-anímica ha pasado de las tradicionales liturgias, las asambleas y las congregaciones con fines políticos, al empleo de nuevos medios para la manipulación de las mentes y las ideas que le conforman, tales como periódicos, literatura, arte, radio, televisión y, ahora, el ciberespacio.

El siguiente nivel evolutivo de esta forma de guerra se perfila con el uso de inteligencias artificiales para que sean los algoritmos los que planeen, diseñen y ejecuten procesos de diferenciación, clasificación, separación, segmentación, aislamiento y exclusión de todas aquellas personas cuyas acciones promuevan la *estabilidad (y en consecuencia -son seres- "funcionales") y las otras -personas- que perturban tal estabilidad (y que, por lo tanto, son "disfuncionales")* [...].[68]

El control psico-kinésico de los entes clasificados como patológicos en y a través del ciberespacio (ciudadanos, empresas o instituciones estatales y no estatales) se encuentra limitado por y acotado al desarrollo de innovaciones tecnológicas. Dada la cantidad de naciones con acceso a las TIC, las acciones emprendidas se codifican en el terreno de la ciberseguridad, la ciberdefensa y la ciberguerra como formas posibles de violencia.

---

66 Véase TISSOT, René, *Función simbólica y psicopatología*, México, Fondo de Cultura Económica, 1992.

67 Véase NATIONAL GEOGRAPHIC, *Los experimentos secretos de la CIA*, Grandes Enigmas de la Historia, Barcelona, Editorial Sol 90, 2012. Entre los proyectos destacan el conocido MK ULTRA, el programa psíquico *Stargate*, el *Proyecto Jedi*, entre los que se han dado a conocer públicamente y cuyas fuentes abrevan de la *Operación Paperclip* con la que miles de científicos nazis fueron absorbidos por las agencias militares y de inteligencia estadounidenses en las que continuaron sus experimentos e investigaciones después de la Segunda Guerra Mundial.

68 SAXE-FERNÁNDEZ, John, "Etiología de la patología revolucionaria y profilaxis contrarrevolucionaria", *Revista Mexicana de Ciencias Políticas y Sociales*, México, nueva época, año XXI, núm. 81, julio-septiembre de 1975, pp. 99-130.

La amplia diversidad de *entes disfuncionales* para la consecución de los objetivos de los actores que ejecutan tácticas psico-cognitivas y neocorticales[69] a través del ciberespacio son convertidos en objetos de ataque en cualquier escenario real o probable donde se vean amenazados o atacados los intereses corporativos, de la delincuencia organizada y/o transnacional, o de los propios Estados.

En este sentido, desde el siglo XIX, tal como puede observarse en el planteamiento de Carl von Clausewitz,[70] la guerra ha sido comprendida como el último eslabón dentro una serie de sucesos concatenados cuyo objetivo, la mayoría de las veces,[71] es de naturaleza política. De ahí que los procesos que llevan a la decisión para hacer (o no) una guerra se valoren desde una gran cantidad de variables, y dentro de esta ponderación, la estrategia de comunicación enemiga es de enorme relevancia. Es decir, se torna fundamental comprender cómo su base poblacional interna y externa logra ser convencida para apoyar las medidas totalizantes que representan colocar a una nación en estado de guerra. George Kennan definió esto en octubre de 1947, justamente a inicios de la Guerra Fría, al expresar que *no es la fuerza militar rusa la que nos amenaza, es el poder político ruso*.[72]

Ubicar empírica, conceptual y analíticamente los escenarios de conflicto no es una tarea sencilla. Pero una vez dilucidados, representan la piedra fundacional de cualquier doctrina política o militar, así como de las estrategias nacionales. Esto constituye el preludio de cualquier proceso de toma de decisiones porque se sabe quiénes son los enemigos potenciales o reales y, por lo tanto, es posible proyectar y aplicar las estrategias o contramedidas necesarias para enfrentarlos.

La violencia derivada de la guerra comunicacional pretende garantizar el apoyo de la población al controlar sus percepciones sobre la

69 Véase SZAFRANSKI, Richard, *Neocortical Warfare? The Acme of Skill*, Military Review, noviembre 1994, pp. 41-55, https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch17.pdf.

70 VON CLAUSEWITZ, Carl, *De la Guerra,* México, Colofón, 2006.

71 Es prudente señalar que cuando se habla de teoría de la guerra, su violencia inherente cobra una gran variedad de formas, al igual que las circunstancias que le dan origen. Muchas veces se cree que existen explicaciones unívocas y que debemos olvidar aquellas que puedan comprometer la evidencia empírica que configura el proceso. Pero tampoco puede explicarse exclusivamente desde una postura mecanicista la relación existente entre las causas y motivos que desatan la violencia, la guerra y sus objetivos finales. Por el contrario, la mayoría de las veces se encuentran separados por la incertidumbre contenida en cualquier fenómeno social y, más aún, la que se manifiesta como caos en cualquier escenario de guerra.

72 Diplomático, historiador y académico estadounidense, creador de la doctrina de la contención que fue un pilar estratégico durante toda la Guerra Fría.

realidad por medio de manipulaciones audiovisuales espectaculares que buscan producir estados afectivos que permitan una fácil y profunda penetración de ideas y discursos específicos, así como aletargar los cuerpos y distraer las mentes con formas de entretenimiento hedonistas. De esta manera se busca eliminar la mayor cantidad posible de barreras, trabas y oposiciones por parte de la sociedad, para así poder realizar otro tipo de acciones consideradas prioritarias, pero que serían rechazadas por razones morales, religiosas o jurídicas.

En la historia hay muchos casos que ilustran esta forma de guerra, pero para contextualizar lo dicho en los tiempos actuales, consideremos la *operación especial* del ejército ruso en el oeste de Ucrania. El gobierno ruso ha señalado que a través de ella busca acabar con las fuerzas antagónicas en aquel país y con los grupos dirigentes que los apoyan irrestrictamente.[73] El portal de noticias *Russia Insider*[74] ha vinculado a una alta funcionaria del gobierno canadiense en acciones de apoyo al régimen ucraniano y, en particular, a la facción del mismo que subvenciona con armas, equipo, logística y dinero (además de apoyo político) al batallón Azov, que pregona una supuesta supremacía racial ucraniana sobre los rusos, ahora catalogado como organización terrorista por el Tribunal Supremo de Rusia.[75] Asimismo, el portal antes mencionado recuerda el árbol genealógico de la alta funcionaria y da cuenta de cómo fue educada por su abuelo, un conspicuo simpatizante y militante del III Reich.

En respuesta, el gobierno de Canadá publicó una declaración[76] que fue replicada por los gobiernos de los países que integran la Organización

73 PRESIDENT OF RUSSIA, *Address by the President of the Russian Federation*, The Kremlin, Moscú, 24 de febrero de 2022, http://en.kremlin.ru/catalog/countries/UA/events/67843; MINISTRY OF FOREIGN AFFAIRS OF THE RUSSIAN FEDERATION, *Foreign Minister Sergey Lavrov's interview with TV channels RT, NBC News, ABC News, ITN, France 24 and the PRC Media Corporation*, Moscú, 3 de marzo de 2022, https://mid.ru/en/press_service/minister_speeches/1802677.

74 QUINN, Michael, *The Large and Influential Ukrainian Diaspora in Canada - Good Russian TV Profile*, Russia Insider, 2 de marzo de 2019, https://russia-insider.com/en/large-and-influential-ukrainian-diaspora-canada-good-russian-tv-profile/ri26029; PIKE, Cameron, *Canada's Nazi Problem*, Russia Insider, 6 de febrero de 2018, https://russia-insider.com/en/canadas-nazi-problem/ri22463; PARKER, Dean, *Why Is Canada's Foreign Minister Proud of Her Family's Nazi Past?*, Russia Insider, 5 de abril de 2017, https://russia-insider.com/en/why-canadas-foreign-minister-proud-her-familys-nazi-past/ri19435.

75 CHÁVEZ RINCÓN, Melissa, *Tribunal Supremo de Rusia declara al regimiento de Azov como grupo terrorista*, France24, 3 de agosto de 2022, https://www.france24.com/es/europa/20220803-tribunal-supremo-de-rusia-declara-al-regimiento-de-azov-como-grupo-terrorista.

76 GOUVERNEMENT DU CANADA, *Déclaration au nom du président de la Coalition pour la liberté en ligne: Un appel à l'action sur la désinformation parrainée par l'État en Ukraine*, Affaires mondiales, Ottawa, 2 de marzo de 2022, https://www.canada.ca/fr/affaires-mondiales/nouvelles/2022/03/declaration-au-nom-du-president-de-la-coalition-pour-la-liberte-en ligne-un-appel-a-laction-sur-la-desinformation-parrainee-par-letat-en-ukraine.html.

del Tratado del Atlántico Norte (OTAN), donde acusa que toda la información proveniente de Rusia no es más que un despliegue de operaciones de desinformación que atenta contra las libertades individuales y los valores democráticos, por lo que no pueden ser difundidas en el *mundo democrático*, pues vulnera el Estado de Derecho en el que se fundamenta. De ahí que esta toma de postura se utilice para justificar la censura en la difusión de cualquier tipo de información proveniente de los canales mediáticos oficiales y no oficiales que no comuniquen la *verdad*, es decir, cuando expongan todo tipo de información que se considere contraria a los intereses de Canadá y de la OTAN.

Como se puede observar, la guerra comunicacional devela un posicionamiento estratégico en el campo de batalla ciberespacial, mediático y diplomático. Por lo tanto, es menester prestar atención a las acciones que ocurren en estos campos, considerando que, ante la ausencia de una regulación jurídica internacional y mecanismos de control sobre lo que se considera que son discursos verdaderos y legítimos, es necesario desarrollar capacidades operativas propias del Estado mexicano. Esto para hacer frente a las amenazas informáticas, comunicacionales y cognitivas que podrían menoscabar sus fundamentos, sin percatarse de ello más que hasta el momento en que estas formas sutiles de beligerancia manifiestan sus catastróficas consecuencias.

IV. CONCLUSIONES SOBRE EL MARCO TEÓRICO Y CONCEPTUAL DE LA CIBERSEGURIDAD

El concepto mismo de ciberseguridad y otros relacionados, como ciberguerra y cibercrimen no son unívocos. La doctrina y las instituciones públicas de diferentes Estados no ofrecen definiciones homogéneas. Esto se debe a que atienden al contexto presente en cada país y a los intereses de actores estatales y no estatales.

También es patente la falta de definiciones formales a nivel internacional. Por ende, el Poder Legislativo debe ser cuidadoso al incluir y definir conceptos en los ordenamientos jurídicos. Como se desprende de este capítulo, la ciberseguridad puede ser entendida en su faceta de defensa y seguridad nacional, o también como una cara de la seguridad pública e interior que atañe a cada persona.

Por ello, es menester trazar las líneas centrales de entendimiento y las bases conceptuales desde una perspectiva geopolítica y geoestraté-

gica que aclaren lo que es la ciberseguridad. Esta comprende las operaciones conducidas en el ciberespacio, la dimensión electromagnética e informacional, acciones que pueden ser realizadas por Estados u organizaciones internacionales, con el fin de atacar y dañar los sistemas computacionales y las redes de información de otra nación.

Un aspecto íntimamente relacionado, la ciberdefensa, se transforma en ciberguerra cuando la dinámica del conflicto afecta las capacidades para garantizar que los propios intereses del Estado no sean socavados en una lógica de dominio de espectro completo frente a otros entes públicos o privados, nacionales o transnacionales. Adicionalmente, se observan tácticas de guerra comunicacional que develan un posicionamiento estratégico en el campo de batalla ciberespacial, mediático y diplomático.

Dada la multiplicidad de elementos que pueden integrar las definiciones del objeto analizado, en el siguiente capítulo se presentará un estudio de derecho comparado que busca, entre otras finalidades, precisar los conceptos e instituciones jurídicas que las legislaciones sobre ciberseguridad tienden a incluir. A partir de este ejercicio de análisis y síntesis se derivarían algunos conceptos, definiciones y arreglos institucionales que una ley mexicana podría incorporar.

CAPÍTULO TERCERO

MARCO JURÍDICO QUE REGULA LA CIBERSEGURIDAD

En el presente capítulo se analiza y sintetiza el marco normativo internacional y nacional vigente sobre la ciberseguridad o que regula aspectos estrechamente relacionados. En resumen, se observa que a nivel internacional existen algunos instrumentos vinculantes y otros no obligatorios para el Estado mexicano, que regulan algunos elementos, pero cuyo desarrollo está a cargo de los congresos nacionales. En el ámbito doméstico, algunos órganos del Estado mexicano cuentan con ordenamientos de tipo reglamentario o administrativo, pero no existe una legislación actualizada, especializada ni abundante en esta materia.

I. MARCO JURÍDICO INTERNACIONAL SOBRE LA CIBERSEGURIDAD

1. *Convenio sobre la ciberdelincuencia (Convenio de Budapest)*

El Convenio sobre la Ciberdelincuencia o Convenio de Budapest fue elaborado en 2001 por el Consejo de Europa para combatir los delitos informáticos.[77] Es el único tratado internacional vinculante en la materia y constituye una especie de guía, ley modelo o acuerdo marco para que los Estados Parte: 1) implementen en su ordenamiento jurídico la legislación pertinente para investigar y perseguir penalmente los delitos cometidos en contra de sistemas o medios informáticos, o mediante el uso de los mismos, y 2) faciliten la cooperación internacional.[78]

El capítulo I define lo que se entiende por *sistema informático*, *datos informáticos*, *proveedor de servicios* y *datos relativos al tráfico*. El capítulo II establece las medidas que deberán adoptarse a nivel nacional respecto al derecho penal sustantivo, divididas en cuatro grandes categorías de delitos:

1) Contra la confidencialidad, la integridad y la disponibilidad de los datos

77 CONSEJO DE EUROPA, *Convention on Cybercrime*, Budapest, ETS, núm. 185, 2001, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

78 CENTENO, Danya, *México y el Convenio de Budapest: posibles incompatibilidades*, México, Red en Defensa de los Derechos Digitales, junio 2018, p. 3.

y los sistemas informáticos (acceso ilícito, intercepción ilícita, ataques a la integridad de los datos o del sistema, abuso de los dispositivos).
2) Informáticos (falsificación y fraude informático).
3) Relacionados con el contenido (pornografía infantil).
4) Relacionados con infracciones a la propiedad intelectual.

El convenio también establece la responsabilidad de las personas jurídicas. Respecto a las medidas procesales, dispone la conservación rápida de datos informáticos almacenados, la revelación parcial rápida de datos relativos al tráfico, su registro y confiscación, su obtención en tiempo real, así como la obligación de promulgar normas legislativas sobre jurisdicción penal.

El capítulo III señala los principios y mecanismos de cooperación internacional respecto a la extradición y asistencia mutua, incluso en ausencia de acuerdos internacionales aplicables. Se debe recordar que el Convenio de Budapest no es un instrumento que obligue al Estado mexicano, pero se expone su contenido por su relevancia para la comunidad internacional y por ser el tratado más específico en la materia.

Este tratado se encuentra abierto para que otros Estados no miembros de la Unión Europea puedan adherirse. Así lo han hecho países como Argentina, Australia, Canadá, Chile, Colombia, Costa Rica, EE. UU., entre otros. El Estado mexicano es observador y se le ha invitado a adherirse.[79] Inclusive, ambas cámaras del Congreso de la Unión han aprobado puntos de acuerdo para exhortar al Ejecutivo Federal y/o al Senado a continuar los procesos correspondientes.[80]

Sin embargo, se ha señalado la posible incompatibilidad del convenio respecto al marco jurídico mexicano porque *deja un amplio margen de discrecionalidad para ciertos delitos debido a la vaguedad, imprecisión, apertura o amplitud de su definición*, y no *delimita los mínimos y máximos de punibilidad aplicables para cada delito ni identifica el*

79 CONSEJO DE EUROPA, *Adhesión al Convenio de Budapest sobre la Ciberdelincuencia: Beneficios*, 2021, https://rm.coe.int/cyber-buda-benefits-junio2021a-es/1680a2e4de#:~:text=En%20junio%202021%2C%2066%20Estados,Tonga%2C%20otros%202%20Page%202.

80 Por ejemplo, COMISIÓN DE RELACIONES EXTERIORES DEL SENADO DE LA REPÚBLICA, *Dictamen de la Comisión de Relaciones Exteriores, a los puntos de acuerdo por los que se exhorta al Ejecutivo Federal a iniciar los trabajos necesarios para la adhesión de México al Convenio sobre la Ciberdelincuencia, o Convenio de Budapest*, (Senado de la República), Gaceta del Senado, 11 de marzo de 2021, https://infosen.senado.gob.mx/sgsp/gaceta/64/3/2021-03-11-1/assets/documentos/Dict_Com_Relaciones_Exteriores_Ciberdelincuencia_Convenio_Budapest.pdf.

bien jurídico tutelado por cada uno.[81] También es posible que las capacidades técnicas y operativas de algunas instituciones de seguridad pública resulten insuficientes para aplicarlo e implementarlo.[82]

Junto con esto, se han emitido dos protocolos adicionales. Uno es el *Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos* de 2003.[83] Posteriormente, el 12 de mayo de 2022, veintidós países, entre los cuales se encuentran Estados Unidos, España y Estonia,[84] firmaron el *Segundo Protocolo Adicional al Convenio de Budapest, relativo al refuerzo de la cooperación y la divulgación de pruebas electrónicas*.[85] Como su nombre lo indica, este documento complementario aborda el hecho de que los ciberdelitos pueden trascender las fronteras políticas nacionales, por lo que la cooperación internacional es necesaria para combatirlos.

2. *Tratado entre México, Estados Unidos y Canadá (T-MEC)*

El T-MEC es un instrumento internacional vinculante para el Estado mexicano y contiene al menos dos capítulos relacionados con la materia, uno expresamente referido a la ciberseguridad del comercio electrónico.

Así, el capítulo 18 regula las telecomunicaciones, mientras que el artículo 18.3, numeral 4, referente a su acceso y uso, señala que:

> ...una parte podrá tomar medidas necesarias para asegurar la seguridad y confidencialidad de los mensajes o para proteger la pri-

81 CENTENO, Danya, *op. cit.*, p. 8.

82 MARTINS DOS SANTOS, Bruna, *Convenio de Budapest sobre la Ciberdelincuencia en América Latina: Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México*, Derechos Digitales América Latina, 2022, p. 31.

83 CONSEJO DE EUROPA, *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)*, Estrasburgo, 2003, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189.

84 CONSEJO DE EUROPA, *Mejora en la cooperación y la divulgación de pruebas electrónicas: 22 países firman el nuevo Protocolo al Convenio sobre Ciberdelincuencia*, 12 de mayo de 2022, (16 de mayo de 2022), www.coe.int/es/web/portal/-/enhanced-co-operation-and-disclosure-of-electronic-evidence-22-countries-sign-new-protocol-to-cybercrime-convention.

85 CONSEJO DE EUROPA, *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)*, Estrasburgo, 2022, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224.

> vacidad de los datos personales de los usuarios finales de las redes o servicios públicos de telecomunicaciones, siempre que aquellas medidas no se apliquen de tal manera que pudieran constituir un medio de discriminación arbitraria o injustificable, o una restricción encubierta al comercio de servicios.

Asimismo, destaca el capítulo 19 sobre comercio digital, pues se refiere expresamente a la ciberseguridad en su artículo 19.15. Este reconoce que las amenazas cibernéticas menoscaban la confianza en el comercio digital, por lo que los Estados Parte procurarán: a) desarrollar las capacidades de sus instituciones responsables de la respuesta a incidentes, y b) fortalecer los mecanismos de colaboración para cooperar en identificar y mitigar las intrusiones maliciosas o la diseminación de códigos maliciosos que afecten a las redes electrónicas, siendo la utilidad de esos mecanismos resolver y tratar con los incidentes cibernéticos, así como intercambiar información para el conocimiento y las mejores prácticas. También precisa que los enfoques basados en riesgos pueden ser más efectivos que la regulación prescriptiva para tratar las amenazas.

Finalmente, el capítulo 20 sobre derechos de propiedad intelectual, en su artículo 20.85, establece los procedimientos y sanciones penales en casos de falsificación dolosa de marcas o piratería dolosa lesiva del derecho de autor o derechos conexos a escala comercial. También regula la protección de señales de satélite y cable encriptadas portadoras de programas (artículo 20.86), el uso de *software* por el gobierno (artículo 20.87), a los proveedores de servicios de internet (artículo 20.88), así como los recursos legales y limitaciones para enfrentar infracciones al derecho de autor (artículo 20.89).

3. *Objetivos de Desarrollo Sostenible*

Como ya fue señalado, el ciberespacio ha sido significativamente utilizado para cometer delitos y actos de violencia entre personas y Estados. Por ello, el Objetivo 16 de la Agenda 2030 de la ONU, busca promover sociedades pacíficas e inclusivas, facilitar el acceso a la justicia para todos y construir a todos los niveles instituciones eficaces e inclusivas que rindan cuentas cobra especial relevancia.

Debido a que diversas conductas ilícitas o expresamente delictivas son cometidas a través de las redes digitales en contra de niños, niñas

y adolescentes, tales como el acoso sexual y la trata, resulta necesario señalar que la meta específica 16.2 persigue poner fin al maltrato, la explotación, la trata y todas las formas de violencia y tortura contra los niños. En ese sentido, la prevención, investigación y sanción de conductas como el *grooming* que se efectúa, por ejemplo, a través de plataformas de videojuegos, podrían ser medios eficaces para disminuir su prevalencia.

También se debe considerar que diversos delitos, tales como la trata de personas, el tráfico de armas, narcóticos y otros bienes ilícitos son cometidos en muchas ocasiones por personas insertas en redes de delincuencia organizada. Por ello, cobran especial relevancia las metas 16.4 y 16.a, las cuales plantean reducir las corrientes financieras y de armas ilícitas, fortalecer la recuperación y devolución de los activos robados y luchar contra todas las formas de delincuencia organizada, así como fortalecer las instituciones nacionales para crear la capacidad de prevenir la violencia y combatir el terrorismo y la delincuencia. Una legislación nacional tendiente a contrarrestar la ciberdelincuencia y otras formas de violencia cibernética representaría un avance para cumplir con este mandato internacional.

Adicionalmente, el objetivo 17, referente a los medios de implementación, señala en sus metas 17.6 y 17.8 que se debe mejorar la cooperación regional e internacional en materia de ciencia, tecnología e innovación y el acceso a estas, y que se debe poner en pleno funcionamiento el banco de tecnología y el mecanismo de apoyo a la creación de capacidad en materia de ciencia, tecnología e innovación para los países menos adelantados, así como aumentar la utilización de tecnologías instrumentales, en particular la tecnología de la información y las comunicaciones. En este aspecto, el intercambio de conocimientos y el aumento de capacidades en materia cibernética resulta fundamental, pues podrían fungir como mecanismos para que Estados como el mexicano promuevan la investigación en materia de ciberseguridad, incrementen su capacidad para evitar ciberataques y recuperarse de ellos, derivando en la reducción de los costos asociados a este tipo de ataques.

4. *Agenda sobre Ciberseguridad Global de la Unión Internacional de Telecomunicaciones (UIT)*

Esta agenda, lanzada en 2007, *es un marco de cooperación interna-*

cional destinado a mejorar la seguridad y la confianza en la sociedad de la información.[86] Contiene cinco pilares para guiar a los países en el desarrollo de capacidades con la finalidad de abordar la seguridad ciberdigital de manera responsable: 1) medidas legales, 2) medidas técnicas y procedimentales, 3) estructuras organizacionales, 4) desarrollo de capacidades y 5) cooperación internacional. Posteriormente, la UIT desarrolló la Guía de Ciberseguridad Nacional en 2011, donde se enfatizan los valores, la cultura y los intereses nacionales como la base para el desarrollo efectivo de toda estrategia nacional.[87]

Posteriormente a su lanzamiento, se ha detectado el surgimiento de nuevas tecnologías de seguridad digital, como las tecnologías de *libro mayor distribuido* (por ejemplo, las cadenas de bloques o *Blockchain*), las cuales ofrecen mecanismos eficaces para salvaguardar los sistemas y los datos conexos de entes públicos y privados. También se ha reconocido que son cada vez más los países que avanzan hacia la adopción de sistemas de identidad digital, con la consecuente necesidad de protegerlos.[88]

Adicionalmente, se reconoce que las TIC son un medio imprescindible para alcanzar los Objetivos de Desarrollo Sostenible, y que para ello es importante que las personas confíen en el uso de las TIC. Al respecto, la UIT ha reunido a diferentes partes interesadas para que colaboren en iniciativas como ayudar a los países a definir su estrategia nacional de ciberseguridad, fortalecer su infraestructura mediante la elaboración y aplicación de normas internacionales de seguridad, establecer sus equipos de intervención en caso de incidentes informáticos, desplegar iniciativas de protección de la infancia en línea, así como crear la capacidad y los conocimientos humanos necesarios.[89]

---

86 UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, *La Agenda sobre Ciberseguridad Global*, (23 de mayo de 2022), https://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=09&ipage=18&ext=html#:~:text=La%20Agenda%20sobre%20Ciberseguridad%20Global%20(GCA)%20de%20la%20UIT%2C,la%20sociedad%20de%20la%20informaci%C3%B3n.

87 UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, *Agenda sobre Ciberseguridad Global (GCA) de la Unión Internacional de Telecomunicaciones*, http://www.sistematizacion.com.ar/cuadernillos/oea/4/4_7_15_1_2_2.pdf.

88 SECRETARIO GENERAL DE LA UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, *Transmisión del informe del expresidente del Grupo de Expertos de Alto nivel de la Agenda sobre Ciberseguridad Global*, Documento C19/58-S, Ginebra, 6 de mayo de 2019.

89 *Idem*.

II. MARCO JURÍDICO NACIONAL SOBRE LA CIBERSEGURIDAD

1. *Constitución Política de los Estados Unidos Mexicanos*

La Constitución Política de los Estados Unidos Mexicanos (CPEUM) no regula expresamente la materia de ciberseguridad. Sin embargo, existen disposiciones referentes a las telecomunicaciones, a la protección de datos personales, a la seguridad pública y la nacional, entre otros elementos, que pueden sentar las bases jurídicas para normarla. Sin perjuicio de su vigencia, algunas normas constitucionales podrían desarrollar un sistema jurídico más completo que contemple tanto los derechos y obligaciones de las personas usuarias como el régimen de competencias distribuidas entre los órganos responsables de los sectores relativos a la ciberseguridad.

Por ejemplo, el artículo 6o. constitucional reconoce el derecho a la información. Su párrafo tercero señala que 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. El apartado A, fracción I, establece un límite a ese derecho, ya que la información pública puede ser reservada temporalmente por razones de interés público y seguridad nacional. Por su parte, el apartado B, fracción I, dispone que, en materia de radiodifusión y telecomunicaciones, el Estado garantizará a la población su integración a la sociedad de la información y el conocimiento mediante una política de inclusión digital universal.

En relación con el dispositivo señalado, el artículo 28 regula al Instituto Federal de Telecomunicaciones, órgano autónomo que tiene por objeto el desarrollo eficiente de la radiodifusión y las telecomunicaciones, y puede otorgar concesiones para el uso del espectro radioeléctrico, entre otras funciones. Dicho instituto podría jugar un papel fundamental para asegurar una conectividad segura, así como fomentar la educación de usuarios, empresas e instituciones públicas para un uso seguro de las redes y dispositivos electrónicos.

Por su parte, el párrafo segundo del artículo 16 constitucional señala que toda persona tiene derecho a la protección de sus datos personales. Este reconocimiento es fundamental porque los ciberataques dirigidos a la ciudadanía tienden a afectar negativamente sus datos personales, por ejemplo, a través de la suplantación de identidad, fraudes ciberné-

ticos, secuestro de información, entre otras conductas delictivas. Además, como se ha visto, algunas instituciones públicas han padecido el robo de información y la difusión indebida de datos personales.

Los párrafos décimo segundo y décimo tercero del artículo precitado disponen la inviolabilidad de las comunicaciones privadas y permiten su intervención en casos penales cuando la fiscalía así lo solicite y la autoridad judicial lo autorice. En este sentido, la intervención de comunicaciones podría representar un instrumento clave para la prevención, investigación y sanción de los ciberdelitos.

La ciberseguridad también puede ser analizada desde las diversas variantes de la seguridad como función esencial del Estado. Así, el artículo 21 constitucional regula la seguridad pública (prevención, investigación y persecución de los delitos) a cargo de las corporaciones policiales y los órganos de procuración de justicia (fiscalías), establece el Sistema Nacional de Seguridad Pública y crea la Guardia Nacional. Además, los párrafos tercero y cuarto del artículo 22 constitucional disponen la extinción de dominio, figura que podría ser aplicada para recuperar bienes en el caso de los productos y ganancias de la delincuencia organizada que opere a través del ciberespacio.

Las normas hasta ahora señaladas reconocen los derechos de las personas. Por ello, deben ser interpretadas a la luz del artículo 1o. constitucional, el cual establece el mandato general para todas las autoridades de tratarlas en condiciones de igualdad y no discriminación. Es decir, cualquier norma relativa a la ciberseguridad deberá ser acorde al marco de los derechos humanos reconocidos en la Constitución y en los tratados internacionales de los cuales el Estado mexicano es parte, sobre todo en lo que concierne a la privacidad.

