UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
PROGRAMA DE POSGRADO EN CIENCIAS POLÍTICAS Y SOCIALES

EVALUACIÓN DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD EN MÉXICO DESDE EL ENFOQUE CTS

TESIS
QUE PARA OPTAR POR EL GRADO DE:
MAESTRO EN ESTUDIOS EN RELACIONES INTERNACIONALES

PRESENTA:
MARCO ANTONIO LOPÁTEGUI TORRES

DIRECTORA:

MARÍA JOSEFA SANTOS CORRAL
INSTITUTO DE INVESTIGACIONES SOCIALES

MÉXICO, CIUDAD DE MÉXICO, ABRIL DE 2019

Dedicatoria

A mi compañero de viaje

Óscar Guillermo Campillo del Campo

A mi madre y a mi padre

Migdalia Torres Cruz

In memóriam

Marco Antonio Lopátegui Martínez

Vitta est bella

A mis cómplices

María Josefa Santos Corral

Gabriela Pérez Domínguez

Agradecimientos

A mi directora de Tesis, doctora María Josefa Santos Corral, es lo de hoy

A las lectoras y lectores de este trabajo, por su generosidad, maestra María del Consuelo Dávila Pérez; doctora Rebeca Nadia Ximena De Gortari Rabiela; doctor Rodrigo Díaz Cruz y doctor Omar García Ponce de León

A mi alma máter, la UNAM

A una mujer extraordinaria, doctora María Angélica Cuéllar Vázquez ♡

A mis entrañables maestras y maestros: doctor Alejandro Chanona Burguete, doctora Yleana Margarita Cid Capetillo, maestro Dámaso Morales Ramírez y doctora Graciela Arroyo Pichardo (+)

A Harbhajan Singh Khalsa Yogiji, Yogi Bhajan, por sus enseñanzas

A Gurujodha Singh Khalsa, por su amorosa guía

A Joti Kaur y Atma Prakash Kaur, faros en mi camino

Epígrafe

Frente a los cambios históricos van surgiendo igualmente cambios de paradigma y de conceptos. Al mismo tiempo, se hacen presentes enfoques contradictorios representativos de nuevas formas de lucha y de intereses opuestos. De lo que se trata entonces es de reesructurar el conocimiento necesario para comprender las nuevas realidades y tratar de resolver sus problemas. Así, en el campo del conocimiento social, frente a las realidades de inicios del siglo XXI y al pensamiento unidimensional que parecía ser único, empiezan a fortalecerse pensamientos alternos que, además de una tarea de desconstrucción del pensamiento occidental o céntrico que se impuso en una gran parte del mundo (el mundo colinizado) -con todo y sus críticos- desde hace aproximadamente cinco siglos, ahora se regeneran y difunden conocimientos con otras visiones e interpretaciones de la realidad mundial. Este nuevo conocimiento trata de contemplar al mundo no sólo como ocurrencia de hechos y registro de cifras. Hay una vuelta -por demás impostergable- a la perspectiva humanista de la ralidad que no sólo pone de relieve lo esencial del ser humano como individuo, como sociedad y como especie, sino que destaca el valor de la gran diversidad histórico-cultural de la humanidad, resultante de una dinámica ancestral en la que múltiples interacciones de los hombres entre sí y con su entorno natural han hecho del planeta un impresionante mosaico de pueblos y formas de vida diferentes.

Este nuevo tipo de conocimiento debe partir de una visión holística del mundo: debe concebir a la realidad como un todo complejo y dinámico en donde sus diferentes componentes y fuerzas interactúan, en donde cada uno de los grupos y sociedades que forman la diversidad humana tiene derecho a ser tomados en cuenta y a desarrollar sus propias perspectivas del mundo, según el papel que hayan representado en la vasta dinámica de acciones e interacciones intersocietales. El problema, entonces, no es de objetividad, sino de reconocer su papel en la compleja espiral de las acciones y relaciones internacionales y humanas que han dibujado la faz que actualmente presenta nuestra humanidad, en sus grandezas y miserias, semejanzas y diferencias, logors y fracasos. Todo ello será, al mismo tiempo, una contribución al conocimiento y reconocimiento del carácter histórico-cultural del quehacer científico.

Graciela Arroyo Pichardo
México, 2013

Índice

Introducción.

En la presente investigación se presenta la Estrategia Nacional de Ciberseguridad (ENCS) desarrollada para México durante el sexenio del presidente Enrique Peña Nieto (2012-2018), desde la mirada crítica de los estudios de ciencia, tecnología y sociedad (CTS).

