MRCET

MAESTRÍA EN REGULACIÓN Y COMPETENCIA ECONÓMICA DE LAS TELECOMUNICACIONES

INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

“Análisis sobre el establecimiento de una Agencia Nacional de Ciberseguridad con base en las Recomendaciones de la Estrategia Nacional de Ciberseguridad”

(TIPO DE PROYECTO)
Que para obtener el grado de MAESTRO EN REGULACIÓN Y COMPETENCIA ECONÓMICA DE LAS TELECOMUNICACIONES

Presenta: Verónica Ávila Hernández

Asesor: Mtro. Iván Díaz González

Ciudad de México, febrero, 2022.

CONACYT

INFOTEC POSGRADOS

ift INSTITUTO FEDERAL DE TELECOMUNICACIONES

Autorización de impresión

INFOTEC
POSGRADOS

AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA

Maestría en Regulación y Competencia Económica de las Telecomunicaciones, MRCET

Ciudad de México, 08 de febrero de 2022
INFOTEC-DAIC-GCH-CSE-023/2022.

La Gerencia de Capital Humano / Gerencia de Investigación hacen constar que el trabajo de titulación intitulado

"Análisis sobre el establecimiento de una Agencia Nacional de Ciberseguridad con base en las Recomendaciones de la Estrategia Nacional de Ciberseguridad"

Desarrollado por la alumna: **Verónica Ávila Hernández** y bajo la asesoría del **Mtro. Iván Díaz González** cumple con el formato de Biblioteca. Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Asimismo, se hace constar que no debe material de la biblioteca de INFOTEC.

Vo. Bo.

Lic. Juan Ramón Abarca Damián
Coordinador de Biblioteca

Anexar a la presente autorización al inicio de la versión impresa del trabajo referido que ampara la misma.

C.p.p Servicios Escolares

Agradecimientos

A Dios por la vida y las oportunidades que me da para lograr mis metas.

A Pablo por su espera y la alegría que me transmite todos los días para continuar esforzándome a ser un ejemplo y una guía en su camino.

A mi madre, que de manera constante y sin reservas me apoya y me impulsa en el desarrollo profesional, laboral y personal. Gracias a mi hermana, esposo e hijo, por ayudarme sin condiciones, con amor y cariño.

A Rubén Fernando por su amistad incondicional, por acompañarme durante mis estudios de posgrado y por los desvelos que compartimos para concluir una etapa más juntos. Gracias a Sergio, Pedro Antonio, Zurisadai, Giovanni, Estefanía Soraya y demás amigos, quienes con su guía y apoyo me animan e inspiran.

A mis profesores y compañeros de clase, con quienes aprendí y compartí momentos de éxito.

Al Mtro. Iván Díaz y la Dra. Vanessa Díaz, por su orientación y seguimiento a la presente investigación, quienes me transmitieron sus conocimientos y su interés por la elaboración del presente trabajo.

Al Instituto Federal de Telecomunicaciones por la oportunidad que me otorgó para realizar un posgrado, así como a las personas que hacen posible la capacitación constante de los servidores públicos que laboran en dicho Órgano Autónomo.

A la Universidad Nacional Autónoma de México, mi alma mater, y al Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación, por encargarse de proporcionar las herramientas para el desarrollo de profesionistas competitivos.

Tabla de contenido

Tabla de contenido 3

Introducción 6

Capítulo 1. Conceptos fundamentales de Ciberseguridad y perspectiva internacional 10

1.1 Elementos de la Ciberseguridad 11

1.2 Protección de la información 12

1.3 Seguridad en sistemas 15

1.4 Control de Riesgo 19

1.5 Infraestructuras críticas 21

1.6 Perspectiva internacional sobre ciberseguridad 23

Capítulo 2. La Estrategia Nacional de Ciberseguridad 32

2.1 Introducción a la ENCS desde el ámbito internacional 32

2.2 Publicación de la ENCS 35

2.3 Ejes de la ENCS 37

2.4 Perspectiva del marco institucional de la ENCS 42

Capítulo 3. La regulación de la ciberseguridad en las telecomunicaciones 46

3.1 Ciberseguridad en infraestructuras y sistemas de telecomunicaciones 49

3.2 La seguridad en los servicios de telecomunicaciones y la información 50

3.3 Participación de instituciones públicas en el ámbito de la ciberseguridad de telecomunicaciones 52

3.4 Participación de instituciones privadas en el ámbito de la ciberseguridad de telecomunicaciones 57

Capítulo 4. Propuesta de una Agencia Nacional de Ciberseguridad 63

4.1 Consideraciones sobre una agencia nacional de ciberseguridad 65

4.2 Forma de organización 70

4.3 Marco legal aplicable 71

4.3.1 Órgano de decisión 71

4.3.2 Autonomía administrativa 72

4.3.3 Organigrama 73

4.3.4 Capacidad regulatoria 74

4.3.5 Cooperación **74**
4.3.6 Gestión de riesgos **75**
4.3.7 Ámbito de atribuciones **75**
4.3.8 Supervisión y Sanción .....¡Error! Marcador no definido.
4.3.9 Rendición de cuentas **76**

Conclusiones **79**

Bibliografía **83**

Siglas y abreviaturas

CERT	Equipo de Respuesta ante Emergencias de Cómputo
CIDGE	Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico
CNBV	Comisión Nacional Bancaria y de Valores
CPEUM	Constitución Política de los Estados Unidos Mexicanos
DOF	Diario Oficial de la Federación
ENCS	Estrategia Nacional de Ciberseguridad
ENISA	Agencia de Seguridad de las Redes de la Información de la Unión Europea
IFT	Instituto Federal de Telecomunicaciones
IMC	Índice Mundial de Ciberseguridad
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
NIST	Instituto Nacional de Estándares y Tecnología
OEA	Organización de los Estados Americanos
PND	Plan Nacional de Desarrollo
PSN	Programa para la Seguridad Nacional
SCT	Secretaría de Comunicaciones y Transportes
SE	Secretaría de Economía
SEDENA	Secretaría de la Defensa Nacional
SEGOB	Secretaría de Gobernación
SEMAR	Secretaría de la Marina
SHCP	Secretaría de Hacienda y Crédito Público
SRE	Secretaría de Relaciones Exteriores
TI	Tecnología de Información
TIC	Tecnologías de la Información y la Comunicación
UE	Unión Europea
UIT	Unión Internacional de Telecomunicaciones

Introducción

La inclusión de los medios digitales en cada actividad de la vida cotidiana, el enfoque de derechos humanos hacia aspectos estrechamente ligados a las telecomunicaciones, el potencial para fines bélicos del espacio digital, además de la innovación e interdependencia hacia las tecnologías que en recientes meses se han acrecentado, son factores que obligan a que la ciberseguridad sea abordada desde una perspectiva de esfuerzos conjuntos entre áreas técnicas, políticas, administrativas, por destacar algunas.

Precisamente, la tecnología ha forzado a que diversas disciplinas converjan en los mismos objetivos, tales como: el acceso digital, la conectividad, la resiliencia, la justicia penal, la diplomacia, la seguridad y defensa dentro y fuera del país, la economía y el comercio e, inclusive, aquellas tecnologías emergentes. Es así como la ciberseguridad está adquiriendo enfoques de todos los involucrados en el ambiente digital, lo que ha conducido a los gobiernos para poner en marcha o adoptar legislación nacional respecto de la ciberseguridad, sobre todo aquellos Estados cuyo desarrollo no contemplaba un marco regulatorio o no se encontraba actualizado.

En ese orden de ideas, la revisión a la normatividad aplicable a la materia debe ser analizada para su reestructuración o actualización con base en los nuevos retos que el ciberespacio conlleva. En el caso en particular de México, actualmente se tiene legislación encaminada a la protección del ciberespacio, así como una Estrategia Nacional de Ciberseguridad. Sin embargo, las acciones concretas han sido escasas hasta ahora, puesto que no existe un ordenamiento cuyo tema central sea la ciberseguridad y dicha estrategia no fue desarrollada de la manera prevista.

En 2017, en la Estrategia Nacional de Ciberseguridad se estableció la Subcomisión de Ciberseguridad para su adopción, cuyas atribuciones quedaron truncadas con el cambio de gobierno en 2018, dadas las características de su creación y diseño en su estructura, traduciéndose esto en un freno a la gestión en la política de ciberseguridad.

Sobre esto último, diversos entes han planteado la posibilidad de la creación de una agencia nacional de ciberseguridad que se enfoque en el desarrollo,

coordinación e implementación de la estrategia nacional en la materia, además de desarrollar protocolos, marcos operativos y responsabilidades para la ciber-resiliencia y gestionar su cumplimiento. No obstante, ¿requiere el Estado mexicano de una agencia reguladora independiente para abordar la problemática de ciberseguridad y la ciber-resiliencia en el ámbito de las telecomunicaciones?

Al respecto, se plantea la hipótesis de que la escasa autonomía y unificación de funciones legales conferidas a la Subcomisión de Ciberseguridad influyen en la falta de coordinación entre los diversos sectores para abordar los temas de ciberseguridad en México, incluidos los fines para los cuales fue creada.

El presente trabajo tiene como objetivo principal analizar las acciones del Estado mexicano en materia de ciberseguridad en las telecomunicaciones e identificar cuáles son los elementos que denotan y concluyen en la necesidad de la creación de una agencia nacional de ciberseguridad, así como las características mínimas que, en su caso, debería contemplar dicha agencia.

En seguimiento a lo anterior, el primer capítulo está encaminado a resaltar los elementos de la ciberseguridad y la perspectiva internacional que se tienen respecto de la materia, haciendo énfasis en las aportaciones de diversas organizaciones y países centrados en políticas del ciberespacio.

Por lo que respecta al segundo capítulo, éste tiene un enfocado de revisión a la Estrategia Nacional de Ciberseguridad, los elementos que influyeron para su publicación y los aspectos principales que aborda. Asimismo, en dicho apartado se estudia la creación de la Subcomisión de Ciberseguridad.

El tercer capítulo señala la regulación de ciberseguridad en las telecomunicaciones desde la parte lógica y física, introduciendo aquellos elementos que deben ser observados en el aspecto legal del entorno digital. Además, este capítulo destaca la participación de los diversos sectores en el contexto de ciberseguridad.

Finalmente, por lo que respecta al cuarto capítulo, se plantean las características mínimas que debería tener un órgano encargado de determinar el marco legal aplicable en aspectos de seguridad digital en las telecomunicaciones, proporcionar los vínculos entre los sectores involucrados y generar en éstos el

sentido de responsabilidad conjunta correspondiente con sus intereses particulares y los intereses de la nación.

Capítulo 1. Conceptos fundamentales de ciberseguridad y perspectiva internacional

Capítulo 1. Conceptos fundamentales de ciberseguridad y perspectiva internacional

Para entender el entorno digital, es necesario adentrarse a sus características, así como a los conceptos que frecuentemente son utilizados para definir los elementos que lo conforman. Esto, con el objetivo de plantear de manera clara las particularidades del ciberespacio y partir de éstas para implementar políticas específicas y útiles a la materia.

En otro orden de ideas, la frecuencia con que se utilizan los dispositivos y las herramientas tecnológicas, así como la relevancia que tienen éstos en nuestra vida cotidiana debe ser uno de los diversos factores a considerar al momento de plantear la implicación de la seguridad de la información y de los dispositivos, para contrarrestar las acciones mal intencionadas que se ejecutan en beneficios de unos cuantos, las cuales afectan desde lo individual hasta lo global, siendo el desconocimiento de los elementos fundamentales para la ciberseguridad uno de los riesgos que comúnmente proviene de quienes hacen uso de dispositivos y herramientas tecnológicas.

En esa tesitura, las naciones requieren de herramientas, organizaciones y estructuras de ciberseguridad que garanticen una defensa estratégica preventiva y reactiva con la colaboración de los involucrados, quienes deben tener responsabilidades y atribuciones para actuar con base en los principios y objetivos diseñados por cada gobierno.

Además de una estrategia nacional de ciberseguridad, que enmarca las prioridades del gobierno, el sector privado y la sociedad en dicho ámbito y establece las iniciativas técnicas, de procesos, de política y de regulación que requieren implementar los entes públicos para cubrir sus objetivos, así como la mecánica de su implementación y gestión, el gobierno debe garantizar que las políticas y regulaciones relacionadas con la información y la tecnología existentes, fijen las obligaciones del Estado, la sociedad y las instituciones privadas en la ejecución de

dicha estrategia, asegurando también la protección a la privacidad y la información de forma holística[1].

1.1 Elementos de la ciberseguridad

El planteamiento de políticas relacionadas con la materia que nos ocupa debe contemplar la gestión de riesgos, lo que conlleva una aproximación racional y proporcionada a la ciberseguridad, e impulsar el uso de herramientas técnicas adecuadas para tales fines, tomando en cuenta la ciber-resiliencia, cuyo concepto se define como "*la capacidad de los sectores público, privado y de la sociedad para mantenerse seguros de forma sostenida en el tiempo, para tomar decisiones inmediatas con información veraz y para recuperarse rápidamente de vulneraciones sufridas*"[2].

La protección que implica la ciberseguridad se basa en los siguientes puntos a destacar: la información, la infraestructura, los servicios y las personas que acceden al ciberespacio(UIT, 2007, citado por García, 2019). En relación con esto, la UIT ha establecido que tales aspectos deben ser considerados para salvaguardar su integridad tomando en cuenta los siguientes elementos:

Tabla 1. *Elementos fundamentales de la ciberseguridad*

Capacidad de un sistema para:	Objetivos de la seguridad	Medios de seguridad
Poder utilizarse	• Disponibilidad • Perdurabilidad • Continuidad • Confianza	• Dimensionamiento • Redundancia • Procedimientos de explotación y de copia de seguridad
Ejecutar acciones	• Seguridad de funcionamiento • Fiabilidad • Perdurabilidad • Continuidad • Exactitud	• Concepción • Prestaciones • Ergonomía • Calidad de servicio • Mantenimiento operacional
Permitir el acceso de entidades autorizadas (ningún acceso ilícito)	• Confidencialidad (preservación del secreto) • Integridad (ninguna modificación)	• Control de acceso • Autentificación • Control de errores • Control de coherencia • Encriptación

[1] Abusaid, D., Cristofori, A., Fernández, R. & Waisser, S. (2018) *Perspectiva de ciberseguridad en México». COMEXI y McKinsey & Company*. https://consejomexicano.org/multimedia/1528987628-817.pdf.

[2] González, J. M., Albornoz, M. M., & Ramírez, M. S. M. (2019, abril). Ciberseguridad Nacional. Periódica, LIV(148). https://www.inap.mx/portal/images/pdf/rap148.pdf.

Demostrar las acciones	• No rechazo • Autenticidad (ninguna duda) • Ninguna contestación	• Certificación • Grabación, rastreo • Firma electrónica • Mecanismos de prueba

Fuente: "*Ciberseguridad ¿Por qué es importante para todos?*", Arreola, A., 2019, México: Siglo XXI Editores México.

De lo anterior se desprende que los objetivos de la seguridad están encaminados para que un sistema sea útil, efectúe las acciones para las cuales está diseñado dando el acceso exclusivo a quienes incumba y que produzca los resultados esperados. Cabe mencionar que dichos objetivos son aplicables a sistemas, lo cual abarca desde un dispositivo personal hasta una red integral.

Los organismos públicos tienen acceso a información sensible de la sociedad en general, así como acceso a infraestructura crítica[3] del país para el cumplimiento de sus fines. Lo anterior, genera situaciones de riesgo y vulnerabilidades en el sector público que pueden afectar a los particulares, perjudicando la integridad de la información, la infraestructura utilizada por el Estado y la confiabilidad de los entes públicos.

En ese sentido, el gobierno tiene la responsabilidad de garantizar la protección de la información de los ciudadanos, enfrentar los riesgos y contrarrestar los ataques a la infraestructura que posee y opera, y asegurar la integridad de las instituciones públicas a efecto de mantener la confianza respecto de la gestión de procesos y de gobernabilidad.

1.2 Protección de la información

La generación, uso, almacenamiento, envío, recuperación y disposición final de la información tiene como base principal procesos y tecnologías que dependen de un alto nivel de confiabilidad para el logro de objetivos específicos, lo cual está estrechamente relacionado con la seguridad de la información, misma que emana de buenas prácticas y esquemas normativos que proporcionan una guía.

[3] Infraestructura crítica: "…*el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones*". Unión Europea. (julio 2016). *Directiva (UE) 2016/1148 del Parlamento Europeo del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión*. Diario Oficial de la Unión Europea L 194.

Al introducir el concepto de seguridad de la información queda de manifiesto que se pretende conservar su confidencialidad de accesos no autorizados, impedir alteraciones indebidas que pongan en riesgo la integridad de la información y se asegure la disponibilidad de ésta, para lo cual, la seguridad de la información se basa en los siguientes principios[4]:

i. Confidencialidad. Se refiere a la accesibilidad exclusiva de quienes están autorizados para conocer la información, cuyo objetivo es evitar que ésta sea divulgada sin los permisos respectivos y bajo condiciones específicas.

ii. Integridad. Este principio le da la característica a la información de ser precisa, oportuna, completa y coherente, mismas que no pueden ser preservadas por una máquina, por lo que se definen dos aspectos, para tales efectos: la integridad de los datos y la integridad del sistema.

   La integridad de los datos versa sobre la alteración de la información y los programas es exclusiva de las personas autorizadas para tal efecto.

iii. Disponibilidad. El concepto de disponibilidad está dirigido a garantizar que la información proporcionada por un sistema sea de manera eficaz y siempre se tenga accesibilidad a la misma, siendo una persona autorizada para dicho acceso.

iv. Autentificación. Es la acción de identificar a la entidad que genera la información. En la recepción de un mensaje, el sistema debe asegurarse que lo recibe de quien lo ha mandado, y no otra persona que haya suplantado la identidad del emisor.

v. No repudio. No debe darse la negación del servicio por parte del origen ni el destinatario de un mensaje. Es decir, el no repudio evita que se niegue la transmisión de un mensaje por parte del transmisor o el receptor.

El primer principio antes mencionado ha sido causa de grandes controversias puesto que trastoca, entre otros, los derechos humanos fundamentales de la privacidad y la libertad de expresión, así como diversos aspectos éticos. Asimismo,

---

[4] Díaz, P. & Reyes, A. (2015). *Buenas prácticas de seguridad alineadas al ISO/IEC 27002 para el aseguramiento de equipos Linux-Debian pertenecientes a un CERT*. UNAM. http://132.248.9.195/ptd2015/mayo/0729528/0729528.pdf

este principio se relaciona de manera estrecha con la confianza y el manejo adecuado de la información por cada usuario, quienes son los más vulnerables en los sistemas informáticos.

La protección de la intimidad y la confidencialidad de la información se ha convertido en uno de los retos a superar para los gobiernos, los cuales han hecho frente a los mismos a través de diversos mecanismos como son: educación sobre el ciberespacio y sus riesgos, campañas de concientización sobre lo que no se debe compartir en las redes, marcos normativos e instituciones que amparan y protegen la confidencialidad de las comunicaciones, así como el tratamiento de datos personales.