Asimismo, las normas sobre derechos humanos deben ser complementadas con estructuras orgánicas que procuren y garanticen su efectividad. Al respecto, el artículo 73 constitucional establece las facultades del Congreso de la Unión para legislar sobre diversas materias directa o indirectamente relacionadas con la ciberseguridad. Es decir, algunas competencias podrían encontrar relación directa con la materia, porque inciden sobre las telecomunicaciones y las tecnologías digitales, que son un medio, mientras que otras tocan temas tangencialmente relacionados, como el caso de los datos personales o los archivos gubernamentales. Aquí se presenta un cuadro que sintetiza la materia

que puede regular y su fundamento normativo.

Tabla 2. Facultades constitucionales del Congreso de la Unión para expedir o reformar leyes relacionadas con la ciberseguridad

Materia	Fracción del artículo 73 constitucional
Comercio, intermediación y servicios financieros	X
Levantar y sostener a las instituciones armadas de la Unión, y reglamentar su organización y servicio	XIV
Nacionalidad, condición jurídica de los extranjeros, ciudadanía	XVI
Vías generales de comunicación, tecnologías de la información y la comunicación, radiodifusión, telecomunicaciones, banda ancha e Internet	XVII
Tipos penales específicos, delitos federales, delincuencia organizada, procedimientos penales	XXI
Bases de coordinación en materia de seguridad pública, organizar la Guardia Nacional y las demás instituciones de seguridad pública en materia federal	XXIII
Seguridad privada	XXIII Bis
Función educativa, derechos de autor y propiedad intelectual	XXV
Inversión mexicana, inversión extranjera, transferencia de tecnología y generación, difusión y aplicación de los conocimientos científicos y tecnológicos, así como ciencia, tecnología e innovación	XXIX-F
Seguridad nacional	XXIX-M
Protección de datos personales	XXIX-O
Derechos de niñas, niños y adolescentes	XXIX-P
Homologación de registros civiles, registros públicos inmobiliarios y de personas morales	XXIX-R
Transparencia gubernamental, acceso a la información y protección de datos personales en posesión de las autoridades	XXIX-S
Organización y administración homogénea de los archivos públicos	XXIX-T
Responsabilidades administrativas de los servidores públicos	XXIX-V
Derechos de las víctimas	XXIX-X
Procedimientos civiles y familiares	XXX

Fuente: Elaboración propia.

También se deben considerar las facultades del presidente de la República contenidas en el artículo 89 constitucional, como son nombrar, con aprobación del Senado, a los integrantes de los órganos colegiados encargados de la regulación en materia de telecomunicaciones (fracción III), coroneles y otros oficiales del Ejército, Armada y Fuerza Aérea Nacionales (fracciones IV y V), preservar la seguridad nacional y disponer de la Fuerza Armada permanente para la seguridad interior y defensa exterior de la Federación (fracción VI), disponer de la Guardia Nacional (fracción VII), así como dirigir la política exterior y celebrar tratados internacionales (fracción X). Estas disposiciones cobran relevancia para la materia de ciberseguridad y ciberdefensa, puesto que las fuerzas armadas son las instituciones encargadas de preservar las seguridades exterior y nacional, siendo la Guardia Nacional la institución policial federal encargada de la seguridad pública.

Adicionalmente, si se regulara la materia a través de una ley general aplicable a todos los niveles de gobierno, deberían ser considerados los artículos 115, 116, 117, 118, 122 y 124, que establecen las bases generales de organización y funcionamiento en los municipios, las entidades federativas y la Ciudad de México, y la cláusula residual de competencias, respectivamente.

Por último, destaca el artículo transitorio tercero del decreto del 5 de febrero de 2017 por el que se reformó y adicionó la Constitución en materia de mecanismos alternativos de solución de controversias, mejora regulatoria, justicia cívica e itinerante, y registros civiles, el cual dispone que la ley general en materia de registros civiles deberá prever, entre otros elementos: medidas de seguridad física y electrónica, la posibilidad de realizar trámites con firmas digitales, consultas y emisiones vía remota.[90]

Como se puede observar, la Constitución mexicana contiene disposiciones tangencialmente relacionadas con los fenómenos de ciberseguridad y ciberdefensa. Sin embargo, no existe alguna mención explícita a ellas, y tampoco una facultad expresa para regular la materia.

2. *Leyes federales*

Del mismo modo que en el nivel constitucional, tampoco existen disposiciones legales en el orden jurídico mexicano que se refieran expresamente a la ciberseguridad, pero sí otras que regulan elementos conexos

90 Publicado en el Diario Oficial de la Federación el 5 de febrero de 2017.

como los delitos cometidos a través de sistemas informáticos o en contra de ellos.

En este sentido, el Código Penal Federal sanciona la comunicación de contenido sexual con personas menores de dieciocho años de edad o que no tienen capacidad para comprender el significado del hecho o para resistirlo, la violación a la intimidad sexual por medios electrónicos, la corrupción de personas menores o que no tienen capacidad para comprender o resistir el hecho, la pornografía de personas menores o que no tienen capacidad para comprender el hecho o resistirlo, la revelación, divulgación o utilización indebida de información o imágenes obtenidas por intervención de comunicaciones privadas, así como el acceso ilícito a sistemas y equipos de informática. También tipifica los ataques a las vías de comunicación y las formas de violación de correspondencias.

La legislación mercantil, específicamente el Código de Comercio, regula el Registro Único de Garantías Mobiliarias, que es electrónico, así como el comercio electrónico. La legislación fiscal, en particular el Código Fiscal de la Federación, norma los medios electrónicos, los comprobantes fiscales digitales, entre otros elementos tecnológicos que requieren medidas de seguridad y pueden ser objeto de infracciones o delitos cibernéticos.

Por su parte, las leyes de protección de datos personales en posesión de sujetos obligados y de los particulares obligan a implementar medidas de seguridad para proteger los datos personales, permiten el uso de sistemas de cómputo en la nube y establecen algunas infracciones y delitos relacionados con el uso indebido de los datos. En el mismo sentido, la Ley General de Archivos obliga a establecer programas de seguridad de la información para la preservación a largo plazo de los documentos de archivos electrónicos.

Respecto a la violencia contra la mujer, la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia sanciona la violencia digital y establece las medidas de protección para evitar mayores daños a los derechos de la víctima.

La Ley General del Sistema Nacional de Seguridad Pública prevé normas relacionadas con elementos de la ciberseguridad y la ciberresiliencia. Por ejemplo, contempla la obligación de adoptar medidas de seguridad para proteger las bases de datos que integran el Sistema

Nacional de Información (SNI), las sanciones por el ingreso doloso al mismo, la adopción de medidas para bloquear permanentemente las señales de telefonía celular o de radiocomunicación en el perímetro de los centros de readaptación social, la formulación e implementación de políticas de cooperación internacional para la prevención y persecución de delitos con un componente extraterritorial, así como el desarrollo de las especialidades policiales de alto desempeño. A pesar de que estas disposiciones resultan esenciales, podrían ser insuficientes para generar un sistema completo y coherente que coadyuve a evitar y disminuir los efectos negativos de los ciberataques.

En un tenor similar, el Código Nacional de Procedimientos Penales prevé, entre otros supuestos, el uso de medios electrónicos durante el proceso penal, la intervención de comunicaciones privadas, así como el aseguramiento de productos relacionados con delitos de propiedad intelectual y derechos de autor. Sin embargo, no contiene disposiciones específicamente referidas a evidencias digitales similares a las contenidas en el Convenio sobre la Ciberdelincuencia. Sin ser exhaustivo, en el anexo 1 se resume la normativa constitucional y legal vigente en México sobre ciberseguridad.

3. *Otros ordenamientos*

A diferencia de lo que acontece con la normativa constitucional y legal, algunas normas y ordenamientos administrativos en México sí prevén explícitamente definiciones, órganos y procedimientos relacionados con la ciberseguridad (véase el anexo 2 donde se incluye un listado no exhaustivo de las normas administrativas en materia de ciberseguridad y su contenido relevante para la presente obra).

A manera de ejemplo, el Reglamento de la Ley de la Guardia Nacional regula la intervención de comunicaciones privadas y las operaciones encubiertas y de usuarios simulados. También prevé que la Dirección General de Inteligencia es competente para determinar métodos de comunicación y redes de información policial para recoger datos relacionados con las formas de organización y modos de operación de las organizaciones delincuenciales. La Dirección General Científica puede vigilar, identificar, monitorear y rastrear la red pública de internet para prevenir conductas delictivas. Además, la Dirección General de Investigación puede establecer y operar métodos de comunicación

y redes de información policial para acopio y clasificación oportuna de los datos delictivos.

Por su parte, el Reglamento de la Secretaría de Seguridad y Protección Ciudadana establece que la Dirección General de Gestión de Servicios, Ciberseguridad y Desarrollo Tecnológico está facultada para proponer, dar solución y seguimiento a los incidentes en materia de ciberseguridad e informática. Inclusive, el Consejo Nacional de Seguridad Pública acordó en diciembre de 2021 implementar un Registro Nacional de Incidentes Cibernéticos (RNIC).

Las instituciones castrenses también han creado áreas especializadas en ciberseguridad tanto de su institución como de la sociedad. Por ejemplo, el Programa Sectorial de Defensa Nacional 2020-2024 establece la necesidad de fortalecer las capacidades del Centro de Operaciones del Ciberespacio.

Respecto a la Secretaría de Marina, la persona titular de la Jefatura del Estado Mayor General de la Armada de México tiene la facultad para planear, conducir y ejecutar actividades de seguridad y ciberdefensa para la protección de la infraestructura crítica de dicha secretaría. Asimismo, su programa sectorial establece como estrategia prioritaria fortalecer las capacidades de seguridad en el ciberespacio para coadyuvar con la seguridad nacional y la seguridad interior. Para ello, creó la Unidad de Ciberseguridad (EMGA-UNICIBER), encargada de planear, conducir y ejecutar las actividades de seguridad de la información, ciberseguridad y ciberdefensa para la protección de la infraestructura crítica de la secretaría.

En otro tenor, destaca el Reglamento Interior del Banco de México, donde se establece que la Dirección de Ciberseguridad tiene la competencia de establecer políticas, lineamientos y estrategias institucionales para fortalecer la ciberseguridad y definir el programa de ciberseguridad y ciberresiliencia de la institución.

Una de las escasas normas mexicanas en la materia es la Norma Mexicana NMX-I-62443-4-1-NYCE-2021, que describe los requisitos del ciclo de vida del desarrollo de productos relacionados con la ciberseguridad para los productos de uso en el entorno de sistemas de control y automatización industrial.

En el ámbito educativo, el Reglamento Interior de la Secretaría de Educación Pública (SEP) contempla la Dirección General de Tecnolo-

gías de la Información y Comunicaciones, que funge como enlace de la SEP con instituciones y empresas tanto nacionales como internacionales relacionadas con la informática, las comunicaciones y la ciberseguridad. Incluso algunos programas sectoriales contemplan educar a la población sobre los riesgos de navegar en internet y las maneras de minimizarlos para evitar ser víctima de posibles hechos delictivos.

Desde la óptica internacional y geopolítica, el Programa Sectorial de Relaciones Exteriores 2020-2024 señala como acción puntal el seguimiento y la atención del avance del comportamiento responsable de los Estados en el ciberespacio dentro del contexto de la seguridad internacional.

Del breve recuento de normas administrativas relativas a la ciberseguridad y del anexo 2 que las detalla, se puede deducir que algunos órganos autónomos, como el Banco de México y el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), así como dependencias y entidades de la Administración Pública Federal, tales como la SEMAR, la SEDENA y la Guardia Nacional, han emitido disposiciones que detallan sus competencias para abordar la materia. No obstante, esta multiplicidad de disposiciones administrativas no constituye un sistema regulatorio completo y coherente, puesto que existen diversos aspectos de la ciberseguridad que necesariamente deben estar previstos en las leyes, ya que pueden afectar los derechos y libertades de las personas.

4. *Impacto normativo u ordenamientos que podrían regular aspectos de la ciberseguridad*

Como se desprende del análisis de las iniciativas en materia de ciberseguridad presentadas hasta el día de hoy, el Poder Legislativo federal encuentra diversas posibilidades: expedir nuevas leyes, reformar leyes vigentes, o una combinación de ambas. Ahora bien, si optara por expedir una ley, tendría que valorar si debe ser de tipo general, nacional o federal. Sobre este punto, es común que otros Estados nacionales que han legislado al respecto, como Estonia y Singapur, establezcan las definiciones y bases generales de coordinación en la legislación emitida por el congreso nacional. Además, en el caso de los Estados federados, como Estados Unidos, Argentina y Brasil, se deja un margen menor de actuación a los congresos locales, puesto que la ciberseguridad y la ciberdefensa son elementos que rara vez se limitan a las fronteras de las divisiones político-administrativas subnacionales.

Otra disyuntiva radica en la conveniencia o no de modificar el texto constitucional, por ejemplo, el artículo 73 para facultar expresamente al Congreso de la Unión, o diversas disposiciones para vincular la ciberseguridad con la seguridad pública y la seguridad nacional. Al respecto, se debe considerar que la técnica legislativa tiende a recomendar el establecimiento de aspectos generales en los textos constitucionales, mientras que las disposiciones más detalladas deberían ser reservadas a la ley.

Asimismo, existen diversos ordenamientos que podrían ser modificados para crear un sistema normativo moderno, completo y coherente que facilite disminuir los efectos nocivos de los ciberataques. Al respecto, podrían ser necesarios procesos de armonización de las leyes procesales (por ejemplo, el Código Nacional de Procedimientos Penales), sustantivas (Código Penal Federal, entre otras) y orgánicas (de la Administración Pública Federal, de la Fiscalía General de la República, del Poder Judicial de la Federación, entre otras). No obstante, por razones de coherencia normativa, todas las reformas planteadas deben encontrarse estrechamente relacionadas, de modo que no se establezcan sistemas diferenciados para responder ante los efectos nocivos de actividades que no suelen discriminar entre la naturaleza de la institución pública amenazada o atacada.

Ahora bien, si se determinara la necesidad de crear un nuevo organismo no parlamentario, tal como una conferencia específica o una comisión en el seno del Sistema Nacional de Seguridad Pública, la ley que lo regula sería el ordenamiento propicio para ser modificado. Como se verá más adelante, una posible ventaja de la creación de una institución específica en la materia radica en que podría contar con los elementos suficientes para su especialización, dado el alto nivel técnico que se requeriría para abordar el tema de ciberseguridad. Por otro lado, la creación de múltiples organismos podría resultar en una pulverización de funciones que tornen inoperante un esquema normativo tendente a coordinar las acciones encaminadas a evitar y responder ante ciberataques.

También se podría analizar la necesidad de reformar las normas que regulan la organización y funcionamiento del Congreso de la Unión. Suponiendo que se optara por crear una nueva comisión u órgano parlamentario bicameral que supervise a los órganos encargados de diseñar e implementar estrategias, programas y políticas de ciberseguridad, se

requeriría reformar la ley orgánica del congreso y los reglamentos unicamerales. Lo mismo sucedería si se decidiera crear una comisión específica encargada de los temas en ciberseguridad dentro de cada cámara. En este aspecto, las comisiones legislativas ya existentes en el seno de ambas cámaras, tales como las de justicia, seguridad ciudadana, y ciencia y tecnología, podrían desarrollar la facultad de control sin necesidad de reformas.

III. CONCLUSIONES SOBRE EL MARCO REGULATORIO DE LA CIBERSEGURIDAD

A partir de la revisión del marco jurídico mexicano, se identificaron diversas disposiciones que regulan de manera directa y expresa, o indirecta y tácita, la materia de ciberseguridad. Asimismo se logró identificar algunos órganos encargados de la ciberseguridad en México, si bien estos tienden a enfocarse en la seguridad de los sistemas de las propias instituciones a las que están adscritos.

Por ejemplo, existen áreas específicas dentro de los organismos constitucionalmente autónomos, tales como el Banco de México. También se encontraron áreas en dependencias del Poder Ejecutivo, tales como la Unidad de Ciberseguridad de la Secretaría de Marina o diversas direcciones de la Guardia Nacional, la cual incluso cuenta con un equipo nacional de respuesta a incidentes cibernéticos. Otras dependencias no cuentan con áreas específicas, pero se encargan de aspectos relacionados con la ciberseguridad, por ejemplo, la Secretaría de Infraestructura, Comunicaciones y Transportes al incidir sobre el ciberespacio, o la Secretaría de Educación Pública al implementar campañas educativas sobre la navegación segura en internet.

Es posible afirmar que los poderes legislativo y judicial pueden conocer, en el ámbito de sus competencias, de cuestiones sobre ciberseguridad. Algunos órganos de ambas cámaras del Poder Legislativo federal, tales como las comisiones de seguridad ciudadana, defensa, marina, comunicaciones y transportes, ciencia, tecnología e innovación, entre otras, pueden conocer sobre la materia mediante sus funciones legislativas y de control. Por su parte, la legislación procesal penal prevé el control jurisdiccional mediante jueces que autorizan o no la intervención de comunicaciones privadas a solicitud de una fiscalía local o la federal.

Como se puede observar, no hay una única institución encargada de la materia que coordine a las demás autoridades. A partir del análisis comparado que se expondrá en el siguiente capítulo, se dará cuenta de ciertas características presentes en otros países que regulan la ciberseguridad, tales como la existencia de una agencia nacional cibernética adscrita a la esfera del Poder Ejecutivo, pero con altos niveles de autonomía.

El diagnóstico del marco jurídico nacional también arroja que existen pocas definiciones directamente relacionadas con la materia a nivel legal. Los conceptos estrechamente relacionados o propios de la ciberseguridad se encuentran definidos principalmente en las normas administrativas aplicables al régimen interno de diversos órganos del Estado mexicano.

Lo anterior parecería soportar la hipótesis que afirma la insuficiencia del marco jurídico mexicano para hacer frente a las vulnerabilidades, amenazas y ataques cibernéticos. Por ello, en lo siguiente se expondrá un estudio que sintetiza la regulación de otras cinco naciones con la finalidad de nutrir el debate legislativo que pretenda elaborar normas adecuadas al contexto mexicano.

CAPÍTULO CUARTO

ESTUDIO COMPARADO DE LA REGULACIÓN SOBRE LA CIBERSEGURIDAD

I. METODOLOGÍA

Una vez considerada la normativa nacional en materia de ciberseguridad, expuesta en el capítulo tercero, se debe mencionar que, para desarrollar una comparación respecto al marco jurídico mexicano, se eligieron casos ejemplares y casos similares. Por un lado, Estados Unidos, Estonia y Singapur fueron seleccionados porque son Estados referentes en materia de inclusión y educación digital, y se encuentran muy avanzados respecto a la regulación sobre el ciberespacio, tal como lo indica su posición en el Índice Global de Ciberseguridad del año 2020 elaborado por la Unión Internacional de Telecomunicaciones. Por otro lado, Argentina y Brasil son Estados federados con niveles de desarrollo político y económico similares al de México, han sido blanco de ciberataques masivos y cuentan con cierto desarrollo legislativo en la materia.

El análisis comparativo se articula a partir de tres categorías principales: 1) normativa, 2) principales órganos encargados, y 3) facultad de control parlamentario.

También se presentan datos descriptivos, tales como población total, población con acceso a internet,[91] porcentaje poblacional con acceso a internet, posición en el Índice Global de Ciberseguridad 2020 de la Unión Internacional de Telecomunicaciones (UIT) y, en su caso, la fecha de adhesión al Convenio de Budapest, todo lo cual se sintetiza en el siguiente cuadro, y se precisa que los casos se ordenaron de acuerdo a su posición en el Índice Global de Ciberseguridad.

91 La distinción entre zonas urbanas y rurales es relevante. Sin embargo, no es posible realizar la diferencia en todos los casos a partir de los datos disponibles.

Tabla 3. Datos sobre países seleccionados para el estudio comparado

País	Población total	Población con acceso a internet	Porcentaje de la población con acceso a internet	Posición en el Índice Global de Ciberseguridad 2020[92]	Fecha de adhesión al Convenio de Budapest
EE. UU.	332,129,757	297,322,868	89.5	1	29/09/2006
Estonia	1,326,535	1,276,521	96.2	3	12/05/2003
Singapur	5,896,686	5,173,907	87.7	4	-
Brasil	213,993,437	160,010,801	74.8	18	16/12/2021
México	131,116,964	100,200,000	76.4	52	-
Argentina	45,605,826	41,586,960	91.2	91	05/06/2018

Fuente: Elaboración propia con base en CONSEJO DE EUROPA, *Chart of signatures and ratifications of Treaty 185*, (12 de mayo de 2022), https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185, INTERNET WORLD STATS, *Usage and population statistics,* (2 de mayo de 2022), https://www.internetworldstats.com; y UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, *Global Cybersecurity Index 2020*, ITU Publications, 2021, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

II. CASOS

1. *Estados Unidos (EE. UU.)*

Sin duda alguna, EE. UU. es un blanco común de ciberataques por parte de quienes buscan contrarrestar su poderío económico y militar. Es por ello que ha respondido con abundantes regulaciones y órganos encargados de la ciberseguridad, ciberdefensa y ciberresiliencia. No es casual que se ubique en la primera posición del Índice Global de Ciberseguridad 2020 de la UIT. Aproximadamente el 89.5% de su población cuenta con acceso a internet y el país se adhirió al Convenio de Budapest el 29 de septiembre de 2006.

A. *Normativa*

EE. UU. comenzó abordando *la ciberseguridad a través de estatutos, re-*

92 UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, *Global Cybersecurity Index 2020*, ITU Publications, 2021, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

gulaciones y requisitos de la industria privada específicos del sector. A nivel federal, numerosas agencias imponen estándares de ciberseguridad a través de una variedad de mecanismos regulatorios y de aplicación.[93] Por ejemplo, los servicios financieros y el sector salud son los más regulados en materia de ciberseguridad, ya que las instituciones de estos ramos son obligadas a proteger sus sistemas e información digitales. No obstante, durante la última década, se han regulado aspectos más generales como la seguridad de las infraestructuras críticas de información. En la siguiente tabla se sintetizan los ordenamientos estadounidenses sobre ciberseguridad y sus contenidos, presentados en orden cronológico.

Tabla 4. Normativa de Estados Unidos relativa a la ciberseguridad

Ordenamiento	Contenido
Ley de Responsabilidad y Portabilidad del Seguro de Salud de 1996 (*Health Insurance Portability and Accountability Act*, HIPAA)	• Su regla de privacidad prohíbe a los proveedores y a las empresas de atención médica divulgar información protegida a cualquier persona que no sea un paciente y sus representantes autorizados sin su consentimiento. • Regula los expedientes clínicos electrónicos y sus medidas de seguridad. • Autoriza divulgar información de salud a los funcionarios encargados de hacer cumplir la ley mediante órdenes judiciales.
Ley Gramm-Leach-Bliley de 1999[94]	• Regula el intercambio de información entre entidades del sector bancario, los requisitos para la protección de datos personales y la obligación de establecer y difundir una política de privacidad.
Ley de Investigación y Desarrollo de Ciberseguridad (*Cyber Security Research and Development Act*)[95]	• Autoriza el financiamiento en investigación y desarrollo de la seguridad informática y de las redes y programas de becas de investigación. • Define conceptos como incidente, seguridad de la información, sistema de seguridad nacional, entre otros. • Autoriza al Departamento de Seguridad Nacional (*Department of Homeland Security*, DHS) para aplicar las políticas de seguridad de la información en los sistemas del Poder Ejecutivo federal que no sean de seguridad nacional, incluida la prestación de asistencia técnica y el despliegue de tecnologías para dichos sistemas. • Establece las facultades de la Oficina de Gestión y Presupuesto (*Office of Management and Budget*, OMB) para supervisar las prácticas de seguridad de la información de las agencias federales. • Proporciona un marco para garantizar la efectividad de los controles de seguridad de la información.

93 CIBERSEGURIDAD, *Normativa EE. UU.*, (15 de abril de 2022), https://ciberseguridad.com/normativa/eeuu.

94 *Gramm-Leach Bliley Act*, Public Law 106–102, 113 Stat. 1338, 12 de noviembre de 1999, https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf.

95 Cyber Security Research and Dev*elopment Act*, Public Law 107–305, 116 Stat. 2367, 27 de noviembre de 2002, https://www.congress.gov/107/plaws/publ305/PLAW-107publ305.pdf.

Ordenamiento	Contenido
	• Exige que el Director de la Oficina de Gestión y Presupuesto informe al Congreso sobre la eficacia de las políticas de seguridad de la información y los procedimientos de notificación de violación de datos.
Ley de Protección de Ciberseguridad Nacional (*National Cybersecurity Protection Act of 2014*)[96]	• Proporciona un marco para garantizar la efectividad de los controles de seguridad de la información. • Establece un centro de operaciones para la ciberseguridad (*National Cybersecurity and Communications Integration Center*), dependiente de la Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA), que funge como una interfaz civil federal para el intercambio multidireccional e intersectorial de información relacionada con ciberamenazas, medidas defensivas, riesgos de ciberseguridad, análisis, alertas e incidentes.
Ley de mejora de la ciberseguridad de 2014 (*Cybersecurity Enhancement Act of 2014*)[97]	• Busca promover la asociación público-privada voluntaria y continua para mejorar la ciberseguridad y reforzar la investigación y el desarrollo de la mano de obra y la educación de la ciudadanía en temas de ciberseguridad. • Las agencias y departamentos desarrollarán y actualizarán cada 4 años un plan estratégico de investigación y desarrollo sobre ciberseguridad basado en una evaluación de riesgos. • El Instituto Nacional de Estándares y Tecnología (*National Institute of Standards and Technology*, NIST) apoyará la investigación en materia de ciberseguridad a través de programas y actividades. • Busca educar a la sociedad sobre los riesgos y medidas de seguridad mediante programas y concursos. • Establece un programa federal de becas de 3 años para estudios sobre ciberseguridad.
Ley de evaluación del personal de ciberseguridad (*Cybersecurity Workforce Assessment Act*)[98]	• Exige al Secretario de Seguridad Nacional que evalúe el personal de ciberseguridad del departamento a su cargo y desarrolle una estrategia global de personal capacitado en la materia, así como de becas para su formación.
Ley de intercambio de información sobre ciberseguridad (*Cybersecurity Information Sharing Act of 2015*)[99]	• Permite el intercambio de información sobre el tráfico de internet entre el gobierno y las empresas de tecnología. • Define conceptos como ciberataque (*cyber attack*) cibercampaña de consecuencia significativa (*cyber campaign of significant consequence*), amenaza de ciberseguridad (*cybersecurity threat*), respuesta a incidentes *(incident response*), entre otros.

96 *National Cybersecurity Protection Act of 2014*, Public Law 113–282, 128 Stat. 3066, 18 de diciembre de 2014, https://www.congress.gov/113/statute/STATUTE-128/STATUTE-128-Pg3066.pdf.

97 *Cybersecurity Enhancement Act of 2014,* Public Law 113–274, 128 Stat. 2971, 18 de diciembre de 2014, https://www.congress.gov/113/statute/STATUTE-128/STATUTE-128-Pg2971.pdf.

98 *Cybersecurity Workforce Assessment Act,* Public Law 113–246, 128 Stat. 2880, 18 de diciembre de 2014, https://www.congress.gov/113/statute/STATUTE-128/STATUTE-128-Pg2880.pdf.

99 *Cybersecurity Information Sharing Act of 2015*, 114, S. 754, 27 de octubre de 2015, https://www.congress.gov/114/bills/s754/BILLS-114s754es.pdf.

Ordenamiento	Contenido
Ley de Innovación y Competitividad de los Estados Unidos (*American Innovation and Competitiveness Act*)[100]	• Prevé la investigación en ciberseguridad. • Faculta al Instituto Nacional de Estándares y Tecnología (NIST) para sensibilizar a la población sobre las normas de ciberseguridad voluntarias y dirigidas por la industria y las mejores prácticas para proteger las infraestructuras críticas.
Ley de ciberseguridad para pequeñas empresas del NIST (*NIST Small Business Cybersecurity Act*)[101]	• Obliga al Director del NIST a difundir directrices para ayudar a las pequeñas empresas a identificar, evaluar, gestionar y reducir sus riesgos de ciberseguridad.
Ley de la Agencia de Ciberseguridad y Seguridad de la Infraestructura de 2018 (*Cybersecurity and Infrastructure Security Agency Act of 2018*)[102]	• Define conceptos como infraestructura crítica de información (*critical infrastructure information*), riesgo de ciberseguridad (*cybersecurity risk*), programa de protección de infraestructuras críticas, sistema seguro, entre otros. • Reforma la Agencia de Ciberseguridad y Seguridad de la Infraestructura (*Cybersecurity and Infrastructure Security Agency*, CISA), la cual: o Depende del Departamento de Seguridad Interior. o Dirige los programas, las operaciones y la política de ciberseguridad y de seguridad de las infraestructuras críticas. o Se coordina con las entidades federales y no federales, incluidas las internacionales, para llevar a cabo actividades de ciberseguridad y seguridad de infraestructuras críticas. o Designa a un coordinador de ciberseguridad en cada estado.
Ley de Mejora de la Ciberseguridad del Internet de las Cosas[103]	• Establece normas mínimas de seguridad para los dispositivos del Internet de las Cosas que son propiedad o están controlados por el gobierno federal. • Obliga al contralor general a presentar ante comisiones del Senado y de la Cámara de Representantes un informe sobre la efectividad de las guías elaboradas y sobre los proyectos diseñados para ayudar en la gestión de posibles vulnerabilidades de seguridad asociadas al uso de dispositivos, redes y sistemas tradicionales de tecnologías de la información.