Desde principios del sexenio del presidente Enrique Peña Nieto, ante el uso cada vez más generalizado de las TIC en las actividades cotidianas de individuos, organizaciones privadas y públicas, así como el riesgo inherente del uso de dichas tecnologías, se reconoció la necesidad de incluir al entorno cibernético en las tareas de seguridad a nivel multidimensional a lo que respondió la ENCS que se inscribe en el Plan Nacional de Desarrollo 2013-2018. La estrategia es transversal y contribuye al logro de los objetivos del Programa para un Gobierno Cercano y Moderno 2013-2018, al Programa Nacional para la Seguridad Pública 2014-2018 y al Programa para la Seguridad Nacional 2014-2018.

En noviembre del año 2017, se presentó la Estrategia Nacional de Ciberseguridad, documento oficial donde se muestra el contexto y los fundamentos sobre los que se asienta la visión del Estado mexicano respecto al tema de la ciberseguridad. Es un instrumento donde se despliega una serie de principios, objetivos y ejes transversales con la intención manejar el ciberespacio como un entorno confiable y resiliente.

En la ENCS se reconoce la complejidad y naturaleza transfronteriza de las dinámicas de la era digital, por lo que se advierte la necesidad de abordar la ciberseguridad de forma integral, colaborativa, holística y transversal, con la meta de que cualquier esfuerzo sobre dicho fenómeno evolucione en el tiempo, apostando al esfuerzo conjunto de todos los sectores sociales.

Ante tales propósitos, se plantea la necesidad de analizar si los lineamientos del documento mencionado y las acciones ejecutadas a partir del mismo en materia de ciberseguridad, han estado cumpliendo los propios objetivos de la Estrategia. Para esto, resulta imperioso, llevar a cabo un diagnóstico de las condiciones de ciberseguridad en el país durante el sexenio (2012-218) y evaluar lo realizado, para

así, determinar si realmente la ENCS está planteada de la forma más adecuada posible y si su implementación puede lograr los resultados planeados.

La parte formal del objeto de estudio se complementa al examinarlo desde la visión integral que brindan los estudios CTS. Esta propuesta significa un viraje analítico sobre la forma de abordar los fenómenos tecnológicos a nivel global. Por lo que se considera que es la forma más completa de estudiar un objeto de estudio como la ciberseguridad en México.

México tiene 129 163 276 habitantes (2018), de los cuales, 79.1 millones son internautas. Esto significa que más del 64% de los mexicanos tiene la capacidad de internarse en el ciberespacio. Un número que implica un avance significativo en penetración de Internet durante el sexenio, ya que la cantidad de cibernautas incrementó en más de un 75% (en 2012 había 45.1 millones).

Las principales actividades de los mexicanos son interactuar en redes sociales, utilizar el correo electrónico, escuchar música y, cada vez, se realizan más compras en línea y tramites gubernamentales. Asimismo, de acuerdo a la Asociación de Internet MX, el 78% se conectan preferentemente desde dispositivos móviles y los internautas pasan más tiempo conectados que años anteriores, pues en el 2018 alcanzaron las 8 horas con 12 minutos de conexión al día, es decir, una tercera parte del tiempo total de su vida cotidiana se encuentran en línea.

Esto muestra que, en la cotidianeidad del mexicano promedio, cada vez son menos las restricciones para internarse al ciberespacio, por más tiempo y sin distinción de lugar, lo que implica riesgos ante el descuido o la poca conciencia que pudiera tener la sociedad en temas de protección cibernética y eleva la importancia de la ejecución de acciones para proteger a la población en general y brindar confianza para que los cibernautas sigan conectándose al ciberespacio.

La División Científica de la Policía Federal –instancia encargada del cuidado, vigilancia y atención del ciberespacio- ha informado que en la primera parte del sexenio se atendieron cerca de 60 mil incidentes, relacionados con ataques cometidos principalmente contra los tres niveles de gobierno (53 por ciento), el ámbito académico (26 por ciento) y el sector privado (21 por ciento). Las denuncias sobre ataques cibernéticos están focalizadas en los siguientes tipos de crímenes:

suplantación y robo de identidad (68 por ciento), fraude cibernético (17 por ciento) y ataques a sitios web (15 por ciento). La Policía Federal también informó la identificación y desactivación de 5 mil 549 sitios de Internet apócrifos que usurpaban la identidad de instancias financieras y gubernamentales con fines de fraude.

En 2015, la firma PwC señaló que México era el segundo país más atacado en América Latina y el número de ciberataques creció 40% entre 2013 y 2014 afectando a 10 millones de víctimas. En 2016, la empresa *CISCO Systems* señaló que se generaba gran cantidad de malware en el país. La firma británica *Control Risks* identificó que los ciberataques estaban dirigidos más a los ciudadanos que a las grandes corporaciones, señaló las amenazas más comunes eran las menos sofisticadas, tales como Denegación de Servicio (DDoS), los Troyanos y los programas maliciosos; también señaló que el crimen organizado utilizó malware y spam como medio para extorsionar a ciudadanos y falsificar su identidad.