En relación con esto último, y por lo que respecta a las acciones realizadas por el gobierno de México para salvaguardar los derechos relacionados al tratamiento de datos personales de los ciudadanos por parte del Estado, fue hasta la aprobación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicada en el DOF el 11 de junio de 2002 que se crea el Instituto Federal de Acceso a la Información y es el primer ordenamiento que contempla los principios generales para el tratamiento de datos personales en posesión del sector público.

Posteriormente, se llevaron a cabo dos reformas a la CPEUM, los días 30 de abril y 1 de junio de 2009, por las que la protección de datos personales pasa a ser un derecho fundamental y, después, se reconoce como garantía, respectivamente.

Después, el 5 de mayo de 2015 se publicó en el DOF la Ley General de Transparencia y Acceso a la Información Pública, mediante la cual el INAI. Actualmente, el INAI es un órgano constitucional que cuenta con autonomía operativa, presupuestaria y de decisión, pertenece a la administración pública federal y se encarga de promover y difundir el ejercicio del derecho a la información; resolver sobre la negativa a las solicitudes de acceso a la información y proteger los datos personales en poder de las dependencias y entidades[5].

[5] Artículo 33 de la Ley Federal de Transparencia y Acceso a la Información Pública. http://www.inea.gob.mx/transparencia/pdf/LFTAIPG.pdf.

Asimismo, la CPEUM brindó a dicho órgano la competencia para conocer de los asuntos relacionados con el acceso a la información pública y la protección de datos personales de cualquier autoridad, entidad, órgano u organismo que forme parte de alguno de los Poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicatos que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal; con excepción de aquellos asuntos jurisdiccionales que correspondan a la Suprema Corte de Justicia de la Nación[6]. Adicionalmente, este organismo debe conocer de los recursos que interponen los particulares respecto de las resoluciones de los organismos autónomos especializados de las entidades federativas que determinen la reserva, confidencialidad, inexistencia o negativa de la información, de conformidad con la Ley General de Transparencia y Acceso a la Información Pública[7].

1.3 Seguridad en sistemas

Ahora bien, como se mencionó anteriormente, las actuaciones para preservar la seguridad en el ciberespacio son preventivas y reactivas, es decir, por un lado, es importante prepararse a posibles ataques y evitar descuidos que debiliten esa preparación, además de dar atención a las amenazas que se producen diariamente. En relación con la prevención, diversas entidades han diseñado esquemas que guían a los sectores implicados para evaluar riesgos y analizar amenazas y vulnerabilidades, a efecto de crear un entorno seguro en sus sistemas.

Sobre esto último, el Instituto Nacional de Estándares y Tecnología (*NIST*, por sus siglas en inglés) elaboró la NIST-SP-800-35 denominada "*Guide to Information Technology Security Servicies*" [Guía de Servicios de Seguridad de Tecnología de la Información], con una orientación aplicada a las agencias gubernamentales, a efecto de guiar la administración, implementación y selección de los servicios de seguridad de TI con base en el ciclo de vida de ésta. El objetivo

---

[6] Artículo 6 de la Constitución Política de los Estados Unidos Mexicanos. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf.

[7] Artículo 41 de la Ley Federal de Transparencia y Acceso a la Información Pública. http://www.inea.gob.mx/transparencia/pdf/LFTAIPG.pdf.

que emana del citado documento es colaborar con quienes están a cargo de la gestión respecto de la administración y la implementación de los servicios de seguridad, para que tomen decisiones adecuadas a fin de satisfacer las necesidades de la organización[8].

En ese orden de ideas, el documento antes mencionado alude a la existencia de seis fases del ciclo de vida de la seguridad de la TI, mismas que se indican a continuación:

Figura 1. *Fases del ciclo de vida de la seguridad de la TI*

Fuente: Elaboración propia con información de la NIST-SP-800-35

Este ciclo de vida inicia con la determinación de si se requiere de la implementación de un servicio de seguridad de la TI para generar beneficios a la organización y sus procesos. La segunda y tercera fase consiste en valorar el entorno en el que será aplicado el servicio de que se trate y las posibles soluciones del servicio, respectivamente. La cuarta fase se refiere a la selección de una solución por parte de la organización, así como la inclusión del equipo que se encargará de desarrollar la disposición respectiva del servicio y su implementación. Posteriormente, se ejecuta un monitoreo constante con las mejoras a que haya lugar asegurando así el funcionamiento óptimo del servicio como parte de la sexta fase y,

[8] Grance, T, Hash, J., Stevens, M., O'Neal, K. & Bartol, N. (2003). *Guide to Information Technology Security Services*. 0 ed. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-35.

en la última fase, hay una transición en la que el servicio se interrumpe o finaliza, de acuerdo con las necesidades de la organización.

En cada una de las fases antes mencionadas existen diversos actores que participan en función al tipo de servicio, de organización y de las disposiciones diseñadas para dicho servicio, por lo que los roles y las responsabilidades pueden variar de conformidad con lo señalado anteriormente.

Por otro lado, el desarrollo de la tecnología tiende a requerir de actualizaciones en los servicios de seguridad que se implementan, incluso genera nuevos servicios y, tomando en cuenta que las políticas abarcan un ámbito genérico, las organizaciones deben desarrollar estándares y programas con procedimientos que brinden claridad en la ejecución de soluciones de seguridad.

A efecto de proporcionar servicios de seguridad, se han establecido CERT, que son grupos de especialistas en tecnología que brindan servicios de respuesta y gestión de seguridad ante problemas cibernéticos en dispositivos y herramientas tecnológicas, por lo que también se denomina Equipo de Respuesta a Incidentes Informáticos[9].

El origen de los CERT se remonta a la década de los 80's derivado de la propagación del gusano Morris en diversos sistemas a nivel mundial, con lo que se produjo una reacción por parte de los especialistas y administradores de sistemas TI, quienes advirtieron la necesidad de coordinación y estructura de resiliencia a incidentes cibernéticos, creando para tales efectos el primer *CERT Coordination Center* a cargo de la Agencia de Proyectos de Investigación Avanzada de Defensa (*DARPA,* por sus siglas en inglés)[10].

En lo sucesivo, los CERT fueron implementándose hasta extenderse a nivel mundial, con características variadas, según las necesidades de cada nación, y para

---

[9] Existen diversas denominaciones para los CERT en función del nombre que adoptan por país mencionando de forma enunciativa más no limitativa las siguientes: CERT or CERT/CC (Computer Emergency Response Team / Coordination Center), CSIRT (Computer Security Incident Response Team), IRT (Incident Response Team), CIRT (Computer Incident Response Team), SERT (Security Emergency Response Team). Bronk, H. Thorbruegge, M. & Hakkaja, M. (2006). *CSIRT Setting up Guide in English*. Report/Study. https://www.enisa.europa.eu/publications/csirt-setting-up-guide.

[10] Riquelme, R. (2020). *¿Qué dice la ley de ciberseguridad propuesta por Miguel Ángel Mancera?. El Economista*, sec. Tecnología. https://www.eleconomista.com.mx/tecnologia/Que-dice-la-ley-de-ciberseguridad-propuesta-por-el-senador-Mancera-20200917-0046.html.

dar respuesta a los ataques y amenazas del entorno digital de forma proactiva y reactiva. Asimismo, a fin de disminuir el número de incidentes, los CERT brindan servicios educacionales, emiten alarmas en situaciones de vulnerabilidad tanto en hardware como en software e informan a los usuarios sobre la detección de virus o alguna otra amenaza que se presente.

El costo que representan los incidentes cibernéticos es muy alto, por lo que dar una atención pronta y eficaz a los ataques es indispensable. En ese sentido, los CERT tienen la capacidad y competencia para detectar y atender las irrupciones en el ciberespacio, además de que colaboran para subsanar las afectaciones producidas por dichos incidentes.

Al respecto, cada vez son más las funciones y servicios atribuidos a un CERT y la creación de éstos está enfocada a sectores específicos como gubernamental, académico, comercial, militar, entre otros. Derivado de lo anterior, los servicios que proporcionan los CERT se determinan por el sector al que están dirigidos.

En el caso de México, existen diversos CERT que atienden entornos específicos como el CERT UNAM y CERT UACH en el ámbito académico, el CERT MX del sector gubernamental, así como algunos constituidos por empresas privadas que proporcionan soluciones variadas a sus clientes, por ejemplo, IQSec CERT, CERTDSI Totalsec, Global Cybersec, SCITUM-CERT.

En relación con lo anterior y respecto de las acciones efectuadas por el estado mexicano, destaca que la Dirección General Científica de la Guardia Nacional está a cargo del CERT MX el cual vigila la integridad de la infraestructura tecnológica estratégica de la nación. Para tal efecto, este Centro lleva a cabo acciones de prevención e investigación respecto de conductas ilícitas por medios informáticos, monitorea la red pública de Internet a fin de identificar conductas constitutivas de delito, además realiza actividades de investigación en el ciberespacio y de ciberseguridad en la mitigación de riesgos de amenazas y ataques cibernéticos[11].

---

[11] Policía Federal. (2018). *Centro Nacional de Respuesta a Incidentes Cibernéticos de la Policía Federal*. gob.mx. http://www.gob.mx/policiafederal/articulos/centro-nacional-de-respuesta-a-incidentes-ciberneticos-de-la-policia-federal?idiom=es.

1.4 Control de riesgo

Así como es importante desarrollar servicios que garanticen la seguridad de los sistemas por parte de las entidades de gobierno, se requiere la colaboración de los que hacen uso de tales sistemas, quienes deben tomar sus propias medidas para enfrentar amenazas y riesgos en el entorno digital en el que se desenvuelven.

En ese sentido, han sido desarrollados métodos de análisis eficaces para facilitar la labor de contrarrestar los ataques en el ciberespacio. Al respecto destaca la norma NIST SP 800-30 denominada "*Guide for Conducting Risk Assessments*" [Guía para la Conducción de Evaluación de Riesgos], emitida por el NIST, cuyo enfoque se relaciona con la metodología para análisis de riesgos en los sistemas informáticos.

En relación con lo anterior, la norma antes referida define a los riesgos como la medida del grado de la amenaza que enfrenta una entidad ya sea por el impacto que implicaría si un evento ocurre o por la probabilidad de que suceda éste. Es así que, los riesgos de seguridad informática son aquellos que se derivan de la pérdida de los principios de la información y reflejan los posibles impactos adversos en las operaciones de una entidad.

Asimismo, la citada norma establece que los niveles de riesgo pueden ser determinados a través de factores, siendo los principales los siguientes: amenaza, vulnerabilidad, impacto, probabilidad y condición predisponente.

En ese orden de ideas, una amenaza es cualquier circunstancia o evento que puede tener un impacto negativo en una entidad por motivos de acceso no autorizado a la información, divulgación, destrucción y/o denegación del servicio, de conformidad con lo señalado por la NIST-SP-800-30.

Por lo que respecta a la vulnerabilidad, la norma en comento aborda este concepto como una debilidad de un sistema informático ante las amenazas. Las vulnerabilidades están relacionadas con los controles que no han sido aplicados a los sistemas, o bien, después de ser implementados conservan una debilidad.

La probabilidad, por su parte, es uno de los factores de riesgo que se basa en el análisis de la expectativa de que una determinada amenaza sea capaz de

aprovechar una vulnerabilidad en específico. Mientras que, el impacto, se refiere al nivel de daño que se puede esperar como resultado de un evento no deseado.

Cabe mencionar que los modelos para la evaluación de riesgos van en función del enfoque que cada organización establece, además de las necesidades a cubrir, por lo que dichos modelos son específicos y sus alcances definen las bases para generar un sistema de seguridad para esa entidad en particular.

En seguimiento a lo anterior, la Directiva NIS[12] destaca que los operadores de servicios esenciales, tales como bancos, empresas de telecomunicaciones, empresas suministradoras de energía, entre otros, deben informar al Estado cuando sean afectados por incidentes graves de seguridad en los sistemas informáticos, así como realizar planes de evaluación de riesgos que permitan identificar esos riesgos. En ese sentido, se requiere promover y desarrollar una cultura de gestión de riesgos, que involucren evaluación de riesgos e implementación de medidas de seguridad equivalentes a los riesgos enfrentados, por medio de reglamentación adecuada y prácticas voluntarias de la industria[13].

Al respecto, si bien el estado mexicano no cuenta con una ley aprobada respecto del delito cibernético, desde el 17 de mayo de 1999 se reformó el Código Penal Federal en el que se adicionó un capítulo denominado "*Acceso ilícito a sistemas y equipos de informática*", que comprende los artículos 140 bis, 211 bis 1 al 211 bis 7, 244, 245, 246 y 247, los cuales prevén el delito informático[14]. Asimismo, a principios de septiembre de 2020, se presentó una iniciativa de ley para regular la seguridad del espacio cibernético en México. Para tal efecto, se propuso modificar el Código Penal Federal y la Ley General del Sistema Nacional de Ciberseguridad,

---

[12] La Directiva NIS para la seguridad de redes y sistemas de información, fue adoptada por la Unión Europea para legislar en materia de ciberseguridad dentro de los países miembros. Es una iniciativa que proporciona las medidas legales para incrementar el nivel de ciberseguridad y podría ser seguida en otras regiones del mundo.

[13] Banco Interamericano de Desarrollo, y Organización de los Estados Americanos. (2020). *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe*. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

[14] Llamas, J. (septiembre, 2020). *Observaciones y estudio de la iniciativa que expide la Ley General de Ciberseguridad en México*. Foro Jurídico (blog). https://forojuridico.mx/observaciones-y-estudio-de-la-iniciativa-que-expide-la-ley-general-de-ciberseguridad-en-mexico/.

con la finalidad de que los delitos cibernéticos sean normados y sancionados por una Ley General de ciberseguridad[15].

1.5 Infraestructuras críticas

Cuando se habla de infraestructura crítica, se hace referencia al conjunto de activos tecnológicos imprescindibles que interactúan entre sí a fin de proporcionar servicios indispensables a las personas. Tales activos pueden ser instalaciones físicas o virtuales, redes de datos, redes industriales, sistemas de información, bases de datos, sistemas de control industrial, procesos automatizados o cualquier componente tecnológico que permita la provisión o seguimiento de un servicio esencial para el bien común y el sostenimiento económico de una nación[16].

La realidad es que los activos no están exentos de sufrir un incidente de ciberseguridad debido al importante número de amenazas que existen en el ciberespacio. El impacto de un incidente puede afectar a diferentes sectores de un país como, por ejemplo, el de la salud, la administración pública, el financiero, el de las telecomunicaciones o los proveedores de energía, entre otros[17].

En este contexto se debe tener en cuenta que los servicios vitales o críticos de un país están respaldados por infraestructuras críticas y que estas infraestructuras críticas están formadas por activos críticos que deben ser protegidos. Las infraestructuras críticas pueden clasificarse de la siguiente manera, de acuerdo con su prestación[18]:

i. De servicio. Las infraestructuras críticas de servicio proveen servicios vitales a un país y para ellas, la disponibilidad constituye la condición especial. La falta de disponibilidad genera un gran impacto en los ciudadanos. Las mayores amenazas que tienen este tipo de infraestructuras son: los ataques de denegación de servicio distribuidos y

---

[15] Riquelme, R. (2020). *¿Qué dice la ley de ciberseguridad propuesta por Miguel Ángel Mancera?. El Economista*, sec. Tecnología. https://www.eleconomista.com.mx/tecnologia/Que-dice-la-ley-de-ciberseguridad-propuesta-por-el-senador-Mancera-20200917-0046.html.

[16] Aguirre, A. (2017). *Ciberseguridad en Infraestructuras Críticas de Información*. Universidad de Buenos Aires. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1115_AguirrePonceAA.pdf.

[17] Aguirre, A. (2017). *Ciberseguridad en Infraestructuras Críticas de Información*. Universidad de Buenos Aires. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1115_AguirrePonceAA.pdf.

[18] Aguirre, A. (2017). *Ciberseguridad en Infraestructuras Críticas de Información*. Universidad de Buenos Aires. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1115_AguirrePonceAA.pdf.

el *malware* que tiene por objetivo alterar el funcionamiento de los sistemas principales[19].

ii. De información. Las infraestructuras críticas de información almacenan, procesan o transfieren información de tipo confidencial o sensible para su propietario. El propietario de la información puede ser una organización proveedora de servicios vitales, instituciones públicas o privadas o un ciudadano. La información es el activo crítico de estas infraestructuras, por lo tanto, se debe garantizar su confidencialidad, integridad y disponibilidad. Las mayores amenazas que tienen estas infraestructuras son: fraudes, robo de información confidencial y malware dedicado a secuestrar información sensible[20].

La adopción de nuevas tecnologías sin considerar los debidos controles de ciberseguridad en las infraestructuras críticas genera potencialmente nuevos vectores de amenazas, especialmente en los ambientes industriales porque se conectan redes seguras con entornos no seguros como Internet. Las amenazas buscan aprovechar una debilidad o ausencia de controles en los sistemas para explotar una vulnerabilidad[21].

La ciberseguridad aplicada en las infraestructuras críticas permite reducir los riesgos sobre los activos críticos de una nación, mediante la aplicación de políticas, normas, procedimientos, herramientas y/o buenas prácticas de seguridad en el ciberespacio [22].

En ese sentido, es necesario trabajar sobre el campo de la ciberseguridad para minimizar los riesgos a los que se exponen las infraestructuras críticas. Los gobiernos deben promover la creación de una estrategia de ciberseguridad para

---

[19] Aguirre, A. (2017). *Ciberseguridad en Infraestructuras Críticas de Información*. Universidad de Buenos Aires. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1115_AguirrePonceAA.pdf.
[20] Aguirre, A. (2017). *Ciberseguridad en Infraestructuras Críticas de Información*. Universidad de Buenos Aires. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1115_AguirrePonceAA.pdf.
[21] Aguirre, A. (2017). *Ciberseguridad en Infraestructuras Críticas de Información*. Universidad de Buenos Aires. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1115_AguirrePonceAA.pdf.
[22] Aguirre, A. (2017). *Ciberseguridad en Infraestructuras Críticas de Información*. Universidad de Buenos Aires. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1115_AguirrePonceAA.pdf.

proteger la información y los servicios vitales de un país, y reconocer la importancia de la protección de las infraestructuras críticas de información[23].

1.6 Perspectiva internacional sobre ciberseguridad

La materia de ciberseguridad ha cobrado gran relevancia para los gobiernos, quienes han comenzado a desarrollar estrategias nacionales, puntos de referencia y marcos para entender a sus organismos y las vulnerabilidades a las que están expuestas. Hay una constante en la ciberseguridad que es el hecho de que las infraestructuras y los servicios dependen de un futuro digital, además de que es un tema central para el bienestar económico, lo cual incrementa la preocupación de los Estados para agilizar la generación de regulación respecto de la seguridad cibernética.

En ese sentido, países como Estados Unidos, Alemania y Países Bajos han estudiado el impacto de la economía digital sobre su producto interno bruto en la actualidad y su comportamiento a futuro. Por tal motivo, destaca la priorización en función del impacto que representa cada sector, para garantizar la gestión del riesgo y la resiliencia dentro de los procesos generales de planificación comercial[24].

Por su parte, Estados Unidos ha buscado impulsar las inversiones voluntarias de la industria a fin de reducir el riesgo cibernético, en lugar de generar regulación al respecto. No obstante, dicha nación ha desarrollado estándares, metodologías, procesos, y procedimientos alineados al enfoque político, de negocio y tecnología que abordan los riesgos del entorno digital[25].