100 *American Innovation and Competitiveness Act*, Public Law 114–329, 130 Stat. 2969, 6 de enero de 2017, https://www.congress.gov/114/plaws/publ329/PLAW-114publ329.pdf.

101 *NIST Small Business Cybersecurity Act*, Public Law 115–236, 132 Stat. 2444, 14 de agosto de 2018, https://www.congress.gov/115/plaws/publ236/PLAW-115publ236.pdf.

102 *Cybersecurity and Infrastructure Security Agency Act of 2018*, Public Law 115–278, 132 Stat. 4168, 16 de noviembre de 2018, https://www.congress.gov/115/plaws/publ278/PLAW-115publ278.pdf.

103 *Internet of Things Cybersecurity Improvement Act of 2020*, Public Law 116–207, 134 Stat. 1001, 4 de diciembre de 2020, https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.pdf.

Ordenamiento	Contenido
Ley del Consorcio Nacional de Preparación para la Ciberseguridad de 2021 (*National Cybersecurity Preparedness Consortium Act of 2021*)[104]	• Autoriza al Secretario de Seguridad Nacional a trabajar con consorcios de ciberseguridad para atender riesgos e incidentes de ciberseguridad • Obliga al Secretario de Seguridad Nacional a hacer planes y estrategias de ciberseguridad, por ejemplo, la *Estrategia de seguridad nacional para mejorar la ciberseguridad de los gobiernos estatales, locales, tribales y territoriales* (*Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments*).
Ley de 5G y Más Allá Seguros de 2020 (*Secure 5G and Beyond Act of 2020*)[105]	• Exige al Presidente que desarrolle una estrategia para garantizar la seguridad de los sistemas e infraestructuras de telecomunicaciones móviles de nueva generación en Estados Unidos y ayudar a los aliados y socios estratégicos a maximizar la seguridad de los sistemas, infraestructuras y programas informáticos de telecomunicaciones móviles de nueva generación.
Ley de respuesta y recuperación cibernéticas de 2021 (*Cyber Response and Recovery Act of 2021*)[106]	Establece, regula y define: • Conceptos como *incidente significativo* (*significant incident*), entendido como un incidente o grupo de incidentes relacionados que resulten, o puedan resultar, en un daño demostrable para los intereses de la seguridad nacional, las relaciones exteriores o la economía nacional, la confianza pública, las libertades civiles o la salud y seguridad públicas de la población. • La declaración de un incidente significativo. • El Fondo de Respuesta y Recuperación Cibernética (*Cyber Response and Recovery Fund*) para asegurar un mínimo de recursos presupuestarios.
Ley de Autorización de la Defensa Nacional para el año fiscal 2021 (*National Defense Authorization Act for Fiscal Year* 2022)[107]	• Establece la Oficina del Ciber Director Nacional (*Office of the National Cyber Director*). - Depende de la Oficina Ejecutiva del Presidente. - Su titular es designado por el presidente con la aprobación del Senado por un período indefinido. - Asesora al presidente y a los consejos de seguridad nacional e interior sobre las políticas y estrategias de seguridad cibernética y de respuesta a incidentes. - Formula y coordina la Estrategia Nacional Cibernética (*National Cyber Strategy*).

104 *National Cybersecurity Preparedness Consortium Act of 2021*, Public Law 117–122, 136 Stat. 1193, 12 de mayo de 2022, https://www.congress.gov/117/plaws/publ122/PLAW-117publ122.pdf.

105 *Secure 5G and Beyond Act of 2020*, Public Law 116–129, 134 Stat. 223, 23 de marzo de 2020, https://www.congress.gov/116/plaws/publ129/PLAW-116publ129.pdf.

106 *Cyber Response and Recovery Act of 2021*, Public Law 117, S.1316, 22 de abril de 2021, https://www.congress.gov/117/bills/s1316/BILLS-117s1316is.pdf.

107 *National Defense Authorization Act for Fiscal Year 2022*, Public Law 117–81, 135 Stat. 1541, 27 de diciembre de 2021, https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf.

Ordenamiento	Contenido
Código de los Estados Unidos, Título 6, Capítulo 1 (Organización de la Seguridad Nacional) subcapítulo XVIII, parte A – Ciberseguridad e Infraestructura de Seguridad.	Obliga a establecer: • Un sistema federal de detección y prevención de intrusiones. • Una base de datos nacional de activos. • La oficina conjunta de planificación cibernética (*Joint cyber planning office*). • Los coordinadores estatales de ciberseguridad. • Las agencias de gestión de riesgos sectoriales (*sector risk management agencies*). • El Comité Consultivo de Ciberseguridad. • Programas de becas, educación, formación, reclutamiento y retención de recursos humanos especializados en ciberseguridad. • Programas de subvenciones de ciberseguridad estatal y local. • Programas nacionales de ejercicios cibernéticos. • Programa *CyberSentry* para supervisar y detectar riesgos de ciberseguridad en las infraestructuras críticas.
Código de los Estados Unidos, Título 6, Capítulo 6 – Ciberseguridad, subcapítulo II— mejora de la ciberseguridad federal y subcapítulo III—otras materias sobre ciberseguridad.	• Regula la aprehensión y persecución de cibercriminales internacionales, concepto que define como un individuo (1) que probablemente cometió un ciberdelito o un delito contra la propiedad intelectual en contra de los intereses de los Estados Unidos o de sus ciudadanos, y (2) para quien un juez de Estados Unidos ha emitido una orden de detención o la Interpol haya difundido una notificación internacional de búsqueda. • Dispone la mejora de la ciberseguridad en el sector salud y de los servicios de emergencia.

Fuente: Elaboración propia con base en la revisión de la normativa de EE. UU.

Además, debido a la estructura federal de EE. UU., los estados también han emitido leyes y normas administrativas para regular en temas de ciberseguridad y ciberdelincuencia. Por ejemplo, desde 2003 el estado de California exige que cualquier compañía que mantenga datos personales y sufra una violación de seguridad debe revelar los detalles del evento; en 2016 prohibió el uso de *ransomware,* y en 2019 prohibió el uso de *bots* para interactuar con otra persona en línea con la intención de engañarla e incentivar una transacción comercial o influir en su voto.[108]

B. *Organismos*

EE. UU. cuenta con diversos organismos encargados de planear, coordinar, implementar y supervisar las estrategias, políticas y programas

108 Debido a la multiplicidad de normas a nivel estatal, se sugiere consultar la recopilación sobre legislación en materia de ciberseguridad que elabora la Conferencia Nacional de Legislaturas Locales: NATIONAL CONFERENCE OF STATE LEGISLATURES, *Cybersecurity Legislation 2021*, (22 de mayo de 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2021.aspx#2021.

en materia de seguridad cibernética y de las infraestructuras críticas. Por ejemplo, el Instituto Nacional de Estándares y Tecnología (*National Institute of Standards and Technology* o NIST) creó un Marco de Seguridad Cibernética para desarrollar un conjunto voluntario y consensuado de normas, directrices, mejores prácticas, metodologías y procesos a fin de reducir de forma rentable los riesgos cibernéticos para las infraestructuras críticas e identificar, proteger, detectar, responder y recuperarse de incidentes de ciberseguridad.[109]

Por su parte, la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (*Cybersecurity and Infrastructure Security Agency* o CISA) busca garantizar la seguridad, resiliencia y confiabilidad de los sistemas cibernéticos nacionales; impulsar la colaboración con el sector privado, la academia y el gobierno para crear una fuerza de trabajo cibernética; fomentar el desarrollo y el uso de tecnologías seguras, y promover mejores prácticas.[110] El director de la agencia tiene la facultad de establecer una guardia tecnológica nacional denominada *NET Guard*, la cual está compuesta por equipos locales de voluntarios con experiencia en las áreas relevantes de la ciencia y la tecnología con el objetivo de ayudar a las comunidades a responder y recuperarse de los ataques a los sistemas de información y a las redes de comunicaciones.[111]

Por su parte, la Oficina del Ciber Director Nacional (*Office of the National Cyber Director*) fue creada en el marco de la Ley de Autorización de la Defensa Nacional para el año fiscal 2021. El director actúa como el asesor principal del presidente en materia de política y estrategia de ciberseguridad, y se coordina con la industria y las partes interesadas internacionales en esta materia. También busca garantizar la coherencia federal, mejorar la colaboración público-privada e incrementar la resiliencia presente y futura.[112]

Otras instituciones involucradas en materia de ciberseguridad, ciberdefensa y seguridad de infraestructuras críticas de información son: el Departamento de Estado, el Departamento de Defensa, a través de su

109 *National Institute of Standards and Technology Act*, Public Law 100-418, 102 Stat. 1427, https://uscode.house.gov/statviewer.htm?volume=102&page=1427.

110 CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, *Factsheet*, 2021, https://www.cisa.gov/sites/default/files/publications/CISA-Factsheet_16-Dec-2021-V4_508.pdf.

111 *Código de los Estados Unidos*, Título 6, artículo 656.

112 THE WHITE HOUSE, *Office of the National Cyber Director*, (22 de abril de 2022), https://www.whitehouse.gov/oncd.

Cibercomando (*United States Cyber Command*); la Agencia Central de Inteligencia (CIA), la Oficina Federal de Investigación (FBI); la Agencia de Seguridad Nacional (NSA); la Agencia Nacional de Inteligencia Geoespacial (NGA); la Agencia de Inteligencia de Defensa (*Defense Intelligence Agency*), así como las agencias sectoriales.[113]

C. *Control parlamentario*

El Congreso de los Estados Unidos ejerce un amplio control sobre los actos del Ejecutivo, y debido a las implicaciones para la seguridad nacional y exterior, la ciberseguridad es una cuestión dentro de ello, tal como lo evidencian diversas secretarías de Estado que deben presentar ante el Congreso estrategias y planes para implementar y supervisar sus funciones en este rubro.

En particular, el Contralor General debe presentar bimestralmente un informe con los resultados del estudio sobre el estado de la ciberseguridad ante la Comisión de Comercio, Ciencia y Transporte del Senado y la Comisión de Ciencia, Espacio y Tecnología de la Cámara de Representantes.[114]

También las agencias y departamentos competentes, a través del Consejo Nacional de Ciencia y Tecnología (*National Science and Technology Council*) y del Programa de Investigación y Desarrollo de Redes y Tecnologías de la Información (*Networking and Information Technology Research and Development Program*), presentan a aquellas comisiones el plan estratégico de ciberseguridad, una actualización cuatrienal y la hoja de ruta de implementación.

Respecto a la formación y contratación de personas especializadas en ciberseguridad, el director de la Fundación Nacional de Ciencias (*National Science Foundation*) es el encargado de evaluar e informar periódicamente al Congreso sobre el éxito de la contratación de personas becadas. Asimismo, también notifica sobre la adopción de mecanismos automatizados para el intercambio de indicadores de amenazas y medidas defensivas. Finalmente, presenta a la Comisión de Seguridad Nacional y Asuntos Gubernamentales del Senado y a la Comisión de Seguridad Nacional de la Cámara de Representantes un informe anual sobre el progreso en el desarrollo de las capacidades ciberdefensivas.

113 *Código de los Estados Unidos,* Título 6, artículo 652.

114 *Cybersecurity Enhancement Act... cit.*

Por último, la Oficina del Ciber Director Nacional es responsable de informar anualmente al presidente y al Congreso sobre la implementación y efectividad de las políticas y estrategias cibernéticas nacionales, así como también acerca de las ciberamenazas que enfrentan, entre muchas otras cuestiones.

2. *Argentina*

Argentina es un Estado sudamericano, federal y presidencialista en el cual 91.2% de su población cuenta con acceso a internet. El país se ubicó en la posición 91 del Índice Global de Ciberseguridad 2020 de la UIT y se adhirió al Convenio de Budapest el 5 de junio de 2018.[115]

Su Centro Nacional de Respuesta a Incidentes Informáticos (CERT.ar) registró un total de 591 ataques durante 2021, cifra 261% mayor a la del 2020, donde el 55% de los incidentes reportados correspondieron a *phishing*. Los ciberataques más dañinos que se registraron fueron por *ransomware* (*software* malicioso), los cuales afectaron principalmente a organizaciones privadas y públicas, y dentro de estas últimas, a las del sector financiero.[116]

En 2015, la Presidencia de la República emitió un decreto para reestructurar el control gubernamental de la infraestructura crítica nacional y creó la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad, institución dependiente de la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad, bajo el control de la Secretaría de Gabinete de la Jefatura de Gabinete de Ministros.[117] En el ámbito de la investigación de delitos, se estableció un punto focal en materia de ciberdelincuencia a cargo de la oficina del Ministerio Público Fiscal.[118]

---

115 Ley 27.411, Convenio Sobre Ciberdelito del Consejo de Europa, de 15 de diciembre de 2017, *Boletín Oficial*, Argentina, https://www.argentina.gob.ar/normativa/nacional/ley-27411-304798.

116 DIRECCIÓN NACIONAL DE CIBERSEGURIDAD, *Incidentes informáticos. Informe anual de incidentes de seguridad informática registrados en el 2021 por el CERT.ar.*, Argentina, febrero, 2022, pp. 2 y 3, https://www.argentina.gob.ar/sites/default/files/2022/02/informe_2_cert_2021_f_.pdf.

117 Decreto 1067/2015, Incorporase al anexo I del artículo 1° del Decreto n° 357 de fecha 21 de febrero de 2002, sus modificatorios y complementarios —organigrama de aplicación de la Administración Pública Nacional centralizada—, apartado XI, la Subsecretaría de Protección de Infraestructuras Criticas de Información y Ciberseguridad en el ámbito de la Secretaria de Gabinete de la Jefatura de Gabinete de Ministros, de 10 de junio de 2015, *Boletín Oficial*, 12 de junio de 2015, núm. 33149, Argentina, p. 1, http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=247971.

118 CIBERSEGURIDAD, *Normativa Argentina*, (18 de mayo de 2022), https://ciberseguridad.com/normativa/latinoamerica/argentina.

Debido a que el gobierno y comercio electrónicos siguen en crecimiento, las instituciones públicas argentinas han llevado a cabo campañas para educar a la ciudadanía en temas de ciberseguridad. Por ejemplo, *Internet Sano* del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC), a cargo de la Jefatura de Ministros, se centra en mejorar las prácticas para un uso seguro de internet,[119] y *Con Vos en la Web*, conducido por el Ministerio de Justicia y Derechos Humanos, se ha buscado desarrollar competencias para una adecuada ciudadanía digital a través de recomendaciones y tutoriales sobre el uso seguro de internet y las redes sociales.[120]

Al igual que otras naciones, el gobierno argentino ha desarrollado e implementado una Estrategia Nacional de Ciberseguridad[121] en coordinación con diversos organismos públicos, instituciones académicas y el sector privado. Las Fuerzas Armadas también realizan periódicamente Ejercicios Nacionales de Respuesta a Incidentes Cibernéticos (ENRIC) para desarrollar buenas prácticas e inspeccionar el nivel de seguridad en los sistemas informáticos.

A. *Normativa*

Argentina cuenta con una amplia y diversa normativa en materia de ciberseguridad, aunque la mayoría de las normas son de naturaleza administrativa. Cuatro leyes torales conforman su sistema jurídico sobre ciberseguridad: 1) el Código Penal, modificado mediante las reformas conocidas como *Ley de Delito Informático* y la *Ley de Grooming*; 2) la Ley de Inteligencia Nacional; 3) la Ley de Protección de los Datos Personales, y 4) la Ley de Firma Digital,[122] todas ellas desarrolladas mediante normas de carácter administrativo. La siguiente tabla resume los principales ordenamientos relativos a la ciberseguridad del Estado argentino, los cuales se exponen en orden cronológico.

---

119 JEFATURA DE GABINETE DE MINISTROS, *Internet Sano*, (18 de mayo de 2022), http://seguridadinformatica.sgp.gob.ar/paginas.dhtml?pagina=52.

120 MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, *Acerca de Con Vos en la Web*, (18 de mayo de 2022), https://www.argentina.gob.ar/justicia/convosenlaweb.

121 Resolución 829/2019, Estrategia Nacional de Ciberseguridad, de 24 de mayo de 2019, *Boletín Oficial*, 28 de mayo de 2019, https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-829-2019-323594/texto.

122 JEFATURA DE GABINETE DE MINISTROS, *Normativa - Ciberseguridad*, (13 de mayo de 2022), https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad/normativa.

Tabla 5. Normativa de Argentina relativa a la ciberseguridad

Ordenamiento	Contenido
Ley 25.326 de Protección de los Datos Personales[123]	• Su objeto es la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios de tratamiento de datos tanto públicos como privados. • El responsable o usuario de datos personales debe adoptar las medidas necesarias para garantizar su seguridad y confidencialidad. • Sanciona a la persona que, a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, acceda a un banco de datos personales.
Ley 25.506 de Firma Digital[124]	• Reconoce la eficacia jurídica de la firma electrónica y de la firma digital. • Regula los certificados digitales y los certificadores licenciados. • Establece los derechos y obligaciones del titular de un certificado digital. • Establece las autoridades y un régimen de sanciones. • Instaura la Infraestructura de Firma Digital y el sistema de auditoría.
Ley 26.388 de Delito Informático[125]	• Modifica el Código Penal de la Nación para introducir nuevos tipos penales, todos en materia informática.
Resolución 580/2011[126]	• Crea el Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad (ICIC). • Busca elaborar un marco regulatorio específico para identificar y proteger las infraestructuras estratégicas y críticas de las entidades y jurisdicciones, los organismos interjurisdiccionales, y las organizaciones civiles y del sector privado que así lo requieran, además de fomentar la cooperación y colaboración.
Disposición ONTI 3/2013[127]	• Aprueba la Política de Seguridad de la Información Modelo. • Regula la seguridad de la información, la evaluación, el tratamiento y la gestión de riesgos.

123 Ley 25.326, Protección de los Datos Personales, de 4 de octubre de 2000, *Boletín Oficial*, 2 de noviembre de 2000, núm. 29517, Argentina, p. 1, http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=64790.

124 Ley 25.506, Firma Digital, de 14 de noviembre de 2001, *Boletín Oficial*, 14 de diciembre de 2001, núm. 29796, Argentina, p. 1, http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm.

125 Ley 26.388, Código Penal, modificación, de 4 de junio de 2008, *Boletín Oficial*, 25 de junio de 2008, núm. 31433, Argentina, p. 1, http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm.

126 Resolución 580/2011, Créase el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad. Objetivos, de 28 de julio de 2011, *Boletín Oficial*, 2 de agosto de 2011, núm. 32204, Argentina, p. 10, http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm.

127 Disposición 3/2013, Apruébase la "Política de Seguridad de la Información Modelo", de 27 de agosto de 2013, *Boletín Oficial*, 2 de septiembre de 2013, núm. 32713, Argentina, p. 12, https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-3-2013-219163/texto.

Ordenamiento	Contenido
Ley 26.904 de *grooming*[128]	• Modifica el Código Penal para considerar como delito el que un adulto contacte por medios electrónicos a menores de edad con el propósito de cometer cualquier delito contra la integridad sexual.
Ley 27.126, Agencia Federal de Inteligencia[129]	• Modifica la Ley 25.520 de Inteligencia Nacional. • Crea la Agencia Federal de Inteligencia. • Decreta que los organismos del Sistema de Inteligencia Nacional serán supervisados por la Comisión Bicameral del Congreso argentino con la finalidad de fiscalizar que su funcionamiento se ajuste a la normativa. • La Comisión Bicameral tendrá facultades para investigar de oficio.
Resolución 234/2016[130]	• Aprueba el Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos. • Define conceptos como *ciberdelito*, *grooming*, *evidencia digital*, *hash*, *dirección IP*, entre otros.
Decreto 577/2017[131]	• Crea al Comité de Ciberseguridad, integrado por representantes de diversos ministerios, el cual deberá elaborar la Estrategia Nacional de Ciberseguridad.
Resolución 1523/2019[132]	• Aprueba las definiciones de *Infraestructuras Críticas* y de *Infraestructuras Críticas de Información*. • Su Anexo II incluye un Glosario de Términos de Ciberseguridad.[133]
Resolución 829/2019[134]	• Aprueba la Estrategia Nacional de Ciberseguridad 2019.
Disposición 1/2021[135]	• Crea el Centro Nacional de Respuesta a Incidentes Informáticos (CERT.ar.), dependiente de la Dirección Nacional de Ciberseguridad.

128 Ley 26.904, Código Penal, incorporación, de 13 de noviembre de 2013, *Boletín Oficial*, 11 de diciembre de 2013, núm. 32783, Argentina, p. 1, http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=223586.

129 Ley 27.126, Creación de la Agencia Federal de Inteligencia, modificación Ley n° 25.520, de 3 de marzo de 2015, *Boletín Oficial*, 5 de marzo de 2015, núm. 33083, Argentina, p. 1, http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243821/norma.htm.

130 Resolución 234/2016, Protocolo general en la investigación y proceso de recolección de pruebas en ciberdelitos, de 7 de junio de 2016, *Boletín Oficial*, 14 de junio de 2016, núm. 33399, Argentina, p. 25, http://servicios.infoleg.gob.ar/infolegInternet/anexos/260000-264999/262787/norma.htm.

131 Decreto 577/2017, Comité de Ciberseguridad, creación, de 28 de julio de 2017, *Boletín Oficial*, 31 de julio de 2017, núm. 33677, Argentina, p. 3, http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/277518/norma.htm.

132 Resolución 1523/2019, Definición de Infraestructuras Críticas, de 12 de septiembre de 2019, *Boletín Oficial*, 18 de septiembre de 2019, núm. 34200, Argentina, p. 15, http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do;jsessionid=E46ECDAB0CF7AC108F7AF9884A6F32D1?id=328599.

133 Anexo II, Glosario de Términos de Ciberseguridad, *Boletín Oficial*, 30 de agosto de 2019, Argentina, https://www.argentina.gob.ar/sites/default/files/infoleg/res1523-2.pdf.

134 Resolución 829/2019, Estrategia Nacional de Ciberseguridad, de 24 de mayo de 2019, *Boletín Oficial*, 28 de mayo de 2019, Argentina, https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-829-2019-323594/texto.

135 Disposición 1/2021, Centro Nacional de Respuesta a Incidentes Informáticos (CERT.art) – créase, de 19 de febrero de 2021, *Boletín Oficial*, 22 de febrero de 2021, núm. 34591, Argentina, p. 101, http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=347311.

Ordenamiento	Contenido
Decisión Administrativa 641/2021[136]	• Establece los requisitos mínimos de seguridad de la información para organismos públicos.
Disposición 8/2021[137]	• Aprueba la *Guía introductoria a la Seguridad para el Desarrollo de Aplicaciones WEB*.
Disposición 6/2021[138]	• Crea al Comité Asesor para el Desarrollo e Implementación de Aplicaciones Seguras.

Fuente: Elaboración propia con base en la revisión de la normativa de Argentina.

B. *Organismos*

El conjunto normativo previamente sintetizado ha dado lugar a la creación de diversas estructuras orgánicas que, en alguna medida, son coordinadas por el Gobierno federal. Algunas se encargan de responder ante incidentes cibernéticos, otras asesoran técnicamente a la administración pública; algunas diseñan la estrategia de ciberseguridad, mientras que otras más se encargan de implementarla. A continuación, se exponen los principales organismos encargados de la ciberseguridad en Argentina.

Tabla 6. Organismos en Argentina encargados de la ciberseguridad

Organismo	Funciones
Agencia Federal de Inteligencia	• Depende del Poder Ejecutivo y es el órgano superior del Sistema de Inteligencia Nacional. • Su titular es designado por el Ejecutivo con acuerdo del Senado. • Produce inteligencia nacional sobre eventos que puedan afectar la defensa nacional, la seguridad interior e inteligencia criminal, referida a delitos federales complejos relativos a terrorismo, narcotráfico, tráfico de armas, trata de personas, ciberdelitos, atentatorios contra el orden económico y financiero, y delitos contra los poderes públicos y el orden constitucional.
Centro Nacional de Respuesta a Incidentes Informáticos (CERT.ar)[139]	• Creado en 2021, coordina la gestión de incidentes de seguridad a nivel nacional y presta asistencia en aquellos que afectan a las entidades y jurisdicciones del sector público nacional, así como a las infraestructuras críticas de información.

136 Decisión Administrativa 641/2021, *Boletín Oficial*, 28 de junio de 2021, Argentina, https://www.argentina.gob.ar/normativa/nacional/decisi%C3%B3n_administrativa-641-2021-351345/texto.

137 Disposición 8/2021, *Boletín Oficial*, 10 de noviembre de 2021, Argentina, https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-8-2021-356582/texto.

138 Disposición 6/2021, *Boletín Oficial*, 4 de diciembre de 2021, Argentina, https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-6-2021-348661/texto.

139 Disposición 1/2021, Centro Nacional de Respuesta a Incidentes Informáticos... *cit.*; JEFATURA DE GABI-

Organismo	Funciones
Comité Asesor para el Desarrollo e Implementación de Aplicaciones Seguras	• Brinda asesoramiento a la Subsecretaria de Tecnologías de Información y las Comunicaciones y a la Dirección Nacional de Ciberseguridad en la elaboración de guías y protocolos de principios y buenas prácticas relacionadas con la seguridad en el desarrollo, contratación e implementación de aplicaciones informáticas utilizadas por los organismos públicos nacionales.
Comité de Ciberseguridad[140]	• Creado en 2017. • Se encuentra en la órbita de la Secretaría de Gobierno de Modernización de la Jefatura de Gabinete de Ministros. • Está integrado por representantes de la citada secretaría, de la Secretaría de Asuntos Estratégicos de la Jefatura de Gabinete de Ministros, del Ministerio de Defensa, del Ministerio de Seguridad, del Ministerio de Relaciones Exteriores y Culto y del Ministerio de Justicia y Derechos Humanos • Es presidido por el Secretario de Gobierno de Modernización. • Se encarga de elaborar la Estrategia Nacional de Ciberseguridad.
Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad[141]	• Depende de la dirección de la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad. • Su responsabilidad primaria es participar en todos los aspectos relativos a la ciberseguridad y protección de las infraestructuras críticas, lo que comprende la generación de capacidades de detección, defensa, respuesta y recuperación ante incidentes del sector público nacional.[142]
División de Delitos Tecnológicos de la Policía Federal Argentina[143]	• Depende del Ministerio de Seguridad. • Investiga los casos de delitos informáticos. • Proporciona información sobre la manera de detectar y comunicar ciberataques.
Equipo de Respuesta a Incidentes de Seguridad Informática del Ministerio de Seguridad de la Nación Argentina (MINSEG-CSIRT)	• Es el equipo de respuesta a incidentes de seguridad informática formado por personal de las cuatro fuerzas de seguridad federales: Gendarmería Nacional, Policía Federal, Policía de Seguridad Aeroportuaria y Prefectura Naval.[144]
Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad	• Asiste a la Secretaría de Gabinete de la Jefatura de Gabinete de Ministros en la formulación de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras críticas del sector público nacional, de las organizaciones civiles, del sector privado y del ámbito académico que así lo requieran, fomentando la cooperación y colaboración.[145]

NETE DE MINISTROS, *CERT.ar*, (3 de abril de 2022), https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar.

140 Decreto 577/2017... *cit.*

141 JEFATURA DE GABINETE DE MINISTROS, *Ciberseguridad*, (3 de abril de 2022), https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad.

142 *Idem*.

143 JEFATURA DE GABINETE DE MINISTROS, *Denunciar un delito informático*, (8 de mayo de 2022), https://www.argentina.gob.ar/denunciar-un-delito-informatico.

144 MINISTERIO DE SEGURIDAD DE ARGENTINA, *MINSEG-CSIRT*, (3 de abril de 2022), https://csirt.minseg.gob.ar.

145 Decreto 1067/2015... *cit.*

Organismo	Funciones
Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) de la Procuración General de la Nación	• Creada en 2015. • Busca robustecer la capacidad de respuesta en materia de detección, persecución y represión de la criminalidad organizada. • Podrá conocer de casos sobre ilícitos constituidos por ataques a sistemas informáticos, o cuando el medio comisivo principal o accesorio de una conducta delictiva incluya la utilización de sistemas informáticos, con especial atención en el ámbito de la criminalidad organizada y crímenes en los que sea necesario realizar investigaciones en entornos digitales. • También realiza tareas de formación, capacitación y comunicación.[146]

Fuente: Elaboración propia.