La Comisión Nacional de Seguridad informó que durante la presente administración se han emitido más de mil alertas preventivas de seguridad cibernética. Se destacó la alerta sobre el virus CTB-Locker que obstruye el acceso al contenido de los archivos de la computadora con el fin de extorsionar a la víctima a cambio de recuperarla.

Asimismo, un estudio del Instituto para México del Centro Wilson, en un capítulo dedicado al crimen organizado y el cibercrimen en México, describe una larga lista de actividades criminales de estos grupos a través de Internet, como el robo de identidad, fraudes, extorsiones, secuestros, tráfico de órganos y armas, así como la emergencia de grupos de cibervigilantes enfrentados con cárteles de la droga para contrarrestarlos. A esto se le suman otras amenazas cibernéticas particulares a nivel interno, como son los grupos subversivos y activistas anónimos que han adquirido experiencia, herramientas y capacidades avanzadas.

México es la economía 15 del mundo y ha registrado crecimiento sostenido en los últimos años; es también una de las economías más abiertas, con alto intercambio comercial con Estados Unidos y su cercanía con dicha potencia convierte a México en un territorio geopolítico estratégico, estas razones permiten

reconocer lo critico que puede llegar a ser en México un problema generalizado de inseguridad cibernética.

Todos los datos señalados, demuestran que México se encuentra en un punto de inflexión, en el que puede comenzar a ser blanco principal de diversas amenazas y ataques cibernéticos en la región, pero también puede fortalecerse en el ámbito para ser un referente y una pieza clave en la configuración de estrategias regionales de ciberseguridad.

Para intentar contrarrestar las vulnerabilidades, la ciberseguridad se está volviendo cada vez más relevante en la agenda de los tomadores de decisiones a nivel global. Estos datos justifican el objeto de estudio que se desarrollará en la presente investigación, la necesidad de realizar un diagnóstico y evaluación de la ENCS y conocer las verdaderas condiciones de la ciberseguridad en México y evaluar los resultados de la misma, al contrastar los objetivos planteados con los datos generados una vez aplicada la Estrategia.

Para conducir la investigación, se plantea responder la siguiente pregunta ¿Cuál ha sido el nivel de desempeño del Estado mexicano en materia de ciberseguridad durante el presente sexenio y de qué manera el enfoque de los estudios CTS permite realizar una evaluación integral sobre el desarrollo de la Estrategia Nacional de Ciberseguridad? Como apoyo, se desplegarán las siguientes cuestiones concretas sobre cada tema que se abordará:

- ¿Qué son los estudios CTS y porqué su enfoque contribuye en la realización de un análisis integral del fenómeno de la ciberseguridad?
- ¿Qué es el ciberespacio y cómo se ha configurado a nivel global?
- ¿Por qué es importante la ciberseguridad a nivel internacional y cuáles son los principales peligros en el ciberespacio?
- ¿Cómo cambia la percepción del fenómeno de la ciberseguridad a través del enfoque crítico de los estudios CTS?
- ¿Qué indica la Estrategia Nacional de Ciberseguridad publicada en 2017?
- ¿Cuál es el estatus de la ciberseguridad en México en la actualidad?

- ¿Cuál es el nivel de desempeño de Estado mexicano en la materia a partir de la implementación de la Estrategia Nacional de Ciberseguridad del 2017?

A priori, buscando dar respuesta a la cuestión general y sus preguntas derivadas, se formula una hipótesis que plantea que a través del enfoque de los estudios CTS, se puede establecer que la Estrategia Nacional de Ciberseguridad en México está basada en una visión determinista de los fenómenos tecnológicos, por lo que es necesario realizar un viraje analítico para ejecutar un diagnóstico y evaluación sobre las condiciones actuales de la ciberseguridad, es por eso que no se han podido desplegar ni desarrollar de manera óptima, hasta el momento, las líneas de acción planteadas en la Estrategia.

Para comprobar la hipótesis, se revisarán los postulados de los estudios CTS, se buscará conocer a fondo lo que significa el ciberespacio para la sociedad internacional y las implicaciones globales de la ciberseguridad; a partir de estos elementos se examinara una serie de datos y acciones que permitan, en primer lugar, conocer el estatus de la ciberseguridad en México durante el presente sexenio y, en segundo lugar, culminar con una evaluación a la ENCS, entonces se podrán desplegar una serie de conclusiones con el propósito de coadyuvar en mejorar la ciberseguridad en el país.