Es así que, en febrero de 2014, Estados Unidos publicó el marco para mejorar la seguridad cibernética en las infraestructuras críticas, mismo que contempla estándares de aplicación voluntaria para que las organizaciones evalúen, administren y respondan a los riesgos de la seguridad digital. Este marco está encabezado por cinco principios: identificar, detectar, proteger, responder y

---

[23] Aguirre, A. (2017). *Ciberseguridad en Infraestructuras Críticas de Información*. Universidad de Buenos Aires. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1115_AguirrePonceAA.pdf.

[24] Hathaway, M. (2018). *Gestión del Riesgo Cibernético Nacional*. OEA. https://www.oas.org/es/sms/cicte/ESPcyberrisk.pdf.

[25] Hathaway, M. (2018). *Gestión del Riesgo Cibernético Nacional*. OEA. https://www.oas.org/es/sms/cicte/ESPcyberrisk.pdf.

recuperar. De acuerdo a los datos recabados por Hathaway, en 2019, el 30 % de las organizaciones de Estados Unidos, incluido el gobierno, utiliza el marco como apoyo en la evaluación de su postura de riesgo y efecto de asumir una responsabilidad en maximizar la protección de sus redes y datos confidenciales[26].

Por lo que respecta a Alemania, el gobierno federal ha ampliado sus capacidades para defender el ciberespacio, demostrando así su capacidad para proporcionar seguridad en el entorno digital, dado el número de amenazas a las que se ha enfrentado constantemente, siendo éstas cada vez más complejas.

En ese orden de ideas, el Ministerio Federal de Defensa en conjunto con el Ejército Federal de Alemania, tienen a su cargo la defensa nacional, incluida la ciberseguridad. Sobre esto último, el 26 de abril de 2017, Alemania publicó su más reciente Estrategia Nacional 2016 [Cyber Security Strategy for Germany 2016], dejando atrás la estrategia correspondiente a la materia que se publicó en 2011. Cabe mencionar que, el pilar regulatorio en el ámbito digital para el caso de Alemania es la Ley de Seguridad Informática publicada en julio de 2015, misma que establece los estándares mínimos que deben cumplir las empresas en relación con la seguridad de tecnología de la información[27].

En adición a lo anterior, el 11 de agosto de 2020 fue creada la Agencia para la Innovación en Ciberseguridad, encargada de la protección de sistemas informáticos, con el fin de garantizar la operación de la administración, libre de interferencias, y la economía alemana; dependiente del Ministerio Federal de Defensa (*BMVg*, por sus siglas en alemán) y del Ministerio Federal del Interior, Construcción y Comunidad (*BMI*, por sus siglas en alemán).

La agencia en comento tiene como objetivo principal la adjudicación de contratos para investigación, con miras a la innovación en ciberseguridad y tecnología relativa a seguridad de la sociedad alemana, además de encaminar la investigación a la seguridad interna, derivado de las atribuciones de esa autoridad. El enfoque de la creación de esa ciber-agencia es alentar a la industria a la aplicación de tecnología nueva, de manera que se desarrolle la innovación de éstas.

---

[26] Hathaway, M. (2018). *Gestión del Riesgo Cibernético Nacional.* OEA. https://www.oas.org/es/sms/cicte/ESPcyberrisk.pdf.

[27] *Bundesministerium der Verteidigung*, s/f. https://www.bmvg.de/de/themen/cybersicherheit

Es de resaltar que el dirigente de esta agencia ha dejado en claro que la labor de ésta no es investigar, sino gestionar, coordinar, estimular, informar y evaluar aspectos de la seguridad digital que le competen al Estado alemán[28].

Dada la creación reciente de la ciber-agencia, y de acuerdo con lo mencionado por su dirigente, uno de los mayores retos es identificar científicos y expertos en ciberseguridad que aborden las problemáticas alemanas, por lo que es una de las tareas primordiales de la agencia en comento, así como la motivación para que los jóvenes formen parte de la responsabilidad social[29].

Otro de los objetivos de la citada entidad, es conservar la soberanía tecnológica en el ambiente digital y proporcionar incentivos, financiamientos y coordinación a la investigación relacionadas con ciberseguridad.

Ahora bien, en la UE se clasifica la participación de los actores involucrados en la materia de ciberseguridad en 3 grupos principales. El primero se refiere a los actores creados para garantizar la seguridad digital en la UE, como la Agencia de la Unión Europea para la Ciberseguridad, institución creada en 2004, o la Red Judicial Europea contra la Ciber-delincuencia, creada en 2016[30].

El segundo grupo está conformado por organismos (células, comités, oficinas, grupos de trabajo o centros), que tienen como objetivo principal estimular la colaboración entre los principales actores en la materia que nos ocupa. Finalmente, en la última categoría se ubican los actores que por su propia naturaleza terminan adquiriendo funciones y competencias encaminadas a dicho ámbito[31].

Las características bajo las cuales se rige la UE, es un aliciente para desarrollar políticas innovadoras y enfocadas al bienestar de las naciones que la conforman, con una óptica más amplia, a efecto de que dichas políticas sean de aplicación general.

---

[28] Igel, C. (mayo, 2020). *Im Interview: Forschungsdirektor der Cyberagentur*. https://www.bmvg.de/de/aktuelles/interview-forschungsdirektor-der-cyberagentur-258548.

[29] Igel, C. (mayo, 2020). *Im Interview: Forschungsdirektor der Cyberagentur*. https://www.bmvg.de/de/aktuelles/interview-forschungsdirektor-der-cyberagentur-258548.

[30] Dermutas, A. (junio, 2020). *La evolución normativa de la ciberseguridad en la Unión Europea y su impacto político a nivel de actores, objetivos y recursos*.

[31] Dermutas, A. (junio, 2020). *La evolución normativa de la ciberseguridad en la Unión Europea y su impacto político a nivel de actores, objetivos y recursos*.

En materia de ciberseguridad, dada la constante evolución que implica, la UE no es excepción de las amenazas que derivan del ciberespacio, es así que en 2003 fue aprobada la Estrategia de Europea de Seguridad conducida por temas como terrorismo, la proliferación de armas de destrucción masiva, los conflictos regionales, la descomposición Estado-Nación y la delincuencia organizada, la cual no tocaba temas inherentes a la seguridad nacional.

En 2004, la UE creó la Agencia de Seguridad de las Redes de la Información de la Unión Europea en un entorno en el que la ciberseguridad comenzó a tener relevancia. Lo anterior, es el punto del que parte la UE para comprometerse a garantizar la protección del espacio digital. Asimismo, en 2007 se impulsó la creación del Programa Europeo para la Protección de Infraestructuras Críticas[32].

Es hasta 2010 que la Estrategia de Seguridad Interior incluye de manera oficial la ciberseguridad como uno de los mayores desafíos en común para toda Europa, e incluye conceptos como la ciberdelincuencia, destacando ésta dentro de las principales amenazas a las que se enfrentaría Europa. Posteriormente, en 2013 se da a conocer la Estrategia Europea de Ciberseguridad, que sucedió a la Agenda Digital de Europa, también publicada en ese mismo año. Esta última contempló la ciberseguridad por lo que se enlazó con la estrategia en comento[33].

Por otra parte, la nueva Estrategia de Ciberseguridad de la UE se basa en la Estrategia Digital de Europa y en la Estrategia de la UE para la Unión de la Seguridad, ambas, publicadas durante 2020. En dicho documento se propone la focalización de cuatro pilares de la ciberseguridad: el mercado interior, la aplicación de la ley, diplomacia y defensa para reforzar la resiliencia colectiva de Europa, a efecto de contrarrestar las amenazas del espacio cibernético; y para garantizar a la

[32] Unión Europea. (julio 2016). *Directiva (UE) 2016/1148 del Parlamento Europeo del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión*. Diario Oficial de la Unión Europea L 194.
[33] Unión Europea. (julio 2016). *Directiva (UE) 2016/1148 del Parlamento Europeo del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión*. Diario Oficial de la Unión Europea L 194.

sociedad y a las empresas, beneficios de servicios y herramientas digitales fiables, con mayor conectividad[34].

La Estrategia de Ciberseguridad de referencia, aborda propuestas concretas para el establecimiento de tres instrumentos principales: regulatorios, de inversión y de política contemplando las siguientes líneas de acción:

1. Resiliencia, soberanía, tecnológica y liderazgo.
2. Desarrollar la capacidad operativa para prevenir, disuadir y responder.
3. Promover un ciberespacio abierto.

Dichas líneas incluyen medidas de las que destacan la construcción de un escudo para el ciberespacio, a través de la creación de una red de centros de operaciones de seguridad cuya base es la inteligencia artificial, aquellas medidas abocadas a la seguridad 5G, las medidas para el establecimiento de la Joint Cybersecurity Unit y el desarrollo del Marco de Gestión de crisis de ciberseguridad, así como las relativas a la lucha contra la delincuencia y la cooperación internacional[35].

Cabe destacar que se pretende alcanzar una inversión de 4,500 millones de euros para el desarrollo de la citada estrategia, aproximadamente, provenientes de los Estados miembros y la industria, especialmente de los Centros de Competencias en Ciberseguridad y la Red de Centros de Coordinación, y se planea proporcionar apoyos económicos a las medianas empresas de dicha inversión[36].

En otro orden de ideas, el 7 de junio de 2019 fue publicado el Reglamento 2019/881[37] del Parlamento Europeo y del Consejo de 17 de abril de 2019, relativo a las funciones de ENISA y a la certificación relativa a la ciberseguridad de las tecnologías de la información y la comunicación.

---

[34] Departamento de Seguridad Nacional. (diciembre, 2017). *Nuevo paquete de ciberseguridad de la Unión Europea*. https://www.dsn.gob.es/es/actualidad/sala-prensa/nuevo-paquete-ciberseguridad-uni%C3%B3n-europea.

[35] Departamento de Seguridad Nacional. (diciembre, 2017). *Nuevo paquete de ciberseguridad de la Unión Europea*. https://www.dsn.gob.es/es/actualidad/sala-prensa/nuevo-paquete-ciberseguridad-uni%C3%B3n-europea.

[36] Departamento de Seguridad Nacional. (diciembre, 2017). *Nuevo paquete de ciberseguridad de la Unión Europea*. https://www.dsn.gob.es/es/actualidad/sala-prensa/nuevo-paquete-ciberseguridad-uni%C3%B3n-europea.

[37] Parlamento Europeo (2019). *Reglamento Europeo de Ciberseguridad*. https://dpd.aec.es/reglamento-europeo-de-ciberseguridad/.

El citado reglamento se rige por dos propósitos principales, el primero, respecto al establecimiento de los objetivos, tareas y aspectos organizativos de ENISA y, el segundo, como soporte del marco para la creación de esquemas europeos relativos a la certificación de ciberseguridad, a fin de garantizar productos, servicios y procesos TIC con un nivel adecuado de seguridad en la materia que nos ocupa para la UE.

A partir de la entrada en vigor del reglamento de referencia, la ENISA es el punto de referencia y conocimiento de ciberseguridad en la EU[38] y tiene las siguientes funciones a su cargo:

- Colaborar con el desarrollo y la implementación de la política y del derecho de la EU[39];
- Apoyar en la creación de capacidades de ciberseguridad[40];
- Ayudar en la cooperación entre los Estados miembros, las instituciones, órganos y organismos de la Unión y partes interesadas[41];
- Mercado, certificación de la ciberseguridad y normalización[42];
- Conocimiento e información[43];
- Sensibilización y educación[44];
- Investigación e innovación[45];
- Cooperación internacional[46].

---

[38] Parlamento Europeo (2019). *Reglamento Europeo de Ciberseguridad*. https://dpd.aec.es/reglamento-europeo-de-ciberseguridad/.
[39] Parlamento Europeo (2019). *Reglamento Europeo de Ciberseguridad*. https://dpd.aec.es/reglamento-europeo-de-ciberseguridad/.
[40] Parlamento Europeo (2019). *Reglamento Europeo de Ciberseguridad*. https://dpd.aec.es/reglamento-europeo-de-ciberseguridad/.
[41] Parlamento Europeo (2019). *Reglamento Europeo de Ciberseguridad*. https://dpd.aec.es/reglamento-europeo-de-ciberseguridad/.
[42] Parlamento Europeo (2019). *Reglamento Europeo de Ciberseguridad*. https://dpd.aec.es/reglamento-europeo-de-ciberseguridad/.
[43] Parlamento Europeo (2019). *Reglamento Europeo de Ciberseguridad*. https://dpd.aec.es/reglamento-europeo-de-ciberseguridad/.
[44] Parlamento Europeo (2019). *Reglamento Europeo de Ciberseguridad*. https://dpd.aec.es/reglamento-europeo-de-ciberseguridad/.
[45] Parlamento Europeo (2019). *Reglamento Europeo de Ciberseguridad*. https://dpd.aec.es/reglamento-europeo-de-ciberseguridad/.
[46] Parlamento Europeo (2019). *Reglamento Europeo de Ciberseguridad*. https://dpd.aec.es/reglamento-europeo-de-ciberseguridad/.

De igual forma, este reglamento busca dotar de credibilidad a los productos, servicios y procesos de TIC con relación a la ciberseguridad, a través de la certificación de estos.

Finalmente, por lo que hace a la Agencia de la Unión Europea para la Ciberseguridad, ésta es el punto central de conocimiento y alta especialización en ciberseguridad en la UE, la cual colabora con los Estados miembros para que estén mejor equipados y preparados a efecto de prevenir, detectar y dar respuesta a los problemas de seguridad de la información[47].

Esta agencia, ofrece soluciones y asesoría al sector público y privado, con el objetivo de organizar ejercicios ante situaciones de crisis cibernéticas a escala y para contribuir con la elaboración de estrategias nacionales en la materia, así como fomentar la cooperación entre los CERT de dichos Estados[48].

Adicionalmente, la citada agencia realiza publicaciones de informes y estudios relacionados con ciberseguridad y ayuda en la elaboración de políticas y legislación de la EU respecto de la seguridad de las redes y de la información. Lo anterior, en contribución al desarrollo económico del mercado interior europeo[49].

Actualmente, el rol de la agencia en comento ha sido ampliado para incorporar funciones relevantes en materia de ciberseguridad las cuales se relacionan con seis áreas:

- Experiencia: evaluar y aprobar el conocimiento europeo para abordar los desafíos en la materia.
- Política: dar soporte a la política elaborada e implementada por la UE al respecto.
- Capacidad: apoyar el desarrollo de capacidades relacionadas con ciberseguridad.
- Cooperación: incentivar la cooperación dentro de la EU en materia de ciberseguridad.
- Certificación apoyar en el desarrollo e implementación del marco legal para certificación de productos, servicios y proceso en ciberseguridad.

[47] ENISA. *European Union Agency for Cybersecurity*. https://www.enisa.europa.eu/.
[48] ENISA. *European Union Agency for Cybersecurity*. https://www.enisa.europa.eu/.
[49] ENISA. *European Union Agency for Cybersecurity*. https://www.enisa.europa.eu/.

- Habilitar: reforzar el impacto de ENISA y su eficiencia.

Por último, resulta importante señalar que las prioridades en materia de ciberseguridad por parte de la EU se centran en el desarrollo e implementación de políticas, desarrollo de capacidades, conocimiento, información e incremento de conciencia, acciones relacionadas con el mercado como la estandarización o certificación, investigación e innovación, así como cooperación operativa y administración de riesgos[50].

[50]ENISA. *European Union Agency for Cybersecurity*. https://www.enisa.europa.eu/.

Capítulo 2. La Estrategia Nacional de Ciberseguridad

Capítulo 2. La Estrategia Nacional de Ciberseguridad

El gobierno mexicano inició esfuerzos encaminados al reconocimiento de derechos fundamentales, la seguridad en un entorno digital, el desarrollo y publicación de una Estrategia Nacional de Ciberseguridad, la modificación e introducción de nuevos marcos normativos relativos al sector de telecomunicaciones, entre otros.

No obstante, el seguimiento que tuvieron dichas políticas quedó mermado y, hoy en día, no se tiene un marco que regule de manera específica la ciberseguridad en las telecomunicaciones. En ese sentido, es relevante analizar los elementos clave que dieron paso a una de las primeras acciones de México en el aspecto de seguridad digital que fue la publicación de la Estrategia Nacional de Ciberseguridad.

2.1 Introducción a la ENCS desde el ámbito internacional

La propia definición de ciberseguridad que emitió la UIT en la Recomendación UIT-T X.1205 realza la importancia de herramientas como políticas, directrices, acciones y prácticas idóneas, entre otros, que se requieren para garantizar la seguridad en el entorno cibernético[51]. Dicha definición considera tres propiedades de la seguridad: i) disponibilidad; ii) integridad, que puede incluir la autenticidad y el no repudio, y iii) confidencialidad.

Asimismo, la UIT ha destacado, en varias ocasiones, la importancia de mantener un entorno digital seguro, para generar un desarrollo sustentable en las naciones, tanto económico como social. Adicionalmente, este organismo reconoce que las ciberamenazas representan retos cada vez más complejos y la labor de

[51] La UIT definió en la Recomendación UIT-T X.1205, que la ciberseguridad es: "*El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. (…)*". UIT. (agosto, 2008). *X.1205: Aspectos generales de la ciberseguridad*. https://www.itu.int/rec/T-REC-X.1205-200804-I/es.

contrarrestarlos compromete a los sectores público y privado, por lo que la cooperación entre ambos debe ser cada vez más estrecha y de manera pronta.

Entre los diversos mecanismos que desarrolla la UIT con la finalidad de coadyuvar con los Estados miembros para la inclusión de marcos o estrategias nacionales, a efecto de enfrentar los retos que implica la ciberseguridad, es la publicación del IMC, que permite resaltar el avance de cada país en acciones para fortalecer la resiliencia e impulsar a las naciones para que introduzcan esta materia dentro de sus planes de desarrollo. Este IMC tiene como objetivo reflejar el nivel de compromiso de los Estados miembros en cinco aristas: medidas jurídicas, medidas técnicas, medidas organizativas, creación de capacidades y cooperación internacional: cuyo resultado es directamente la respuesta del grado de preparación de cada país para garantizar un entorno digital seguro[52].

En relación con las medidas organizativas, la UIT enmarca la importancia de que el Estado ponga en marcha un objetivo estratégico general, a través de una estrategia nacional, además de que es necesario habilitar a que existan organismos que pongan en marcha esa estrategia, la evalúen y definan el éxito o fracaso de la misma, resaltando que "*Sin una estrategia nacional, un modelo de gobernanza y un organismo supervisor, la labor de los diferentes sectores e industrias se dispersa y queda inconexa, frustrando el intento de lograr la armonización nacional del desarrollo de la capacidad de ciberseguridad*"[53].

Por lo que hace a la publicación del IMC en el año 2015, la valoración de México fue de 18 puntos en la clasificación mundial, con un índice de 0.324, cuyo valor representa el nivel de preparación para la ciberseguridad o su compromiso con ésta, siendo el 1 el país más preparado, con un índice de 0.824, y el 29 el más bajo, cuyo índice fue de 0[54]. Cabe mencionar que, al momento de realizar la citada evaluación, los puntos considerados en dicha evaluación para México en el área de

---

[52] UIT. (abril de 2015). *Índice mundial de ciberseguridad y perfiles de ciberbienestar*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdf.