C. *Control parlamentario*

La Ley 27.126, que modificó la Ley de Inteligencia Nacional, señala que los organismos pertenecientes al Sistema de Inteligencia Nacional serán supervisados por la Comisión Bicameral con la finalidad de fiscalizar que su funcionamiento se ajuste estrictamente a las normas. Dicha comisión tendrá amplias facultades para controlar e investigar de oficio.

3. *Brasil*

Al igual que Argentina, México y Estados Unidos, Brasil es una república presidencialista y federal. Con el 74.8% de su población con acceso a internet y debido a su desarrollo regulatorio y a sus capacidades institucionales, se ubicó en la posición 18 del Índice Global de Ciberseguridad 2020 de la UIT. Comenzó el proceso de adhesión al Convenio de Budapest el 16 de diciembre de 2021. En 2020 fue *el país con mayor índice de víctimas de phishing*.[147] Según estimaciones de 2017, *la ciberdelincuencia provocó pérdidas anuales en Brasil por valor de 20.000.000.000 €,* convirtiéndose en *el segundo país del mundo con más pérdidas por ciberataques, solo detrás de China*.[148]

Debido a la gran cantidad de ciberataques, el Estado brasileño ha tratado de hacerles frente desde hace algunas décadas.[149] A diferencia de la

146 MINISTERIO PÚBLICO FISCAL, *Unidad Fiscal Especializada en Ciberdelincuencia*, (3 de abril de 2022), https://www.mpf.gob.ar/ufeci.

147 ESPAÑA EXPORTACIÓN E INVERSIONES (ICEX), *El mercado de la ciberseguridad en Brasil*, España, 2021, p. 3.

148 *Ibidem*, p. 4.

149 NEVES DE MOURA FILHO, Ronaldo *et al.*, "Regulación de la ciberseguridad en el sector de telecomunicaciones de Brasil: un balance de incentivos en un contexto de neutralidad tecnológica", *Revista Latinoamericana de Economía y Sociedad Digital*, núm. 2, agosto 2021, p. 4, DOI: 10.53857/KMFK7888.

mayor parte del subcontinente, ha buscado estructurar una política propia de ciberseguridad, lo cual fue motivado por las amenazas percibidas ante el crecimiento de usuarios de internet en el país y por su involucramiento activo con la agenda internacional de gobernanza en internet.[150] Las autoridades se han centrado en desarrollar las capacidades para enfrentar la ciberdelincuencia y el ciberactivismo interno, al igual que en ampliar la capacidad del Estado para mitigar las ciberamenazas a nivel internacional.[151]

El primer conjunto normativo brasileño referido a aspectos de la ciberseguridad data de 1984, el cual introdujo la *Política Nacional de Informática* para establecer instrumentos legales y técnicos con el propósito de proteger la confidencialidad de los datos, así como la privacidad y seguridad de personas físicas y jurídicas, privadas y públicas.[152] En 2000 se formuló la primera *Política de Seguridad de la Información*, centrada en la administración pública federal, con el objetivo de defender la soberanía nacional y proteger derechos fundamentales, como la intimidad y la privacidad.[153] En 2003 se instituyó la Cámara de Relaciones Exteriores,[154] órgano consultivo de la Presidencia de la República encargado de implementar los programas de seguridad de la información y cibernética.[155] En 2006 se creó la Dirección de Seguridad de la Información y las Comunicaciones dentro de la estructura del Gabinete de Seguridad Institucional.[156]

Más tarde, en 2008, dicho gabinete publicó una norma para regular la *Gestión de Seguridad de la Información y las Comunicaciones en la Administración Pública Federal*,[157] y en 2010 publicó el *Libro*

150 CRUZ LOBATO, Luisa, "La política brasileña de ciberseguridad como estrategia de liderazgo regional", *URVIO, Revista Latinoamericana de Estudios de Seguridad*, Quito, núm. 20, junio 2017, p. 17, DOI: http://dx.doi.org/10.17141/urvio.20.2017.2576.

151 CIBERSEGURIDAD, *Normativa Brasil*, (27 de abril de 2022), https://ciberseguridad.com/normativa/latinoamerica/brasil.

152 Lei nº 7.232, de 29 de outubro de 1984. Dispõe sobre a Política Nacional de Informática, e dá outras providências, *Diário Oficial da União*, 30 de octubre de 1984, Brasilia, p. 15841, http://www.planalto.gov.br/ccivil_03/leis/l7232.htm.

153 Decreto nº 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, *Diário Oficial da União*, 14 de junio de 2000, núm. 114, Brasilia, p. 2, http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm.

154 Decreto nº 4.801, de 6 de agosto de 2003. Cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo, *Diário Oficial da União*, 7 de agosto de 2003, Brasilia, p. 8, http://www.planalto.gov.br/ccivil_03/decreto/2003/d4801.htm.

155 NEVES DE MOURA FILHO, Ronaldo *et al*., *op. cit*., p. 4.

156 GABINETE DE SEGURIDAD INSTITUCIONAL, *Política Nacional de Segurança da Informação - PNSI*, (27 de mayo de 2022), https://www.gov.br/gsi/pt-br/assuntos/dsi/politica-nacional-de-seguranca-da-informacao-pnsi.

157 Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008. Disciplina a Gestão de Segurança da Infor-

Verde sobre Seguridad Cibernética en Brasil.[158] Ese mismo año, el Departamento de Seguridad de la Información y Comunicaciones publicó la *Guía de Referencia para la Protección de Infraestructuras Críticas de Información*. Por su parte, el Ministerio de Defensa publicó en 2012 el *Libro Blanco de la Defensa Nacional*,[159] el cual trata aspectos de las estrategias de guerra en el medio cibernético.[160]

Ante tal variedad de normas, guías e instrumentos de política pública, se ha señalado que *en el ordenamiento jurídico y normativo brasileño, la ciberseguridad presenta distintas vertientes diferenciadas por su objeto y dependiendo del organismo responsable*.[161] Cuando se busca proteger las infraestructuras críticas para garantizar la estabilidad política y económica, la protección de la sociedad y de los derechos e intereses de las personas, el Gabinete de Seguridad Institucional es el organismo a cargo. Si el objeto es un bien propiedad del Estado que implique a las infraestructuras críticas para la defensa y la soberanía nacional, o en casos de guerra cibernética, el Ministerio de Defensa y las Fuerzas Armadas son los órganos competentes.[162] Inclusive, estas crearon un Comando de Defensa Cibernética, una Escuela Nacional de Defensa Cibernética y un Centro de Ciberdefensa del Ejército (CDCiber).

Recientemente se ha aseverado que *la quinta generación de conectividad móvil de banda ancha se perfila como un catalizador de cambios de paradigma sobre la forma en la que Brasil aborda la ciberseguridad*.[163] En este contexto surgió la Política Nacional de Seguridad de la Información de 2018[164] y la Estrategia Nacional de Seguridad Ci-

---

mação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências, *Diário Oficial da União*, Brasilia, junio de 2008, https://www.gov.br/governodigital/pt-br/legislacao/14_IN_01_gsidsic.pdf.

158 PRESIDENCIA DE LA REPÚBLICA *et al*., *Livro Verde: Segurança Cibernética no Brasil*, Brasilia, 2010, https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2015/10/Livro_Verde_SEG_CIBER.pdf.

159 PRESIDENCIA DE LA REPÚBLICA *et al*., *Livro Branco de Defesa Nacional*, Brasil, 2012, https://www.gov.br/defesa/pt-br/arquivos/2012/mes07/lbdn.pdf.

160 NEVES DE MOURA FILHO, Ronaldo *et al*., *op. cit*., p. 4.

161 *Idem*.

162 *Idem*.

163 *Ibidem*, p. 5.

164 Decreto n° 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional, *Diário Oficial da União*, 27 de diciembre de 2018, núm. 248, Brasilia, p. 23, https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm.

bernética de 2020.[165] Esta última busca armonizar los intereses y esfuerzos de la administración pública, empresas privadas, academia y de la sociedad civil. Sus acciones y objetivos proponen perfeccionar la estructura de ciberseguridad para promover la resiliencia del país frente a amenazas y ataques en el entorno digital, así como su confiabilidad en el escenario internacional.[166]

Respecto a la implementación de la tecnología 5G, el Gabinete de Seguridad Institucional publicó normas que establecen requisitos mínimos de ciberseguridad, especificaciones técnicas y la diversificación de proveedores para las redes de telecomunicaciones utilizadas por el Gobierno Federal.[167] La Agencia Nacional de Telecomunicaciones (ANATEL), ente regulador del sector, aborda la ciberseguridad de manera transversal, en cooperación con otros actores involucrados. Esta publicó en 2020 el *Reglamento de Ciberseguridad Aplicada al Sector de Telecomunicaciones (R-Ciber)*,[168] el cual busca promover una política de ciberseguridad para los prestadores de servicios de telecomunicaciones.[169]

Finalmente, algunos estados brasileños también cuentan con equipos de enjuiciamiento especializados, además de equipos de reacción y respuesta ante incidentes cibernéticos. Asimismo, existen centros de respuesta privados o que atienden a instituciones específicas como el CSIRT de la Cámara de Diputados de Brasil.[170] A continuación se sintetizan y exponen en orden cronológico las principales normas brasileñas que regulan la ciberseguridad.

---

165 Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética, *Diário Oficial da União*, 6 de febrero de 2020, núm. 26, Brasilia, p. 6, https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm.

166 NEVES DE MOURA FILHO, Ronaldo *et al*., *op. cit.*, p. 5.

167 Instrução Normativa nº 4, de 26 de março de 2020. Dispõe sobre os requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G, *Diário Oficial da União*, 27 de marzo de 2020, núm. 60, Brasilia, p. 2, https://www.in.gov.br/web/dou/-/instrucao-normativa-n-4-de-26-de-marco-de-2020-250059468.

168 Resolução nº 740, de 21 de dezembro de 2020. Aprova o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, *Diário Oficial da União*, 24 de diciembre de 2020, núm. 246, Brasilia, p. 55, https://www.in.gov.br/en/web/dou/-/resolucao-n-740-de-21-de-dezembro-de-2020-296152776.

169 NEVES DE MOURA FILHO, Ronaldo *et al*., *op. cit.*, p. 6.

170 Para conocer todos los centros de respuesta a incidentes cibernéticos, públicos y privados, en Brasil, véase CERT.BR, *Grupos de Segurança e Resposta a Incidentes (CSIRTs) Brasileiros*, (22 de mayo de 2022), https://www.cert.br/csirts/brasil.

A. *Normativa*

La siguiente tabla muestra la normativa brasileña existente en materia de ciberseguridad, presentada en orden cronológico.

Tabla 7. Normativa de Brasil relativa a la ciberseguridad

Ordenamiento	Contenido
Ley n° 12.527, de 18 de noviembre de 2011[171]	• Regula los procedimientos para garantizar el derecho de acceso a la información pública y sus restricciones, así como los procedimientos de clasificación, reclasificación y desclasificación.
Decreto n° 7.724 del 16 de mayo de 2012[172]	• Reglamenta la Ley n° 12.527 de 18 de noviembre de 2011. • Precisa las medidas y procedimientos de seguridad de la información pública.
Decreto n° 7.845 del 14 de noviembre de 2012[173]	• Regula los procedimientos para la acreditación de la seguridad y el tratamiento de la información clasificada en el ámbito del Poder Ejecutivo federal. • Establece el Centro de Seguridad y Acreditación.
Ley n° 12.737 sobre delitos cibernéticos[174]	• Modifica el Código Penal y tipifica delitos cibernéticos para sancionar la: o Intrusión de dispositivos informáticos. o Interrupción de un servicio telemático o información de utilidad pública, o impedir o dificultar su restablecimiento. o Falsificación de tarjeta de crédito o débito.

171 Lei n° 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências, *Diário Oficial da União*, 18 de noviembre de 2011, núm. 221-A, Brasilia, p. 1, http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm.

172 Decreto n° 7.724, de 16 de maio de 2012. Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição, *Diário Oficial da União*, 16 de mayo de 2012, Brasilia, p. 1, http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Decreto/D7724.htm.

173 Decreto n° 7.845, de 14 de novembro de 2012, Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento, *Diário Oficial da União*, 16 de noviembre de 2012, Brasilia, p. 1, http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Decreto/D7845.htm.

174 Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências, *Diário Oficial da União*, 3 de diciembre de 2012, núm. 232, Brasilia, p. 1, http://planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.

Ordenamiento	Contenido
Ley n° 12.965 (Marco Civil de Internet)[175]	• Establece principios, garantías, derechos y deberes para el uso de Internet en Brasil. • Determina las directrices de actuación de la federación, estados, distrito federal y municipios. • Define conceptos como internet, terminal, dirección IP, administrador del sistema autónomo, conexión a internet, registro de conexión, aplicaciones de internet, entre otros. • Regula la neutralidad de la red. • Regula la protección y conservación de registros, datos personales y comunicaciones privadas.
Ordenanza No. 85, de 26 de junio de 2017[176]	• Establece reglas básicas para el uso de la Terminal de Comunicación Segura (TCS) propiedad del Gobierno federal, proporcionada por la Agencia Brasileña de Inteligencia.
Ley No 13.709, Ley General de Protección de Datos Personales[177]	• Prevé el tratamiento de datos personales, incluso en medios digitales, por una persona natural o por una persona jurídica de derecho público o privado con el fin de proteger los derechos fundamentales de libertad e intimidad y el libre desarrollo de la personalidad.
Medida Provisional 869/2018	• Complementa la Ley No 13.709 sobre protección de datos personales y precisa las competencias de la Autoridad Nacional de Protección de Datos (ANPD).
Decreto n° 9.573, del 22 de noviembre de 2018[178]	• Aprueba la Política Nacional de Seguridad de Infraestructuras Críticas. • Asigna a la Dirección de Seguridad Institucional de la Presidencia de la República la vigilancia de la infraestructura crítica en el ámbito de la administración pública federal. • Define *infraestructura crítica* como: *instalaciones, servicios, bienes y sistemas cuya interrupción o destrucción, total o parcial, cause graves impactos sociales, ambientales, económicos, políticos, internacionales o para la seguridad del Estado y de la sociedad.*

175 Lei Nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, *Diário Oficial da União*, 24 de abril de 2014, núm. 77, Brasilia, p. 1, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

176 Portaria No. 85, de 26 de junho de 2017. Estabelece regras básicas de utilização do Terminal de Comunicação Segura (TCS) fornecido pela Agência Brasileira de Inteligência (ABIN), *Diário Oficial da União*, 27 de junio de 2017, núm. 121, Brasilia, p. 7, https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&data=27/06/2017&pagina=7.

177 Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais, *Diário Oficial da União*, 15 de agosto de 2018, núm. 157, Brasilia, p. 59, http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

178 Decreto n° 9.573, de 22 de novembro de 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas, *Diário Oficial da União*, 23 de noviembre de 2018, núm. 225, Brasilia, p. 40, http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9573.htm.

Ordenamiento	Contenido
Decreto nº 9.637, del 26 de diciembre de 2018[179]	Instituye la Política Nacional de Seguridad de la Información en el ámbito de la administración pública federal, la cual comprende: • Ciberseguridad. • Defensa cibernética. • Seguridad física y protección de datos organizacionales. • Acciones encaminadas a garantizar la disponibilidad, integridad, confidencialidad y autenticidad de la información.
Ley nº 13.844, del 18 de junio de 2019[180]	• Establece la Oficina de Seguridad Institucional de la Presidencia de la República (*Gabinete de Segurança Institucional*).
Decreto nº 9.819, de 3 de junio de 2019[181]	• Establece la Cámara de Relaciones Exteriores y Defensa Nacional del Consejo de Gobierno (*Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo*), órgano consultivo que tiene por objeto aprobar, promover la articulación y monitorear la implementación de programas y acciones sobre seguridad de las infraestructuras críticas, seguridad de la información, ciberseguridad, entre otras.
Decreto nº 10.222 del 5 de febrero de 2020[182]	• Aprueba la Estrategia Nacional de Ciberseguridad para el cuatrienio 2020-2023.
Decreto nº 10.363 del 21 de mayo de 2020[183]	• Establece las facultades del Departamento de Seguridad de la Información, tales como planificar y supervisar la actividad de seguridad de la información nacional, así como mantener el Centro Gubernamental de Tratamiento y Respuesta a Incidentes Cibernéticos.
Decreto Nº 10.569, de 9 de diciembre de 2020[184]	• Aprueba la Estrategia Nacional de Seguridad de Infraestructuras Críticas.
Resolución Nº 740/2020	• Busca promover una política de ciberseguridad para los prestadores de servicios de telecomunicaciones supervisada por el organismo regulador (ANATEL).

179 Decreto nº 9.637, de 26 de dezembro de 2018... *cit.*

180 Lei nº 13.844, de 18 de junho de 2019. Estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios, *Diário Oficial da União*, 18 de junio de 2019, núm. 116-A, Brasilia, p. 4, http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13844.htm.

181 Decreto Nº 9.819, de 3 de junho de 2019. Dispõe sobre a Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, *Diário Oficial da União*, núm. 106, 4 de junio de 2019, Brasilia, p.2, http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9819.htm.

182 Decreto nº 10.222, de 5 de fevereiro de 2020... *cit.*

183 Decreto nº 10.363, de 21 de maio de 2020, Altera o Decreto nº 9.668, de 2 de janeiro de 2019, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República, e remaneja e transforma cargos em comissão, *Diário Oficial da União*, núm. 97, 22 de mayo de 2020, Brasilia, p. 7, https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10363.htm.

184 Decreto Nº 10.569, de 9 de dezembro de 2020. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas, *Diário Oficial da União*, núm. 236, 10 de diciembre de 2020, Brasilia, p. 8, https://www.in.gov.br/en/web/dou/-/decreto-n-10.569-de-9-de-dezembro-de-2020-293251357.

Ordenamiento	Contenido
Instrucción normativa nº 1, de 27 de mayo de 2020[185]	• Aprueba la Estructura de Gestión de la Seguridad de la Información en los órganos y entidades de la administración pública federal, con el objeto de garantizar la disponibilidad, integridad, confidencialidad y autenticidad de la información a nivel nacional.
Instrucción normativa nº 2, de 24 de julio de 2020[186]	• Obliga a todos los órganos y entidades que tengan competencia para administrar la infraestructura de red de su organización a crear un equipo de prevención, tratamiento y respuesta a incidentes cibernéticos.
Instrucción Normativa nº 4 de 26 de marzo de 2020[187]	• Establece los requisitos mínimos de ciberseguridad para las redes de telecomunicaciones utilizadas por la Administración Pública Federal directa e indirecta. • Aboga por el cumplimiento de especificaciones técnicas y la diversificación de proveedores con el fin de mitigar los riesgos.
Decreto nº 10.641, del 2 de marzo de 2021[188]	• Detalla la organización y funcionamiento del Comité de Gestión de Seguridad de la Información.
Instrucción normativa GSI/PR nº 3, del 28 de mayo de 2021[189]	• Regula los procesos de gestión que deben observar los órganos y entidades de la administración pública federal en la planeación y ejecución de sus acciones en materia de seguridad de la información.
Decreto nº 10.748, del 16 de julio de 2021[190]	• Establece la Red Federal de Gestión de Incidentes Cibernéticos, la cual tiene como objetivo mejorar la coordinación entre los órganos y entidades de la administración pública federal directa, autárquica y fundacional para la prevención, tratamiento y respuesta a los incidentes cibernéticos, con el fin de elevar el nivel de resiliencia en seguridad.

185 Instrução Normativa Nº 1, de 27 de maio de 2020. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal, *Diário Oficial da União*, 28 de mayo de 2020, núm. 101, Brasilia, p. 13, https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215.

186 Instrução Normativa Nº 2, de 24 de julho de 2020, Altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal, *Diário Oficial da União*, 27 de julio de 2020, núm. 142, Brasilia, p. 3, https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-2-de-24-de-julho-de-2020-268684700.

187 Instrução Normativa nº 4, de 26 de março de 2020...*cit*.

188 Decreto nº 10.641, de 2 de março de 2021. Altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional, *Diário Oficial da União*, 3 de marzo de 2021, núm. 41, Brasilia, p. 1, https://www.in.gov.br/en/web/dou/-/decreto-n-10.641-de-2-de-marco-de-2021-306212181.

189 Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021. Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal, *Diário Oficial da União*, 31 de mayo de 2021, núm. 101, Brasilia, p. 15, https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172.

190 Decreto nº 10.748, de 16 de julho de 2021. Institui a Rede Federal de Gestão de Incidentes Cibernéticos, *Diário Oficial da União*, 19 de julio de 2021, núm. 134, Brasilia, p. 2, https://www.in.gov.br/en/web/dou/-/

Ordenamiento	Contenido
Instrucción normativa n° 5, de 30 de agosto de 2021[191]	• Establece los requisitos mínimos de seguridad de la información para el uso de soluciones de computación en la nube por parte de las dependencias y entidades de la administración pública federal.
Ordenanza GSI/PR NO. 93, de 18 de octubre de 2021[192]	• Aprueba el glosario de seguridad de la información.

Fuente: Elaboración propia con base en la revisión de la normativa de Brasil.

Como se puede observar, Brasil cuenta con abundante normativa de tipo legal y administrativo que regula diversos aspectos de la seguridad y la defensa cibernéticas. Destaca que las disposiciones referidas a las redes sociales de la Ley n° 12.965, de 23 de abril de 2014, han sido declaradas inconstitucionales por el Supremo Tribunal Federal de Brasil.

B. *Organismos*

Al igual que EE. UU. y Argentina, el Estado brasileño cuenta con una diversidad de organismos encargados de diseñar, implementar y evaluar las políticas y programas de ciberseguridad y ciberdefensa. Por ejemplo, cuenta con instituciones encargadas de la seguridad informática de las distintas dependencias de la Administración Pública Federal, centros de respuesta a incidentes federales y locales, públicos y privados, y una agencia coordinadora. Asimismo, la vertiente de la ciberdefensa ante amenazas e incidentes provenientes del exterior está a cargo de las Fuerzas Armadas brasileñas. La siguiente tabla resume los principales organismos competentes y sus funciones más importantes.

decreto-n-10.748-de-16-de-julho-de-2021-332610022.

191 Instrução Normativa Nº 5, de 30 de agosto de 2021. Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal, *Diário Oficial da União*, 31 de agosto de 2021, núm. 165, Brasilia, p. 2, https://in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684.

192 Portaria GSI/PR Nº 93, de 18 de outubro de 2021. Aprova o glossário de segurança da informação, *Diário Oficial da União*, 19 de octubre de 2021, núm. 197, Brasilia, p. 36, https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370.

Tabla 8. Organismos en Brasil encargados de la ciberseguridad

Organismo	Funciones
Agencia Brasileña de Inteligencia (*Agência Brasileira de Inteligência*)	• Creada por la ley 9.883, del 7 de diciembre de 1999. • Órgano de la Presidencia de la República, vinculado a la Oficina de Seguridad Institucional. • Proporciona al presidente de la República y a sus ministros información y análisis estratégicos, oportunos y confiables, necesarios para la toma de decisiones relacionadas con la seguridad del Estado y de la sociedad, y aquellos que involucran defensa, relaciones exteriores, seguridad interior, desarrollo socioeconómico y desarrollo científico-tecnológico.[193]
Agencia Nacional de Telecomunicaciones (ANATEL)	• Conoce de los asuntos de protección de datos relacionados con los servicios de telecomunicaciones. • Emitió los Requisitos de Ciberseguridad para Equipos de Telecomunicaciones. • Certifica y aprueba los equipos de telecomunicaciones, desde los más simples, como los sensores con interfaces de comunicación inalámbrica, hasta los más complejos, como los equipos centrales de la red del operador.194 • Promueve acciones de concientización entre los usuarios, como la campaña educativa *#ConexãoSegura* y el *Movimento #FiqueEsperto*.
Centro de Ciberdefensa del Ejército, CDCiber (*Centro de Defesa Cibernética - Ministério da Defesa do Brasil*)	• Creada en 2010. • Unidad encargada de coordinar los aspectos estratégicos y operativos de la arquitectura de ciberdefensa de Brasil.[195]
Centro de Estudios, Respuesta y Tratamiento de Incidentes de Seguridad en Brasil (*Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil*, CERT.br)	• Creado en 1997 por iniciativa del Comité Gestor de Internet de Brasil (CGI.br). • Es un tipo de centro de respuesta a incidentes de seguridad (CSIRT). • Busca incrementar el nivel de seguridad y capacidad de manejo de incidentes de las redes de internet en Brasil.[196] • Promueve la educación sobre seguridad cibernética. • Proporcionar capacitación formal en gestión de incidentes. • Monitorea las tendencias actuales en tecnología.
Centro de Estudios e Investigaciones en Tecnología de Redes y Operaciones (CEPTRO.br)	• Impulsa iniciativas y proyectos que apoyen o mejoren la infraestructura de internet en Brasil. • Subsidia a los proveedores de acceso con información que permita la mejora continua de las redes. • Promueve cursos de buenas prácticas operativas para profesionales de los Sistemas Autónomos, las redes que componen Internet.[197]

193 OFICINA DE SEGURIDAD INSTITUCIONAL, *Agência Brasileira de Inteligência*, (24 de mayo de 2022), https://www.gov.br/abin/pt-br/acesso-a-informacao/institucional/a-abin.

194 AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, *Segurança Cibernética*, (24 de mayo de 2022), https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica.

195 ESCRITÓRIO DE PROJETOS DO EXÉRCITO BRASILEIRO, *Programa Defensa Cibernética*, (26 de mayo de 2022), http://www.epex.eb.mil.br/index.php/defesa-cibernetica.

196 CERT.BR, *Sobre o CERT.br*, (24 de mayo de 2022), https://www.cert.br/sobre.

197 CEPTRO.BR, *Sobre o CEPTRO.br*, (24 de mayo de 2022), https://www.ceptro.br/quem-somos.

Organismo	Funciones
Centro de Estudios sobre Tecnologías Web (Ceweb.br)	• Fomenta la innovación y un mejor uso de la internet. • Elabora cursos, estudios y recomendaciones. • Realiza convenios de cooperación y espacios de discusión y colaboración permanente. • Incentiva la adopción de nuevos lineamientos y acciones sobre: Internet de las Cosas, pagos web, web y televisión digital, sitio web automotriz y los estudios web como interfaz de la nueva economía.[198]
Centro de Información y Coordinación de Ponto BR (*Núcleo de Informação e Coordenação do Ponto BR*, NIC.br)	• Aplica los lineamientos del Comité Gestor de Internet. • Entidad civil sin fin de lucro, regida por el derecho privado. • Responsable de las funciones administrativas y operativas relacionadas con el dominio .br.[199]
Centro de Prevención, Tratamiento y Atención de Incidentes Cibernéticos Gubernamentales (CTIR Gov - *Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo*)[200]	• Creado mediante la Instrucción normativa n° 1, de 27 de mayo de 2020. • Coordina a los equipos de tratamiento y respuesta a incidentes cibernéticos de las entidades de la administración pública federal. • Es el órgano encargado de prevenir y responder ante los incidentes de ciberseguridad del gobierno federal.
Centro Regional de Estudios para el Desarrollo de la Sociedad de la Información (Cetic.br)	• Creado en 2005. • Monitorea la adopción de tecnologías de información y comunicación (TIC) en Brasil. • Es un departamento del Centro de Información y Coordinación de Ponto BR (NIC.br), vinculado al Comité Gestor de Internet de Brasil (CGI.br). • Participa en talleres y la producción de directrices para sensibilizar a padres, educadores y usuarios en general. • Funciona como plataforma multisectorial para compartir experiencias y estimular debates entre diversos actores sobre los desafíos de medir las TIC y temas emergentes relacionados con el desarrollo de las sociedades de la información y el conocimiento.[201]
Comité de Gestión de Seguridad de la Información (CGSI)	• Creado el 26 de diciembre de 2018. • Asesora a la Oficina de Seguridad Institucional de la Presidencia de la República (GSI-PR) en actividades relacionadas con la seguridad de la información.[202] • Se compone de la mayoría de los ministerios, la Oficina del Fiscal General, el Banco Central de Brasil, y la Autoridad Nacional de Protección de Datos.

198 CEWEB.BR, *Atividades e Atribuições do Ceweb.br*, (24 de mayo de 2022), https://www.ceweb.br/atividades-e-atribuicoes-do-ceweb-br.

199 NIC.BR, *Atividades*, (24 de mayo de 2022), https://www.nic.br/atividades.

200 OFICINA DE SEGURIDAD INSTITUCIONAL, *CTIR Gov - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo*, (24 de mayo de 2022), https://www.gov.br/ctir/pt-br.

201 CETIC.BR, *Saiba Mais Sobre o Cetic.br*, (24 de mayo de 2022), https://www.cetic.br/pt/pagina/saiba-mais-sobre-o-cetic/92.

202 OFICINA DE SEGURIDAD INSTITUCIONAL, *Comitê Gestor da Segurança da Informação - CGSI*, (24 de mayo de 2022), https://www.gov.br/gsi/pt-br/assuntos/dsi/comite-gestor-da-seguranca-da-informacao-cgsi.