El objetivo general de la presente investigación es realizar un diagnóstico y una evaluación integral sobre la Estrategia Nacional de Ciberseguridad en México durante el periodo 2012-2018, a través del enfoque de estudios en Ciencia, Tecnología y Sociedad. Se buscará cumplir este propósito bajo dos pautas referenciales para evaluarla, así como hacer observaciones puntuales en cada eje transversal, sobre cómo un enfoque integral –basado en la visión de los estudios CTS- podría dar un viraje sustancial a la ENCS, tanto en su concepción como en su implementación, que se traduciría en una asimilación de la propia Estrategia en la sociedad mexicana.

Para abarcar lo antes planteado, en el primer capítulo se revisarán los estudios CTS. Llevando a cabo una revisión de los principales enfoques sobre la innovación tecnológica a lo largo de la evolución de la sociedad internacional en los

siglos XX y XXI. Se expondrán las premisas fundamentales de la tradición instrumental de la innovación tecnológica, sus alcances, límites y la manera como se constituyó en un enfoque hegemónico. Esto se contrastará con la tradición interpretativa de la innovación tecnológica, sus principales planteamientos y la crítica que hace a la tradición instrumental.

En este campo, los estudios sobre ciencia, tecnología y sociedad (CTS), la Teoría del actor red y la Construcción Social de la Tecnología, representan una oportunidad interesante para conformar un marco explicativo que cuestiona los fundamentos de la tradición hegemónica instrumental de la innovación. Dicha exploración nos permitirá caracterizar la innovación a través de los estudios CTS en relaciones internacionales y sentará las bases para hacer una posterior propuesta sobre la evaluación de la estrategia de ciberseguridad para México.

En el segundo capítulo se caracterizará a la ciberseguridad como un reto en la sociedad internacional. Para entender todo lo que implica la ciberseguridad y su importancia a nivel internacional, es necesario revisar el concepto del ciberespacio y cómo se ha configurado en un entorno de interacción humana a nivel global, alcanzando una relevancia tal que los actores de la sociedad internacional han detectado la necesidad de protegerse ante los riesgos a la seguridad en un plano diferente a las amenazas que tradicionalmente han existido.

Además, se analizarán algunas de las características y *modus operandi* de los ciberdelitos más comunes. Se describirán los más frecuentes a nivel internacional, qué son, cómo funcionan, en qué casos se utilizan y algunos datos sobre su nivel de incidencia, se buscará conocer todos los ámbitos que tocan las amenazas cibernéticas poder identificarlas en sus objetivos y formas de operar.

Una vez entendido lo que implica la ciberseguridad, se destacará su carácter internacional, por lo que será necesario conocer las formas en que se ha abordado a la ciberseguridad a nivel global y extraer las lecciones necesarias para realizar, posteriormente, una evaluación de la Estrategia en México.

En el capítulo 3, se conocerá el documento donde se plasma la Estrategia Nacional de Ciberseguridad, pero se explicará bajo el enfoque de los estudios CTS, con el que se observa en la presente investigación. Para lograr dicho objetivo, se

expondrá la forma en que la visión crítica de los estudios CTS permite dar un viraje al diagnóstico y evaluación de una estrategia de ciberseguridad para dar una perspectiva integral, global y alejada del determinismo tecnológico.

Se realizará la revisión del documento que ostenta la Estrategia Nacional de Ciberseguridad en México, donde el enfoque previamente explicado, permitirá examinar sus fundamentos y contextos. También se conocerán los principios en qué se sustenta, los objetivos que persigue, los ejes que la guían y el marco institucional por el cual se aplicará.

Una vez explicado el enfoque con el que se debe abordar el fenómeno de la ciberseguridad y revisada la Estrategia en forma y fondo, se tendrán los elementos necesarios para entrar en el estudio de caso y realizar el diagnóstico y la evaluación de la ciberseguridad, focalizados en lo que –en el supuesto institucional- debería derivar la ENCS, comparado con los estándares internacionales y la realidad de los datos, es decir, el ser *versus* el deber ser.

En el cuarto capítulo, se desplegará un análisis sobre la situación actual de la ciberseguridad y una evaluación de la Estrategia. Se conocerá el estatus general de la ciberseguridad durante el sexenio del presidente Enrique Peña Nieto, se comparará el documento de la Estrategia con un marco de referencia global y se examinarán los esfuerzos por ejecutar las acciones planteadas en la misma.

Este último capítulo se dividirá en dos secciones. La primera para conocer las condiciones generales de la ciberseguridad a lo largo del presente sexenio (2012-2018), por lo cual, se conocerán las principales incidencias en el tema de la ciberseguridad, las acciones y esfuerzos de los distintos actores y sectores sociales durante el periodo. La segunda parte será una evaluación de la ENCS, observada a partir de dos estándares: primero, bajo una referencia global de buenas prácticas en ciberseguridad y; segundo, ante los propios lineamientos de la ENCS, pero cotejándolos con las actividades realizadas desde la publicación de la misma.