[53] UIT. (abril de 2015). *Índice mundial de ciberseguridad y perfiles de ciberbienestar*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdf.

[54] Los resultados se basaron en cuestionarios aplicados a los Estados miembros respecto de la situación en materia de ciberseguridad correspondiente a 2014, según lo señalado en la propia publicación del IMC 2015.

medidas organizativas fueron los siguientes: i) la creación del Comité Especializado de Seguridad de la Información para el desarrollo de una Estrategia Nacional de Seguridad de la Información, ii) que no se contaba con una ruta de gobernanza para la ciberseguridad, iii) que la Policía Federal era el órgano responsable de la política de ciberseguridad.

En 2017, la UIT publicó el IMC correspondiente a ese año, en el que México destaca en la región de las Américas en el tercer lugar en la tabla de posición, con un índice de 0.66, quedando por debajo de Estados Unidos de América y Canadá, con índices de 0.91 y 0.81, respectivamente. Dentro del ranking global, México se posicionó en el lugar 28 de 193 participantes, para lo cual se contempló la encuesta correspondiente al año 2016[55].

Aunque en la publicación de la UIT no se mencionan los aspectos relativos a las medidas organizativas evaluadas para México, el contexto nacional lo podemos conocer a través de las publicaciones del Tercer y Cuarto Informe de Gobierno de los periodos 2015-2016[56] y 2016-2017[57], respectivamente. En los citados informes, se identifica la integración de las correspondientes Agendas Nacionales de Riesgos 2016 y 2017, en las que se aborda la ciberseguridad como uno de los factores que vulnera el desarrollo económico del país. Adicionalmente, se sometió a consulta pública el primer proyecto de la Estrategia Nacional de Ciberseguridad.

Por último, de conformidad con los resultados obtenidos en la publicación del IMC 2018, México cae un lugar a nivel regional ocupando la cuarta posición con un índice de 0.629 y en el ranking global cayó hasta la posición 63 entre los 175 países participantes. A pesar de que no se dan detalles de la valoración, con tales resultados, es evidente la falta de atención, de acciones relativas a la seguridad digital y de compromisos del Estado para sostener una coordinación que garantice la ciberseguridad[58].

---

[55] UIT. (2017). *Global Cybersecurity Index 2017*, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf.

[56]Presidencia de la República. (agosto, 2016). *4to. Informe de Gobierno 2015-2016*. México. https://framework-gb.cdn.gob.mx/cuartoinforme/4IG_Escrito_27_08_16_COMPLETO.pdf.

[57] Presidencia de la República. (agosto, 2017). *5to. Informe de Gobierno 2016-2017*. México. https://issuu.com/ejecentral6/docs/quinto_informe_de_gobierno_2017

[58] UIT. (2018). *Global Cybersecurity Index (GCI) 2018*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

De lo anterior se desprende que, la publicación de una Estrategia Nacional de Ciberseguridad en 2017 fue el punto clave para resaltar que el Estado comenzaba a ocuparse de uno de los retos organizacionales que muchos países, hoy en día, no han logrado esbozar. En ese sentido, parecería que esa Estrategia marcaría el inicio de grandes cambios para abordar la seguridad en el entorno digital, sin embargo, la publicación más reciente del IMC muestra lo contrario, dejando en claro que las propuestas vertidas en el citado documento no se tradujeron en resultados palpables, dada la falta de continuidad para su implementación.

2.2 Publicación de la ENCS

El Plan Nacional de Desarrollo 2013-2018 (PND 2013-2018), publicado en el DOF el 20 de mayo de 2013, estableció dentro de sus acciones, el Objetivo 1.2. relativo a garantizar la seguridad nacional y, para lograr éste, se definieron 5 Estrategias, de las cuales, la 1.2.3. está enfocada a fortalecer la inteligencia del Estado Mexicano para identificar, prevenir y contrarrestar riesgos y amenazas a la seguridad nacional. En ese sentido, una de las líneas de acción que se desprende de la Estrategia 1.2.3. es la de diseñar e impulsar una estrategia de seguridad de la información, a efecto de garantizar la integridad, confidencialidad y disponibilidad de la información de las personas e instituciones públicas y privadas en México[59].

En ese sentido, el 30 de abril de 2014, se publicó en el DOF el Programa para la Seguridad Nacional 2014-2018 (PSN 2014-2018), mismo que, de acuerdo con lo señalado por el Gobierno de México, es el documento rector de la política de seguridad nacional del Estado. Por tal motivo, y con el fin de alinearse al objetivo 1.2 del PND 2013-2018, el PSN 2014-2018 estableció dos Objetivos Estratégicos con sus respectivos objetivos específicos y estrategias. Al respecto, la Estrategia 2.1.2., del Objetivo 2.1., se definió para "*Desarrollar una política de Estado en materia de seguridad cibernética y ciberdefensa, para proteger y promover los intereses y objetivos nacionales"*, cuyas líneas de acción están enfocadas a

[59] Poder Ejecutivo Federal. (mayo, 2013). *Plan Nacional de Desarrollo 2013-2018*. https://www.snieg.mx/contenidos/espanol/normatividad/MarcoJuridico/PND_2013-2018.pdf

impulsar y homologar los esquemas de seguridad de la información para prevenir y enfrentar ataques cibernéticos, designar el ente público encargado de emitir, evaluar e impulsar el cumplimiento de la política de seguridad y ciberdefensa para el Ejecutivo Federal, entre otros[60].

El 2 agosto de 2017, la OEA, a petición del Gobierno Mexicano, publicó el documento denominado *"Hacia una Estrategia Nacional de Ciberseguridad. Consolidación de las Consultas a Actores Nacionales",* mismo que se enfoca a: (i) Industria; (ii) Sector Financiero; (iii) Sociedad Civil, Derechos Humanos (DD.HH.) y Usuario Final; (iv) Academia y Comunidad Técnica; y (v) Gobierno[61]. A través de las discusiones coordinadas por dicha organización con expertos internacionales, quienes compartieron las mejores prácticas en materia de ciberseguridad, se destacaron diversos comentarios relacionados con el borrador de la Estrategia Nacional de Ciberseguridad elaborado por el Gobierno Mexicano[62], los cuales se enuncian a continuación:

i. Alcances de la Estrategia Nacional de Ciberseguridad
ii. Enfoque Basado en el Riesgo
iii. Terminologías (estandarización)
iv. Gobernanza (definición clara del marco de gobernanza)
v. Plan de Acción (definición de acciones concretas)

Al mismo tiempo, la OEA publicó el "*Documento de Trabajo ENCS v.1*", el cual se avoca a la revisión de cada una de las secciones planteadas en el borrador de la Estrategia Nacional de Ciberseguridad y proporciona comentarios específicos para las mismas[63].

---

[60] Poder Ejecutivo Federal. (abril, 2014). *Programa para la Seguridad Nacional 2014-2018*. http://dof.gob.mx/nota_detalle.php?codigo=5342824&fecha=30/04/2014.

[61] OEA. (2017). *Documento de Trabajo ENCS v.1.* https://www.sites.oas.org/cyber/Documents/Mexico%20-%20Anexo%20-%20Consolidacion%20de%20Consultas%20Documento%20ENCS.pdf

[62] OEA. (2017). *Documento de Trabajo ENCS v.1.* https://www.sites.oas.org/cyber/Documents/Mexico%20-%20Anexo%20-%20Consolidacion%20de%20Consultas%20Documento%20ENCS.pdf

[63] OEA. (2017). *Documento de Trabajo ENCS v.1.* https://www.sites.oas.org/cyber/Documents/Mexico%20-%20Anexo%20-%20Consolidacion%20de%20Consultas%20Documento%20ENCS.pdf

En seguimiento a lo anterior y una vez concluida la consulta pública del proyecto presentado por el Gobierno de México, el 13 de noviembre de 2017 se publicó la ENCS cuyo objetivo general, indicado en la misma, es "*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*"[64].

2.3 Ejes de la ENCS

Para entrar al análisis de las bases sobre las cuales se establecieron los objetivos de la ENCS, es importante conocer el contexto que enmarca a la misma, puesto que, desde esa perspectiva podemos apreciar la motivación bajo la cual se desarrolló el enfoque que da el Gobierno de la República a dicho documento. En ese sentido, cabe resaltar que, si bien, desde el PND 2013-2018 se tenía un objetivo encaminado al fortalecimiento de la inteligencia del Estado para prevenir y contrarrestar riesgos y amenazas contra la seguridad nacional, la ENCS reconoce que las TIC son de uso cotidiano en todos los sectores, lo cual ha permitido el desarrollo económico, social y político. Derivado de lo anterior, el Gobierno de México previó la necesidad de generar una Estrategia y justificó la elaboración de la misma para coordinar las acciones dirigidas a la sociedad, los entes públicos y privados, a fin de concientizarlos respecto del daño que implican los incidentes cibernéticos y la relevancia de contar con un ambiente digital seguro, que permita el uso de las TIC de manera responsable. Además, la ENCS deja en claro que la suma de esfuerzos de aquellos que están involucrados en materia de ciberseguridad dará paso al uso de las TIC en un entorno libre, responsable y confiable.

En relación con lo anterior, la ENCS consideró tres ejes rectores, mismos que se describen a continuación:

A. Perspectiva de derechos humanos.

[64] Poder Ejecutivo Federal. (noviembre, 2017). *Estrategia Nacional Ciberseguridad*. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf.

Una de las grandes contribuciones que se tuvo para el desarrollo de la ENCS por parte de los especialistas en el Programa de Ciberseguridad dirigido por la OEA, fue el enfoque sobre DDHH que motivó a hacer adecuaciones al proyecto originalmente planteado por el Gobierno de la República. Para ello, se argumentó la necesidad de plasmar los DDHH desde la visión de la ENCS y no abordarlos solamente en el contexto de libertad de expresión, sino también aludir a los derechos de salud, acceso a la educación, cultura e infraestructura cibernética. Adicionalmente, se destacó la importancia de definir el concepto de "seguridad nacional", a efecto de evitar que el mismo sea motivo de vulnerabilidad para los derechos humanos.

En consonancia, la ENCS plantea como primer eje la promoción, respeto y cumplimiento de los derechos humanos en cualquier acción que se ejecute en materia de ciberseguridad. Lo anterior, encamina las acciones del Gobierno Mexicano a salvaguardar los derechos de todos los involucrados en entorno digital y realza la prioridad de estos ante cualquier actuación que derive de la seguridad cibernética.

Al respecto, no pasa desapercibido que el propio contacto con el ciberespacio ha generado nuevos derechos y formas de ejercer aquellos que ya están definidos, a lo que se le conoce como la cuarta generación de derechos humanos[65], los cuales son ejercidos en un entorno en común por los individuos que transportan información dentro de una misma red.

En ese sentido, resulta importante que se fijen los límites de los derechos y las libertades, en virtud de que, la protección de unos podría significar la negación de otros. Es así que Bustamante manifiesta la existencia de un conflicto entre derechos y libertades y plantea el siguiente cuestionamiento: ¿dónde se debe establecer la frontera entre el derecho a la libertad de expresión o de investigación y el derecho a la protección de la información personal?

Partiendo de esa idea, es importante resaltar que, si bien, la ENCS contempló una perspectiva de DDHH, la responsabilidad del Estado para con la sociedad no

[65] Bustamante, J. (2012). *Los derechos humanos de cuarta generación y sus implicaciones en la sociedad contemporánea.*

se debe acotar a los derechos fundamentales para proteger la integridad humana, sino que también debe velar por los derechos y libertades del entorno digital e, inclusive, redefinir algunos de los conceptos relacionados a dicho entorno, con la finalidad de garantizar la protección a cada una de las partes involucradas.

B. Enfoque basado en gestión de riesgos.

Desde la descripción que se introduce en la visión de la ENCS se advierte la meta para que México esté debidamente preparado ante los riesgos que implica el uso de las TIC. Del mismo modo, en el citado documento se reconoce que uno de los motivos que orilló a su desarrollo es precisamente el aumento de los riesgos y amenazas en el ciberespacio y dicho argumento es retomado dentro de la justificación de la ENCS.

El nivel de riesgo que representa el uso de las redes va en función de la vulnerabilidad que se desprende del usuario, la infraestructura y la información que conforman el espacio digital. Es por ello que la evaluación de los riesgos no se limita al estudio de amenazas en el ciberespacio, sino que tiene un enfoque metodológico sobre los tres aspectos mencionados anteriormente, lo cual permite dimensionar la eficiencia de las medidas de seguridad que se pretenden implementar.[66]

En relación con esto, poco sentido tendría enfocarse a que las infraestructuras fueran inmunes a la introducción de agentes ajenos a las mismas para evitar la fuga de la información que circula en la red, cuando no se concientiza al usuario el debido cuidado del aseguramiento de tal información con la encriptación necesaria para la evasión de espionaje. En consecuencia, la debida observación a los elementos implicados en una red asegura la preparación adecuada para una resiliencia acorde al escenario en particular de cada estado.

Es evidente que los riesgos no pueden eliminarse en su totalidad, puesto que, en la medida en que los sistemas de seguridad se robustecen, las amenazas actúan sobre los puntos débiles de los mecanismos de protección. Sin embargo, la evaluación continua de los riesgos en el ciberespacio permite diseñar respuestas

[66] Martin, Paul-Edouard. (julio, 2015). *Inseguridad Cibernética en América Latina: Líneas de reflexión para la evaluación de riesgos*. no. 79.

óptimas[67], lo que se traducirá en impacto positivo en el empleo de las telecomunicaciones para el desarrollo de las naciones.

En consonancia con lo anterior, de las recomendaciones realizadas al proyecto de la ENCS en las mesas de discusión dirigidas por la OEA en 2017, destaca que "*los riesgos debían considerarse no sólo desde la tecnología, sino también desde los procedimientos y las personas*"[68]. Además, se discutió respecto de la importancia que tiene la Seguridad Nacional y el carácter de prioridad en cuanto a nivel de protección se trata para dicho rubro.

Derivado de lo anterior, la ENCS atiende a la exigencia natural de contar con la capacidad para tomar acciones preventivas y de corrección ante una amenaza o riesgo del ciberespacio[69], y se definen diversos objetivos que se vinculan con este segundo eje en el citado documento para atender la cultura sobre ciberseguridad, la gestión de infraestructuras críticas, el desarrollo de estándares y criterios técnicos, entre otros.

El enfoque de la ENCS es acertado en el sentido de que parte de la postura preventiva y correctiva, con objetivos alineados a generar las condiciones para una cultura cibernética en la población, proteger la información y los sistemas informáticos de las instituciones públicas y desarrollar capacidades para la prevención de riesgos y amenazas en el entorno digital. Sin embargo, desde la publicación de la ENCS, el impulso de acciones orientadas a la adecuación del marco jurídico nacional y el desarrollo de mecanismos de autorregulación, no tuvieron ninguna materialización como estaba previsto en dicho instrumento.

C. Colaboración multidisciplinaria y de múltiples actores.

El presente eje está ligado al anterior en el sentido de que los involucrados en el entorno digital juegan diferentes papeles para el funcionamiento y uso de las redes y, al mismo tiempo, convergen en el mismo entorno. Esto último hace que

---

[67] Martin, Paul-Edouard. (julio, 2015). *Inseguridad Cibernética en América Latina: Líneas de reflexión para la evaluación de riesgos*. no. 79.
[68] Bustamante, J. (2012). *Los derechos humanos de cuarta generación y sus implicaciones en la sociedad contemporánea*.
[69] Poder Ejecutivo Federal. (noviembre, 2017). *Estrategia Nacional Ciberseguridad*. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf.

todos los actores del ciberespacio tengan objetivos en común y las implicaciones negativas del uso de la tecnología se traduzca en daños a cada una de las partes.

En ese orden de ideas, los objetivos en común impulsan a los participantes del ambiente digital a generar la cooperación para generar seguridad y confianza, con lo que se benefician todos y hay una menor inversión en varios aspectos de los diversos sectores implicados. Si bien la experiencia de las instituciones permite el desarrollo de mecanismos de defensa, no siempre se cuenta con los recursos necesarios para su materialización. De igual forma, los alcances que podrían significar las políticas implementadas por el sector público dejan de ser positivos sin la noción requerida para la aplicación de esas políticas. Tales ejemplos, destacan que la coordinación entre todos los involucrados es indispensable para lograr el objetivo en común de enfrentar las amenazas y prevenir los riesgos.

Así, la ENCS reconoce la contribución de los especialistas que comentaron el proyecto inicial, haciendo mención de que, una de las constantes en el análisis respectivo, fue la identificación de la necesidad de colaboración y cooperación entre los diversos sectores como la parte central para el desarrollo, seguimiento y evaluación de la ENCS[70].

Por tal motivo, la citada Estrategia señala en este eje, la obligada colaboración multidisciplinaria por parte de todos los involucrados, "…*con un enfoque de gobernanza de internet en materia de ciberseguridad, que permita el desarrollo integral, transversal y holístico de la Estrategia y facilite la participación abierta y transparente de los mismos*…"[71].

Adicionalmente, dado que las amenazas y los riesgos en el mundo digital no son exclusivos de una nación, sino que son una constante a nivel internacional, la colaboración a la que se refiere este eje no está limitada a los actores nacionales, sino que, además, busca la cooperación de organismos internacionales que

---

[70] Poder Ejecutivo Federal. (noviembre, 2017). *Estrategia Nacional Ciberseguridad*. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf.

[71] Poder Ejecutivo Federal. (noviembre, 2017). *Estrategia Nacional Ciberseguridad*. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf.

permitan generar estrategias acordes con los problemas a los que se enfrenta la sociedad global.

2.4 Perspectiva del marco institucional de la ENCS

La autoridad competente encargada de dirigir la estrategia nacional de que se trate debe estar contemplada dentro de ésta, la cual tendrá funciones de coordinación, orientación y supervisión de la ejecución de la estrategia, según lo establecido en la "*GUÍA PARA LA ELABORACIÓN DE UNA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD*", publicada por la UIT en 2018.

Asimismo, en el documento antes referido, se menciona que la gestión que desarrolle dicha autoridad debe estar encaminada a la definición y claridad de funciones, responsabilidades, procesos, potestades de decisión y tareas necesaria para dar garantía de la ejecución efectiva de la estrategia, además de que se debe garantizar que la autoridad competente tenga la capacidad de implicar y dirigir a los actores, de acuerdo con las acciones que corresponda en materia de ciberseguridad.

A pesar de que la publicación de la guía en comento fue hasta 2018, los grupos de trabajo que analizaron el proyecto de la ENCS vislumbraron que, para la implementación de la estrategia, sería necesario contar con una agencia pública que coordinara a los distintos participantes, a efecto de liderar la ciberseguridad en México y sumar esfuerzos[72].

Destaca la recomendación de las mesas de trabajo encargadas de estudiar el proyecto de la ENCS, respecto del establecimiento de un coordinador nacional con experiencia y comprensión general de la ciberseguridad, así como alinear los objetivos estratégicos con los involucrados más relevantes en la materia.

Por su parte, la ENCS indica que, en principio, la coordinación para su implementación y seguimiento está a cargo de una Subcomisión de Ciberseguridad adscrita a la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico. En seguimiento a lo anterior, esta estrategia aborda en una de las secciones el

[72] Bustamante, J. (2012). *Los derechos humanos de cuarta generación y sus implicaciones en la sociedad contemporánea*.

marco institucional, que la citada Comisión aprobó la creación de la Subcomisión de Ciberseguridad, conformada por diversas entidades de la administración pública federal, para el desarrollo integral, holístico y transversal de la ENCS desde el Ejecutivo Federal y la generación óptima de coordinación entre los involucrados[73].