Organismo	Funciones
Comité Gestor de Internet de Brasil (CGI.br)[203]	• Establece lineamientos para el uso y desarrollo de internet en Brasil y para la implementación del registro de nombres de dominio, asignación de direcciones IP y administración relacionada con el dominio ".br". • Promueve estudios y recomienda procedimientos para la seguridad en Internet. • Propone programas de investigación y desarrollo que permitan mantener el nivel de calidad técnica e innovación en el uso de Internet.[204]
Departamento de Seguridad de la Información (*Departamento de Segurança da Informação*)[205]	• Mantiene un CSIRT, el CTIR.gov, que proporciona servicios de respuesta a incidentes y recopilación de datos para la Administración Pública Federal. • Cuenta con la Coordinación General de Prevención, Tratamiento y Atención de Incidentes Cibernéticos Gubernamentales y la Coordinación General de Gestión de Seguridad de la Información.
Grupo Técnico de Ciberseguridad y Gestión de Riesgos de Infraestructuras Críticas, GT-Ciber (*Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica*)	• Depende de ANATEL y es responsable de definir estándares sobre configuración de equipos, requisitos técnicos y proveedores; compartir informaciones y buenas prácticas, así como sensibilizar, capacitar, estudiar e interactuar con las Comisiones Brasileñas de Comunicación (CBC).[206]
Oficina de Seguridad Institucional de la Presidencia de la República (*Gabinete de Segurança Institucional*, GSI/PR)[207]	• Encargada de planificar, coordinar y supervisar la actividad de seguridad de la información en el ámbito de la administración pública federal, lo que incluye la ciberseguridad, gestión de incidentes informáticos, protección de datos, acreditación de seguridad y manejo de información confidencial.
Oficina para la Represión de la Delincuencia Cibernética de la Policía Federal (*Serviço de Repressão a Crimes Cibernéticos*)	• Es la principal entidad encargada de investigar los delitos cibernéticos. • Cuenta con un laboratorio forense digital. • Investiga delitos contra instituciones públicas federales con consecuencias interestatales e internacionales. • Involucrado en la investigación electrónica de fraudes (banca electrónica y estafas de tarjetas de crédito) y redes criminales que promueven el abuso infantil en línea.

Fuente: Elaboración propia.

C. *Control parlamentario*

El control parlamentario en materia de ciberseguridad del Estado brasileño es llevado a cabo por la Cámara de Diputados y el Senado

203 Decreto Nº 4.829, de 3 de setembro de 2003. Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências, *Diário Oficial da União*, 4 de septiembre de 2003, Brasilia, p. 24, http://www.planalto.gov.br/ccivil_03/decreto/2003/d4829.htm.

204 COMITÉ GESTOR DE INTERNET EN BRASIL, *Acerca de CGI.br*, (24 de mayo de 2022), https://cgi.br/sobre.

205 OFICINA DE SEGURIDAD INSTITUCIONAL, *Departamento de Segurança da Informação*, (24 de mayo de 2022), https://www.gov.br/gsi/pt-br/assuntos/dsi.

206 P&D BRASIL, *GT-Ciber - Anatel*, (26 de mayo de 2022), https://pedbrasil.org.br/gt-ciber-anatel-2.

207 OFICINA DE SEGURIDAD INSTITUCIONAL, *O que é*, (24 de mayo de 2022), https://www.gov.br/gsi/pt-br/acesso-a-informacao/institucional/intro.

Federal, o cualquiera de sus comisiones, las cuales pueden interpelar a los ministros de Estado y a cualquier otro titular de los órganos subordinados a la Presidencia de la República. El Congreso Nacional también verifica si la aplicación de los recursos públicos se ha realizado conforme a la ley a través del Tribunal de Cuentas de la Unión, teniendo la facultad de exigir aclaraciones a cualquier persona que maneje dinero, bienes y valores públicos.[208]

En este sentido, el congreso brasileño puede llamar a comparecer a las o los ministros de Estado encargados de la seguridad de la información pública y privada, la seguridad de las infraestructuras críticas y de la defensa nacional.

4. *Estonia*

Con un 96.2% de su población con acceso a internet, se ubica en la tercera posición del Índice Global de Ciberseguridad 2020 de la UIT, adhiriéndose al Convenio de Budapest el 12 de mayo de 2003. Alrededor del 99% de los servicios públicos son accesibles por internet. Hay más de 5.000 servicios públicos y privados en los que las personas pueden identificarse mediante una firma electrónica nacional. Debido a este alto nivel de digitalización, el país ha sido blanco de ciberataques, entre los que destaca el ocurrido en 2007, el cual tuvo una gran resonancia a nivel mundial por ser el más grande y coordinado en contra de un Estado que se había registrado hasta entonces. Por ello, el Estado estonio ha desarrollado estrategias e iniciativas para prevenirlos y mitigar sus impactos.[209]

Esta nación de Europa oriental fue una de las primeras en desarrollar una estrategia nacional de ciberseguridad en 2008, la cual fue actualizada en 2014. La primera estableció procedimientos e instituciones para asegurar una eficiente división del trabajo y cooperación entre organismos; la segunda enfatizó la protección de las infraestructuras críticas, el combate al cibercrimen y la mejora de las capacidades de seguridad informática. También sentó las bases para desarrollar un ambiente legislativo propicio para garantizar la ciberseguridad, la cooperación internacional y

208 CÁMARA DE LOS DIPUTADOS, *El Congreso Nacional*, (24 de mayo de 2022), https://www2.camara.leg.br/espanol/the-brazilian-parliament.

209 HÜBNER, Risto, "The Privacy, Data Protection and Cybersecurity Law Review: Estonia", *The Law Reviews*, 5 de noviembre de 2021, https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/estonia#footnote-030-backlink.

el desarrollo del sector de ciberseguridad en la economía.[210]

Estonia cuenta con una estrategia o plan de protección de infraestructuras críticas. Asimismo, el gobierno está obligado a establecer medidas de seguridad para determinados sistemas de información vitales. La legislación y las regulaciones obligan a establecer un plan de seguridad de la información, un inventario de los sistemas y la clasificación de los datos, las prácticas y los requisitos de seguridad asignados según los niveles de riesgo; a realizar, al menos, una auditoría anual de ciberseguridad, así como un informe público sobre la capacidad gubernamental en materia de ciberseguridad. La legislación también establece la obligación de notificar los incidentes de ciberseguridad e incluye una definición de *protección de infraestructuras críticas*.[211]

El Estado estonio implementa estrategias educativas, de concienciación desde temprana edad y de formación de recursos humanos. Cuenta con un equipo de respuesta a emergencias informáticas bien establecido, el CERT Estonia, bajo el control de la Autoridad de Sistemas de Información. También realiza periódicamente ejercicios nacionales de ciberseguridad. Ha diseñado una tecnología de *blockchain* propia y utilizada en otros países para garantizar que las redes, los sistemas y los datos no se vean comprometidos, asegurando así la privacidad de los datos.[212] A pesar de que no existe una obligación formal, las instituciones públicas colaboran estrechamente con las organizaciones pertinentes del sector privado.[213]

De manera similar al Estado brasileño, Estonia enfatiza el componente internacional de la ciberseguridad y trata de erigirse como líder e impulsor de iniciativas en la región. Con ello contribuye al desarrollo de consensos alrededor de normas universalmente aceptadas y enfatiza la aplicabilidad de los derechos humanos en el ciberespacio.[214]

A pesar de los grandes avances del sector público en la materia, el sector privado aún se considera en rezago. Además, la regulación sobre protección de datos no es del todo eficaz, pues carece de una legislación

210 MINISTRY OF FOREIGN AFFAIRS, *Cyber Security*, (27 de mayo de 2022), https://vm.ee/en/cyber-security.

211 BSA THE SOFTWARE ALLIANCE, *Country: Estonia, EU Cybersecurity Dashboard*, 2008, pp. 1-3, https://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_estonia.pdf.

212 E-ESTONIA, *KSI Blockchain*, (28 de mayo de 2022), https://e-estonia.com/solutions/cyber-security/ksi-blockchain.

213 BSA THE SOFTWARE ALLIANCE, *op. cit.*, p. 1.

214 MINISTRY OF FOREIGN AFFAIRS, *op. cit.*

que obligue a cada dependencia pública a contar con un jefe de información o de seguridad. No existen asociaciones público-privadas formales y hasta el día de hoy no hay prospectos ni planes para desarrollarlas.[215]

A. *Normativa*

En la siguiente tabla se muestra la normativa de Estonia en materia de ciberseguridad, presentada en orden cronológico.

Tabla 9. Normativa de Estonia relativa a la ciberseguridad

Ordenamiento	Contenido
Ley de Instituciones de Crédito (*Credit Institutions Act*)[216]	• Establece reglas sobre la información sujeta al secreto bancario. • Estipula que los datos de los clientes están sujetos al secreto bancario y son confidenciales, así como sus excepciones. • Obliga a las instituciones crediticias a adoptar medidas de seguridad y protección de su información.
Ley de Información Pública (*Public Information Act*)[217]	• Garantiza que toda persona tenga la oportunidad de acceder a la información pública, establece restricciones en cuanto al acceso a la información que contiene datos personales o de seguridad nacional, y obliga a adoptar medidas de seguridad para resguardar la integridad de los sistemas de información.
Código Penal Estonio (*Penal Code*)[218]	• Sanciona penalmente diversas conductas relacionadas directa e indirectamente con los delitos informáticos, por ejemplo: obstaculización de la operación de sistemas informáticos, terrorismo a través de medios informáticos, infracción de los derechos de autor en sistemas informáticos, uso ilegal de la identidad de otra persona, solicitud de acceso a pornografía infantil y visualización de la misma, difusión de programas espía (*spyware*), programas maliciosos (*malware*) o virus informáticos, fraude y preparación de delitos informáticos, interferencia o daño a sistemas vitales de servicios públicos, entre otros.

215 BSA THE SOFTWARE ALLIANCE, *op. cit.*, pp. 2-3.

216 Krediidiasutuste seadus, de 9 de febrero de 1999, *Riigi Teataja*, vol. I, 23, 1999, Estonia, p. 349, https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/503062022001/consolide.

217 Avaliku teabe seadus, de 15 de noviembre 2000, *Riigi Teataja*, vol. I, 92, 2000, Estonia, p. 597, https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/522032022002/consolide.

218 Karistusseadustik, de 6 de junio de 2001, *Riigi Teataja*, vol. I, 61, 2001, Estonia, p. 364, https://www.riigiteataja.ee/en/eli/522012015002/consolide.

Ordenamiento	Contenido
Ley de Comunicaciones Electrónicas (*Electronic Communications Act*)[219]	• Incorpora a la legislación estonia los requisitos derivados de la directiva de la Unión Europea sobre privacidad electrónica. • Establece una obligación general para los proveedores de comunicaciones de mantener la confidencialidad de toda la información que posean. • Autoriza a la Autoridad de Vigilancia Técnica (*Technical Surveillance Authority*) de Estonia a exigir que cualquier proveedor de comunicaciones realice una auditoría de seguridad cuando así sea solicitado. • Obliga a las empresas de comunicaciones de notificar a la mayor brevedad posible los casos de violación de datos personales que se hayan producido en relación con la prestación de servicios de comunicaciones. • Obliga a las empresas de comunicaciones a conservar metadatos de comunicaciones durante el período de un año a partir de la fecha de la comunicación y facilitar el acceso a dichos datos a las autoridades gubernamentales.
Ley sobre secretos de Estado e información clasificada de Estados extranjeros (*State Secrets and Classified Information of Foreign States Act*)[220]	• Asigna a la información que se considera como secreto de Estado un nivel de clasificación, según un sistema de cuatro niveles, los cuales representan la importancia de la información para las diversas funciones del gobierno estonio y de los gobiernos extranjeros, incluyendo el nivel de riesgo que implicaría la divulgación de la información. • Exige una inspección anual de la integridad del sistema en el que se encuentran almacenados los secretos de Estado.
Ley de Emergencia (*Emergency Act*)[221]	• Identifica las infraestructuras críticas de Estonia y regula la organización y los procedimientos de respuesta a las emergencias relacionadas.
Ley de Prevención del Blanqueo de Capitales y la Financiación del Terrorismo (*Money Laundering and Terrorist Financing Prevention Act*)[222]	• Prevé normas sobre el tratamiento de datos personales en relación con la prevención del uso de los sistemas financieros para el blanqueo de capitales y la financiación del terrorismo.
Ley de Ciberseguridad *(Cybersecurity Act*)[223]	• Establece los principios, obligaciones y requisitos para mantener la ciberseguridad de la red y los sistemas de información esenciales para el funcionamiento de la sociedad y de las autoridades estatales y locales, la responsabilidad y la supervisión de la red y los sistemas de información, así como las bases para la prevención y resolución de incidentes cibernéticos. • Define conceptos como *red y sistema de información*, *seguridad de los sistemas*, *incidente cibernético*, *mercado en línea*, *servicio de computación en la nube*, *equipo de respuesta a incidentes informáticos*, entre otros. • Regula a los proveedores de servicios digitales. • Establece la obligación a cargo de los proveedores de servicios de notificar incidentes cibernéticos.

219 Elektroonilise side seadus, de 8 de diciembre de 2004, *Riigi Teataja*, vol. I, 87, 2004, Estonia, p. 593, https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/518032022002/consolide.

220 Riigisaladuse ja salastatud välisteabe seadus, de 25 de enero de 2007, *Riigi Teataja*, vol. I, 16, 2007, Estonia, p. 77, https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/521052020005/consolide.

221 Hädaolukorra seadus, de 8 de febrero de 2017, *Riigi Teataja*, vol. I, 3 de marzo de 2017, Estonia, https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/501122021001/consolide.

222 Rahapesu ja terrorismi rahastamise tõkestamise seadus, de 26 de octubre de 2017, *Riigi Teataja*, vol. I, 17 de noviembre de 2017, Estonia, p. 2, https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/524032022001/consolide.

223 Küberturvalisuse seadus, de 9 de mayo de 2018, *Riigi Teataja*, 23 de mayo de 2018, Estonia, https://

Ordenamiento	Contenido
Ley de Protección de Datos Personales (*Personal Data Protection Act*)[224]	• Regula la protección y tratamiento de los datos personales de las personas físicas por parte de las autoridades policiales en la prevención y persecución de delitos y ejecución de penas. • Establece la responsabilidad por las infracciones a la Regulación General de Protección de Datos de la Unión Europea.
Reglamento sobre las medidas de seguridad de los sistemas de información de los servicios vitales y los activos de información conexos (*Regulation on Security Measures for Information Systems of Vital Services and Related Information Assets 2013*)	• Regula la aplicación de las medidas de seguridad de los sistemas de información. • Exige a las entidades que se dedican a los *servicios vitales* que designen a una persona para que notifique a la Autoridad de Sistemas de Información de Estonia en caso de presentarse algún incidente de seguridad, incluidos los del ámbito ciberdigital.

Fuente: Elaboración propia con base en la revisión de la normativa de Estonia.

B. *Organismos*

A continuación, se exponen sucintamente los organismos estonios encargados de la ciberseguridad.

Tabla 10. Organismos en Estonia encargados de la ciberseguridad

Organismo	Funciones
Autoridad del Sistema de Información de Estonia (*Information System Authority*, ISA)	• Es la autoridad nacional competente de Estonia en materia de seguridad de las redes y de la información. • Dirige el desarrollo de los sistemas nacionales de tecnologías de la información. • Garantiza la ciberseguridad nacional, incluido el funcionamiento sostenible de un Estado electrónico seguro.[225] • Es notificado respecto a los incidentes de ciberseguridad y mantiene la base de datos respectiva.
Centro de Coordinación Industrial, Tecnológica y de Investigación de Estonia (*Estonian Cybersecurity Industrial, Technology and Research Coordination Centre*)	• Creado por obligación dispuesta en el artículo 6 de la Regulación (EU) 2021/887 del Parlamento Europeo y del Consejo. • Se encarga de implementar las decisiones de su homólogo a nivel europeo. • Sus funciones son especificadas en las regulaciones que emita el ministro encargado de la materia.
Comité de Estrategia de Ciberseguridad (*Cyber Security Strategy Committee*)	• Supervisa la implementación de la estrategia de ciberseguridad. • Elabora reportes anuales para el gobierno y mide el progreso de la implementación a la luz del plan de implementación.

www.riigiteataja.ee/en/eli/523052018003/consolide.

224 Isikuandmete kaitse seadus, de 12 de diciembre de 2018, *Riigi Teataja*, 4 de enero de 2019, Estonia, p. 11, https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/523012019001/consolide.

225 HÜBNER, Risto, *op. cit.*

Organismo	Funciones
Departamento de Respuesta a Incidentes Cibernéticos (*Cybersecurity Incident Response Department, CERT Estonia*)	• Establecido en 2008. • Coordina las medidas de seguridad y respuesta a incidentes entre todas las redes estonias.
Inspección de Protección de Datos (*Data Protection Inspectorate*)	• Supervisa el cumplimiento de los requisitos previstos en la Ley de Protección de Datos Personales y la legislación europea y nacional relacionada con el tratamiento de datos personales.
Liga Nacional de Ciberdefensa de Estonia (*Estonian National Cyber Defence League*)	• Es una unidad de ciberrespuesta formada por profesionales de las tecnologías de la información y representantes de entidades relacionadas con las infraestructuras críticas.
Ministerio de Asuntos Exteriores	• Estonia es líder en cuestiones cibernéticas a nivel internacional. Para este Estado, la ciberseguridad se ha convertido en una parte integral de sus asuntos internos, pero también de sus relaciones internacionales y económicas, por lo que la considera como un aspecto integral de la seguridad.[226]
Vaata Maailma (the Look@ World Foundation)	• Fundada en 2001, es una asociación público-privada dedicada a promover el uso de Internet y los servicios de las TIC. • Está compuesta por proveedores de telecomunicaciones estonios e internacionales. • Lleva a cabo varios proyectos, principalmente de carácter educativo, que abarcan el uso seguro de internet y los ordenadores.

Fuente: Elaboración propia.

C. *Control parlamentario*

Estonia es una república unitaria parlamentaria, por lo que el congreso (*Riigikogu*), que es unicameral, ejerce un control de los actos del Primer Ministro, quien es el jefe de gobierno, y del Presidente, quien es el jefe de Estado designado por el propio parlamento según el artículo 65 de su constitución nacional.

El artículo 74 de la Constitución de Estonia dispone que cada diputado tiene derecho a formular preguntas al Gobierno de la República y sus miembros. En esa medida, las agencias y organismos que dependen del Primer Ministro directamente o de algún ministerio en particular rendirán cuentas ante alguno de los cuatro tipos de comisiones del propio poder legislativo: permanentes, selectas, de investigación y de estudio, según la Ley de Reglas de Procedimiento y Normativa Interna del Parlamento (*Riigikogu Rules of Procedure and Internal Rules Act*).[227]

226 MINISTRY OF FOREIGN AFFAIRS, *op. cit.*

227 Riigikogu kodu- ja töökorra seadus, de 11 de febrero de 2003, *Riigi Teataja*, vol. I, 44, 2003, Estonia, p. 316, https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/504062020005/consolide.

Respecto al tema bajo estudio, el artículo 14 de la Ley de Ciberseguridad dispone expresamente que la supervisión del Estado y del gobierno sobre el cumplimiento de los requisitos previstos en dicha ley es ejercida por cuatro órganos: a) la Autoridad del Sistema de Información de Estonia, b) la Autoridad de Reglamentación Técnica y de Protección de los Consumidores (*Consumer Protection and Technical Regulatory Authority*), c) el Centro de Coordinación Industrial, Tecnológica y de Investigación de Estonia (*Estonian Cybersecurity Industrial, Technology and Research Coordination Centre*) y d) la autoridad de seguridad pertinente. Por lo tanto, las personas titulares de estas cuatro autoridades podrían eventualmente ser requeridas por la comisión competente del parlamento para contestar interpelaciones o preguntas respecto a los avances en la implementación de la ley.

5. *Singapur*

El 87.7% de la población de esta república unitaria y parlamentaria cuenta con acceso a internet. Singapur se ubica en la cuarta posición del Índice Global de Ciberseguridad 2020 de la UIT. A diferencia de los demás casos estudiados, no forma parte del Convenio de Budapest.

Sin embargo, cuenta con un *Plan Maestro para un Ciberespacio más Seguro 2020*, el cual se basa en el segundo pilar de la Estrategia de Ciberseguridad de Singapur de 2016. La Agencia de Ciberseguridad de Singapur desarrolló el plan maestro en consulta con la industria respectiva y la academia para elevar el nivel general de ciberseguridad de los usuarios individuales, las comunidades, las empresas y las organizaciones. El plan comprende tres ejes: asegurar la infraestructura digital básica, proteger las actividades en el ciberespacio y capacitar a la población.[228]

La estrategia de ciberseguridad singapurense de 2021 actualizó a su predecesora del año 2016 y fue desarrollada en consulta con múltiples partes interesadas, incluidos los sectores industriales y académicos tanto locales como extranjeros. Pretende defender activamente el ciberespacio, simplificar la ciberseguridad para los usuarios finales y promover el desarrollo de normas y estándares cibernéticos internacionales con base en tres pilares estratégicos: construir una infraestructura resilien-

228 CYBER SECURITY AGENCY OF SINGAPORE, *Singapore's Safer Cyberspace Masterplan 2020*, octubre 2020, https://www.csa.gov.sg/News/Publications/safer-cyberspace-masterplan.

te, posibilitar un ciberespacio más seguro y mejorar la cooperación cibernética internacional. Para ello, se impulsa a partir de dos habilitadores: el desarrollo de un ecosistema de ciberseguridad vibrante y una sólida cantera de cibertalentos.[229]

A. *Normativa*

La tabla siguiente resume la normativa vigente de Singapur en materia de ciberseguridad, presentada en orden cronológico.

Tabla 11. Normativa de Singapur relativa a la ciberseguridad

Ordenamiento	Contenido
Ley sobre el uso indebido de ordenadores y ciberseguridad (*Computer Misuse and Cybersecurity Act*) de 1993[230]	• Regula la protección de material informático en contra del acceso o modificación no autorizados.
Ley de ciberseguridad (*Cybersecurity Act*) de 2018[231]	• Autoriza a la Agencia de Ciberseguridad para adoptar medidas, tales como la designación de expertos o medidas de emergencia con el propósito de prevenir, gestionar y responder a las amenazas e incidentes de seguridad cibernética. • Regula a los propietarios de infraestructura de información crítica y a los proveedores de servicios de seguridad cibernética. • Define conceptos como ordenador, programa informático, sistema informático, infraestructura crítica de información, ciberseguridad, incidente de ciberseguridad, servicio de ciberseguridad, amenaza de ciberseguridad, vulnerabilidad de ciberseguridad, entre otros. • Instituye al Comisionado de Ciberseguridad (*Commissioner of Cybersecurity*), a un Comisionado Adjunto y uno o más Comisionados Asistentes, todos bajo el cargo del Primer Ministro, para realizar funciones de promoción, procuración, investigación, respuesta, monitoreo, representación, formulación de estándares, educación, entre otras. • Regula la infraestructura crítica de información, la designación, las facultades, el acopio de información, las prácticas, los estándares, el deber de informar incidentes, auditorías, evaluaciones de riesgos, pruebas de seguridad, entre otros aspectos. • Establece medidas procesales como facultades de investigación, cautelares y protección de informantes. • Provee una lista de servicios esenciales. • Establece un marco para el intercambio de información sobre ciberseguridad.

229 CYBER SECURITY AGENCY OF SINGAPORE, *The Singapore Cybersecurity Strategy 2021*, Singapur, 2021, https://www.csa.gov.sg/-/media/Csa/Documents/Publications/The-Singapore-Cybersecurity-Strategy-2021.pdf.

230 Computer Misuse Act 1993, (2020 revised edition), *Government Gazette*, 30 de agosto de 1993, Singapur, https://sso.agc.gov.sg/Act/CMA1993.

231 Cybersecurity Act 2018, (No. 9 of 2018), *Government Gazette*, 16 de marzo de 2018, Singapur, https://sso.agc.gov.sg/Acts-Supp/9-2018.

Ordenamiento	Contenido
Ley de Protección contra la Falsedad y la Manipulación en Línea (*Protection From Online Falsehoods and Manipulation Act*) de 2019[232]	• Busca prevenir la comunicación electrónica respecto a declaraciones falsas, suprimir el apoyo y contrarrestar los efectos de dicha comunicación, evitar el uso de cuentas para dicha comunicación y la manipulación de la información, y permitir medidas para mejorar la transparencia de la publicidad política en línea. • Autoriza suprimir la financiación, la promoción y otros tipos de apoyo a los sitios web que comunican repetidamente declaraciones falsas de acontecimientos en Singapur. • Permite que se tomen medidas para detectar, controlar y salvaguardar el comportamiento inauténtico coordinado y otros usos indebidos de las cuentas en línea y los *bots*.

Fuente: Elaboración propia con base en la normativa de Singapur.

B. *Organismos*

Singapur también cuenta con diversos organismos encargados de velar por la seguridad informática, prevenir incidentes y responder ante su ocurrencia, identificar y formular buenas prácticas, educar a la población en general y a personas que busquen dedicarse a la ciberseguridad en particular, así como para coordinar a los diversos actores públicos y privados en la materia. En la siguiente tabla se enlistan estos organismos y sus funciones principales.

Tabla 12. Organismos en Singapur encargados de la ciberseguridad

Organismo	Funciones
Agencia de Ciberseguridad (*Cyber Security Agency*)	• Creada en 2015. • Encargada de proteger el ciberespacio de Singapur. • Depende de la Oficina del Primer Ministro y actúa bajo la dirección del Ministerio de Comunicaciones e Información. • Sus tres principales metas son proteger la seguridad nacional, impulsar una economía digital y proteger el estilo de vida digital.[233] • Protege y defiende la infraestructura crítica de información. • Promueve la cooperación internacional.

232 Protection from Online Falsehoods and Manipulation Act 2019, *Government Gazette*, 2 de octubre de 2019, Singapur, https://sso.agc.gov.sg/Act/POFMA2019?WholeDoc=1.

233 CYBER SECURITY AGENCY OF SINGAPORE (CSA), *Our Organisation*, (6 de mayo de 2022), https://www.csa.gov.sg/Who-We-Are/Our-Organisation.

Organismo	Funciones
Alianza para la concienciación sobre la ciberseguridad (*Cyber Security Awareness Alliance*)	• Formada por representantes del gobierno, empresas privadas, asociaciones comerciales y organizaciones sin fines de lucro. • Busca promover y mejorar la concienciación y la adopción de buenas prácticas de ciberseguridad entre los ciudadanos y las empresas de Singapur.[234]
Consorcio de Ciberseguridad de Singapur (*Singapore Cybersecurity Consortium*)	• Creado para la colaboración entre la industria, la academia y el gobierno con el fin de fomentar la investigación, la formación de la mano de obra y la concienciación tecnológica en materia de ciberseguridad. Está financiado por un programa nacional y tiene su sede en la Universidad Nacional de Singapur.[235]
Equipo de respuesta a emergencias informáticas de Singapur (*Singapore Computer Emergency Response Team*, SingCERT)	• Responde a los incidentes de ciberseguridad en Singapur. • Facilita la detección, resolución y prevención de incidentes relacionados con la ciberseguridad en internet.[236]
Grupo de Ciberseguridad (*Cyber Security Group*)	• Agencia encargada de la ciberseguridad para el sector gubernamental, con el mandato de proteger las TIC y los sistemas inteligentes del gobierno de Singapur para construir un gobierno digital confiable. • Adopta un triple enfoque: 1) desarrollar capacidades de ciberseguridad, 2) colaborar con los organismos de toda la administración y 3) forjar asociaciones con la industria para aumentar las capacidades gubernamentales.[237]
Ministerio de Comunicaciones e Información (*Ministry of Communications and Information*)	• Dirige a la Agencia de Ciberseguridad de Singapur. • Colabora en la elaboración de programas, políticas y planes sobre la ciberseguridad de la nación.[238]
Panel de expertos en tecnología operativa y ciberseguridad (*Operational Technology Cybersecurity Expert Panel*)	• Fue establecido en mayo de 2021. • Permite a los profesionales de la ciberseguridad de la tecnología operativa de Singapur, a los operadores, a los investigadores y a los responsables políticos del gobierno, de los sectores de las infraestructuras críticas de la información, de la academia y de otras industrias de la tecnología operativa tener acceso directo a expertos.[239]

Fuente: Elaboración propia.

234 CYBER SECURITY AGENCY OF SINGAPORE (CSA), *Cyber Security Awareness Alliance*, (6 de mayo de 2022), https://www.csa.gov.sg/Who-We-Are/committees-and-panels/cyber-security-awareness-alliance.

235 SINGAPORE CYBERSECURITY CONSORTIUM, *About Us*, (7 de mayo de 2022), https://sgcsc.sg.

236 CYBER SECURITY AGENCY OF SINGAPORE (CSA), *About SingCERT*, (6 de mayo de 2022), https://www.csa.gov.sg/singcert/Who-We-Are.

237 GOVERNMENT TECHNOLOGY AGENCY, *Cyber Security Group (CSG)*, (6 de mayo de 2022), https://www.tech.gov.sg/products-and-services/cyber-security-group.

238 MINISTRY OF COMMUNICATIONS AND INFORMATION, *Cyber Security*, (6 de mayo de 2022), https://www.mci.gov.sg/portfolios/cyber-security/what-we-do.