La evaluación, además de ir desplegando un análisis cualitativo, tendrá un valor cuantitativo y, con base en los resultados de la investigación, se presentarán algunas consideraciones sobre la ENCS.

De esta manera, se tendrán los elementos suficientes para definir si se encuentra planteada adecuadamente para su correcta aplicación y si efectivamente podrá cumplir su objetivo primordial, de fortalecer 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.

The future is already here…
It just isn't evenly distributed yet.
William Gibson[1]

1. Los estudios CTS, de la tradición instrumental a las relaciones internacionales, la evolución de los principales enfoques teóricos sobre la innovación tecnológica

La tradición instrumental de la innovación tecnológica ha sido el enfoque hegemónico sobre el cual se han construido un importante número de interpretaciones sobre las implicaciones de los cambios científico-tecnológicos en la sociedad internacional, particularmente durante el siglo XX. Después de la Segunda Guerra Mundial, con la arquitectura internacional derivada de ésta, comenzaron a proliferar estudios que, desde enfoques críticos, observaron a la tecnología como resultado de complejas dinámicas sociales y no como un elemento externo a la sociedad misma.

En el presente capítulo se lleva a cabo una revisión de los principales enfoques sobre la innovación tecnológica a lo largo de la evolución de la sociedad internacional en los siglos XX y XXI. Por lo que se expondrán, en primer lugar, las premisas fundamentales de la tradición instrumental de la innovación tecnológica, sus alcances, límites y la manera como se constituyó en un enfoque hegemónico. Lo anterior se contrastará con la tradición interpretativa de la innovación tecnológica, sus principales planteamientos y la crítica que hace a la tradición instrumental. En este campo, los estudios sobre ciencia, tecnología y sociedad (CTS), la Teoría del actor red y la Construcción Social de la Tecnología, representan una oportunidad interesante para conformar un marco explicativo que cuestiona los fundamentos de la tradición hegemónica instrumental de la innovación.

Dicha exploración nos permitirá caracterizar la innovación a través de los estudios CTS en relaciones internacionales y sentará las bases para hacer una

[1] Traducción al español: *El futuro ya está aquí, sólo que no está distribuido de manera uniforme*.

propuesta posterior sobre la construcción de una agenda integral de ciberseguridad para México en un contexto de cambios políticos, económicos y sociales.

1.1 La tradición instrumental de la innovación tecnológica.

El siglo XX y lo que va del XXI se constituyen como un crisol para comprender los grandes cambios que enfrenta la humanidad como resultado de la llamada cuarta revolución, la digital. La segunda mitad del siglo XX se distinguió por un proceso de innovaciones científicas y tecnológicas, particularmente en la información y la electrónica, así como por los cambios en las estructuras organizacionales para automatizar los procesos, hecho que colocó a la innovación en el centro de la discusión y de los esquemas explicativos de las ciencias sociales dedicados al estudio de la tecnología.

En primer lugar, se debe abordar el concepto de innovación tecnológica, a partir del entendimiento de los teóricos especializados en el tema, más reconocidos a nivel global, como lo fue Joseph Shumpeter quien, en la década de los cuarentas del silgo XX, consideraba que "el impulso fundamental que pone y mantiene en movimiento a la máquina capitalista procede de los nuevos bienes de consumo, de los nuevos métodos de producción y transporte, de los nuevos mercados, de las nuevas formas de organización industrial"[2], por lo que se requería estar en innovación constante.

Pero, desde su perspectiva, las pequeñas innovaciones incrementales o aditivas a tecnologías o procesos ya existentes, si no tenían un impacto que cambiara algún producto, al mercado o a la estructura organizacional, no eran consideradas como innovaciones sino como invenciones. Para Schumpeter, lo importante eran las innovaciones capaces de provocar cambios revolucionarios, transformaciones decisivas en la sociedad y en la economía.[3] Por innovaciones identificaba a "toda introducción en el mercado de un nuevo bien o una nueva clase

[2] Joseph Schumpeter, *Capitalismo, socialismo y democracia*, edicion en español, Ediciones Folio, Barcelona, 1996, p. 12.