En ese tenor, uno de los objetivos de la Subcomisión de Ciberseguridad fue articular esfuerzos del Ejecutivo Federal y producir criterios universales para las dependencias y entidades de la administración pública federal que contribuirían a la concepción de la ENCS, para dar continuidad a ésta con acciones generales y especiales[74]. Sin embargo, los esfuerzos por llevar a cabo la citada labor quedaron truncados con el cambio de gobierno, debido al nulo seguimiento a la estrategia de referencia.

Asimismo, el Plan Nacional de Desarrollo 2018-2024 (PND 2018-2024) enfocó sus propuestas en fortalecer las capacidades institucionales para alcanzar diversos objetivos estratégicos, de los que destaca establecer un Sistema Nacional de Inteligencia, fortalecer y mantener la seguridad dentro del país y garantizar la defensa exterior, promover el concepto de cultura de Seguridad Nacional, así como mejorar las capacidades tecnológicas de investigación científica en cuanto a seguridad pública, seguridad interior, generación de inteligencia estratégica y procuración de justicia, sin darle auge a la seguridad en el ambiente digital.

Por su parte, el 1 de septiembre de 2020, el Senador Migue Ángel Mancera presentó una iniciativa para expedir una ley que regule el ámbito de ciberseguridad a nivel nacional. Esta propuesta tiene como base la modificación del Código Penal Federal y la Ley General del Sistema Nacional de Seguridad, con miras de normar la seguridad de la información y los ciberdelitos, y sancionarlos a través de una nueva Ley General de Ciberseguridad[75].

---

[73] Poder Ejecutivo Federal. (noviembre, 2017). *Estrategia Nacional Ciberseguridad*. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf.

[74] González, J. M., Albornoz, M. M., & Ramírez, M. S. M. (2019, abril). Ciberseguridad Nacional. *Periódica*, *LIV*(148). https://www.inap.mx/portal/images/pdf/rap148.pdf.

[75] Riquelme, R. (septiembre, 2020). ¿Qué dice la ley de ciberseguridad propuesta por Miguel Ángel Mancera? *El Economista*. Sec. Tecnología. https://www.eleconomista.com.mx/tecnologia/Que-dice-la-ley-de-ciberseguridad-propuesta-por-el-senador-Mancera-20200917-0046.html.

Adicionalmente, el Senador pone en tela de juicio la existencia de una estrategia nacional de ciberseguridad, en virtud de que las cifras en delitos cibernéticos continuaron aumentando, la materia de ciberseguridad no fue contemplada en el PND 2018-2024 y en el Informe de Gobierno de 2020 son mínimas las acciones. En ese sentido, se propone la creación de una estrategia que unifique las líneas de acción de las entidades federativas del país, con sus respectivas áreas de protección de forma homogénea[76].

Cabe mencionar que la citada propuesta se orientó a establecer una tipificación de los delitos del espacio cibernético y a sancionarlos y, de ser aprobada, la Ley General en Ciberseguridad sería reglamentaria del artículo 6 constitucional, relativo a la libertad de expresión, acceso a la información y a las TIC.

En consecuencia, la ENCS quedó rebasada con esta propuesta que busca establecer nuevas labores para reestructurar un marco normativo, actualizar la estrategia nacional de ciberseguridad, definir la política del Estado en la materia en comento por medio de un Centro Nacional de Ciberseguridad, a cargo del Secretario Ejecutivo del Sistema Nacional de seguridad Pública, en colaboración con el Instituto Federal de Telecomunicaciones, así como dar seguimiento al cumplimiento de las acciones de este Centro a través de una Comisión Permanente de Ciberseguridad del Consejo Nacional de Seguridad Pública. Lo anterior, con el enfoque de generar la coordinación efectiva entre instituciones, la protección de infraestructura crítica, la revisión y verificación del cumplimiento de la normatividad que se expida en la materia, entre otros aspectos.

[76] Riquelme, R. (septiembre, 2020). ¿Qué dice la ley de ciberseguridad propuesta por Miguel Ángel Mancera? *El Economista*. Sec. Tecnología. https://www.eleconomista.com.mx/tecnologia/Que-dice-la-ley-de-ciberseguridad-propuesta-por-el-senador-Mancera-20200917-0046.html.

Capítulo 3. La regulación de la ciberseguridad en las telecomunicaciones

Capítulo 3. La regulación de la ciberseguridad en las telecomunicaciones

El número de sectores que se involucran con el entorno digital es cada vez mayor y de manera global, incrementando con ello la interacción entre gobiernos, organizaciones públicas y privadas, fabricantes, particulares, entre otros. Dada esa universalización de tecnologías y la escasa regulación para el advenimiento del desarrollo digital, se tiene una evolución en el nivel de riesgos y vulnerabilidades de las partes involucradas, con herramientas no convencionales, obligando así a dichos sectores a progresar en la resiliencia cibernética[77].

Por lo que respecta al sector de las telecomunicaciones, a partir de la reforma constitucional en materia de telecomunicaciones en 2013, existe un aumento significativo en el despliegue de infraestructura y la convergencia en la prestación de servicios de telecomunicaciones. No pasa desapercibido que la implementación y el despliegue de redes públicas de telecomunicaciones trae consigo requisitos que demandan los usuarios y hasta los propios operadores de los sectores de telecomunicaciones y radiodifusión, siendo uno de éstos la ciberseguridad.

Al respecto, es de señalar que la seguridad cibernética contempla todos los elementos que pudieran traducirse en un riesgo para la integridad digital de un ente en particular, un sistema, una aplicación o infraestructura, lo cual no se limita sólo a la seguridad de la información, misma que se enfoca a los procesos y prácticas organizacionales para resguardar el ámbito empresarial, es decir, el primer concepto en comento abarca prácticas tecnológicas y políticas, desde la defensa y protección, hasta la ofensiva y lo subversivo. En ese orden de ideas, la seguridad cibernética persigue políticas nacionales e internacionales a través de medios informáticos y tecnológicos, más allá de, únicamente, la protección y defensa de la nación y sus infraestructuras de información[78].

---

[77] Estrada, Carlos. (abril, 2019). *Atlas de riesgos para la Seguridad Nacional Cibernética en México*. https://www.inap.mx/portal/images/pdf/rap148.pdf.
[78] Estrada, Carlos. (abril, 2019). *Atlas de riesgos para la Seguridad Nacional Cibernética en México*. https://www.inap.mx/portal/images/pdf/rap148.pdf.

Lo anterior, ha derivado en nuevas formas organizacionales entre el sector público y privado, a efecto de poder anticiparse, responder, reponerse e, incluso, contraatacar ante un incidente en el espacio digital, para proteger la operación continua de dichos sectores.

Por otro lado, se debe tomar en cuenta que los ataques cibernéticos, en cualquiera de sus formas, contra los organismos de gobierno, organizaciones, empresas paraestatales y todos aquellos particulares a quienes se les cede o concesiona operaciones, recursos, servicios, entre otros, para contribuir con el cumplimiento de las atribuciones y/o funciones del Estado, representa diversos riesgos que afectan a toda la sociedad, dada la información a la que tiene acceso el gobierno derivado de las facultades a su cargo.

No obstante, el tema de ciberseguridad no es competencia únicamente de los gobiernos; si bien el Estado plantea las directrices para conducir una sociedad y garantizar el bien común, la seguridad digital abarca diversos aspectos que requieren de la atención de todos los involucrados en ese entorno, como fabricantes, usuarios, prestadores de servicios, técnicos, por mencionar algunos.

En relación con esto, en su artículo *"La seguridad de las telecomunicaciones: nuevos desafíos"*, Horcajo destaca tres planos para situar la seguridad en las telecomunicaciones: físico, lógico y ontológico. Por lo que respecta al primero, resalta la infraestructura activa, pasiva, el flujo de información y los sistemas de operación y gestión asociados, requieren una protección por las normas del acceso y alteración a los que están expuestos y por los contingentes de medios técnicos y humanos de vigilancia para la supervisión y aseguramiento de su disponibilidad y estado[79].

El segundo plano del que habla Horcajo es la protección de las telecomunicaciones por lo que hace a la integridad del tráfico y su contenido, a efecto de evitar sustracciones, destrucciones o alteraciones de éstos. El último plano se enfoca a la seguridad ontológica de las telecomunicaciones, es decir, la

[79] Horcajo, A. (abril, 2020). La seguridad de las telecomunicaciones: nuevos desafíos. *El Economista*. https://www.eleconomista.es/firmas/noticias/10464683/04/20/La-seguridad-de-las-telecomunicaciones-nuevos-desafios.html.

veracidad y certeza de la información que se propaga, garantizando en todo momento los derechos fundamentales[80].

En ese sentido, los ataques cibernéticos pueden ser dirigidos a cualquier individuo, empresa, organización o institución gubernamental, situación que pone en riesgo a la sociedad en general que tiene acceso a los servicios de telecomunicaciones, ya que todo indicio de vulnerabilidad representa una oportunidad para quienes llevan a cabo actos ilícitos, de distintas magnitudes.

Aunado a lo anterior, entre las diversas causas, destaca la falta de cultura sobre ciberseguridad que, en general, es un factor que atenta en contra de diversos sectores que forman parte de la economía, los servicios y productos que requiere una sociedad para su desarrollo óptimo. La inexistencia de un marco normativo, políticas o estrategias cuyo propósito sea la defensa de la información y de los sistemas informáticos, es una de las principales causas que se traduce en efectos negativos y una escasa participación de los involucrados para fortalecer mecanismos de resiliencia cibernética y coadyuvar en las acciones relacionadas con la seguridad digital a nivel nacional.

Por otro lado, la creación de mecanismos que permitan la protección de estructuras estratégicas, cuyos componentes procesen información y códigos, sienta las bases para el desarrollo de estrategias ofensivas, toda vez que, ante las amenazas, la seguridad se conduce con procedimientos de respuesta específicos. En relación con esto, los países desarrollan formas para fortalecer la protección del ciberespacio mediante instrumentos, con una perspectiva militar, ya que, con frecuencia, los ataques tienen intereses bélicos. La consideración de que el ambiente digital es un espacio para dar paso a guerras es a lo que expertos y especialistas han denominado el quinto dominio de guerra, puesto que es una extensión de las acciones convencionales que desarrollan los ejércitos y, representa una nueva forma de ataque-defensa[81].

---

[80] Horcajo, A. (abril, 2020). La seguridad de las telecomunicaciones: nuevos desafíos. *El Economista*. https://www.eleconomista.es/firmas/noticias/10464683/04/20/La-seguridad-de-las-telecomunicaciones-nuevos-desafios.html.

[81] Aguirre, J. (2019). Cambios en la seguridad internacional en el marco de la globalización: el caso de la ciberseguridad y sus desafíos para la Seguridad Nacional de México (2012-2018). UNAM. http://132.248.9.195/ptd2019/septiembre/0795609/Index.html.

3.1 Ciberseguridad en infraestructuras y sistemas de telecomunicaciones

Los ataques en el entorno digital provienen de componentes físicos o lógicos, por ello es importante establecer disposiciones que regulen la ciberseguridad en redes de telecomunicaciones, así como en los sistemas con los cuales operan éstas. En ese sentido las normas básicas y los estándares establecidos a nivel internacional tienen como objetivo evitar, retrasar, detectar y defender a los sistemas e infraestructuras para prevenir riesgos y amenazas.

Por lo que refiere al entorno físico es necesario que se cumplan diversos procedimientos de seguridad tales como la ubicación de equipos, contemplando los perímetros de seguridad para proteger las áreas donde éstos se almacenan, controles para validar que sólo ingrese personal autorizado y monitoreo de dichas entradas; además, asegurar el establecimiento de medidas de protección contra los cortes de energía y fallos en sistemas auxiliares, así como protocolos para el despliegue de cableado, tipos de conexiones físicas permitidas y diseño de redes[82].

Asimismo, se deben definir procesos o políticas de seguridad que generen una efectividad en el entorno físico y en la infraestructura lo cual conlleva el control sobre tiempos sin servicio por incidentes relacionados, número de incidentes ocasionados por fallas o vulnerabilidades en el sistema físico, frecuencia de la revisión y evaluación de riesgos.

Desde el diseño, la planeación e instalación, previo a la entrada en operación de la red de telecomunicaciones, es posible la aplicación de criterios orientados a minimizar los riesgos cibernéticos. Se debe contemplar en el diseño, la instalación y operación de redes y sistemas, el desarrollo de procesos de análisis y gestión de riesgos que permitan identificar las vulnerabilidades, amenazas y riesgos inmersos en el uso, almacenamiento, procesamiento y transmisión de la información; considerando la protección, detección, respuesta y recuperación ante incidentes de

[82] López, A., Escobar, E. (2014). Revisión de las normas de seguridad en las redes y telecomunicaciones.

ciberseguridad que se presenten, apoyando a mantener un espacio digital seguro y resiliente.

Por lo que hace al entorno lógico, es necesario el seguimiento de normas y procedimientos que mantengan la integridad, medio y confiabilidad de la información necesario para la misión de un ente, sin afectar la operatividad de los procesos.

Sobre esto, en los aspectos que se relacionan con la seguridad lógica destacan la validación de datos de entrada y salida, el control de procesamiento interno, la integridad de los mensajes, las políticas de uso de controles criptográficos, gestión de claves, control de software[83].

En virtud de lo anterior, se deben aplicar mecanismos que aseguren que la implementación y operación de las redes de telecomunicaciones se apeguen a los estándares, protocolos, recomendaciones y demás disposiciones aplicables.

Para tal efecto, se requiere de identificación de responsabilidades, procedimientos de supervisión, validación de informes de resolución de incidentes a través de estándares y políticas de seguridad a efectos de mitigar los riesgos, que contemplen la evolución de la materia de que se trata.

Ahora bien, es conviene el uso de normas internacionalmente aceptadas como base para el establecimiento de requisitos de seguridad de las redes de telecomunicaciones a fin de que la prestación y utilización de servicios y mecanismos de seguridad minimicen sus costos de protección por debajo de aquellos que se protegen. Siendo así, es importante buscar la adaptabilidad de la seguridad a los servicios que se protegen, crear mecanismos y servicios de seguridad flexibles, así como definir perfiles de seguridad para cumplir la diversidad de servicios de redes de telecomunicaciones, dado el número de combinaciones de características de seguridad posibles.

3.2 La seguridad en los servicios de telecomunicaciones y la información

[83] López, A., Escobar, E. (2014). Revisión de las normas de seguridad en las redes y telecomunicaciones.

Las afectaciones o interrupciones a los servicios de telecomunicaciones representan graves perjuicios al bienestar, la salud y la seguridad de la sociedad en general; a la integridad de las instituciones públicas e, inclusive, a la seguridad nacional, derivado del incremento del uso de tales servicios; lo cual será cada vez más significativo en la medida que se extiendan y profundicen los procesos de digitalización. Bajo ese tenor, se observa que la amplia extensión y comparativa facilidad de acceso de las redes y sistemas de telecomunicaciones, denotan a éstos como objetivos atractivos para actos criminales.

En particular, resulta relevante la emisión de normas que cubran aspectos de gestión de riesgos en materia de ciberseguridad para la prestación de servicios de telecomunicaciones, con el objetivo de analizar el impacto operacional, así como los riesgos y controles de mitigación. Por lo anterior, deben considerarse elementos tales como la prevención, detección, análisis, notificación, contenidos, erradicación, recuperación y verificación de los respectivos informes.

En seguimiento a esto, cualquier operador de servicios de telecomunicaciones, por ejemplo, debe establecer medidas técnicas y de organización para gestionar los riesgos de ciberseguridad de las redes y sistemas que utiliza para la prestación de servicios de telecomunicaciones a sus usuarios y, también, deben adoptar medidas de gestión que garanticen la disponibilidad, integridad y confidencialidad de las redes y sistemas que utilizan para prestar servicios de telecomunicaciones, tomando en cuenta, al menos, el tipo de organización, la naturaleza y contexto de los servicios prestados, la tecnología disponible y los riesgos asociados.

Del mismo modo, se requiere del diseño, implementación, práctica y evaluación de planes de respuesta ante incidentes que garanticen la continuidad en la prestación de los servicios de telecomunicaciones, con indicadores clave que permitan dar seguimiento a las incidencias, para lo cual, es posible contemplar en disposiciones el uso obligatorio de los citados planes y el registro de reportes de incidencias.

En suma, es necesario establecer los mecanismos de coordinación de acciones orientadas a disminuir ciber-ataques, sus efectos e impactos y la contribución oportuna para la normalización y estabilización de los servicios afectados.

Ahora bien, por lo que respecta al uso de nuevas tecnologías y sistemas, se debe garantizar la operación y seguridad de las partes sensibles de la red y la obligación de resguardar la confidencialidad, disponibilidad y e integridad de la información que se transmita, haciendo uso de las medidas inherentes a la protección de la información.

La seguridad de la información conlleva garantizar los principios de ésta, los cuales se encuentran estrechamente relacionadas con la privacidad. Los conceptos de seguridad de la información y privacidad deben considerarse en forma integral para proteger datos recopilados, almacenados, transmitidos y analizados por los sistemas y redes de cualquier organismo[84]. Tomando en cuenta lo anterior, la normatividad aplicable a la protección de datos debe prevalecer como parte integral de las disposiciones que se emitan en materia de ciberseguridad.

3.3 Participación de instituciones públicas en el ámbito de la ciberseguridad de telecomunicaciones

En el Estado recae la facultad de garantizar 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; para lo cual establecerá condiciones de competencia efectiva en la prestación de dichos servicios[85].

Asimismo, para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias, se regirán por diversos principios y bases, entre los que destaca que

[84] González, J. M., Albornoz, M. M., & Ramírez, M. S. M. (2019, abril). Ciberseguridad Nacional. Periódica, LIV(148). https://www.inap.mx/portal/images/pdf/rap148.pdf.

[85] Artículo 6 de la Constitución Política de los Estados Unidos Mexicanos. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf.

la información relativa a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes[86].

En el sector público, cada órgano tiene funciones y atribuciones específicas, con diferentes enfoques y objetivos encaminados a satisfacer las necesidades de la población a través de un rol estratégico, táctico u operativo, en función a su importancia dentro de una materia en particular. Asimismo, es importante resaltar que, para el ejercicio de sus funciones, los entes públicos hacen uso de redes de telecomunicaciones.

En ese sentido, aquellas instituciones que se involucran en temas económicos, de seguridad pública y nacional, defensa e inteligencia, son claves para mantener la estabilidad en el país, por lo que, las mismas deben contar con una eficiente respuesta operativa ante los actos ilícitos en el ciberespacio a fin de preservar la seguridad cibernética[87].