239 CYBER SECURITY AGENCY OF SINGAPORE (CSA), *Operational Technology Cybersecurity Expert Panel*, (6 de mayo de 2022), https://www.csa.gov.sg/Who-We-Are/committees-and-panels/operational-technology-cybersecurity-expert-panel.

C. *Control parlamentario*

Debido a que Singapur es una república parlamentaria con un poder ejecutivo bicéfalo, el parlamento unicameral ejerce un control de los actos tanto del Primer Ministro, que es el jefe de Gobierno, como del presidente, que es el jefe de Estado.

En específico, la Ley de Ciberseguridad de 2018 dispone que el Primer Ministro podrá nombrar, de entre los funcionarios públicos o empleados de un organismo creado por ley, a un Comisario de Ciberseguridad, a un Comisionado Adjunto, y a uno o más Comisionados Auxiliares de Ciberseguridad, para asistir al Comisionado en el cumplimiento de sus obligaciones y funciones. El Comisario está obligado a asesorar al gobierno sobre las necesidades y políticas nacionales en materia de ciberseguridad, así como a representar al gobierno en materia de ciberseguridad a nivel internacional.

El ordenamiento antes mencionado establece que el Primer Ministro podrá nombrar como Comisario Adjunto con respecto a una infraestructura de información crítica a un funcionario público de otro ministerio, o a un empleado de un organismo estatutario a cargo de otro ministerio, cuando este supervise o regula una industria o un sector al que pertenezca la infraestructura de información crítica.

Por lo tanto, son diversos funcionarios los que podrían llegar a ser requeridos para contestar preguntas parlamentarias en materia de ciberseguridad, ya que es el Primer Ministro el facultado para designarlos. Del mismo modo, la Agencia de Ciberseguridad de Singapur, que depende del Ministerio de Comunicaciones e Información, rinde cuentas ante el Poder Legislativo. Para ello, se establece que al inicio de cada sesión hay un periodo para que los miembros del parlamento cuestionen a los ministros sobre sus acciones y responsabilidades al frente de los diferentes ministerios que conforman el gobierno. Las preguntas pueden ser presentadas por cualquier miembro y las respuestas pueden ser expresadas de forma oral o escrita.[240]

240 CENTRO DE ESTUDIOS INTERNACIONALES GILBERTO BOSQUES, *Características y funcionamiento del Parlamento de Singapur en el marco de la visita de su Presidenta, Halimah Yacob al Senado de la República*, nota informativa, Senado de la República, 25 de abril de 2017, p. 4.

III. CONCLUSIONES DEL ESTUDIO COMPARADO DE LA REGULACIÓN SOBRE CIBERSEGURIDAD

A partir de un análisis inductivo sobre los cinco casos anteriormente expuestos, es decir, con base en las particularidades observadas para identificar patrones regulares, es posible derivar algunos elementos comunes que se encuentran en todos o en la mayoría de los órdenes jurídicos nacionales estudiados, los cuales se resumen en la siguiente tabla:

Tabla 13. Elementos comunes sobre ciberseguridad en los marcos jurídicos de otros países

Elemento	Ejemplos
Definiciones	a) Ciberseguridad. b) Amenaza de ciberseguridad. c) Incidente de ciberseguridad/ciberataque. d) Infraestructura crítica de información. e) Entre otras.
Organismos	a) Agencias coordinadoras bajo la esfera de alguna secretaría o ministerio pertinente (seguridad, comunicaciones, tecnología). b) Órganos públicos que monitorean e investigan (unidades en corporaciones policiales o en fiscalías). c) Equipos públicos y privados de respuesta a incidentes informáticos.
Programas y políticas	a) Estrategia nacional de ciberseguridad.[241] b) Catálogos de infraestructuras críticas de la información. c) Programas de educación y empleo sobre ciberseguridad y afines. d) Programas de concientización sobre navegación segura para la sociedad, las empresas y los órganos públicos.
Control parlamentario	a) Aprobación de nombramientos. b) Aprobación de estrategias. c) Informes periódicos. d) Posible destitución.
Catálogo de delitos específicos y relacionados	a) Fraude informático. b) Robo o suplantación de identidad. c) Extorsión informática (*phishing*). d) Uso o difusión ilegal de datos personales. e) Acceso ilícito a sistemas informáticos. f) Congestión de sitios de internet. g) Violación de comunicaciones electrónicas privadas. h) Interrupción de servicios telemáticos. i) Delitos contra la integridad sexual de niños, niñas y adolescentes a través de medios digitales (*grooming*, pornografía infantil). j) Relacionados: trata de personas, tráfico de estupefacientes y armas, entre otros.

Fuente: Elaboración propia.

241 Para conocer las diversas estrategias nacionales de ciberseguridad, véase UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, *National Cybersecurity Strategies Repository*, (3 de junio de 2022), https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.

Sería posible abstraer algunas propiedades necesarias de una regulación adecuada a partir de los informes y mediciones respecto al grado de desarrollo en materia de ciberseguridad. Estos podrían servir como una especie de lista de requisitos que una ley en la materia podría considerar incluir.

Por ejemplo, la organización BSA (*The Software Alliance*) desarrolla perfiles de ciberseguridad a partir de un conjunto de preguntas básicas, algunas de las cuales son: 1) ¿existe una estrategia nacional de ciberseguridad?, 2) ¿existe una estrategia o plan para la protección de infraestructuras críticas?, 3) ¿la legislación obliga a adoptar un plan de seguridad de la información por escrito?, 4) ¿la legislación obliga a elaborar un inventario de sistemas y de clasificación de datos?, 5) ¿la legislación obliga a realizar auditorías sobre seguridad, al menos anuales?, 6) ¿la legislación obliga a elaborar informes públicos sobre capacidades cibernéticas del Estado?, 7) ¿la legislación obliga a cada dependencia pública a contar con un jefe o jefa de información o de seguridad de la misma?, 8) ¿la legislación obliga a reportar incidentes de ciberseguridad?, 9) ¿la legislación prevé una definición apropiada de *protección de infraestructura crítica*?, 10) ¿existe un equipo nacional de respuesta a incidentes cibernéticos?, 11) ¿existe una autoridad nacional encargada de la seguridad de las redes y de la información?, 12) ¿se realizan ejercicios de ciberseguridad nacionales?, 13) ¿existen una colaboración formal público-privada?, 14) ¿existe alguna estrategia educativa para aumentar el conocimiento sobre ciberseguridad?[242]

Por su parte, el Banco Interamericano de Desarrollo mide el grado de desarrollo en la materia de ciberseguridad a partir de cinco dimensiones (Política y Estrategia de Ciberseguridad; Cultura Cibernética y Sociedad; Educación, Capacitación y Habilidades en Ciberseguridad; Marcos Legales y Regulatorios; y Estándares, Organizaciones y Tecnologías) que se desglosan en veinticuatro componentes.[243] En específico, el componente referido a los marcos legales y regulatorios podría servir como una base para desarrollar una legislación moderna y adecuada al contexto mexicano.

242 BSA THE SOFTWARE ALLIANCE, *op. cit.*, pp. 1-3.

243 BANCO INTERAMERICANO DE DESARROLLO, *op. cit.*, pp. 43-44.

CONCLUSIONES

La presente investigación buscó probar la hipótesis en la que se afirma que, si el Estado mexicano creara una regulación sobre ciberseguridad moderna, a la altura del contexto social actual y del avance tecnológico, que atienda el problema multidimensionalmente, podría contrarrestar eficazmente los efectos negativos de los ataques cibernéticos a instituciones públicas, privadas y sociedad en general.

Si bien el Estado mexicano cuenta con algunos elementos necesarios para hacer frente a los ataques y amenazas a través de medios y tecnologías digitales, tales como ordenamientos jurídico-administrativos y equipos de respuesta públicos y privados, no es menos cierto que también podría inspirarse en algunas naciones vanguardistas en el desarrollo tecnológico y jurídico sobre ciberseguridad. Esto debido a que la digitalización forma parte de diversos ámbitos tanto de la vida pública como privada, y algunos de estos han sido cada vez más afectados por ciberataques y delitos informáticos, ya sean dirigidos contra instituciones públicas, organizaciones privadas y personas físicas.

Durante la pandemia por COVID-19, México fue uno de los países latinoamericanos que más se vio afectado por ciberataques. Como reacción, se han creado centros de respuesta ante incidentes informáticos (CERTs) públicos y privados. Es decir, el Estado mexicano cuenta con algunos órganos encargados de prevenir, investigar y reaccionar ante este tipo de conductas.

A pesar de la atención que los sectores público y privado han prestado para atender el problema, hace falta un marco regulatorio sólido e innovador que coordine y faculte a diversas autoridades de todos los órdenes de gobierno para que, en el ámbito de sus competencias, aborden la materia de ciberseguridad.

A partir del contraste entre el marco normativo sobre ciberseguridad vigente en México frente al de otras naciones, es posible afirmar que el nacional requiere ser actualizado si lo que se busca es que las instituciones del Estado mexicano cuenten con un conjunto de normas que faciliten detectar, perseguir y sancionar los ciberataques, así como educar a la población sobre la seguridad cibernética.

Además, para un efectivo diseño, planeación y despliegue institucional que combata a la ciberdelincuencia también sería necesaria una es-

trategia nacional de ciberseguridad y un ente institucional que coordine las actividades de todos los actores involucrados.

La falta de regulación ha sido detectada por el Poder Legislativo federal. Diversos grupos parlamentarios de las LXIV y LXV legislaturas del Congreso de la Unión incorporaron este problema público en sus respectivas agendas legislativas. De ahí han derivado varias iniciativas que proponen, entre otras medidas, crear un organismo coordinador, tipificar algunos delitos cibernéticos, considerar a los ciberataques como afectaciones a la seguridad nacional y fomentar la educación para una navegación segura, aunque ninguna se ha convertido en derecho vigente.

Ahora bien, para desarrollar propuestas normativas, sería conveniente que el órgano creador de la norma considere los conceptos y definiciones esenciales en la materia de ciberseguridad. Se asume que esta es un fenómeno cambiante, complejo y transversal a la realidad social e individual, lo cual significa un asunto de interés de Estado. Por ello, se propuso su análisis y comprensión multifactorial.

El concepto mismo de ciberseguridad y otros relacionados, como ciberguerra, cibercrimen, entre otros, no son unívocos. La doctrina y las instituciones públicas de diferentes Estados no ofrecen definiciones homogéneas. Esto se debe a que ellas atienden a las amenazas y ataques cibernéticos y al contexto presente en cada país.

Igualmente es patente la falta de definiciones formales a nivel internacional. Por ende, el Poder Legislativo debe ser cuidadoso al incluir y definir conceptos en los ordenamientos jurídicos. Como se desprende del capítulo II, la ciberseguridad puede ser entendida en su faceta de defensa y seguridad nacional, o también como una cara de la seguridad pública e interior.

Por ello, se intentó trazar las líneas centrales de entendimiento y la base conceptual desde una perspectiva geopolítica y geoestratégica para aclarar lo que es la ciberseguridad. Se dio cuenta de que esta puede comprender las operaciones conducidas en el ciberespacio, la dimensión electromagnética e informacional, y que las acciones pueden ser realizadas por Estados u organizaciones internacionales con el objetivo de atacar y dañar los sistemas computacionales y las redes de información de otra nación.

Un aspecto íntimamente relacionado, la ciberdefensa, puede transformarse en ciberguerra cuando la dinámica del conflicto afecta las ca-

pacidades para garantizar que los propios intereses del Estado no sean socavados en una lógica de dominio de espectro completo frente a otros entes públicos o privados, nacionales o transnacionales. Adicionalmente, se observan tácticas de guerra comunicacional que devela un posicionamiento estratégico en el campo de batalla ciberespacial, mediático y diplomático.

Dada la multiplicidad de elementos que puede integrar la definición del objeto de investigación, se presentó un estudio de derecho comparado que buscó precisar los conceptos e instituciones jurídicas que una legislación sobre ciberseguridad tendería a incluir. A partir de este, se identificaron algunos conceptos, definiciones y arreglos institucionales que una ley mexicana podría incorporar.

El diagnóstico del marco jurídico mexicano reveló que existen diversas disposiciones que regulan de manera directa y expresa, o indirecta y tácita, la materia de ciberseguridad. También se lograron identificar algunos órganos encargados de este aspecto en México, aunque suelen enfocarse en la seguridad cibernética de los sistemas de las propias instituciones a las que están adscritos.

Por ejemplo, existen áreas específicas dentro de los órganos constitucionales autónomos. También se encontraron áreas en dependencias del Poder Ejecutivo, tales como la Unidad de Ciberseguridad de la Secretaría de Marina o diversas direcciones de la Guardia Nacional, la cual incluso cuenta con un equipo nacional de respuesta a incidentes cibernéticos. Otras dependencias no cuentan con áreas específicas, pero sí se encargan de aspectos relacionados con la ciberseguridad, como la educación o la vinculación con otros actores públicos y privados, nacionales e internacionales.

Igualmente es posible afirmar que los poderes legislativo y judicial pueden conocer, en el ámbito de sus competencias, de la materia de ciberseguridad. Así, ambas cámaras del Poder Legislativo federal pueden ejercer sus funciones legislativas para reformar el marco jurídico vigente, y de control para supervisar las acciones de otros órganos del Estado mexicano. Asimismo, la legislación procesal penal prevé el control jurisdiccional de la intervención de comunicaciones privadas a solicitud de una fiscalía local o la federal, aunque esta se estima insuficiente ante la magnitud y complejidad del fenómeno estudiado.

Tampoco existe en México una única institución encargada de la materia que coordine a las demás autoridades. A partir del análisis comparado, se dio cuenta de ciertas características presentes en otros países que regulan la ciberseguridad, tales como la existencia de una agencia nacional cibernética, adscrita a la esfera del Poder Ejecutivo, pero con altos niveles de autonomía.

El diagnóstico del marco jurídico nacional arrojó que existen pocas definiciones directamente relacionadas con la ciberseguridad a nivel constitucional y legal. Los conceptos estrechamente relacionados o propios de la materia se encuentran definidos principalmente en las normas administrativas aplicables al régimen interno de diversos órganos del Estado mexicano.

Todo lo anterior parecería soportar la hipótesis que afirma la insuficiencia del marco jurídico mexicano para hacer frente a las vulnerabilidades, amenazas y ataques cibernéticos, así como para fomentar las capacidades de investigación y desarrollo tecnológicos.

Con la finalidad de nutrir el debate legislativo que busque elaborar normas adecuadas al contexto mexicano, el estudio de derecho comparado permitió derivar algunos elementos comunes, tales como las principales conductas sancionadas por el derecho penal, las instituciones públicas y privadas encargadas de la materia, y la posibilidad de activar algunos mecanismos de control parlamentario, por ejemplo, la aprobación de nombramientos, de estrategias, las comparecencias de funcionarios y la presentación de informes periódicos ante comisiones legislativas, entre otros.

Los marcos normativos analizados tienden a ofrecer definiciones y establecer organismos como las agencias coordinadoras, los órganos de monitoreo e investigación, y equipos de respuesta ante incidentes cibernéticos. De igual forma, contemplan la obligación de establecer programas y políticas, tales como estrategias nacionales de ciberseguridad o programas de capacitación y concienciación. Finalmente se dio cuenta de que a nivel administrativo ya existen normas relativas a la ciberseguridad. En ese sentido, el Poder Legislativo de nuestro país podría retomar algunos de sus contenidos normativos para incorporar ciertos elementos a las leyes mexicanas.

En suma, existen varios pendientes legislativos sobre ciberseguridad en México. Sería conveniente que el Congreso de la Unión considere y

evalúe cuidadosamente los conceptos a incluir, así como sus respectivas definiciones. También podría ponderar la necesidad de elaborar nuevas leyes, y su tipo (general, nacional o federal). Se requeriría analizar cuáles son las reformas necesarias a los ordenamientos vigentes, con el objetivo de mantener la coherencia del sistema jurídico. En ese sentido, se presenta la posibilidad de reformar desde la Constitución, las leyes procesales, sustantivas y orgánicas, hasta los reglamentos unicamerales para crear nuevas comisiones u órganos parlamentarios encargados de la supervisión de la administración pública y otras instituciones en materia de ciberseguridad.

Por su puesto, también se ha planteado la posibilidad de crear uno o más órganos no parlamentarios, por ejemplo, una conferencia específica en el Consejo Nacional de Seguridad Pública, fiscalías especializadas, unidades de policía cibernética, entre otros.

Finalmente, la legislación en materia de ciberseguridad podría contemplar ciertos contenidos mínimos, tales como definiciones precisas, un catálogo de derechos y obligaciones relativos a la ciudadanía digital o al ciberespacio, nuevos tipos penales (aunque no exista adhesión por parte del Estado mexicano, el Convenio de Budapest podría funcionar como guía), un órgano coordinador en la materia y mecanismos específicos de control parlamentario.

REFERENCIAS

1. *Bibliohemerográficas*

AGUIRRE QUEZADA, Juan Pablo, "Ciberseguridad, desafío para México y trabajo legislativo", *Cuadernos de investigación,* núm. 87, Senado de la República, Instituto Belisario Domínguez, marzo 2022.

ANDRESS, Jason y WINTERFELD, Steve, *Cyber Warfare. Techniques, TacTIC and Tools for Security Practitioners*, EE. UU., Syngress, 2011.

AUDITORÍA SUPERIOR DE LA FEDERACIÓN, *Auditoría de TIC a la Secretaría de Hacienda y Crédito Público*, 2019-0-06100-20-0015-2020, México, 2020.

BANCO INTERAMERICANO DE DESARROLLO, *Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte Ciberseguridad 2020*, 2021.

BARRIOS, Miguel Ángel (dir.), *Diccionario latinoamericano de seguridad y geopolítica,* Buenos Aires, Editorial Biblos, 2009.

BBC MUNDO, *México: el ciberataque "sin precedentes" a los bancos del país que causó pérdidas millonarias*, 15 de mayo de 2018.

BSA THE SOFTWARE ALLIANCE, *Country: Estonia, EU Cybersecurity Dashboard*, 2008.

CARR, Jeffrey, *Inside Cyber Warfare*, 2ª edición, EE. UU., O'Reilly, 2011.

CENTENO, Danya, *México y el Convenio de Budapest: posibles incompatibilidades*, México, Red en Defensa de los Derechos Digitales, junio 2018.

CENTRO DE ESTUDIOS INTERNACIONALES GILBERTO BOSQUES, *Características y funcionamiento del Parlamento de Singapur en el marco de la visita de su Presidenta, Halimah Yacob al Senado de la República*, nota informativa, Senado de la República, 25 de abril de 2017.

CERT-MX, *Manual Básico de Ciberseguridad para la Micro, Pequeña y Mediana Empresa*, México, Guardia Nacional, 2018.

CHÁVEZ RINCÓN, Melissa, *Tribunal Supremo de Rusia declara al regimiento de Azov como grupo terrorista*, France24, 3 de agosto de 2022.

CLARKE, Richard A. y KNAKE, Robert K., *Guerra en la red. Los nuevos campos de batalla*, Barcelona, Ariel.

CONSEJO DE EUROPA, *Adhesión al Convenio de Budapest sobre la Ciberdelincuencia: beneficios*, 4 de junio de 2021.

CRUZ LOBATO, Luisa, "La política brasileña de ciberseguridad como estrategia de liderazgo regional", *URVIO, Revista Latinoamericana de Estudios de Seguridad*, Quito, núm. 20, junio 2017.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, *Factsheet*, EE. UU., 2021.

CYBER SECURITY AGENCY OF SINGAPORE, *Singapore's Safer Cyberspace Masterplan 2020*, Singapur, octubre 2020.

------, *The Singapore Cybersecurity Strategy 2021*, Singapur, 2021.

CZOSSECK, C. y GEERS, K. (eds.), "The Virtual Battlefield: Perspectives on Cyber Warfare", *Cryptology and Information Security Series*, vol. 3, 2009.

DEL BARRIO, Javier Martín, *El Secretario General de la ONU dice que hay "ciberguerra entre Estados"*, El País, España, 19 de febrero de 2018.

DIAZGRANADOS, Hernán, *Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021*, Kaspersky Daily, 31 de agosto de 2021.

DIRECCIÓN NACIONAL DE CIBERSEGURIDAD, *Incidentes informáticos. Informe anual de incidentes de seguridad informática registrados en el 2021 por el CERT.ar.*, Argentina, febrero 2022.

ENGDAHL, F. William, *Full Spectrum Dominance: Totalitarian Democracy in the New World Order,* Massachusetts, Third Millennium Press, 2009.

ERBSCHLOE, Michael, *Information Warfare. How to Survive Cyber Attacks*, EE. UU. Osborne/McGraw-Hill, 2001.

ESPAÑA EXPORTACIÓN E INVERSIONES (ICEX), *El mercado de la ciberseguridad en Brasil*, España, 2021.

FORBES, *Lotería Nacional confirma que sí sufrió un ciberataque*, Forbes, 1 de junio de 2021.

------, *México, primer lugar en ciberataques en Latinoamérica*, 30 de noviembre de 2021.

GIBSON, William, *Neuromancer,* Electronic Edition, Nueva York, The Ace Publishing Group, 2003.

GOBIERNO DE CANADÁ, *Déclaration au nom du président de la Coalition pour la liberté en ligne: Un appel à l'action sur la désinformation parrainée par l'État en Ukraine*, Affaires Mondiales, Ottawa, 2 de marzo de 2022.
GOBIERNO DE MÉXICO, *Estrategia Nacional de Ciberseguridad*, México, 2017.
GOBIERNO DE MÉXICO *et al.*, *Glosario de Términos SEDENA - MARINA en Materia de Seguridad en el Ciberespacio*, México, junio 2021.
GOBIERNO DE MÉXICO y SECRETARÍA DE MARINA, *Cartilla de Ciberseguridad de la Secretaría de Marina*, México, 2021.
GÓMEZ FLORES, Laura, *México, segundo lugar mundial en ciberataques: FEM*, La Jornada, México, 4 de octubre de 2021.
GUARNEROS OLMOS, Fernando, *En un trimestre, México registró 80,000 millones de intentos de ciberataques*, Expansión, México, 11 de mayo de 2022.
HÜBNER, Risto, "The Privacy, Data Protection and Cybersecurity Law Review: Estonia", *The Law Reviews*, 5 de noviembre de 2021.
HUISSOUD, Jean-Marc y GAUCHON, Pascal (coords.), *Las 100 palabras de la geopolítica*, Madrid, Akal, 2013.
INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA, *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2020*, [base de datos], México, junio de 2021.
JANCZEWSKI, Lech J. y COLARIK, Andrew M., *Cyber Warfare and Cyber Terrorism*, Nueva York, Hershey, 2008.
KITCHIN, Rob, *Cyberspace: The World in the Wires*, EE. UU., Wiley, 1998.
LANDEROS, Emma, *México: ciberataques a las dependencias de gobierno*, Newsweek, 21 de julio de 2021.
MARTINS DOS SANTOS, Bruna, *Convenio de Budapest sobre la Ciberdelincuencia en América Latina: Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México*, Derechos Digitales América Latina, 2022.
METABASE Q, *Comparativo de Iniciativas en Ciberseguridad*, 2020.
------, *El Estado de la Ciberseguridad en México*, 2021.
MILLS, Charles Wright, *Poder, Política, Pueblo*, México, Fondo de

Cultura Económica, 1973.
MINISTRY OF FOREIGN AFFAIRS OF THE RUSSIAN FEDERATION, *Foreign Minister Sergey Lavrov's interview with TV channels RT, NBC News, ABC News, ITN, France 24 and the PRC Media Corporation*, Moscú, 3 de marzo de 2022.
NATIONAL GEOGRAPHIC, *Los experimentos secretos de la CIA*, Grandes Enigmas de la Historia, Barcelona, Editorial Sol 90, 2012.
NEVES DE MOURA FILHO, Ronaldo *et al*., "Regulación de la ciberseguridad en el sector de telecomunicaciones de Brasil: un balance de incentivos en un contexto de neutralidad tecnológica", *Revista Latinoamericana de Economía y Sociedad Digital*, núm. 2, agosto 2021.
PARKER, Dean, *Why Is Canada's Foreign Minister Proud of Her Family's Nazi Past?*, Russia Insider, 5 de abril de 2017.
PIKE, Cameron, *Canada's Nazi Problem*, Russia Insider, 6 de febrero de 2018.
PRESIDENCIA DE LA REPÚBLICA FEDERATIVA DE BRASIL *et al*., *Livro Verde: Segurança Cibernética no Brasil*, Brasilia, 2010.
------, *Livro Branco de Defesa Nacional*, Brasil, 2012.
PRESIDENCIA DE LA REPÚBLICA, *Acuerdo por el que se expide la Estrategia Digital Nacional 2021-2024*, Diario Oficial de la Federación, México, 6 de septiembre de 2021.
PRESIDENCIA DE LA REPÚBLICA *et al*., *Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos*, México, octubre 2021.
PRESIDENT OF RUSSIA, *Address by the President of the Russian Federation*, The Kremlin, Moscú, 24 de febrero de 2022.
QUINN, Michael, *The Large and Influential Ukrainian Diaspora in Canada - Good Russian TV Profile*, Russia Insider, 2 de marzo de 2019.
RÍOS, Ailyn, *Reprueba Sedena en ciberseguridad*, Reforma, México, 26 de febrero de 2022.
RIQUELME, Rodrigo, *Tres de cada cuatro empresas mexicanas fueron víctimas de ransomware: Sophos*, El Economista, México, 11 de mayo de 2022.
SANTOS CID, Alejandro, *El espionaje del 'caso Pegasus' en México se cobra su primer detenido*, El País, España, 8 de noviembre de 2021.
SAXE-FERNÁNDEZ, John, "Etiología de la patología revolucionaria y profilaxis contrarrevolucionaria", *Revista Mexicana de Ciencias*

Políticas y Sociales, México, nueva época, año XXI, núm. 81, julio-septiembre de 1975.
SECRETARÍA DE COMUNICACIONES Y TRANSPORTES, *Guía de Ciberseguridad para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo al teletrabajo*, México, junio 2020.
SECRETARÍA DE MARINA, *Estrategia Institucional para el Ciberespacio 2021-2024*, México, 2021.
SECRETARÍA DE SEGURIDAD Y PROTECCIÓN CIUDADANA, *Tercer informe de la Estrategia Nacional de Seguridad Pública*, México, abril, 2022.
SECRETARIO GENERAL DE LA UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, *Transmisión del informe del expresidente del Grupo de Expertos de Alto nivel de la Agenda sobre Ciberseguridad Global*, Documento C19/58-S, Ginebra, 6 de mayo de 2019.
SHAKARIAN, Paulo *et al.*, *Introduction to Cyber Warfare. A multidisciplinary Approach*, EE. UU., Syngress, 2013.
SLOTERDIJK, Peter, *Esferas III. Esferología plural*, Madrid, Siruela, 2009.
SOHR, Raúl, *Las guerras que nos esperan*, Chile, Ediciones B, 2000.
SZAFRANSKI, Richard, *Neocortical Warfare? The Acme of Skill*, Military Review, noviembre 1994.
TISSOT, René, *Función simbólica y psicopatología*, México, Fondo de Cultura Económica, 1992.
UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, *Global Cybersecurity Index 2020*, ITU Publications, 2021.
------, *Agenda sobre Ciberseguridad Global (GCA) de la Unión Internacional de Telecomunicaciones*, s.f., s.l.i., s.a.
UNITED STATES DEPARTMENT OF DEFENSE, *Cyber Strategy 2018*, EE. UU., 2018.
VON CLAUSEWITZ, Carl, *De la Guerra,* México, Colofón, 2006.

2. *Normativa nacional*

Constitución Política de los Estados Unidos Mexicanos.
Código de Comercio.
Código Fiscal de la Federación.
Código Nacional de Procedimientos Penales.

Código Penal Federal.
Ley de Aviación Civil.
Ley de Comercio Exterior.
Ley de Firma Electrónica Avanzada.
Ley de Instituciones de Crédito.
Ley de Instituciones de Seguros y de Fianzas.
Ley de la Comisión Federal de Electricidad.
Ley de la Comisión Nacional Bancaria y de Valores.
Ley de la Fiscalía General de la República.
Ley de la Industria Eléctrica.
Ley de Migración.
Ley de Sistemas de Pagos.
Ley del Mercado de Valores.
Ley Federal contra la Delincuencia Organizada.
Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
Ley Federal de Telecomunicaciones y Radiodifusión.
Ley Federal del Derecho de Autor.
Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita.
Ley General de Acceso de las Mujeres a una Vida Libre de Violencia.
Ley General de Archivos.
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Ley General de Títulos y Operaciones de Crédito.
Ley para Regular las Instituciones de Tecnología Financiera.