[3] Omar Montoya Suárez, *Schumpeter, Innovación y Determinismo Tecnológico*, Revista Scientia et Technica Año X, No. 25, agosto 2004, consultado en https://dialnet.unirioja.es/descarga/articulo/4842897.pdf [junio 2018]

de bienes, la introducción de un nuevo método de producción, la apertura de un nuevo mercado en un país —aun existiendo ya en otro—, la conquista de una nueva fuente de suministro de materias primas o productos semielaborados, independientemente de si ya existe o tiene que ser creada, y la implantación de una nueva estructura de mercado."[4]

Keith Pavitt, estudioso de las políticas públicas y promotor del uso de patentes como indicador de desarrollo en ciencia y tecnología, consideraba que Schumpeter "nos dio la definición más útil de innovación como consistente no sólo de nuevos productos y procesos, sino también de nuevas formas de organización, nuevos mercados, y nuevas fuentes de materias primas."[5]

Jacob Schmookler sugirió que el término innovación se aplica "cuando una empresa produce un bien o servicio, o usa un método o insumo que es nuevo para ella; es decir, cuando hace un cambio técnico. La primera empresa en hacer un cambio técnico dado se constituye como una empresa innovadora: su acción es innovación."[6]

Por su parte, el británico Christopher Freeman considera que "una invención es [...] un bosquejo o modelo para un dispositivo, producto, proceso o sistema nuevo o mejorado, [mientras que] una innovación en el sentido económico está acompañada de la primera transacción comercial del nuevo producto, proceso, sistema o dispositivo, aunque la palabra se use para describir todo el proceso."[7]

Rosabeth Moss entiende por innovación 'la generación, aceptación e implementación de nuevas ideas, procesos, productos o servicios.' Puede, pues, ocurrir en cualquier parte de una compañía y puede comprender el uso creativo al igual que una invención original. La aplicación e implementación son parte central de esta definición, que comprende la capacidad de cambiar o de adaptarse.[8]

---

[4] Joseph Schumpeter, *Teoría del desenvolvimiento económico*, Edicion en español, Quinta Reimpresión, Fondo de Cultura Económica, México, 1978, p.25

[5] Enrique Medellín, *Construir la innovación: Gestión de tecnología en la empresa*, Siglo XXI editores, México, 2013, p. 21.

[6] Jacob Schmookler, *Invention and economic growth*, Harvard University Press, Estados Unidos, 1990, p. 2.

[7] Christopher Freeman, John Clark y Luc Soete, U*nemployment and technical innovation: a study of long waves and economic development,* Editorial Burns & Oates, Estados Unidos, 1982, p. 13,

[8] Rosabeth Moss, *The change master: Innovations for productivity in the American Corporation*, Editorial Simon & Schuster, Estados Unidos, 1983, p. 20.

Edward Roberts explica que el proceso de innovación abarca todos los esfuerzos encaminados a la creación de nuevas ideas y lograr que éstas funcionen. La explotación incorpora todas las etapas de desarrollo comercial, aplicación y transferencia, incluyendo el enfoque de ideas o invenciones hacia objetivos específicos, la evaluación de dichos objetivos, la transferencia "aguas abajo" de los resultados de la investigación y/o desarrollo, y la eventual utilización, diseminación y difusión de los resultados basados en la tecnología.[9]

Desde una perspectiva institucional, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) esgrime una concepción más amplia en su tercera edición del Manual de Oslo (2005), define la innovación como "la implementación de un producto (bien o servicio) nuevo o con mejoras significativas, o un proceso, un método de comercialización, o un método organizacional nuevo en una práctica empresarial, organización de trabajo o en relaciones externas."[10] Esta dilucidación comprende los siguientes tipos de innovación:

- Innovación de producto: la introducción de un bien o un servicio nuevo o con mejoras significativas asociadas con sus características o su uso previsto. Esto incluye las mejoras significativas de las especificaciones técnicas, componentes y materiales, software incluido, facilidad de uso y otras características funcionales.
- Innovación del proceso: la implementación de un método de producción o provisión nuevo o con mejoras significativas. Lo anterior incluye los cambios significativos en las técnicas, en el equipo o el software.
- Innovación de marketing: la implementación de un nuevo método de marketing que incluya cambios significativos en el diseño, el empaque, la comercialización, la promoción o el precio del producto.
- Innovación organizacional: la implementación de un nuevo método organizacional en las prácticas comerciales de las empresas, organización del lugar de trabajo y relaciones externas.[11]

[9] Edward Roberts, *Gestión de la Innovación Tecnológica,* Clásicos COTEC 1, Madrid, 1996, p. 14
[10] OCDE*, La Estrategia de Innovación de la OCDE, Empezar Hoy el Mañana*, 2010, p. 22, consultado en http://www.foroconsultivo.org.mx/libros_editados/estrategia_innovacion_ocde.pdf [junio 2018]
[11] Ibíd., pp. 22,23