Partiendo de lo anterior, es relevante señalar que, en cuanto a funciones e investigación en el ámbito de la seguridad del espacio cibernético a nivel nacional, destaca la participación, a manera enunciativa más no limitativa, se mencionan algunas de las acciones que se han desarrollado en el sector público, con motivo del fortalecimiento de la ciberseguridad en las telecomunicaciones y con motivo de sus funciones y/o atribuciones:

- La SHCP, a través de la CNBV, incorpora marcos normativos sobre la seguridad de los sistemas e infraestructura tecnológica de las instituciones de financiamiento colectivo, por medio de la determinación de controles internos que deben cumplir; además de un régimen que procura garantizar la seguridad de la infraestructura tecnológica en que se basan las operaciones, la confidencialidad, integridad y disponibilidad de la información, a cargo de éstas[88].

---

[86] Artículo 6 de la Constitución Política de los Estados Unidos Mexicanos. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf.

[87] Aguirre, J. (2019). Cambios en la seguridad internacional en el marco de la globalización: el caso de la ciberseguridad y sus desafíos para la Seguridad Nacional de México (2012-2018). UNAM. http://132.248.9.195/ptd2019/septiembre/0795609/Index.html.

[88] Comisión Nacional Bancaria y de Valores (2019). RESOLUCIÓN que modifica las Disposiciones de carácter general aplicables a las Instituciones de Tecnología Financiera. https://dof.gob.mx/nota_detalle.php?codigo=5555030&fecha=25/03/2019.

Lo anterior, en virtud de que la operación a través de medios remotos de comunicación electrónica o digital, es el principal canal de comunicación entre las instituciones financieras y sus clientes, por lo que resulta indispensable regular el funcionamiento y uso de equipos, medios electrónicos, ópticos o cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, así como normas pertinentes a la forma en que se autentifican las instituciones y sus clientes, cumpliendo con los principios de neutralidad tecnológica y protección de datos[89].

- Por su parte, la SRE participa en los esfuerzos multilaterales para prevenir y combatir las distintas expresiones de la delincuencia organizada transnacional, fundamentalmente el tráfico ilícito de armas, municiones y componentes, así como en el seguimiento y atención de temas como el avance del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional, entre otros.
- En el ámbito de sus atribuciones, la SEGOB, a través de la Dirección General de Tecnologías de la Información y Comunicaciones, desarrolla políticas y normas en materia de seguridad de la información de observancia general a todas las unidades administrativas y órganos administrativos desconcentrados de la SEGOB, en coordinación con las autoridades competentes y de conformidad con las disposiciones jurídicas aplicables, además, propone modificaciones al marco legal en materia de delitos referentes a la revelación de secretos y acceso ilícito a sistemas y equipos de informática, en coordinación con otras autoridades competentes de la SEGOB o de otras dependencias y entidades de la administración pública federal.
- Por lo que respecta a la SCT, dicha dependencia impulsa acciones relativas a la ciberseguridad para el uso responsable y seguro de los servicios de

[89] Comisión Nacional Bancaria y de Valores (2019). RESOLUCIÓN que modifica las Disposiciones de carácter general aplicables a las Instituciones de Tecnología Financiera. https://dof.gob.mx/nota_detalle.php?codigo=5555030&fecha=25/03/2019.

telecomunicaciones y radiodifusión, incluyendo el servicio de banda ancha e internet; y para el fortalecimiento de la confianza de los usuarios.

- La SE contempló como parte de su Programa Sectorial 2020-2024, fomentar la innovación y el desarrollo económico de los sectores productivos como el primero de sus objetivos prioritarios, del cual destaca la Estrategia 1.1 relativa a impulsar el desarrollo tecnológico en los sectores productivos con la finalidad de disminuir el rezago en innovación. Esto tiene implicaciones directas en nuevos retos para impulsar, a la par, conciencia sobre los riesgos cibernéticos y el desarrollo de marcos legales que garanticen la resiliencia digital en el sector económico.
- Por otro lado, en el Programa Sectorial de Defensa Nacional 2020-2024, SEDENA destaca que uno de los temas relevantes es la seguridad del entorno digital, dado el desarrollo de las tecnologías, así como el vínculo de la información y los datos que maneja dicha dependencia con el uso de las TIC, se puede traducir en vulnerabilidad de no adoptarse las medidas óptimas para la protección. Por tal motivo, SEDENA contempló en la Estrategia Prioritaria 5.6 el "*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*", la cual consta de 6 acciones puntuales, entre las que destacan las relacionadas con el funcionamiento de su Centro de Operaciones del Ciberespacio y la participación de esa dependencia en eventos nacionales e internacionales para mantener la cooperación y coordinación necesaria para el desarrollo de sus funciones[90].
- La SEMAR cuenta con una Unidad de Ciberseguridad que tiene la misión de planear, conducir y ejecutar actividades de seguridad de la información, ciberseguridad y ciberdefensa para la protección de la infraestructura crítica de la Secretaría de Marina–Armada de México por medio del Centro de Ciberdefensa y Ciberseguridad, que realiza actividades de monitoreo y

[90] Secretaría de la Defensa Nacional (2020). PROGRAMA Sectorial de Defensa Nacional 2020-2024. https://dof.gob.mx/nota_detalle.php?codigo=5595529&fecha=25%2F06%2F2020.

detección de la red informática institucional para proporcionar la respuesta a incidentes informáticos de manera oportuna[91].

- Como parte de sus atribuciones, la Guardia Nacional debe realizar investigación para la prevención de los delitos; estudiar, planificar y ejecutar métodos y técnicas de combate a la delincuencia; realizar acciones de vigilancia, identificación, monitoreo y rastreo en la red pública de Internet sobre sitios web, con el fin de prevenir conductas delictivas; y desarrollar, mantener y supervisar fuentes de información en la sociedad que le permitan obtener datos sobre actividades relacionadas con fenómenos delictivos[92].

  La Guardia Nacional está a cargo del CERT-MX, el cual participa en el Foro de Respuestas a Incidentes y Equipos de Seguridad (*FIRST*, por sus siglas en inglés), para fortalecer la cooperación en materia técnica, operativa y de información con entes que tienen la función de salvaguardar la seguridad de otras naciones.

  Dentro de los objetivos del CERT-MX se encuentra impulsar acciones en conjunto con el sector privado para concientizar sobre los efectos de los riesgos cibernéticos, así como el desarrollo de la cultura de prevención del delito cibernético. Además, este centro cuenta con áreas especializadas en prevención e investigación relativas a actos ilícitos del ciberespacio.

- El INAI tiene la atribución de vigilar y verificar que toda persona física o moral de carácter privado que realice tratamiento[93] de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado, en

---

[91] Borredá, J & Valdés, B. (2018, octubre 25). *"La Armada de México contribuye a la protección de las instalaciones estratégicas marítimas del país"* [Entrevista]. https://www.segurilatam.com/entrevistas/la-armada-de-mexico-contribuye-a-la-proteccion-de-las-instalaciones-estrategicas-maritimas-del-pais_20181025.html.

[92] Artículo 9 de la Ley de la Guardia Nacional. https://www.dof.gob.mx/nota_detalle.php?codigo=5561285&fecha=27%2F05%2F2019.

[93] El artículo 3, fracción XVIII, de la Ley General de Protección de Datos Personales en posesión de los Particulares establece la siguiente definición: "*Tratamiento: La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales*".

términos de lo establecido en los artículos 19 y 39 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[94].

- El IFT tiene a su cargo, entre otras, la regulación, promoción y supervisión del uso, aprovechamiento y explotación del espectro radioeléctrico, las redes y la prestación de los servicios de radiodifusión y telecomunicaciones, así como del acceso a infraestructura activa, pasiva y otros insumos esenciales[95].

  Aunado a lo anterior, el IFT debe garantizar la disponibilidad de bandas de frecuencias del espectro radioeléctrico o capacidad de redes para el Ejecutivo Federal, así como de recursos orbitales; esto para seguridad nacional, seguridad pública, conectividad de sitios públicos y cobertura social y demás necesidades, funciones, fines y objetivos a su cargo[96].

  Además, el IFT tiene la atribución de emitir lineamientos de carácter general cuya observancia es obligatoria para los concesionarios y autorizados que prestan el servicio de acceso a Internet, contemplando, entre otras, la preservación de la privacidad de los usuarios y la seguridad de la red.

3.4 Participación de instituciones privadas en el ámbito de la ciberseguridad de telecomunicaciones

El patrón que siguen los vectores de ataque generalmente es el mismo, modificando esencialmente sus procedimientos, tácticas, técnicas y el objetivo final del ataque de espionaje cibernético, con independencia de hacia quiénes sea dirigido dicho ataque. Esto lleva tanto al sector privado como al sector público que requieran de las mismas herramientas o metodologías para contrarrestar riesgos y amenazas y, cada uno, por su parte, tiene niveles de especialización y de acceso a información

[94] Artículos 19 y 39 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. https://www.gob.mx/cms/uploads/attachment/file/123648/Ley_Federal_de_Protecci_n_de_Datos_Personales_en_Posesi_n_de_los.pdf.

[95] Artículo 28 de la Constitución Política de los Estados Unidos Mexicanos. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf.

[96] Artículos 56 y 98 de la Ley Federal de Telecomunicaciones y Radiodifusión. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_200521.pdf.

distintos que, en conjunto, pueden proporcionar resiliencia de alto nivel y mejores resultados en el ámbito de la seguridad cibernética.

Al tratarse de un problema en común, la participación de estos sectores en las acciones para contrarrestarlo, con la finalidad de no comprometer los mecanismos ni las fuentes de información, puede realizarse a través de la compartición de inteligencia, información y demás herramientas que permitan una respuesta eficaz e integral.

De igual forma, la conservación de un entorno cibernético seguro es responsabilidad de todos los involucrados, por lo que, a medida que cada uno asume la parte correspondiente, se desarrolla un ambiente seguro que permite la coordinación, la cooperación y la concientización respectiva. En ese sentido, los esfuerzos no son exclusivos del estado, ya que la intervención de los gobiernos no es suficiente para todo lo que representa la ciber-resiliencia.

Si bien es cierto que el Estado debe proteger la seguridad de la nación, también lo es que la economía, la operación de las redes y el uso de servicios y de tecnologías corresponden a la sociedad en general en la que, especialmente, el sector privado es un participante principal.

En ese sentido, resulta relevante destacar que no siempre las acciones dirigidas a la autorregulación producen resultados efectivos y favorables ante problemáticas generales cuya inacción del gobierno podría implicar daños irreparables al desarrollo y el respeto de los derechos humanos. Por lo que, con independencia de que la protección de los activos del sector privado son responsabilidad de éste, es imprescindible reconocer el momento idóneo en el que deben reformarse y/o emitirse nuevos marcos normativos que protejan y vigilen los intereses de la sociedad en común sin desbalancear o frenar el avance tecnológico.

Al respecto, es de considerar que la perspectiva que se tenga de seguridad digital repercute directamente en la confianza depositada por los involucrados, en consecuencia, es necesario que haya transparencia gubernamental para generar certidumbre, cuidando a la vez que la publicidad no sea motivo de vulnerabilidades.

Por otro lado, tomando en cuenta que las empresas suelen tener grandes afectaciones por fraudes y robos cibernéticos, sobre todo aquellas que son

operadoras de servicios esenciales y de infraestructuras críticas, el sector privado tiende a desarrollar y adoptar tecnologías de la información, antes que el mismo gobierno, convirtiéndose a menudo en pioneros en ese ámbito.

Los ataques dirigidos a las empresas afectan a éstas y a las personas que se relacionan con las mismas, siendo el sistema financiero el más buscado por los *hackers*, dados los datos sensibles que posee y su alta dependencia a los sistemas electrónicos. Aunado a esto, los ataques pueden ser por tiempos prolongados y pueden dispersarse a todos los equipos que conforman la red atacada, creando una mayor vulnerabilidad, por lo que son difíciles de contrarrestar y, para ello, se deben eliminar las debilidades de los sistemas.

Ahora bien, la condición de vida marcada por la pandemia mundial del COVID-19, aumentó el uso de infraestructura digital con un nuevo modelo de riesgos que, anteriormente, las empresas podían controlar desde las redes privadas a las que accedían los trabajadores. La transición a las actividades a distancia se realizó de una manera acelerada e inesperada, reestructurando el entorno y haciendo cada vez más dependiente el desarrollo laboral, económico, educacional, de salud, entre otros, del internet y el uso de las redes de telecomunicaciones. En consecuencia, los ciberataques fluyeron de forma acelerada y se han aprovechado de la falta de coordinación de los entes públicos en distintas jurisdicciones, así como de los líderes empresariales, a través de ataques a infraestructuras críticas, fraudes o robos de datos[97].

Por otro lado, el desarrollo de nuevas tecnologías también acarrea nuevas vulnerabilidades que, en numerosas ocasiones, no son atendidas con la misma prioridad con la que se distribuyen las tecnologías, abriendo paso a más riesgos y menos control en el entorno digital.

En efecto, la inversión en ciberseguridad por parte de las empresas con grandes participaciones en el mercado ha volcado la atención de los criminales cibernéticos hacia las pequeñas y medianas empresas, lo cual es un riesgo aún

[97] Banco Interamericano de Desarrollo, y Organización de los Estados Americanos. (2020). Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

mayor, considerando que estas últimas no cuentan con los recursos financieros y el conocimiento necesario para invertir en ciberseguridad, por lo que no le dan la relevancia que merece la materia en comento[98].

Adicionalmente, el futuro de la economía digital se está centrando en las nuevas tecnologías como la Inteligencia artificial, big data, redes de quinta generación, informática cuántica, IoT, entre otras, que incrementan las oportunidades de ataque y, como se mencionó anteriormente, son el foco central de los nuevos riesgos. Derivado de lo anterior, se requiere que los sectores público y privado colaboren en conjunto para impulsar una cultura sólida que fortalezca la resiliencia cibernética, a través de políticas y estrategias coordinadas.

Dadas las características tan diversas de las empresas, así como el alto costo que representa la ciberseguridad para éstas y a efecto de aumentar los beneficios en lo particular, el sector empresarial realiza concentraciones de empresas y/u organizaciones relacionadas con la materia en comento, lo cual ha permitido dividir las tareas y sumar esfuerzos para madurar la resiliencia en el entorno digital, de formas innovadoras, a bajo costo y con mejores resultados.

Sobre el particular, grupos como el Consejo Nacional de Clústeres de Software y TICs de CANIETI (mxTI), realizan un trabajo coordinado entre los representantes de la industria, el gobierno y las entidades educativas, para el desarrollo de empresas que generan inversión en México[99].

Por su parte, las Organizaciones Sociales Civiles no son entidades ajenas a la problemática que enfrentan habitualmente las sociedades modernas. Al respecto, las organizaciones en comento colaboran en mesas de trabajo, proyectos educacionales, estructuración de planes y programas, entre otros, enfocados a la ciberseguridad en telecomunicaciones.

Finalmente, es importante señalar que el Estado también es apoyado por grupos académicos, los cuales organizan y realizan investigaciones, las cuales,

---

[98] Banco Interamericano de Desarrollo, y Organización de los Estados Americanos. (2020). Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.
[99] Consejo Nacional de Clusters mxTI. https://www.mxti.mx/.

además, disponen de sus espacios, equipos e infraestructura para el desarrollo de pruebas relacionadas con la materia que nos ocupa.

Capítulo 4. Propuesta de una agencia nacional de ciberseguridad

Capítulo 4. Propuesta de una agencia nacional de ciberseguridad

El motivo de requerir la intervención del Estado para garantizar un entorno seguro en las telecomunicaciones, así como la necesidad de sumar esfuerzos enfocados en el cumplimiento del citado objetivo, se avoca a diversas justificaciones identificadas en la presente investigación, de las cuales resaltan las siguientes:

- El incremento y diversidad de riesgos que se relacionan con el ciberespacio.
- La importancia que representan las telecomunicaciones en el desarrollo y crecimiento a nivel nacional.
- La escasa coordinación entre las partes involucradas en el sector de las telecomunicaciones para mejorar y facilitar las acciones encaminadas a la seguridad del ciberespacio.

En ese sentido, se busca alinear acciones hacia objetivos específicos, a través de un organismo que coadyuve en el marco legal aplicable a aspectos de seguridad digital en las telecomunicaciones, proporcione los vínculos entre las partes involucradas y genere en éstas el sentido de responsabilidad conjunta correspondiente con sus intereses particulares y los intereses de la nación.

Al lograr que incrementen los niveles de ciberseguridad en las telecomunicaciones para que, tanto el sector público como el sector privado aceleren las respuestas ante los incidentes cibernéticos y mitiguen el impacto de éstos en dicho sector, es parte de la estrategia para crear confianza en la sociedad respecto de las diversas áreas que involucran las telecomunicaciones, lo que representaría un impacto positivo para México.

De igual forma, la ciberseguridad de las telecomunicaciones también influye de manera positiva en la seguridad en general y en el buen funcionamiento de servicios esenciales, que son medulares para la vida digna de los habitantes de este país y están basados en este sector.

Asimismo, resulta importante incentivar el uso de servicios TIC de última generación que hagan más sostenible la distribución de los servicios a los usuarios,

reemplazando infraestructura ineficiente y menos segura, a efecto de reducir el costo que representan los ciberataques a las infraestructuras críticas.

La creación de un ente público encargado de la coordinación en la materia de ciberseguridad de las telecomunicaciones no tiene como propósito generar mayores cargas administrativas. En oposición a esto, las reglas podrían minimizar y balancear las tareas que cada ente, público o privado, tiene que desarrollar, implementar y conservar, para mantener un entorno digital seguro. En ese orden de ideas, la intención es identificar una metodología que funcione para cada una de las partes involucradas, disminuyendo el costo y conociendo las medidas mínimas para garantizar la ciberseguridad, entre otros aspectos.

Ahora bien, otro aspecto a considerar es que, si bien, de la evaluación y revisión a las recomendaciones en materia de ciberseguridad, se debe contar con un órgano con el mayor nivel de decisión, alto presupuesto y nula influencia de los involucrados para la toma de decisiones, es importante analizar el grado de madurez en la regulación que atraviesa el país.

Al respecto, la ENCS estableció que el seguimiento y la coordinación de ésta estaría a cargo de la Subcomisión de Ciberseguridad. Sin embargo, del análisis realizado a la ENCS por diversas organizaciones se ha concluido que el organismo encargado de la ciberseguridad en México debe desempeñar funciones más relevantes como determinar y coordinar la política en ciberseguridad en los ámbitos económico, social y político, así como gestionar los alcances y la adopción de una estrategia a nivel federal, por lo que también debe evaluar la legislación aplicable en la materia que nos ocupa.

Por su parte, numerosos gobiernos han comenzado a evaluar si sus autoridades reguladoras actuales están debidamente equipadas para manejar los problemas relacionados con un entorno digital. Aunque estas discusiones generalmente se encuentran en las primeras etapas, el análisis implica evaluar si se requiere un nuevo organismo regulador independiente dedicado exclusivamente a cuestiones digitales, si ampliar las funciones y el mandato de un regulador existente de telecomunicaciones y las TIC, y/o si el mejor modelo es un TIC

regulador con otras autoridades gubernamentales responsables de la protección del consumidor, la privacidad y la ciberseguridad, respectivamente[100].

Los reguladores eficaces se aseguran de que sus decisiones sean apropiadas y se alcancen de la manera más objetiva posible para promover la certeza regulatoria y, al mismo tiempo, minimizar los desafíos legales. Involucrar a toda la gama de partes interesadas a través de consultas abiertas es particularmente importante cuando se adopta la regulación digital, tomando en cuenta el alcance que tiene la materia en relación con afectaciones.