3. *Normativa internacional*

American Innovation and Competitiveness Act, Public Law 114–329, 130 Stat. 2969, 6 de enero de 2017.
Anexo II, Glosario de Términos de Ciberseguridad, *Boletín Oficial*, 30 de agosto de 2019, Argentina.
Code of Laws of the United States of America, Cornell Law School, EE. UU.
CONSEJO DE EUROPA, *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and*

xenophobic nature committed through computer systems (ETS No. 189), Estrasburgo, 2003.
------, *Convention on Cybercrime*, Budapest, ETS, núm. 185, 2001.
------, *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)*, Estrasburgo, 2022.
CONSEJO DE SEGURIDAD DE LA ORGANIZACIÓN DE LAS NACIONES UNIDAS, *Resolución 2341 (2017)*, aprobada en su 7882a sesión celebrada el 13 de febrero de 2017.
CORTE PENAL INTERNACIONAL, *Estatuto de Roma*.
Computer Misuse Act 1993, (2020 revised edition), *Government Gazette*, 30 de agosto de 1993, Singapur.
Cybersecurity Act 2018, (No. 9 of 2018), *Government Gazette*, 16 de marzo de 2018, Singapur.
Cyber Response and Recovery Act of 2021, Public Law 117, S.1316, 22 de abril de 2021.
Cyber Security Research and Development Act, Public Law 107–305, 116 Stat. 2367, 27 de noviembre de 2002.
Cybersecurity and Infrastructure Security Agency Act of 2018, Public Law 115–278, 132 Stat. 4168, 16 de noviembre de 2018.
Cybersecurity Enhancement Act of 2014, Public Law 113–274, 128 Stat. 2971, 18 de diciembre de 2014.
Cybersecurity Information Sharing Act of 2015, 114, S. 754, 27 de octubre de 2015.
Cybersecurity Workforce Assessment Act, Public Law 113–246, 128 Stat. 2880, 18 de diciembre de 2014.
Decreto nº 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, *Diário Oficial da União*, 14 de junio de 2000, núm. 114, Brasilia.
Decreto nº 4.801, de 6 de agosto de 2003. Cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo, *Diário Oficial da União*, 7 de agosto de 2003, Brasilia.
Decreto Nº 4.829, de 3 de setembro de 2003. Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências, *Diário Oficial da União*, 4 de septiembre de 2003, Brasilia.

Decreto nº 7.724, de 16 de maio de 2012. Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição, *Diário Oficial da União*, 16 de mayo de 2012, Brasilia.

Decreto nº 7.845, de 14 de novembro de 2012. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento, *Diário Oficial da União*, 16 de noviembre de 2012, Brasilia.

Decreto nº 9.573, de 22 de novembro de 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas, *Diário Oficial da União*, 23 de noviembre de 2018, núm. 225, Brasilia.

Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional, *Diário Oficial da União*, 27 de diciembre de 2018, núm. 248, Brasilia.

Decreto Nº 9.819, de 3 de junho de 2019. Dispõe sobre a Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, *Diário Oficial da União*, núm. 106, 4 de junio de 2019, Brasilia.

Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética, *Diário Oficial da União*, 6 de febrero de 2020, núm. 26, Brasilia.

Decreto nº 10.363, de 21 de maio de 2020. Altera o Decreto nº 9.668, de 2 de janeiro de 2019, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República, e remaneja e transforma cargos em comissão, *Diário Oficial da União*, núm. 97, 22 de mayo de 2020, Brasilia, p. 7.

Decreto Nº 10.569, de 9 de dezembro de 2020. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas, *Diário Oficial da União*, núm. 236, 10 de diciembre de 2020, Brasilia.

Decreto nº 10.641, de 2 de março de 2021. Altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Se-

gurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional, *Diário Oficial da União*, 3 de marzo de 2021, núm. 41, Brasilia.

Decreto nº 10.748, de 16 de julho de 2021. Institui a Rede Federal de Gestão de Incidentes Cibernéticos, *Diário Oficial da União*, 19 de julio de 2021, núm. 134, Brasilia.

Decreto 1067/2015, Incorporase al anexo I del artículo 1º del Decreto nº 357 de fecha 21 de febrero de 2002, sus modificatorios y complementarios -organigrama de aplicación de la Administración Pública Nacional centralizada-, apartado XI, la Subsecretaría de Protección de Infraestructuras Criticas de Información y Ciberseguridad en el ámbito de la Secretaria de Gabinete de la Jefatura de Gabinete de Ministros, de 10 de junio de 2015, *Boletín Oficial*, 12 de junio de 2015, núm. 33149, Argentina.

Decreto 577/2017, Comité de Ciberseguridad, creación, de 28 de julio de 2017, *Boletín Oficial*, 31 de julio de 2017, núm. 33677, Argentina.

Disposición 3/2013, Apruébase la "Política de Seguridad de la Información Modelo", de 27 de agosto de 2013, *Boletín Oficial*, 2 de septiembre de 2013, núm. 32713, Argentina.

Disposición 1/2021, Centro Nacional de Respuesta a Incidentes Informáticos (CERT.art) – créase, de 19 de febrero de 2021, *Boletín Oficial*, 22 de febrero de 2021, núm. 34591, Argentina.

Disposición 8/2021, *Boletín Oficial*, 10 de noviembre de 2021, Argentina.

Disposición 6/2021, *Boletín Oficial,* 4 de diciembre de 2021, Argentina.

Elektroonilise side seadus, de 8 de diciembre de 2004, *Riigi Teataja*, vol. I, 87, 2004, Estonia.

Federal Information Security Modernization Act of 2014, Public Law 113–283, 128 Stat. 3073, 18 de diciembre de 2014.

Gramm-Leach Bliley Act, Public Law 106–102, 113 Stat. 1338, 12 de noviembre de 1999.

Hädaolukorra seadus, de 8 de febrero de 2017, *Riigi Teataja*, vol. I, 3 de marzo de 2017, Estonia.

Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008. Disciplina a Gestão de Segurança da Informação e Comunicações na Adminis-

tração Pública Federal, direta e indireta, e dá outras providências, *Diário Oficial da União*, Brasilia, junio de 2008.

Instrução Normativa nº 4, de 26 de março de 2020. Dispõe sobre os requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G, *Diário Oficial da União*, 27 de marzo de 2020, núm. 60, Brasilia.

Instrução Normativa Nº 1, de 27 de maio de 2020. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal, *Diário Oficial da União*, 28 de mayo de 2020, núm. 101, Brasilia.

Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021. Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal, *Diário Oficial da União*, 31 de mayo de 2021, núm. 101, Brasilia.

Instrução Normativa Nº 2, de 24 de julho de 2020. Altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal, *Diário Oficial da União*, 27 de julio de 2020, núm. 142, Brasilia.

Instrução Normativa Nº 5, de 30 de agosto de 2021. Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal, *Diário Oficial da União*, 31 de agosto de 2021, núm. 165, Brasilia.

Internet of Things Cybersecurity Improvement Act of 2020, Public Law 116–207, 134 Stat. 1001, 4 de diciembre de 2020.

Isikuandmete kaitse seadus, de 12 de diciembre de 2018, *Riigi Teataja*, 4 de enero de 2019, Estonia.

Lei nº 7.232, de 29 de outubro de 1984. Dispõe sobre a Política Nacional de Informática, e dá outras providências, *Diário Oficial da União*, 30 de octubre de 1984, Brasilia.

Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências, *Diário Oficial da União*, 18 de noviembre de

2011, núm. 221-A, Brasilia.
Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências, *Diário Oficial da União*, 3 de diciembre de 2012, núm. 232, Brasilia.
Lei Nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, *Diário Oficial da União*, 24 de abril de 2014, núm. 77, Brasilia.
Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais, *Diário Oficial da União*, 15 de agosto de 2018, núm. 157, Brasilia.
Lei nº 13.844, de 18 de junho de 2019. Estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios, *Diário Oficial da União*, 18 de junio de 2019, núm. 116-A, Brasilia.
Ley 25.326, Protección de los Datos Personales, de 4 de octubre de 2000, *Boletín Oficial*, 2 de noviembre de 2000, núm. 29517, Argentina.
Ley 25.506, Firma Digital, de 14 de noviembre de 2001, *Boletín Oficial*, 14 de diciembre de 2001, núm. 29796, Argentina.
Ley 26.388, Código Penal, modificación, de 4 de junio de 2008, *Boletín Oficial*, 25 de junio de 2008, núm. 31433, Argentina.
Ley 26.904, Código Penal, incorporación, de 13 de noviembre de 2013, *Boletín Oficial*, 11 de diciembre de 2013, núm. 32783, Argentina.
Ley 27.126, Creación de la Agencia Federal de Inteligencia, modificación Ley nº 25.520, de 3 de marzo de 2015, *Boletín Oficial*, 5 de marzo de 2015, núm. 33083, Argentina.
Ley 27.411, Convenio Sobre Ciberdelito del Consejo de Europa, de 15 de diciembre de 2017, *Boletín Oficial*, Argentina.
National Cybersecurity Preparedness Consortium Act of 2021, Public Law 117–122, 136 Stat. 1193, 12 de mayo de 2022.
National Cybersecurity Protection Act of 2014, Public Law 113–282, 128 Stat. 3066, 18 de diciembre de 2014.
National Defense Authorization Act for Fiscal Year 2022, Public Law 117–81, 135 Stat. 1541, 27 de diciembre de 2021.
National Institute of Standards and Technology Act, Public Law 100-418, 102 Stat. 1427.
NIST Small Business Cybersecurity Act, Public Law 115–236, 132 Stat. 2444, 14 de agosto de 2018.

Portaria GSI/PR Nº 93, de 18 de outubro de 2021. Aprova o glossário de segurança da informação, *Diário Oficial da União*, 19 de octubre de 2021, núm. 197, Brasilia.
Portaria No. 85, de 26 de junho de 2017. Estabelece regras básicas de utilização do Terminal de Comunicação Segura (TCS) fornecido pela Agência Brasileira de Inteligência (ABIN), *Diário Oficial da União*, 27 de junio de 2017, núm. 121, Brasilia.
Rahapesu ja terrorismi rahastamise tõkestamise seadus, de 26 de octubre de 2017, *Riigi Teataja*, vol. I, 17 de noviembre de 2017, Estonia.
Resolución 234/2016, Protocolo general en la investigación y proceso de recolección de pruebas en ciberdelitos, de 7 de junio de 2016, *Boletín Oficial*, 14 de junio de 2016, núm. 33399, Argentina.
Resolución 580/2011, Créase el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad. Objetivos, de 28 de julio de 2011, *Boletín Oficial*, 2 de agosto de 2011, núm. 32204, Argentina.
Resolución 829/2019, Estrategia Nacional de Ciberseguridad, de 24 de mayo de 2019, *Boletín Oficial*, 28 de mayo de 2019, Argentina.
Resolución 1523/2019, Definición de Infraestructuras Críticas, de 12 de septiembre de 2019, *Boletín Oficial*, 18 de septiembre de 2019, núm. 34200, Argentina.
Resolução nº 740, de 21 de dezembro de 2020. Aprova o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, *Diário Oficial da União*, 24 de diciembre de 2020, núm. 246, Brasilia.
Riigisaladuse ja salastatud välisteabe seadus, de 25 de enero de 2007, *Riigi Teataja*, vol. I, 16, 2007, Estonia.

4. *Internet*

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, *Segurança Cibernética*, (24 de mayo de 2022).
ASOCIACIÓN MEXICANA DE CIBERSEGURIDAD (AMECI), *Ciberseguridad y protección de datos en México,* 2021, (26 de abril de 2022).
AUDITORÍA SUPERIOR DE LA FEDERACIÓN, *Auditoría de Cumplimiento a Tecnologías de Información y Co- municaciones: 2018-6-90T9N20-0449-2019,* (3 de octubre de 2022).

CÁMARA DE LOS DIPUTADOS, *El Congreso Nacional*, (24 de mayo de 2022).
CEPTRO.BR, *Sobre o CEPTRO.br*, (24 de mayo de 2022).
CERT.BR, *Grupos de Segurança e Resposta a Incidentes (CSIRTs) Brasileiros*, (22 de mayo de 2022).
------, *Sobre o CERT.br*, (24 de mayo de 2022).
CETIC.BR, *Saiba Mais Sobre o Cetic.br*, (24 de mayo de 2022).
CEWEB.BR, *Atividades e Atribuições do Ceweb.br*, (24 de mayo de 2022).
CIBERSEGURIDAD, *Normativa Argentina*, (18 de mayo de 2022).
------, *Normativa EE. UU.*, (15 de abril de 2022).
------, *Normativa Brasil*, (27 de abril de 2022).
COMITÉ GESTOR DE INTERNET EN BRASIL, *Acerca de CGI.br*, (24 de mayo de 2022).
CONSEJO DE EUROPA, *Mejora en la cooperación y la divulgación de pruebas electrónicas: 22 países firman el nuevo Protocolo al Convenio sobre Ciberdelincuencia*, (12 de mayo de 2022).
CSIRTS EN MÉXICO, *Lista de centros de respuesta ante incidentes informáticos*, (19 de mayo de 2022).
CYBER SECURITY AGENCY OF SINGAPORE (CSA), *About SingCERT*, (6 de mayo de 2022).
------, *Cyber Security Awareness Alliance*, (6 de mayo de 2022).
------, *Operational Technology Cybersecurity Expert Panel*, (6 de mayo de 2022).
------, *Our Organisation*, (6 de mayo de 2022).
E-ESTONIA, *KSI Blockchain*, (28 de mayo de 2022).
ESCRITÓRIO DE PROJETOS DO EXÉRCITO BRASILEIRO, *Programa Defensa Cibernética*, (26 de mayo de 2022).
FORBES, *Hackeo masivo a Sedena evidencia vulnerabilidad de ciberseguridad; así fue el ataque,* (3 de octubre de 2022).
GOBIERNO DE MÉXICO, *Alertas de seguridad informática*, (15 de mayo de 2022).
------, *CERT-MX*, (15 de mayo de 2022).
------, *Controla Secretaría de Economía ataque informático*, (3 de octubre de 2022).
GOVERNMENT TECHNOLOGY AGENCY, *Cyber Security Group (CSG)*, (6 de mayo de 2022).

GUEL, Juan Carlos, *Panorama de la ciberseguridad en México*, Conferencia en ANUIES-TIC, Universidad Autónoma de Nuevo León, 2019.
IBM, *¿Qué es la ciberseguridad?*, (3 de octubre de 2022).
INTERNET WORLD STATS, *Usage and population statistics*, (2 de mayo de 2022).
INSTITUTO FEDERAL DE TELECOMUNICACIONES, *Ciberseguridad*, (8 de mayo de 2022).
------, *Ciberseguridad, Reporte ciudadano*, (15 de mayo de 2022).
JEFATURA DE GABINETE DE MINISTROS, *CERT.ar*, (3 de abril de 2022).
------, *Ciberseguridad*, (3 de abril de 2022).
------, *Denunciar un delito informático*, (8 de mayo de 2022).
------, *Internet Sano*, (18 de mayo de 2022).
------, *Normativa - Ciberseguridad*, (13 de mayo de 2022).
MEZA, Nayeli y BUENDÍA, Eduardo, *PemexLeaks: el robo de información que la petrolera quiso ocultar*, (3 de octubre de 2022).
MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS DE ARGENTINA, *Acerca de Con Vos en la Web*, (18 de mayo de 2022).
MINISTERIO DE SEGURIDAD DE ARGENTINA, *MINSEG-CSIRT*, (3 de abril de 2022).
MINISTERIO PÚBLICO FISCAL, *Unidad Fiscal Especializada en Ciberdelincuencia*, (3 de abril de 2022).
MINISTRY OF FOREIGN AFFAIRS, *Cyber Security*, (27 de mayo de 2022).
MINISTRY OF COMMUNICATIONS AND INFORMATION, *Cyber Security*, (6 de mayo de 2022).
NATIONAL CONFERENCE OF STATE LEGISLATURES, *Cybersecurity Legislation 2021*, (22 de mayo de 2022).
NIC.BR, *Atividades*, (24 de mayo de 2022).
OFICINA DE SEGURIDAD INSTITUCIONAL, *Agência Brasileira de Inteligência*, (24 de mayo de 2022).
------, *Comitê Gestor da Segurança da Informação - CGSI*, (24 de mayo de 2022).
------, *CTIR Gov - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo*, (24 de mayo de 2022).
------, *Departamento de Segurança da Informação*, (24 de mayo de

2022).
------, *O que é*, (24 de mayo de 2022).
------, *Política Nacional de Segurança da Informação - PNSI*, (27 de mayo de 2022).
P&D BRASIL, *GT-Ciber – Anatel*, (26 de mayo de 2022).
RAND CORPORATION, *Sitio web oficial*.
REYES, Eréndira, *Ciberdelincuentes filtran documentos internos de la Lotería Nacional*, (3 de octubre de 2022).
RIQUELME, Rodrigo, *Lotería Nacional confirma sustracción de información por delincuentes internacionales*, (3 de octubre de 2022).
SECRETARÍA DE MARINA, *Unidad de Ciberseguridad*, (20 de mayo de 2022).
SINGAPORE CYBERSECURITY CONSORTIUM, *About Us*, (7 de mayo de 2022).
THE WHITE HOUSE, *Office of the National Cyber Director*, (22 de abril de 2022).
UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, *National Cybersecurity Strategies Repository*, (3 de junio de 2022).
------, *La Agenda sobre Ciberseguridad Global*, (23 de mayo de 2022).
UNITED STATES GOVERNMENT, *Sixteenth Air Force (Air Force Cyber)*, (16 de mayo de 2022).
------, *U.S. Army Cyber Command*, (5 de mayo de 2022).

ANEXOS

Anexo 1. Normativa constitucional y legal sobre ciberseguridad vigente en México

Ordenamiento	Artículo(s)	Contenido
Constitución Política de los Estados Unidos Mexicanos	6	Derecho de acceso a las tecnologías de la información y comunicación, banda ancha e internet; políticas de inclusión digital universal.
	16	Derecho a la protección de datos personales, intervención de comunicaciones privadas solo con autorización judicial.
	21	Seguridad pública, Guardia Nacional.
	22	Extinción de dominio.
	28	Instituto Federal de Telecomunicaciones.
	73	Facultad del Congreso de la Unión para legislar en diversas materias.
	89	Facultades del presidente de la República para nombrar a los titulares de las Fuerzas Armadas y disponer de ellas para la seguridad interior y defensa exterior de la nación, así como de la Guardia Nacional.
Código Penal Federal	166 Bis, 167, fr. II y VI, 168 bis, 168 ter, 177	Tipifican los ataques a las vías de comunicación o violación de correspondencia, tales como proporcionar ilícitamente informes acerca de las personas usuarias de servicios de telecomunicaciones; destruir componentes de la red de telecomunicaciones; interferir comunicaciones inalámbricas y satelitales; decodificar señales de telecomunicaciones; comercializar u operar equipos que bloqueen señales de telefonía celular o de radiocomunicación; intervenir indebidamente comunicaciones privadas.
	199 Septies	Comunicación de contenido sexual con personas menores de dieciocho años de edad, o que no tienen capacidad para comprender el significado del hecho, o para resistirlo.
	199 Octies y 199 Nonies	Violación a la intimidad sexual.
	200	Corrupción de personas menores de dieciocho años de edad, o que no tienen capacidad para comprender el significado del hecho, o para resistirlo.
	202	Pornografía de personas menores de dieciocho años de edad, o que no tienen capacidad para comprender el significado del hecho, o para resistirlo.
	211 bis	Revelación, divulgación o utilización indebida o en perjuicio de otro de información o imágenes obtenidas en una intervención de comunicación privada.
	211 bis 1 a 211 bis 7	Acceso ilícito a sistemas y equipos de informática.

Ordenamiento	Artículo(s)	Contenido
Código de Comercio	32 bis 1 a 32 bis 8	Registro Único de Garantías Mobiliarias, que es electrónico.
	89 a 94	Comercio electrónico: mensajes de datos, digitalización de documentos, firma electrónica, prestadores de servicios de certificación, reconocimiento de certificados y firmas electrónicas extranjeras.
	1390 Bis 26	Las audiencias se registrarán por medios electrónicos.
Código Fiscal de la Federación	17-C a 17-L	Medios electrónicos.
	29	Comprobantes fiscales digitales.
	29 bis	Proveedores de certificación de comprobantes fiscales digitales por Internet.
	82-G	Infracciones relacionadas con la obligación de los proveedores de certificación autorizados de cumplir con las especificaciones informáticas que determine el SAT.
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	3, fr. VI	Definición de cómputo en la nube.
	3, fr. XXIII	Definición de medidas de seguridad técnicas para proteger el entorno digital de los datos personales.
	30, fr. VII y VIII	Mecanismos que debe adoptar el responsable de los datos.
	31 a 42	Obligaciones del responsable para mantener las medidas de seguridad para la protección de los datos personales.
	59	Deberes del encargado de los datos personales.
	64	Tratamiento de datos personales en servicios, aplicaciones e infraestructura de cómputo en la nube.
	80 a 82	Bases de datos en posesión de instancias de seguridad, procuración y administración de justicia.
	163, fr. VIII	Sanciones por no establecer medidas de seguridad.
Ley Federal de Protección de Datos Personales en Posesión de los Particulares	19 a 21	Responsable deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales.
	63, fr. XI	Es una infracción vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable.
	67	Es un delito: al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.

Ordenamiento	Artículo(s)	Contenido
Ley General de Archivos	25	Programa anual debe incluir, entre otros, programas seguridad de la información y procedimientos para la generación, administración, uso, control, migración de formatos electrónicos y preservación a largo plazo de los documentos de archivos electrónicos.
	41 al 49	Documentos de archivo electrónicos.
	60 al 63	Conservación de la información.
Ley General de Acceso de las Mujeres a una Vida Libre de Violencia	20 Quáter	Violencia digital.
	20 Sexies	Medidas de protección tratándose de violencia digital.
Ley Federal de Telecomunicaciones y Radiodifusión	1	El objeto de la ley consiste en regular el uso, aprovechamiento y explotación del espectro radioeléctrico, las redes públicas de telecomunicaciones, el acceso a la infraestructura activa y pasiva, los recursos orbitales, la comunicación vía satélite, la prestación de los servicios públicos de interés general de telecomunicaciones y radiodifusión, y la convergencia entre éstos, los derechos de los usuarios y las audiencias, y el proceso de competencia y libre concurrencia en estos sectores.
	2	Señala que el Estado protegerá la seguridad y la soberanía de la Nación y garantizará la eficiente prestación de los servicios públicos de interés general de telecomunicaciones y radiodifusión.
	3	Define conceptos estrechamente relacionados con la ciberseguridad, tales como *arquitectura abierta*, *infraestructura activa*, *infraestructura pasiva*, *interferencia perjudicial*, *internet*, *tráfico*, entre otros.
	15, fr. XIV	Establece que corresponde al IFT resolver las solicitudes de interrupción parcial o total, por hechos fortuitos o causas de fuerza mayor de las vías generales de comunicación en materia de telecomunicaciones y radiodifusión, del tráfico de señales de telecomunicaciones entre concesionarios y de la prestación de servicios de telecomunicaciones y radiodifusión a usuarios finales.
	55	Clasifica las bandas de frecuencia del espectro radioeléctrico. Un tipo es el espectro protegido.
	56	Señala que el IFT garantizará la disponibilidad de bandas de frecuencias del espectro radioeléctrico o capacidad de redes para el Ejecutivo Federal para seguridad nacional y seguridad pública.
	98	Establece que el IFT deberá garantizar la disponibilidad de recursos orbitales para servicios de seguridad nacional, seguridad pública, y otras necesidades, funciones, fines y objetivos a cargo del Ejecutivo Federal.
	127	Señala qué se considerará un servicio de interconexión.
	145	Establece que los concesionarios y autorizados que presten el servicio de acceso a Internet deberán preservar la privacidad de los usuarios y la seguridad de la red, así como tomar las medidas o acciones necesarias para la gestión de tráfico y administración de red a fin de garantizar la calidad o la velocidad de servicio contratada.

Ordenamiento	Artículo(s)	Contenido
Ley General del Sistema Nacional de Seguridad Pública	5, fr. II y XVII	Define bases de datos, y el conjunto de las mismas conformará el Sistema Nacional de Información (SNI).
	7, fr. IX y XII	Las instituciones de seguridad pública deberán coordinarse para generar e intercambiar información mediante las bases de datos del SNI; también garantizar que todos los centros de readaptación social cuenten con equipos para bloquear o anular permanentemente las señales de telefonía celular, de radiocomunicación, o de transmisión de datos o imagen dentro del perímetro de los mismos.
	19	El Centro Nacional de Información será el responsable de regular el SNI; emitir sus lineamientos de uso, manejo y niveles de acceso; vigilar el cumplimiento de los criterios de acceso y hacer del conocimiento de las instancias competentes cualquier irregularidad detectada.
	25, fr. XXI	La Conferencia Nacional de Procuración de Justicia podrá proponer al Centro Nacional de Información los criterios para la integración de la información, funcionamiento, consulta y medidas de seguridad del SNI.
	29	La Conferencia Nacional de Secretarios de Seguridad Pública podrá: • Proponer medidas para vincular el SNI con otros nacionales, regionales o locales, así como la adopción y aplicación de políticas de cooperación internacional. • Desarrollar las especialidades policiales de alto desempeño para hacer frente a los delitos de impacto nacional e internacional. • Proponer los criterios para la integración de la información, consulta y medidas de seguridad del SNI.
	31, fr. VIII	La Conferencia Nacional del Sistema Penitenciario podrá formular los lineamientos para que la federación y las entidades federativas cumplan con la obligación de adquirir, instalar y mantener en operación equipos que permitan bloquear o anular las señales de telefonía celular, de radiocomunicación, o de transmisión de voz, datos o imagen en el perímetro de centros de readaptación social.
	75	Funciones de las instituciones policiales (investigación, prevención y reacción).
	109	Regula el Sistema Nacional de Información en Seguridad Pública.
	109 bis	La SSPC operará la plataforma tecnológica y deberá establecer lineamientos para la funcionalidad, operación, respaldo, reconstrucción y seguridad de la información.
	139	Establece sanciones por el ingreso doloso al SNI y por divulgar información.

Ordenamiento	Artículo(s)	Contenido
Código Nacional de Procedimientos Penales	51	Uso de medios electrónicos durante el proceso penal.
	235	Aseguramiento de productos relacionados con delitos de propiedad intelectual y derechos de autor.
	252, fr. III	Actos de investigación que requieren autorización previa del Juez de control; intervención de comunicaciones privadas y correspondencia.
	291 a 303	Intervención de comunicaciones privadas.
Ley de Seguridad Nacional	5	Amenazas a la seguridad nacional, específicamente aquellas que pudieran relacionarse con el uso, intervención y afectación de sistemas digitales, aunque no están señalados expresamente.
	8, fr. IV; 13, fr. VII; 34; 35; 36; 39; 40; 44; 47 y 48	Reglas de supletoriedad; lineamientos para regular aparatos en la intervención de comunicaciones privadas; definición de intervención.
	15, fr. VIII	Funciones del secretario técnico del Consejo: administrar y sistematizar los instrumentos y redes de información que se den en el Consejo.
	19, fr. IX	Atribuciones del centro: operación de la tecnología de comunicaciones especializadas.
	29 a 32	Información, inteligencia y contrainteligencia; al poder usar cualquier método para la recolección de información.
	46	Obligación de las empresas que presten cualquier servicio de comunicación de conceder las facilidades requeridas por la autoridad en los términos de la ley.
	55	Resguardo de la información generada por con los sistemas de coordinación en materia de Seguridad Nacional.

Ordenamiento	Artículo(s)	Contenido
Ley Federal de Protección a la Propiedad Industrial	344, fr. VII	Por violación a alguno de los derechos de la ley, el Instituto podrá ordenar al infractor la remoción o cese de los actos violatorios de cualquier medio virtual, digital, electrónico, conocido y por conocerse.
	345, fr. III	Un requisito del Instituto para tomar las medidas pertinentes en caso de violación de la ley es la presentación de la información necesaria para identificar las plataformas digitales en las que se ha cometido dicha violación.
	358	Las visitas de inspección también pueden abarcar las plataformas digitales.
Ley Federal del Derecho de Autor	114 bis a 114 quinquies	Medidas tecnológicas de protección.
	114 sexies	Información sobre la gestión de derechos.
	114 septies y 114 octies	Proveedores de internet.
	101 a 106 y 111	Programa de computación.
	107 a 110	Base de datos.
	112 a 114	Prohibición de medios que eliminen la protección técnica de programas de cómputo, transmisiones del espacio electromagnético y redes de telecomunicaciones.
Ley de Aviación Civil	35	Medios electrónicos en el sistema de tránsito aéreo prestados por la SICT.
	47	Contenido del Registro Aeronáutico Mexicano.
Ley de Comercio Exterior	4, fr. VII	Conexión electrónica entre la Secretaría de Economía y la Secretaría de Hacienda y Crédito Público para administrar una restricción o regulación no arancelaria.
	17 A	El cumplimiento de las restricciones y regulaciones no arancelarias deberá demostrarse mediante documentos que cuenten con medidas de seguridad o por medios electrónicos.