En México y América Latina se utilizó, y se sigue haciendo, una definición de innovación tecnológica propuesta por integrantes del Centro para la Innovación Tecnológica de la UNAM, que ya no existe pero que hizo importantes aportaciones en la materia. La definieron como un "proceso que consiste en conjugar oportunidades técnicas con necesidades, integrando un paquete tecnológico que tiene por objetivo introducir o modificar productos o procesos en el sector productivo, con su consecuente comercialización".[12]

No es la intención de la investigación ahondar en más definiciones sobre la innovación, sino en caracterizar y profundizar en su análisis desde las ciencias sociales, pero resultaba necesario tener un entendimiento primario sobre el concepto y conocer algunas de las visiones de sus principales expositores, además de que prácticamente todas esas propuestas han quedado rebasadas, puesto que su concepción se ha ampliado y hecho más compleja. Una vez planteado esto, a continuación, se caracterizarán las distintas visiones que hay de la innovación tecnológica para entender su evolución y utilidad para el presente trabajo.

En el contexto del sistema internacional derivado de la Segunda Guerra Mundial, dotado de una arquitectura institucional propia y con un sistema económico capaz de articular a las economías nacionales en complejas cadenas para la producción de bienes con valores agregados cada vez mayores, el desarrollo científico-tecnológico comenzó a ocupar un lugar privilegiado en las agendas de los Estados, sobre todo porque éstas irían acompañadas de la noción social y el discurso político del progreso.

Desde comienzos de la Guerra Fría, tanto la ciencia como la tecnología se observan como dos conceptos inseparables de la noción de poder y progreso, y es en esta etapa de la historia de las relaciones internacionales donde emerge y se consolida lo que Diaz y Lee caracterizan como la tradición instrumental de la innovación tecnológica que parte de una postura determinista de la tecnología.[13]

¿Cómo se generó y reforzó esta idea determinista de la tecnología? Si bien la técnica es un elemento intrínseco al ser humano, la tecnología encuentra su

[12] Gustavo Cadena et al, *Administración de proyectos de innovación tecnológica*, Gernika, 1986, México, p. 27.
[13] *Cfr*. Rodrigo Díaz y Marta Lee, *La innovación tecnológica: dos aproximaciones teóricas en competencia*, Roberto Varela (ed.), Prospectiva social y revolución científico-tecnológica, UAM, México.

fundamento explicativo en las dos revoluciones industriales de los siglos XVIII y XIX, tal y como señala Miguel Ángel Quintanilla:

> En su origen, el trabajo en las manufacturas inglesas era del mismo tipo que el trabajo artesanal que desde hacía centenares de años se había ido desarrollando en pequeños talleres o en unidades de producción de carácter familiar. De manera que en un principio la Revolución Industrial no supuso una innovación de carácter tecnológico, salvo en el aspecto exclusivo de la organización social del trabajo. Pero supuso un cambio de perspectiva en la "lógica" del sistema productivo, si se nos permite decirlo así, que tuvo consecuencias decisivas para el desarrollo de nuevas técnicas, nuevos instrumentos y nuevas máquinas; pero sobre todo para acelerar el ritmo del cambio tecnológico y para generalizar la incidencia de las innovaciones técnicas en toda la organización social.[14]

La organización social del trabajo, como lo señala Quintanilla, es el epicentro de los cambios derivados de las dos primeras revoluciones industriales y, según los instrumentistas de la innovación, de las subsecuentes dos. A ello deberá incorporarse la base de la organización política. Sin embargo, es común dirigir la atención hacia los avances científicos, inventos e innovaciones tecnológicas porque de algún modo revelan el carácter de cada revolución; dicho de otra manera, la tradición instrumental se basa en que son los elementos técnicos los que revela el fundamento de los grandes cambios de la humanidad a lo largo de la historia.

Esta visión es determinista porque deja de lado la complejidad de los fenómenos sociales y las bases políticas de una sociedad, asimismo, se asienta en una serie de descubrimientos o invenciones para dar forma a toda una gama de procesos de innovación o generar una revolución industrial.

Este pensamiento logró la consolidación de la hegemonía de la tradición instrumental al instaurarse la idea en las cúpulas empresariales, los programas académicos y los proyectos de desarrollo gubernamental basados en la innovación tecnológica, de que el poder y el progreso se lograban si se rompían los límites de manipulación de la naturaleza y la producción industrial, prueba de ello, verbigracia, es la carrera espacial entre los Estados Unidos y la Unión Soviética, en la que dichas potencias centraron su competencia hegemónica durante un par de décadas.

---

[14] Miguel Ángel Quintanilla, *Tecnología: Un enfoque filosófico y otros ensayos de filosofía de la tecnología*, Fondo de Cultura Económica, México, 2005, p. 23.