De esta manera, resulta interesante observar que en México se tiene un órgano autónomo regulador de los sectores de telecomunicaciones y, a efecto de que amplíe sus funciones, es necesario modificar las mismas a través de una reforma constitucional, lo cual puede resultar en la oposición de aquellos que no comprenden el sentido y la importancia de la ciberseguridad en las telecomunicaciones, situación que retrasaría las acciones que deben realizarse a corto plazo, dado el impacto que representa la escaza resiliencia para una nación.

Por otro lado, en la figura de un gobierno que puede controlar áreas que competen el intercambio de información y colaboración conjunta, se ha demostrado que se tiene mayor confianza en organismos que provienen desde la administración pública centralizada. En ese sentido, promulgar una ley en la materia que nos ocupa, desde la que emane un órgano desconcentrado del ente público encargado de la seguridad del espacio de las telecomunicaciones, podría generar mayores expectativas de eficiencia, contrario a que si recaen mayores funciones en un órgano autónomo constitucional.

4.1 Consideraciones sobre una agencia nacional de ciberseguridad

El Estado mexicano debe tener claridad en relación con el aprovechamiento del entorno digital abierto para el crecimiento económico y social por medio de la

[100] UIT. (2020). Digital Regulation Handbook Conference Edition. 218.

reducción a nivel general de riesgo de seguridad del ciberespacio al interior y exterior de la nación, sobre todo para el sector de las telecomunicaciones.

En ese orden de ideas, la ENCS señala en uno de sus tres ejes rectores el enfoque basado en gestión de riesgos, mediante la prevención y corrección. Es necesario concientizar que el riesgo evoluciona constantemente de acuerdo con las características propias del entorno digital y la interacción con éste, por lo que los dirigentes del Estado deben estar comprometidos en la reducción de los riesgos y el aumento de la resiliencia mediante evaluaciones frecuentes de riesgos a nivel nacional y sectorial, adoptando procesos, medidas y políticas apropiadas para la gestión de los riesgos identificados[101].

En relación con esto último, las políticas de seguridad deben responder a un análisis de las amenazas que podrían comprometer la seguridad de los activos críticos y el impacto y probabilidad de que ocurra un evento no deseado, por medio de la relación de los aspectos sensibles, físicos y lógicos que contrarrestan la ciberseguridad en las telecomunicaciones. Una vez identificados los sistemas, infraestructuras y áreas fundamentales de dicho sector a proteger, éstos deben ser ponderados con un valor específico para calcular la probabilidad de que sea vulnerado, lo cual determina los activos más críticos y, en consecuencia, cuáles deben ser los controles que se deben implementar para cada uno de ellos[102].

De esta manera, previo a definir una política, resulta indispensable conocer qué se quiere proteger, contra quién y cómo se dará esa protección. Asimismo, es necesario definir la directriz que adoptará el Estado con respecto a las políticas de seguridad en las telecomunicaciones y los elementos que deben ser considerados, tales como el alcance de la política, sus objetivos, la responsabilidad compartida, los requerimientos para su aplicación y las consecuencias que derivan del comportamiento ilícito en el entorno digital, teniendo en cuenta en todo momento que las políticas por sí mismas no garantizan un ciberespacio de las

---

[101] Hathaway, M. (2018). *Gestión del Riesgo Cibernético Nacional*. OEA. https://www.oas.org/es/sms/cicte/ESPcyberrisk.pdf.

[102] Díaz, P. & Reyes, R. (2015). Buenas prácticas de seguridad alineadas al ISO/IEC 27002 para el aseguramiento de equipos Linux-Debian pertenecientes a un CERT. UNAM. http://132.248.9.195/ptd2015/mayo/0729528/0729528.pdf.

telecomunicaciones seguro, para esto, se deben emplear mecanismos en lo particular y a nivel general que coadyuven al fin en sí[103].

La ENCS señala en su eje transversal "*7. Marco jurídico y autorregulación*" la adecuación al marco jurídico nacional, así como el establecimiento de mecanismos de autorregulación que permitan el desarrollo del entorno digital y prevengan riesgos y amenazas, para lo cual, se contempla la modificación o armonización legislativa enfocada a la sociedad de la información, entre otros.

Ahora bien, asociaciones como la ANUIES y diversos organismos, han manifestado su postura afirmando que las políticas de ciberseguridad deben ser dirigidas por una autoridad nacional de seguridad cibernética competente y dedicada, que trabaje de manera vertical con los principales sectores, con el más alto nivel de gobierno para dirigir, coordinar acciones y monitorear la implementación de una estrategia nacional de ciberseguridad, responsable de las deficiencias y los resultados favorables que se obtengan en la materia. Lo anterior, en virtud de que la seguridad digital es transversal a las distintas áreas que abordan problemáticas y enfoques diversos, por lo que es importante garantizar que la autoridad competente tenga la autoridad posicional, la responsabilidad y el empoderamiento suficiente, tal que permita involucrar y dirigir a todas las partes interesadas según sea necesario.

Por tal motivo, el ente encargado de la ciberseguridad de las telecomunicaciones debe contemplar entre sus atribuciones el planear, ejecutar y auxiliar para el cumplimiento de la estrategia nacional de ciberseguridad, así como la normatividad aplicable a la materia. Además, el organismo debe orientar la política nacional de ciberseguridad en el sector en comento, evaluar el mercado, el entorno, los actores y el ecosistema en general, definir los protocolos de actuación previo, durante y después de un ciberataque, estar alineado a las políticas del Estado y trabajar en coordinación con los demás sectores[104].

---

[103] Díaz, P. & Reyes, R. (2015). Buenas prácticas de seguridad alineadas al ISO/IEC 27002 para el aseguramiento de equipos Linux-Debian pertenecientes a un CERT. UNAM. http://132.248.9.195/ptd2015/mayo/0729528/0729528.pdf.

[104] Guel, J. (2019). CiberSeguridad MX 2020. Encuentro ANUIES-TIC presentado en Encuentro ANUIES-TIC.

Al respecto, los dirigentes de los gobiernos deben tener claro el panorama del riesgo en el entorno digital y las amenazas a sus infraestructuras en red, mismas que deben ser delineadas en las estrategias de ciberseguridad. También, se debe trabajar con las partes interesadas para planificar metodologías de defensa y asignar los recursos económicos y humanos necesarios para el desarrollo de la labor en comento.

No se omite mencionar que la conservación de un ambiente digital seguro en el ámbito de las telecomunicaciones es tarea de todos los que participan para su uso, desde fabricantes de infraestructura, desarrolladores de software, líderes gubernamentales hasta la sociedad en general, por lo que el valor que se dé a la ciberseguridad en dicho sector estará en función de la concientización pública, la educación, la capacitación, la comprensión del impacto en diversos aspectos, el desarrollo de habilidades y el empoderamiento de quienes formen parte de la solución sobre la construcción de una cultura con conocimiento sobre la seguridad del ciberespacio en las telecomunicaciones.

El tercer eje transversal de la ENCS está enfocado a la coordinación y colaboración para la consolidación de un ecosistema de ciberseguridad y la obtención de la capacidad resiliente necesaria para el establecimiento de mecanismos preventivos, proactivos y reactivos que proporcionen confianza y tranquilidad a la sociedad en el uso de las TIC y su aprovechamiento[105].

Por lo tanto, se requiere identificar, priorizar y enfocar los recursos en activos de gran valor y sistemas de alto impacto que demanden mayores niveles de protección, comprender las vulnerabilidades de éstos y priorizar las medidas de seguridad apropiadas y acordes con el nivel de riesgo en cada caso. Aunado a esto, se deben desarrollar los marcos legales regulatorios apropiados para proteger a los ciudadanos contra los ciberdelitos, la interrupción de los servicios de telecomunicaciones y la destrucción de la propiedad; hacer uso de herramientas como la legislación, normas, estándares, disposiciones técnicas, incentivos de mercado, esquemas de cumplimiento voluntarios y demás iniciativas que aumenten

[105] Poder Ejecutivo Federal. (noviembre, 2017). *Estrategia Nacional Ciberseguridad*. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf.

y garanticen la confianza y la seguridad del uso de las TIC, igualmente corregir la deficiencia de productos, procesos y servicios aplicados a la materia que nos ocupa[106].

Cabe destacar que se debe contemplar el monitoreo continuo al sector de las telecomunicaciones y del uso de las más recientes tecnologías para detectar, contrarrestar y resguardar las amenazas, así como desarrollar las capacidades nacionales que se requieran para mejorar la preparación, planificación, respuesta y recuperación ante los riesgos y amenazas significativas de seguridad cibernética que se deriven[107].

Por otro lado, el apoyarse en la política internacional para el desarrollo de estándares de seguridad global y la promoción de acuerdos multilaterales, puede representar una mejora en la seguridad general, la confiabilidad y la resiliencia de las redes interoperables. La propia ENCS consideró el desarrollo de estándares y criterios técnicos y de normalización en materia de ciberseguridad, a efecto de homologar y aplicar las mejores prácticas y procesos en el uso y adopción de las TIC en un ambiente digital seguro, en su quinto eje transversal.

Finalmente, la anticipación a los avances tecnológicos que se pretenden implementar en un futuro y la evaluación de cómo éstos pueden introducir nuevas vulnerabilidades para la nación, o bien, cómo pueden representar dichos avances nuevas herramientas para conservar la seguridad, fiabilidad y resiliencia en los activos de próximas generaciones, dará un panorama abierto al cambio y la actualización del cuidado en la seguridad digital[108].

Así, la ENCS señala en el apartado de alcance y futuro que ésta parte de la idea de evolucionar de acuerdo con las necesidades de la sociedad en relación con la ciberseguridad, a fin de tener la capacidad de adaptación y mejora continua respecto de los retos, riesgos, amenazas y vulnerabilidades implícitas en las tecnologías venideras y las nuevas dinámicas de la sociedad.

---

[106] Hathaway, M. (2018). *Gestión del Riesgo Cibernético Nacional*. OEA. https://www.oas.org/es/sms/cicte/ESPcyberrisk.pdf.

[107] Hathaway, M. (2018). *Gestión del Riesgo Cibernético Nacional*. OEA. https://www.oas.org/es/sms/cicte/ESPcyberrisk.pdf.

[108] Hathaway, M. (2018). *Gestión del Riesgo Cibernético Nacional*. OEA. https://www.oas.org/es/sms/cicte/ESPcyberrisk.pdf.

Para la implementación de las acciones destacadas anteriormente, hay que tener claridad de las funciones, responsabilidades, procesos, derechos de decisión y mecanismos de rendición de cuentas. Estas actividades conllevan también la asignación de recursos dedicados y apropiados para su implementación, por lo que la búsqueda de mecanismos para el financiamiento es esencial, a efecto de disminuir el costo que representa la ciberseguridad de las telecomunicaciones para la nación o que la insuficiencia de recursos evite el fortalecimiento de la resiliencia para el país y el ejercicio de las funciones del Estado.

Por último, es de señalar que los riesgos cibernéticos no pueden ser eliminados, en consecuencia, deben minimizarse a través de la gestión de riesgos, lo cual deriva en evaluaciones y preparación continuas para tener altos niveles de protección, corregir deficiencias y comprender cómo definir y priorizar las medidas de seguridad en función de las vulnerabilidades identificadas de acuerdo con los sectores analizados.

En seguimiento a lo anterior, tomando en cuenta el análisis realizado a lo largo de la presente investigación, se presentan, de manera enunciativa más no limitativa, algunas de las características principales que debe observarse para la creación de un organismo que encabece la coordinación y colaboración en materia de ciberseguridad de las telecomunicaciones, a nivel nacional.

4.2 Forma de organización

Órgano administrativo desconcentrado de la Secretaría de Seguridad y Protección Ciudadana, con autonomía técnica, operativa, de gasto y de gestión, que tiene por objeto investigar, estudiar, desarrollar, aplicar y coordinar tecnologías para la prevención y mitigación de delitos cibernéticos y sus efectos, promover la capacitación profesional y técnica sobre la materia, así como apoyar la difusión de medidas preventivas para conservar un ambiente digital seguro del sector de las telecomunicaciones.

Para efecto de lo anterior, el organismo estará encargado de la coordinación y cooperación de los entes públicos y privados en materia de ciberseguridad, la revisión y elaboración de recomendaciones, con autonomía plena para la emisión

de disposiciones técnicas, lineamientos y acuerdos que le permitan el ejercicio de sus funciones y el cumplimiento de su objeto.

Asimismo, el organismo será encargado de establecer informes técnicos dirigidos a los entes, públicos y privados, con el objetivo de abordar los problemas relacionados a la ciberseguridad de las telecomunicaciones y alinear las acciones de los involucrados a la estrategia nacional de ciberseguridad y las disposiciones vigentes en la materia; así como emitir recomendaciones generales de información y gestión de riesgos para dicho sector y demás sectores relacionados a éste.

4.3 Marco legal aplicable

El organismo deberá contar con disposiciones legales que contemplen concretar la aplicación de la estrategia nacional de ciberseguridad, así como las políticas adecuadas para lograr y mantener un alto nivel de ciberseguridad.

Aunado a lo anterior, se requiere de un marco que permita la interacción y colaboración entre las partes involucradas ante las vulnerabilidades y los posibles ataques en el entorno digital. Por su parte, cada ente debe implementar una gestión de riesgos, mediante la designación de equipos especializados y/o personal capacitado responsable de la administración de incidentes cibernéticos, para lo cual es necesario el acompañamiento de especificaciones técnicas, recomendaciones, informes, entre otras disposiciones que emita el organismo coordinador.

4.3.1 Órgano de decisión

Tomando en cuenta los objetivos a los que se encuentra vinculado el organismo, se pretende contar con un órgano decisivo neutral y transparente, por lo que la dirección del organismo puede recaer en un titular con experiencia técnica y el apoyo de las direcciones generales encargadas de propósitos particulares en la materia, ya que sería favorable contar con las opiniones de expertos que persigan los intereses del Estado y la sociedad en conjunto.

El titular del organismo podría ser designado a propuesta del Ejecutivo Federal con la ratificación de la Cámara de Senadores por el voto de las dos terceras partes de los miembros presentes. Para tal efecto, y como se realiza en este tipo de órganos, el titular deberá ser ciudadano mexicano, tener título profesional y haberse

desempeñado en forma destacada en cuestiones profesionales, de servicio público, o académicas sustancialmente relacionadas con las materias de ciberseguridad y telecomunicaciones. Además, se deberá acreditar, en los términos de la legislación aplicable, los conocimientos técnicos necesarios para el ejercicio del cargo.

4.3.2 Autonomía administrativa

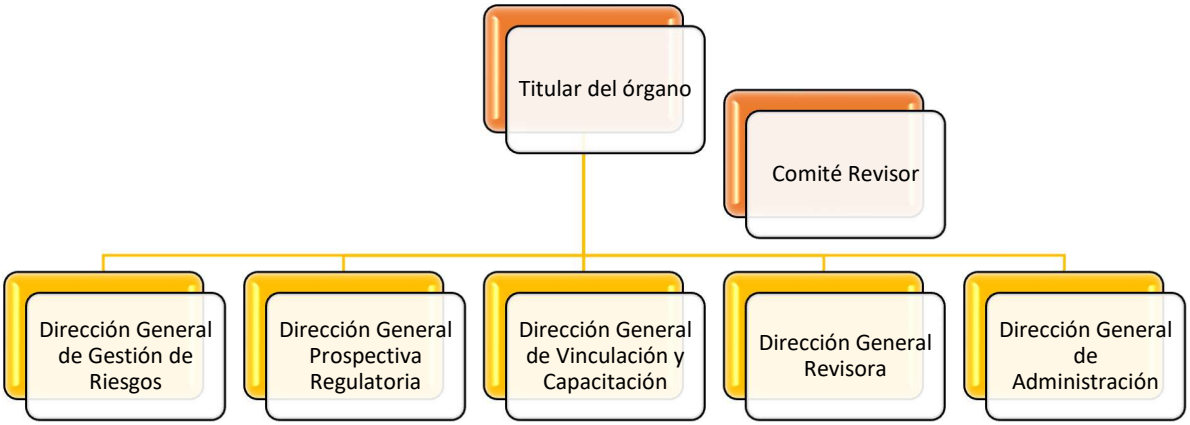
El ejercicio de las funciones del titular del órgano podría optar por un periodo de cuatro años, renovable por una sola ocasión, tomando como referencia la experiencia de órganos de la administración pública federal y los autónomos. Dichas funciones sólo pueden ser terminadas en caso de renuncia, por causa grave debidamente justificada o por una incapacidad definitiva que impida la continuación de su mandato.

Las relaciones de trabajo entre el órgano y sus trabajadores deben ser regulada por la Ley Federal de los Trabajadores al Servicio del Estado, reglamentaria del Apartado B) del artículo 123 Constitucional, con la finalidad de alinearse a las demás dependencias del gobierno.

En otro orden de ideas, las facultades y estructura orgánica del organismo deben estar especificadas en el reglamento interior correspondiente, emitido por la Secretaría de Seguridad y Protección Ciudadana y publicado en el Diario Oficial de la Federación, a fin de que tenga validez jurídica.

Finalmente, el titular del órgano será el responsable de la administración de los gastos.

4.3.3 Organigrama



Fuente: Elaboración propia

En relación con las atribuciones conferidas a cada Dirección General, éstas pueden ir en función de los objetivos establecidos para el órgano propuesto, siendo indispensables las siguientes:

a) **Dirección General de Gestión de Riesgos.** Colaborará con las áreas a cargo de la gestión de riesgos en los organismos gubernamentales y el sector privado, a efecto de identificar acciones que garanticen un entorno digital seguro de las telecomunicaciones.

b) **Dirección General de Vinculación y Capacitación.** Estará a cargo de la vinculación con el sector privado y, en colaboración con dicho sector, de la implementación de áreas de capacitación a los usuarios y audiencias.

c) **Dirección General de Prospectiva Regulatoria.** Encargada de emitir las propuestas de estándares, normas, informes técnicos, recomendaciones generales y cualquier disposición aplicable en materia de ciberseguridad, en coordinación con las Direcciones Generales del órgano. Adicionalmente, esta unidad administrativa estará vinculada con la cooperación internacional.

d) **Dirección General Revisora.** Estará a cargo de la revisión del cumplimiento de los entes sujetos a la implementación a lo establecido en las disposiciones emitidas por el órgano, así como de poner a

consideración del titular la emisión de las recomendaciones que se deriven de las revisiones.

e) **Dirección General de Administración.** Encargada de la administración presupuestal, de recursos humanos y del financiamiento para el cumplimiento de las atribuciones conferidas al órgano.

f) **Comité Revisor.** Su función es asegurar que el organismo lleva a cabo sus tareas en apego a lo señalado en la normatividad vigente.

4.3.4 Capacidad regulatoria

El órgano tendrá facultades para coordinar y generar la cooperación entre particulares y el Estado en materia de ciberseguridad de las telecomunicaciones. Asimismo, tendrá la cooperación de los diversos organismos públicos para el cumplimiento de sus atribuciones, podrá ser consultado en aspectos relacionados a su propósito, a efecto de desarrollar la política de seguridad digital en el sector. Emitirá informes técnicos, recomendaciones generales, estándares, normas, entre otros; coadyuvará con las instituciones públicas y privadas para el seguimiento de dicha reglamentación y tendrá facultades para revisar y emitir las recomendaciones pertinentes en el ámbito de su aplicación.