Ordenamiento	Artículo(s)	Contenido
Ley de Firma Electrónica Avanzada	Varios	Actuaciones electrónicas, documentos electrónicos, medios de comunicación electrónica, medios electrónicos, mensajes de datos y servicios relacionados con la firma electrónica.
	13	Cada dependencia y entidad contara con un sistema de trámites electrónicos con mecanismos de seguridad.
	14	Los mensajes de datos y documentos electrónicos que contengan datos personales estarán sujetos a protección conforme a la normatividad correspondiente.
	21, fr. II	El titular de un certificado digital tendrá, entre otros, el derecho a que los datos e información sean tratados con confidencialidad por la autoridad certificadora.
	25, fr. II	Las autoridades certificadoras están obligadas a adoptar las medidas necesarias para evitar la falsificación, alteración o uso indebido de certificados digitales y de los servicios relacionados a la firma electrónica avanzada.
	25, fr. VI	Las autoridades certificadoras están obligadas a preservar la confidencialidad, integridad y seguridad de los datos personales de los titulares de los certificados digitales.
Ley de Instituciones de Crédito	10, fr. IV, inciso b)	Las solicitudes para organizarse y operar como institución de banca múltiple deberán incluir las medidas de seguridad con las que se preserve la integridad de la información.
	46 bis, fr. IV	La CNBV autorizará el inicio de operaciones (o adición de nuevas) a las instituciones de banca múltiple, cuando entre otras, acrediten contar con una infraestructura de seguridad.
	112 bis, fr. VI	Delito especial, específicamente el relativo a poseer, adquirir, utilizar o comercializar equipos electrónicos de cualquier tecnología para sustraer, copiar o reproducir información de tarjetas de crédito, de débitos, cheques, formatos o esqueletos de cheques o cualquier instrumento de pago de instituciones bancarias con el propósito de obtener recursos económicos, información confidencial o reservada.
	112 quáter fr. I y fr. II	Delito especial, quien acceda a los mecanismos o medios electrónicos o de cualquier otra tecnología del sistema bancario mexicano para obtener recursos económicos, información confidencial o reservada; y quien altere o modifique el funcionamiento de los equipos o medios electrónicos o de cualquier otra tecnología para disponer de efectivo de los usuarios, recursos económicos, información confidencial o reservada.
	112 sextus	Delito especial, a quien se valga, entre otros, de medio electrónico para suplantar la identidad, representación o personalidad de una autoridad financiera o de alguna de sus áreas.
Ley de Instituciones de Seguros y de Fianzas	164, fr. II	Las operaciones realizadas por las Instituciones de Seguros deben sujetarse a las disposiciones dictadas por la Comisión, que, entre otras, atienden a la seguridad de las operaciones.
	259, fr. I	Las operaciones relativas al reaseguramiento y al reafianzamiento, deben sujetarse a las disposiciones dictadas por la Comisión, que, entre otras, atienden a la seguridad de las operaciones.

Ordenamiento	Artículo(s)	Contenido
Ley para Regular las Instituciones de Tecnología Financiera	3, fr. XV y fr. XVI	Define *infraestructura tecnológica* e *instituciones de tecnología financiera* (ITF), las cuales incluyen a las instituciones de fondos de pago electrónico.
	34, fr. IV	Las ITF que operen con activos virtuales deberán divulgar a sus clientes los riesgos que existen por celebrar operaciones con dichos activos, lo que deberá incluir informarles de manera sencilla y clara en su página de internet o medio que utilice para prestar su servicio sobre los riesgos tecnológicos, cibernéticos y de fraude inherentes a los activos virtuales.
	37, fr. III	La CNBV revalidará la autorización a las ITF que cuenten con la infraestructura y los controles internos necesarios para realizar sus operaciones, tales como sistemas operativos, contables y de seguridad.
	39, fr. VI	Las solicitudes para obtener las autorizaciones de la CNBV incluirán las medidas y políticas en materia de control de riesgos operativos, así como de seguridad de la información, incluyendo las políticas de confidencialidad, demostrando que cuentan con un soporte tecnológico seguro, confiable y preciso y con los estándares mínimos de seguridad que aseguren la confidencialidad, disponibilidad e integridad de la información y prevención de fraudes y ataques cibernéticos.
	48	La CNBV y el Banco de México emitirán conjuntamente disposiciones de carácter general en materia de seguridad de la información a cargo de las instituciones de fondos de pago electrónico, incluyendo las políticas de confidencialidad y registro de cuentas sobre movimientos transaccionales, el uso de medios electrónicos, ópticos o de cualquier otra tecnología.
	58 83, fr. III	Las ITF estarán obligadas a establecer medidas y procedimientos para prevenir y detectar actos, omisiones u operaciones ilícitas. En la solicitud de autorización temporal, las sociedades que pretendan operar con Modelos Novedosos deberán incluir las políticas de análisis de riesgo, incluyendo aquellas políticas a seguir en materia de seguridad en la Infraestructura Tecnológica y de seguridad de la información.
	87 fr. II	Los interesados en obtener una autorización deberán presentar la información sobre las políticas de análisis de riesgo, incluyendo aquellas políticas a seguir en materia de seguridad en la Infraestructura Tecnológica y de seguridad de la información.
Ley Federal contra la Delincuencia Organizada	11 bis 1	Contempla que el agente del MP de la federación podrá obtener información por medio de la vigilancia electrónica.
	16 y 18	Contempla la posibilidad de intervenir comunicaciones privadas que sean transmitidas por cualquier medio, entre los que se encuentran los medios electrónicos e informáticos.

Ordenamiento	Artículo(s)	Contenido
Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita	17, fr. XVI	Considera una actividad vulnerable el ofrecimiento habitual y profesional de intercambio de activos virtuales por parte de sujetos distintos a las entidades financieras, que se lleven a cabo a través de plataformas electrónicas, digitales o similares, que administren u operen, facilitando o realizando operaciones de compra o venta de dichos activos propiedad de sus clientes o bien, provean medios para custodiar, almacenar, o transferir activos virtuales. Define activo virtual como toda representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos.
	27, fr. VIII	La entidad colegiada deberá contar con los sistemas informáticos que reúnan las características técnicas y de seguridad necesarias para presentar los avisos de sus integrantes.
	46	La Unidad podrá solicitar a la Secretaría la verificación de información y documentación, en relación con la identidad de personas, domicilios, números telefónicos, direcciones de correos electrónicos, operaciones, negocios o actos jurídicos de quienes realicen Actividades Vulnerables.
Ley de Sistemas de Pagos	6, fr. V	Todo sistema de pagos debe prever en sus normas internas las medidas de seguridad del sistema operativo y las acciones correctivas en caso de fallas.
Ley General de Títulos y Operaciones de Crédito	432, fr. IV	Tipifica como delito en materia de títulos y operaciones de crédito, el alterar, copiar o reproducir la banda magnética o el medio de identificación electrónica, óptica o de cualquier otra tecnología, de tarjetas de servicio, de crédito o en general, instrumentos utilizados en el sistema de pagos.
	432, fr. V	Tipifica como delito sustraer, copiar o reproducir información contenida en tarjetas de servicio, de crédito o en instrumentos utilizados en el sistema de pagos.
	432, fr. VI	Tipifica como delito poseer, adquirir, utilizar o comercializar equipos o medios electrónicos, ópticos o de cualquier otra tecnología para sustraer, copiar o reproducir información contenida en tarjetas de servicio, de crédito o en instrumentos utilizados en el sistema de pagos, con el propósito de obtener recursos económicos, información confidencial o reservada.
	434, fr. I y II	Sanciona el acceso sin causa legítima o sin consentimiento a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología de las entidades emisoras de tarjetas de servicio, de crédito o de instrumentos utilizados en el sistema de pagos, para obtener recursos económicos, información confidencial o reservada, así como alterar el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo que son utilizados por los usuarios del sistema de pagos, para obtener recursos económicos, información confidencial o reservada.

Ordenamiento	Artículo(s)	Contenido
Ley de la Industria Eléctrica	108, fr. XXXII	El CENACE está facultado para mantener la seguridad informática y actualización de sistemas con los que pueda cumplir sus objetivos.
Ley de Migración	20, fr. IX	El Centro de Evaluación está obligado a implementar las medidas de seguridad necesarias para resguardar el contenido de las bases de datos que contengan la certificación de las personas a las que se les haya practicado.
Ley del Mercado de Valores	115, fr. III, inciso b.	El plan general de funcionamiento de las sociedades de las casas de bolsa contendrá las medidas con las que se preserve la integridad de la información.
	208	Obligar a las casas de bolsa a contar con los instrumentos necesarios para proteger los medios electrónicos o digitales en donde almacenen las comunicaciones con sus clientes.
	345	Obligar a los auditores externos a contar con los instrumentos necesarios para proteger la documentación, información y elementos con la que realicen su dictamen.
Ley de la Comisión Federal de Electricidad	12, fr. II y fr. XXI	Entre las funciones del Consejo de Administración se encuentra, entre otras, el establecimiento de directrices de seguridad sobre las actividades de la CFE, entre las que podrían considerarse la ciberseguridad; de igual manera, tiene la función de evaluar, entre otros, el sistema de seguridad.
	45, fr. IX	El Director General debe instrumentar y administrar los sistemas de seguridad de los bienes e instalaciones de la CFE y sus demás empresas, entre los cuales se puede considerar la ciberseguridad.
Ley de la Comisión Nacional Bancaria y de Valores	4, fr. XVI y 5, pr. 3	La Comisión tiene la facultad de investigar y de realizar visitas de inspección por las acciones de personas físicas o morales (que no sean parte del sistema financiero) que hagan suponer violaciones a la ley, dentro de las cuales podrían considerarse inspecciones a medios digitales.

Ordenamiento	Artículo(s)	Contenido
Ley de la Fiscalía General de la República	10, fr. VII	La Fiscalía General deberá establecer los medios de información por medio de los que dé cuenta de sus actividades, no obstante, reservará la información que pueda afectar la seguridad de las personas que intervengan en el proceso penal.
	40, fr. XIX	Los agentes del MP de la Federación tienen, entre otras, la facultad de acceder (conforme a la legislación aplicable) a la información, documentos, registros físicos y electrónicos en poder de las instituciones públicas y privadas.
	42, fr. XII	Los peritos tienen la facultad de proponer la participación del personal de servicios periciales en programas de intercambio de experiencias, conocimientos y avances tecnológicos con otros servicios periciales, procuradurías o fiscalías de otras entidades.
	31	Junto con el sistema institucional de evaluación de resultados se realizará la planeación, determinación y administración de los sistemas y recursos tecnológicos, estableciendo en un sistema de gobierno la información útil para la investigación, inteligencia, desarrollo de estrategias, tácticas y operativas y decisiones administrativas. Sobre esto último debe garantizarse la calidad de la información, así como la seguridad en su conservación y transmisión.

Fuente: Elaboración propia con base en la revisión de la normativa nacional.

Anexo 2. Ordenamientos jurídico-administrativos federales sobre ciberseguridad

Ordenamiento	Contenido
Acuerdo de Adscripción de las Unidades Administrativas del Banco de México, publicado el 31 de octubre de 2013.	• Establece la **Dirección de Ciberseguridad**, así como la Dirección de Seguridad y Organización de la Información, de la cual depende la Gerencia de Seguridad de Tecnologías de la Información y la **Subgerencia del Centro de Defensa de Ciberseguridad**.
Acuerdo por el que se da a conocer el Programa de Cobertura Social 2021-2022 de la Secretaría de Infraestructura, Comunicaciones y Transportes, publicado el 23 de diciembre de 2021.	• Reconoce que para lograr el máximo aprovechamiento de las oportunidades de la digitalización se necesita avanzar en: extender la conectividad, accesibilidad y calidad de las telecomunicaciones; **consolidar la ciberseguridad; adoptar nuevas tecnologías en el sector productivo; y ampliar los servicios del gobierno digital**.
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, publicado el 6 de septiembre de 2021.	• Define conceptos como: activo de información, activo de información esencial, amenaza, arquitectura tecnológica, autenticación electrónica, gobierno digital, incidente de seguridad de la información, plan de recuperación ante desastres, seguridad de la información, entre otros. • Establece **políticas tecnológicas** generales, regula los **procedimientos de contrataciones de tecnologías y seguridad de la información**, las políticas tecnológicas aplicables a los proyectos de TIC y seguridad de la información, aplicadas al correo electrónico, las aplicaciones de cómputo, las plataformas digitales, entre otros medios.
Acuerdo Secretarial Núm. 033 del 13/feb/2017 de la Secretaría de Marina.	• Crea la Unidad de Ciberseguridad (EMGA-UNICIBER), dependiente de la Jefatura del Estado Mayor General de la Armada, incluyendo las capacidades de Ciberseguridad y Ciberdefensa. • Su misión consiste en planear, conducir y ejecutar las actividades de **seguridad de la información, ciberseguridad y ciberdefensa para la protección de la infraestructura crítica de la Secretaría de Marina** - Armada de México y coadyuvar en el esfuerzo nacional para el mantenimiento de la integridad, estabilidad y permanencia del Estado mexicano.[244]

244 SECRETARÍA DE MARINA, *Unidad de Ciberseguridad*, (20 de mayo de 2022), https://www.gob.mx/semar/articulos/unidad-de-ciberseguridad-279197?idiom=es.

Ordenamiento	Contenido
Acuerdos del Consejo Nacional de Seguridad Pública, aprobados en su Cuadragésima Séptima Sesión Ordinaria, celebrada el 16 de diciembre de 2021, publicados el 29 de diciembre de 2021. Acuerdo 10/XLVII/21. Registro Nacional de Incidentes Cibernéticos.	• El Consejo Nacional de Seguridad Pública reconoce la **necesidad de contar con información actualizada en materia de delitos cibernéticos**, así como la planeación de estrategias que contribuyan a generar acciones que permitan la prevención y el combate a dichos eventos; por lo que acuerda la implementación del **Registro Nacional de Incidentes Cibernéticos** (RNIC) en las treinta y dos entidades federativas, a través de las secretarías de seguridad pública estatales en coordinación con la Unidad de Policía Cibernética, la Fiscalía General o en su caso la procuraduría general de la entidad federativa. • Las y los secretarios de seguridad pública estatales gestionarán su conectividad y usuario, con la finalidad de llevar a cabo la captura de todos los incidentes cibernéticos que se susciten en su estado.
Anexo 2 del Acuerdo 09/XLVII/21 del Consejo Nacional de Seguridad Pública: Acuerdo por el que se actualizan los lineamientos para la inscripción y baja en el sistema de administración de usuarios (SAU) del personal designado como responsable del control, suministro, intercambio, actualización y adecuado manejo de la información de las bases de datos del Sistema Nacional de Información (SNI) en seguridad pública, publicado el 20 de abril de 2022.	• Busca garantizar una administración centralizada y segura de los usuarios de los sistemas informáticos que utiliza el SNI. El Área de Administración de Usuarios (AAU) deberá bloquear las cuentas de usuario con actividad sospechosa (virus, conexión en sitios diferentes, duplicidad en la conexión, entre otras irregularidades similares), que pudieran significar una amenaza que comprometa la seguridad de la información e infraestructura del SNI.
Circular 4/2019 dirigida a las Instituciones de Crédito e Instituciones de Tecnología Financiera relativa a las Disposiciones de carácter general aplicables a las Instituciones de Crédito e Instituciones de Tecnología Financiera en las Operaciones que realicen con Activos Virtuales, publicada el 8 de marzo de 2019.	• La **solicitud de autorización para realizar operaciones** deberá ir acompañada de un **marco integral de riesgos** que identifique los riesgos asociados a la operación con **activos virtuales**, tomando en cuenta como mínimo los riesgos de negocio, cambiario, financiero, operativo y **de ciberseguridad**.
Estrategia Institucional para el Ciberespacio 2021-2024 de la Secretaría de Marina.	• Señala las **acciones prioritarias, acciones puntuales de seguridad en el ciberespacio**, líneas de acción específica y **organismos internos** participantes en materia de ciberseguridad.

Ordenamiento	Contenido
Lineamientos Generales para la operación del Expediente para Trámites y Servicios. Secretaría de Economía, publicados el 13 de julio de 2020.	• Define **ciberseguridad** como l*a aplicación de un proceso de análisis y gestión de riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información, así como con los sistemas y procesos usados para ello, que permite llegar a una situación de riesgo conocida y controlada*; API, expediente, metadatos, entre otros conceptos, y establece **un esquema de ciberseguridad** para los expedientes electrónicos.
Manual de Organización General de la Guardia Nacional, publicado el 16 de noviembre de 2021.	• Dirección General Científica: facultada para **aplicar estrategias contra la ciberdelincuencia**, e implementar las acciones de **vigilancia, identificación, monitoreo y rastreo en la red pública de internet**, con la finalidad de prevenir conductas delictivas. • Dirección General de Tecnologías de Información y Comunicaciones: le corresponde liderar el análisis e instrumentación de los sistemas, políticas y procedimientos, con el propósito de **mantener la seguridad, integridad, confidencialidad y disponibilidad de la información contenida en las bases de datos de la Guardia Nacional**.
Manual de Organización General de la Secretaría de Gobernación, publicado el 2 de junio de 2020.	• Reitera que la Dirección General de Tecnologías de la Información y Comunicaciones puede fungir como **enlace de la Secretaría con dependencias, entidades, instituciones y empresas nacionales e internacionales relacionadas con la informática y las telecomunicaciones, ciberseguridad, seguridad de la información**; participar en grupos de trabajo, comités o comisiones interinstitucionales, en materia de seguridad de la información, ciberseguridad, innovación.
Manual de Organización General de la Secretaría de la Defensa Nacional, publicado el 4 de julio de 2017.	• Precisa las atribuciones de la Dirección General de Informática, tales como establecer los lineamientos y estándares técnicos para el empleo del recurso humano e informático, tales como software, hardware, herramientas, infraestructura e insumos para el desarrollo de soluciones tecnológicas de la SEDENA, así como diseñar, proponer, y supervisar los planes de contingencia mediante un ciclo de mejora continua.
Manual de Organización General de la Secretaría de Marina, publicado el 23 de septiembre de 2021.	• Reitera que el Estado Mayor General de la Armada debe planear, conducir y ejecutar actividades de seguridad y ciberdefensa para la protección de la infraestructura crítica de la Secretaría y coadyuvar con las demás instituciones del Estado.
Manual de Organización General de la Secretaría de Seguridad y Protección Ciudadana, publicado el 4 de diciembre de 2020.	• Precisa que la Unidad de Información, Infraestructura Informática y Vinculación Tecnológica tiene como objetivo administrar los servicios que proporcionan la información contenida en las bases de datos, con la finalidad de facilitar su acceso y **se impulse el desarrollo de nuevas tecnologías y de ciberseguridad de interés de la secretaría**.

Ordenamiento	Contenido
Norma Mexicana NMX-I-62443-4-1-NYCE-2021: Electrónica-seguridad para los sistemas de automatización y control industrial-parte 4-1: requisitos del ciclo de vida del desarrollo seguro del producto, publicada el 21 de diciembre de 2021.	• Forma parte de una serie de normas que abordan la cuestión de la seguridad de los sistemas de automatización y control industrial (IACS, *Industrial Automation and Control Systems*, por sus siglas en inglés). • Describe los **requisitos del ciclo de vida del desarrollo de productos relacionados con la ciberseguridad para los productos destinados a su uso en el entorno de sistemas de control y automatización industrial**.
Programa Nacional de Protección de Niñas, Niños y Adolescentes 2021- 2024 de la Secretaría de Gobernación, publicado el 31 de diciembre de 2021.	• El punto 6.4 señala la relevancia del objetivo prioritario 4, referido a las Tecnologías de la Información y Comunicación y Brecha Digital, y reconoce que las TIC pueden generar situaciones de riesgo a la seguridad, integridad, privacidad y a la propia vida de las niñas, niños y adolescentes, por lo que *es indispensable que* ***el acceso a estas herramientas se acompañe de acciones en materia de ciberseguridad tanto a niñas, niños y adolescentes como a las personas cuidadoras****, con la finalidad de mantenerles informados y seguros en línea*. • La estrategia prioritaria 4.4 consiste en asegurar a las niñas, niños y adolescentes el acceso a las TIC mediante la reducción de la brecha digital, así como **fomentar la navegación segura en internet**. • La meta 4.4.3 consiste en **definir e implementar una estrategia de ciberseguridad dirigida a madres, padres, personas cuidadoras, niñas, niños y adolescentes**, para contribuir a la prevención de las violencias, reducir la brecha digital e **impulsar la navegación segura**.
Programa Sectorial de Defensa Nacional 2020-2024, publicado el 25 de junio de 2020.	• Estrategia prioritaria 5.6: Fortalecer las capacidades del **Centro de Operaciones del Ciberespacio** en contra de incidentes de ciberseguridad hacia la **infraestructura crítica de la Secretaría de la Defensa Nacional**.
Programa Sectorial de Marina 2020-2024, publicado el 3 de julio de 2020.	• Estrategia prioritaria 1.4: **fortalecer las capacidades de seguridad en el ciberespacio para coadyuvar con la seguridad nacional y seguridad interior**.
Programa Sectorial de Relaciones Exteriores 2020-2024, publicado el 2 de julio de 2020.	• Acción puntual 5.6.1: Participar activamente en los esfuerzos multilaterales para **prevenir y combatir las expresiones de la delincuencia organizada transnacional**, fundamentalmente el tráfico ilícito de armas, así como en el **seguimiento y atención del avance del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional**.
Programa Sectorial de Seguridad y Protección Ciudadana 2020-2024, publicado el 2 de julio de 2020.	• Estrategia prioritaria 4.2: implementar **procesos de gestión de riesgos** para la protección de los sistemas de información y telecomunicaciones de las plataformas tecnológicas que permitan a las instituciones de seguridad de los tres órdenes de gobierno **proteger la información ante la presencia de ciberataques**.

Ordenamiento	Contenido
Reglamento de la Ley de la Guardia Nacional, publicado el 29 de junio de 2019.	a) El Comandante puede (art. 19, fracciones XI, XII, XIII, XIV y XV): • Proponer los lineamientos para la obtención, procesamiento y aprovechamiento de la información que genere la institución a fin de establecer los **sistemas de información**. • Solicitar a la autoridad judicial la autorización para **requerir información a los concesionarios, permisionarios, operadoras telefónicas y comercializadoras de servicios de telecomunicaciones, de sistemas de comunicación vía satélite, así como la georreferenciación de los equipos de comunicación móvil en tiempo real**. • Solicitar a la autoridad judicial la autorización para la **intervención de comunicaciones privadas**. • Presenciar ante la autoridad judicial competente la **destrucción de la información** resultado de las intervenciones. • Autorizar **operaciones encubiertas** y de **usuarios simulados**. b) La Dirección General de Tecnologías de Información y Comunicaciones puede (art. 30, fracciones I, III, VIII, IX, XI, XII, XIII): • Analizar e instrumentar los sistemas, políticas y procedimientos que permitan garantizar la seguridad, integridad, **confidencialidad y disponibilidad de la información contenida en las bases de datos** de la institución. • Realizar las **auditorías de los sistemas informáticos** de la institución para asegurar que sean utilizados adecuadamente y verificar su **vigencia tecnológica**. • Proporcionar el **soporte técnico** en materia de **sistemas informáticos**, telecomunicaciones y de equipos tecnológicos. • Elaborar y ejecutar los programas de **mantenimiento del equipo de comunicaciones e informático**. • Dictaminar los **estudios de viabilidad** que presenten las unidades para la **adquisición de bienes y servicios informáticos y de telecomunicaciones**. c) La Dirección General de Inteligencia puede (artículo 33): • Establecer, coordinar y dirigir un **centro de inteligencia**. • Instrumentar, operar y resguardar las **bases de datos** de información de la institución. • Consolidar estrategias y mantener **vínculos de inteligencia y de cooperación** en materia de información sobre seguridad pública con organismos nacionales e internacionales. • Determinar métodos de **comunicación y redes de información policial** para el acopio de datos sobre las formas de organización y modos de operación de las organizaciones delincuenciales. d) La Dirección General de Investigación puede establecer y operar **métodos de comunicación y redes de información policial** para acopio y clasificación oportuna de los datos que requieran las unidades de la institución (artículo 34, fracción VI). e) La Dirección General Científica puede **vigilar, identificar, monitorear y rastrear la red pública de internet** para prevenir conductas delictivas (artículo 36, fracción XVI). f) Técnicas especiales de investigación para la prevención: **operaciones encubiertas** y **usuarios simulados**; **intervención de comunicaciones privadas** (artículos 245, 258 y 259).

Ordenamiento	Contenido
Reglamento Interior del Banco de México, modificaciones publicadas el 29 de diciembre de 2020.	• Precisa las atribuciones de la **Dirección de Ciberseguridad**, tales como: establecer políticas, lineamientos y estrategias institucionales para **fortalecer la ciberseguridad del Banco**; **representarlo en foros especializados** y ante otras autoridades en temas relacionados con **seguridad de la información, ciberseguridad y ciberresiliencia**; definir y administrar el **programa de ciberseguridad y ciberresiliencia del Banco**; **requerir información** en materia de seguridad de la información, ciberseguridad, ciberresiliencia e incidentes de ciberseguridad **a las entidades e intermediarios financieros** (artículo 29 bis).
Reglamento Interior de la Secretaría de Educación Pública, publicado el 15 de septiembre de 2020.	• El artículo 29, fracción XIII, faculta a la Dirección General de Tecnologías de la Información y Comunicaciones para fungir como **enlace de la SEP con instituciones y empresas nacionales e internacionales relacionadas con la informática, las comunicaciones y la ciberseguridad**.
Reglamento Interior de la Secretaría de Gobernación, publicado el 31 de mayo de 2019.	• La Dirección General de Tecnologías de la Información y Comunicaciones puede participar en **comités interinstitucionales de seguridad de la información, ciberseguridad** e innovación tecnológica, con dependencias, entidades, instituciones y empresas nacionales e internacionales relacionadas con **informática y telecomunicaciones**, **ciberseguridad y seguridad de la información**, para evaluar y emitir recomendaciones que contribuyan al aprovechamiento de las tecnologías de información y comunicaciones en la SEGOB.
Reglamento Interior de la Secretaría de la Defensa Nacional, publicado en el Diario Oficial de la Federación el 29 de diciembre de 2008, última reforma publicada el 15 de junio de 2016.	• Establece la Dirección General de Informática (art. 57), órgano técnico administrativo encargado de proporcionar información sistematizada en forma rápida, oportuna y confiable para apoyar la toma de decisiones de la SEDENA; y del abastecimiento, **mantenimiento y evacuación de los materiales informáticos**. Facultada para establecer y administrar la infraestructura de cómputo y la adecuada operación de los sistemas locales y remotos; establecer **normas y procedimientos para mantener la seguridad informática**; diseñar, proponer y supervisar la implementación de **planes de contingencias informáticas**, incluyendo la recuperación de la información.
Reglamento Interior de la Secretaría de Marina, publicado el 7 de junio de 2021.	• La persona titular de la Jefatura del Estado Mayor General de la Armada tiene la facultad para planear, **conducir y ejecutar actividades de seguridad y ciberdefensa para la protección de la infraestructura crítica de la Secretaría** y coadyuvar en el ámbito de su competencia con las demás instituciones del Estado (artículo 13, fracción XLII). • La Unidad de Inteligencia Naval es competente para identificar los riesgos y amenazas a la seguridad nacional (artículo 44).
Reglamento Interior de la Secretaría de Seguridad y Protección Ciudadana, publicado el 30 de abril de 2019.	• Su artículo 11 establece la Unidad de Información, Infraestructura Informática y Vinculación Tecnológica. Su artículo 12 establece la **Dirección General de Gestión de Servicios, Ciberseguridad y Desarrollo Tecnológico**, que tendrá, entre otras atribuciones: proponer, dar **solución y seguimiento a los incidentes en materia de ciberseguridad informática**.

Ordenamiento	Contenido
Reglamento que la Cámara de Diputados aplicará durante las situaciones de emergencia y la contingencia sanitaria en las sesiones ordinarias y extraordinarias durante la LXV Legislatura.	• Prevé la adopción de medidas de ciberseguridad para el uso de la plataforma digital que diputados y diputadas pueden utilizar para asistir y votar de manera telemática.
Resolución que modifica las disposiciones de carácter general aplicables a las instituciones de crédito; Secretaría de Hacienda y Crédito Público, publicada el 27 de noviembre de 2018.	• Define Incidente de Seguridad de la Información, Infraestructura Tecnológica¸ Plan Director de Seguridad, entre otros conceptos. • Obliga a mantener controles adecuados que garanticen la confidencialidad, integridad y disponibilidad de la información que procuren su seguridad tanto física como lógica. • Obliga a establecer controles para la identificación y resolución de actos o eventos que puedan generarle a la institución crediticia riesgos derivados de: o La comisión de hechos, actos u operaciones fraudulentas a través de medios tecnológicos. o El uso inadecuado por parte de los usuarios de la infraestructura tecnológica. • En caso de que se presente un Incidente de Seguridad de la Información, obliga a notificar a la Comisión Nacional Bancaria y de Valores (artículo 168 Bis 16).

Fuente: Elaboración propia con base en la búsqueda de la palabra *ciberseguridad* en el Diario Oficial de la Federación.


CÁMARA DE
DIPUTADOS
LXV LEGISLATURA


40 Aniversario
Investigación
Parlamentaria


CEDIP
CENTRO DE ESTUDIOS DE DERECHO
E INVESTIGACIONES PARLAMENTARIAS