4.3.5 Cooperación

La cooperación es el elemento principal que debe tener el organismo, ya que la seguridad digital es responsabilidad de quienes conforman el ciberespacio y hacen uso de las telecomunicaciones, por lo que la labor fundamental es desarrollar un grupo de cooperación que facilite el intercambio de información para generar confianza y seguridad entre los entes y la sociedad.

Adicionalmente, se deben implementar reglas claras para este intercambio de información, así como promover la cooperación operativa como respuesta rápida y eficaz. En ese orden de ideas, el organismo debe establecer disposiciones que favorezcan las relaciones entre los actores y garanticen el intercambio regular de información.

Además, el organismo debe contar con un comité que revise continuamente la normatividad emitida para asegurar la eficacia de las políticas de ciberseguridad

del sector e impulse la actualización correspondiente cuando el funcionamiento de dicha cooperación así lo exija.

4.3.6 Gestión de riesgos

El organismo debe encaminar a los entes para la adopción de medidas de gestión de riesgos, así como para impulsar la formación y concientización relacionada con ciberseguridad en las telecomunicaciones.

Para efecto de lo anterior, es necesario el establecimiento de parámetros que garanticen que los entes, en el ámbito de su aplicación, estén apegados a las medidas técnicas y organizativas adecuadas y proporcionales de gestión de riesgos, a la seguridad de las redes, los sistemas de información e, inclusive, los colaboradores y usuarios. Al respecto, se deben estructurar obligaciones y/o recomendaciones relativas a la notificación de incidentes de ciberseguridad en función con el impacto que representan los mismos y los servicios que se prestan.

La recopilación y seguimiento de los informes que proporcionen los entes permitirá que el organismo realice ajustes en la normatividad vigente, a efecto de fortalecer la cooperación, la responsabilidad del sector, a nivel nacional.

4.3.7 Ámbito de competencias

Si bien, cada ente público tiene sus propias atribuciones en diversos aspectos relacionados con el ámbito de la ciberseguridad digital, se requiere que éstas se encuentren alineadas a un mismo fin que sea consistente con la estrategia nacional de ciberseguridad y tenga como eje principal la conservación de la seguridad en el sector de las telecomunicaciones.

Por tal motivo, el ámbito de atribución que debe tener el organismo no debe conjuntar las atribuciones en comento con aquellas superiores a los demás entes. Sobre el particular, cabe destacar que el objetivo principal es la cooperación y coordinación entre las partes involucradas. En ese orden de ideas, la implementación de un órgano que tenga la formación técnica en el ámbito de la ciberseguridad del sector podría conducir, apoyar y colaborar con los demás entes a que éstos ejerzan sus atribuciones en el ámbito de su competencia y refuercen

los vacíos del marco jurídico, con el conocimiento debido en la materia que nos ocupa.

Por otro lado, la sobrerregulación a la iniciativa privada puede restringir la participación en los mercados, por lo que debe tenerse en cuenta que el organismo debe generar mecanismos para coadyuvar con los entes sin generar mayores cargas administrativas ni imponerse por encima de las atribuciones de otros organismos.

En conclusión, el ámbito de atribución del organismo estaría limitado en función de su aplicación con respecto a otros entes y tendría más un sentido de coadyuvar para que el Estado ejerza sus funciones.

4.3.8 Revisión

El organismo como autoridad revisora permitirá orientar, encaminar y coadyuvar con los entes que no cumplan con las disposiciones mínimas para garantizar un entorno digital seguro de las telecomunicaciones. Además, el monitoreo de las acciones ejecutadas destacaría los vacíos legales o la sobrerregulación que exista, por lo que esto impulsaría la mejora continua del marco legal aplicable.

Una revisión ex ante para entidades esenciales y ex post para entidades importantes, requiriendo este último que las autoridades competentes tomen medidas cuando se les proporcionen evidencia o indicación de que una entidad importante no cumple con los requisitos mínimos de seguridad y notificación de incidentes.

Considerando las implicaciones que representa la omisión de implementación de mecanismos que garanticen la seguridad del entorno digital, el órgano debe elaborar recomendaciones respecto del seguimiento y apego a la normatividad vigente, en el ámbito de su competencia.

4.3.9 Rendición de cuentas

La transparencia del organismo se debe garantizar a través de la rendición de cuentas, haciendo uso de informes de actividades de forma periódica sobre el ejercicio de sus funciones y sus recursos, dando publicidad a los mismos.

Adicionalmente, la información relacionada con dichas actividades debe estar disponible ante la solicitud de cualquier ente público, para el ejercicio de sus funciones.

Conclusiones

Conclusiones

De la investigación realizada con el presente trabajo, queda en evidencia que, la Estrategia Nacional de Ciberseguridad publicada en 2017, careció del seguimiento idóneo para aterrizar sus objetivos. Aunado a esto, si bien es cierto que se estableció la Subcomisión de Ciberseguridad para dar seguimiento a la citada Estrategia, es claro que sus acciones quedaron truncadas una vez que culminó el Plan Nacional de Desarrollo 2013-2018. Lo anterior, en virtud de que el Plan Nacional de Desarrollo 2019-2024 no contempla objetivos vinculados a la operación de dicha Subcomisión, ni marcó la pauta para el impulso de actividades relacionadas con la seguridad del ciberespacio.

Asimismo, la escasa o nula regulación en la materia que nos ocupa es una ventana de oportunidad que aprovechan los criminales en el entorno digital, siendo éste un medio para la ejecución de delitos, el cual debe ser protegido con igual o mayores herramientas con las que se protege un país vía aérea, terrestre y marítima.

De igual forma, los derechos fundamentales de acceso a las TIC y los servicios de telecomunicaciones y radiodifusión, incluyendo banda ancha e Internet, y la libertad de expresión que contemplan los artículos 6º y 7º constitucionales, respectivamente, deben ser garantizados en condiciones de competencia, calidad, pluralidad, cobertura universal, interconexión, convergencia, continuidad, acceso libre y sin interferencias arbitrarias, de conformidad con lo establecido en los artículos antes mencionados. No obstante, garantizar estos derechos fundamentales sin que el Estado cuente con una resiliencia madura en el espacio cibernético, representa un riesgo aún mayor, puesto que se tendría una sociedad completamente conectada con el riesgo latente de que sea víctima de los ataques originados en el entorno digital.

Además, las nuevas tecnologías y la mejora de aquellas existentes conllevan, a su vez, la evolución de riesgos y ataques a la ciberseguridad de las

telecomunicaciones, por lo que la actualización de protocolos que fortalezcan ésta, así como la implementación de acciones que contrarresten dichos riesgos, resulta de gran importancia para permitir el desarrollo en diversos sectores de un país, puesto que, en función del nivel de resiliencia del Estado, hay mayor confianza para la introducción de competidores en los mercados.

Por otra parte, la inacción de las autoridades ante los ataques cibernéticos disminuye la confianza de los usuarios y las audiencias que utilizan las telecomunicaciones para proveer servicios e incrementa el número de delitos que se comenten por este medio. Para contrarrestar esto, se requiere de la implementación de políticas de autentificación, clasificación de la información, controles para la separación entre los procesos de sistemas y los datos a los cuales se les da tratamiento. Al respecto, el establecimiento de normatividad que certifique, entre otros, sitios cibernéticos y empresas dedicadas a la seguridad digital en las telecomunicaciones, así como la emisión de legislación para la educación en ciberseguridad, son de los grandes retos para el estado mexicano que deben abatirse a la brevedad.

En relación con lo anterior, el nivel de independencia y de protección que tuvo la Subcomisión de Ciberseguridad para llevar a cabo los fines con los cuales fue creada, han sido insuficientes para atender las problemáticas de ciberseguridad señaladas en el presente trabajo de investigación, ya que no ha cobrado la debida relevancia dentro de las políticas y los Planes emitidos por el gobierno actual para su operación. Por lo anterior, se concluye que, brindar independencia administrativa para la coordinación de la ciberseguridad en las telecomunicaciones facilitaría la aplicación de normatividad que fortalezca la resiliencia de México ante los ataques cibernéticos que sufre este sector.

Así, el éxito de un organismo que coordine la implementación estrategia nacional de ciberseguridad en las telecomunicaciones en México dependerá, en gran medida, de las características con que sea creado. Por su parte, la propuesta que se aborda en el presente trabajo contempla la creación de un órgano que surja

de la emisión de una ley, considerando la madurez de la regulación que actualmente se tiene y que es una acción que debe ejecutarse en el corto plazo, toda vez que el riesgo de que no exista la debida resiliencia por parte de los que conforman el sector de telecomunicaciones, es cada vez mayor. Por lo que, de proponerse la creación de un órgano constitucional autónomo, como varias recomendaciones en materia de ciberseguridad lo han señalado, implicaría mayor tiempo de planeación y dificultades para su aprobación en relación con el poder que se confiere a ese órgano, lo cual repercute en afectaciones inmediatas en el sector de telecomunicaciones hasta en tanto no se cree un órgano.

Por otro lado, se requiere generar confianza de la necesidad de la existencia de los organismos, así como de las atribuciones que le pueden ser conferidas en función de los resultados que obtiene y, con base en las deficiencias detectadas, aquello que permitiría que éste desarrollara su objeto de la manera óptima. En ese sentido, si se creara inicialmente una agencia autónoma constitucional o un órgano descentralizado con cierta autonomía de decisión, en una materia que, hoy en día, no se ha identificado como prioritaria para el Estado, causaría reticencia y hasta poca credibilidad. En tal virtud, un órgano desconcentrado, puede dar la certeza jurídica que se requiere, a corto plazo y con mayor aceptación.

Ahora, la parte medular de la creación de un organismo en ciberseguridad recae en la urgente colaboración y coordinación que debe existir en la materia con una comprensión multidimensional e internacional, razón por la cual se debe enfocar a dicho organismo en generar metodologías y herramientas orientadas al logro de un objetivo en común, a través de la emisión de informes técnicos, recomendaciones generales, revisiones a las disposiciones, normas, participación internacional, entre otras, que garanticen el uso seguro del ambiente digital de las telecomunicaciones.

En la medida en que el Estado asegure y garantice la seguridad en el entorno digital de las telecomunicaciones, se tendrá mejoras considerables en los sectores relacionados, previendo un aumento en el uso del internet en México, disminución

en la brecha digital y el incremento de personas que emplean las TIC de forma cotidiana, protección a las redes públicas de telecomunicaciones, por mencionar algunos aspectos, lo cual estaría alineado con lo establecido en el artículo 28 constitucional, respecto de garantizar 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.

Bibliografía

Abusaid, D., Cristofori, A., Fernández, R., & Waisser, S. (2018). *Perspectiva de ciberseguridad en México*. COMEXI y McKinsey & Company. https://consejomexicano.org/multimedia/1528987628-817.pdf

Aguirre, A. A. (2017). *Ciberseguridad en Infraestructuras Críticas de Información* [Universidad de Buenos Aires]. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1115_AguirrePonceAA.pdf

Aguirre, J. L. (2019). *Cambios en la seguridad internacional en el marco de la globalización: El caso de la ciberseguridad y sus desafíos para la Seguridad Nacional de México (2012-2018)* [UNAM]. http://132.248.9.195/ptd2019/septiembre/0795609/Index.html

Arreola, A. (2019). *Ciberseguridad: ¿Por qué es importante para todos?* Siglo XXI Editores México.

Asociación Mexicana de la Industria de Tecnologías de Información, A.C., AMITI. (2018). *Ciber-segurizate. Guía para crear un entorno digital más seguro para tu empresa y para ti* (Ciber-segurizate, p. 48). https://guias.amiti.org.mx/guias/Ciber-segurizate.pdf

--------(2019). *Informe Anual de Actividades AMITI. 2019* (p. 43). https://amiti.org.mx/wp-content/uploads/2020/05/Informe-de-Actividades-AMITI-2019.pdf

Banco Interamericano de Desarrollo, & Organización de los Estados Americanos. (2020). *Reporte Ciberseguridad 2020: Riesgos, avances y el camino a*

seguir en América Latina y el Caribe (p. 204). https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Bustamante, J. (2001). *Hacia la cuarta generación de derechos humanos: Repensando la condición humana en la sociedad tecnológica*. *1*, 24.

Chávez, C., & González, P. (2018). *LAS ORGANIZACIONES DE LA SOCIEDAD CIVIL EN MÉXICO. Hacia una reforma de la LFFAROSC*. Instituto Belisario Domínguez y Senado de la República. https://www.comecso.com/wp-content/uploads/2018/12/Cuaderno_LFFAROSC_IBD.pdf

Departamento de Seguridad Nacional. (2020, diciembre 17). *Nuevo paquete de ciberseguridad de la Unión Europea*. https://www.dsn.gob.es/es/actualidad/sala-prensa/nuevo-paquete-ciberseguridad-uni%C3%B3n-europea

Dermutas, A. (2020, junio). *La evolución normativa de la ciberseguridad en la Unión Europea y su impacto político a nivel de actores, objetivos y recursos*. *2*, 114.

Díaz, P. X., & Reyes, A. (2015). *Buenas prácticas de seguridad alineadas al ISO/IEC 27002 para el aseguramiento de equipos Linux-Debian pertenecientes a un CERT* [UNAM]. http://132.248.9.195/ptd2015/mayo/0729528/0729528.pdf

Estrada, C. (2019, abril). *Atlas de riesgos para la Seguridad Nacional Cibernética en México*. *LIV*. https://www.inap.mx/portal/images/pdf/rap148.pdf

Expansión. (2019, mayo 2). *Educación, preponderante para la Amiti*. https://expansion.mx/tecnologia/2019/05/02/educacion-preponderante-para-la-amiti

Gonzalez, J. M., Albornoz, M. M., & Ramírez, M. S. M. (2019, abril). Ciberseguridad Nacional. *Periódica*, *LIV*(148). https://www.inap.mx/portal/images/pdf/rap148.pdf

Grance, T., Hash, J., Stevens, M., O'Neal, K., & Bartol, N. (2003). *Guide to information technology security services* (NIST SP 800-35; 0 ed., p. NIST SP 800-35). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-35

Guel, J. C. (2019). *CiberSeguridad MX 2020* [Encuentro ANUIES-TIC]. Encuentro ANUIES-TIC. https://encuentro-tic.anuies.mx/ctrl-content/uploads/2019/10/CiberSeguridadMX-2020-FINAL-2-2_compressed.pdf

Hathaway, M. (2018). *Gestión del Riesgo Cibernético Nacional*. OEA. https://www.oas.org/es/sms/cicte/ESPcyberrisk.pdf

Igel, C. (2020, mayo 20). *Im Interview: Forschungsdirektor der Cyberagentur* [Entrevista]. https://www.bmvg.de/de/aktuelles/interview-forschungsdirektor-der-cyberagentur-258548

Instituto Federal de Telecomunicaciones. (2018). *Visión regulatoria de las telecomunicaciones y la radiodifusión, 2019-2023* (p. 67). Instituto Federal de Telecomunicaciones.

Ley de la Comisión Nacional Bancaria de Valores, http://www.diputados.gob.mx/LeyesBiblio/pdf/46_090318.pdf

Ley de la Guardia Nacional, http://www.diputados.gob.mx/LeyesBiblio/pdf/LGN_270519.pdf

Ley Federal de e Transparencia y Acceso a la Información Pública Gubernamental, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_270117.pdf

Ley Federal de Fomento a las Actividades Realizadas por Organizaciones de la Sociedad Civil, https://www.profeco.gob.mx/juridico/pdf/l_f_actividades.pdf

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, https://www.gob.mx/cms/uploads/attachment/file/123648/Ley_Federal_de_Protecci_n_de_Datos_Personales_en_Posesi_n_de_los.pdf

Ley Federal de Telecomunicaciones y Radiodifusión, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_110121.pdf

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Ley General de Transparencia y Acceso a la Información Pública, http://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP_130820.pdf

Ley Orgánica de la Administración Pública Federal, http://www.diputados.gob.mx/LeyesBiblio/pdf/153_220120.pdf

Ley Orgánica de la Armada de México, http://www.diputados.gob.mx/LeyesBiblio/pdf/249_190517.pdf

Ley Orgánica del Ejército y Fuerza Aérea Mexicanos, http://www.diputados.gob.mx/LeyesBiblio/pdf/169_210618.pdf

Llamas, J. (2020, septiembre 7). Observaciones y estudio de la iniciativa que expide la Ley General de Ciberseguridad en México. *Foro Jurídico*.

https://forojuridico.mx/observaciones-y-estudio-de-la-iniciativa-que-expide-la-ley-general-de-ciberseguridad-en-mexico/

Martin, P.-E. (2015). *Inseguridad Cibernética en América Latina: Líneas de reflexión para la evaluación de riesgos*. *79*, 17.

Poder Ejecutivo Federal. (2013, 05). *Plan Nacional de Desarrollo 2013-2018.pdf*. https://www.snieg.mx/contenidos/espanol/normatividad/MarcoJuridico/PND_2013-2018.pdf

-------- (2014, 04). *Programa para la Seguridad Nacional 2014-2018*. http://dof.gob.mx/nota_detalle.php?codigo=5342824&fecha=30/04/2014

-------- (2017). *Estrategia_Nacional_Ciberseguridad.pdf*. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

-------- (2020). *Programa Sectorial Defensa Nacional 2020 2024* (p. 95). SEDENA. http://dof.gob.mx/2020/SEDENA/Programa_Sectorial_Defensa_Nacional_2020_2024.pdf

Policía Federal. (2018, 05). *Centro Nacional de Respuesta a Incidentes Cibernéticos de la Policía Federal*. gob.mx. http://www.gob.mx/policiafederal/articulos/centro-nacional-de-respuesta-a-incidentes-ciberneticos-de-la-policia-federal?idiom=es

Reglamento Interior de la Secretaría de Economía, https://www.dof.gob.mx/nota_detalle.php?codigo=5452141&fecha=09/09/2016

Reglamento Interior de la Secretaría de Gobernación, https://www.dof.gob.mx/nota_detalle.php?codigo=5561631&fecha=31/05/2019

Reglamento Interior de la Secretaría de Relaciones Exteriores, https://sre.gob.mx/images/stories/marconormativodoc/regint13.pdf

Reglamento Interior de la Secretaría de Hacienda y Crédito Público, https://www.gob.mx/cms/uploads/attachment/file/299882/Reglamento_Interior_de_la_SHCP_DOF_27_de_septiembre_2017.pdf

Riquelme, R. (2018, enero 22). ¿Qué es un Equipo de Respuesta ante Emergencias Informáticas (CERT)? *El Economista*. https://www.eleconomista.com.mx/tecnologia/Que-es-un-Equipo-de-Respuesta-ante-Emergencias-Informaticas-CERT-20180122-0009.html

Riquelme, R. (2020, 09). ¿Qué dice la ley de ciberseguridad propuesta por Miguel Ángel Mancera? *El Economista*. https://www.eleconomista.com.mx/tecnologia/Que-dice-la-ley-de-ciberseguridad-propuesta-por-el-senador-Mancera-20200917-0046.html

UIT. (2020). *Digital Regulation Handbook Conference edition*. 218.

Unión Europea. (2016). *Directiva (UE) 2016/1148 del Parlamento Europeo del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión*. Diario Oficial de la Unión Europea L 194, 19 de julio de 2016.