Ahora bien, para profundizar en el estudio de la sociedad internacional desde la perspectiva sociotécnica, es necesario conocer las diferentes concepciones articuladas en torno al fenómeno de la innovación, los elementos que las distinguen entre sí, las relaciones que guardan entre sus componentes y hacia dónde dirigen sus enfoques.

Es menester vincular la historia de las relaciones internacionales con el fenómeno de la innovación en el contexto de la globalización, para comprender la compleja dinámica del mundo actual y entender así las actitudes, decisiones y acciones que toman los actores de las relaciones internacionales frente a otros en espacios de poder y cooperación internacional acotados, donde estas relaciones son precisamente las que median el acceso, uso y apropiación tecnológica.

De acuerdo con Rodrigo Díaz Cruz y Martha Lee Vázquez, se hace referencia a la noción de tradición porque "las tradiciones intelectuales no sólo se constituyen a partir de una serie de problemas que se juzgan relevantes, de familias de conceptos y prácticas que son atinentes, o de condiciones sociales propicias en las que emergen, también forman parte de ellas los fundadores resaltados, los hechos ejemplares, las imágenes adustas".[15]

En este sentido, la tradición instrumental de la innovación tecnológica se teje a partir de la necesidad de controlar y orientar las decisiones en el ambiente tecnológico posterior a la Segunda Guerra Mundial, donde es evidente la interdependencia de los actores que definen la innovación y la existencia de un entorno tecnológico con importantes cambios en las estructuras organizacionales. En palabras de los autores referidos, esto se define de la siguiente manera:

> Fundamentalmente a partir de la Segunda Guerra Mundial, la emergencia de las "múltiples tecnologías" exigía instrumentos de coordinación y centralización en la toma y ejecución de decisiones acerca del ejercicio de aquellas. La revolución organizacional, señalamos, fue uno de los instrumentos, ahora cabe matizar. Ésta ha adquirido dirección y sentido en virtud del surgimiento y conformación de una tradición intelectual singular e híbrida: la administración y gestión de la innovación tecnológica. El objetivo básico de esta tradición es el de establecer y coordinar un conjunto de estrategias y tácticas organizacionales que orienten la acción para garantizar, de acuerdo con el principio de

[15] Rodrigo Díaz y Marta Lee, *La innovación tecnológica: dos aproximaciones teóricas en competencia*, Roberto Varela (ed.), Prospectiva social y revolución científico-tecnológica, UAM, México, p. 56.

> efectividad, el éxito de los proyectos de innovación tecnológica. La acción a la que está orientada esta intención-racional que Habermas define como "la acción instrumental o la elección racional o su conjunción".[16]

Con la cita anterior, queda claro que, para Rodrigo Díaz y Martha Lee, el eje que articula la tradición instrumental de la innovación tecnológica (TIIT) es precisamente la intención racional de la administración y gestión de tecnologías. Esta intención racional persigue como fin último el control del ambiente. El éxito o fracaso de un proyecto de innovación tecnológica dependerá, además de la satisfacción de una necesidad, del control del ambiente que pueda ejercerse en el proceso de administración y gestión tecnológica.

Desde la tradición instrumental de la innovación tecnológica, la satisfacción de una necesidad supone el logro de una meta precisa, por lo que, "con el objetivo de obtener ventajas competitivas que les permitan mantenerse en el mercado, las empresas han de promover proyectos de innovación que conjuguen oportunidades técnicas con necesidades de algunos grupos sociales; implantar en el mercado, para su explotación comercial, invenciones y/o modificaciones técnicas".[17]

Como resultado de lo anterior, en la TIIT los términos de éxito y fracaso adquieren relevancia en la medida en que es a partir de tales parámetros como medirán los proyectos de innovación: el objetivo de la innovación es inmutable pero los sucesos deberán estar acotados a casos específicos y delimitados en el tiempo. De esta manera, podrá determinarse si la aplicación de una política específica que instrumente una innovación fue exitosa o fracasó.

Para la TIIT, el éxito o fracaso de los proyectos de innovación es el resultado de un proceso lineal a través del cual se cumplen una serie de etapas encaminadas al logro de un objetivo concreto. Al lograr el objetivo, la innovación es adoptada por la sociedad como un agente exógeno que la impacta y la modifica, detonando nuevos procesos de innovación que, a su vez, modificarán el entorno social. Esto es explicado de manera precisa por Díaz y Lee, a partir de cuatro premisas fundamentales, citadas a continuación:

---

[16] *Ibíd.,* p. 57.
[17] *Ibíd.,* p. 58.

1. Los proyectos de innovación tecnológica son el objeto de análisis y de acción de la TIIT. Los resultados de los mismos son evaluados a partir de un par de algoritmos: será exitoso si ha conjugado una oportunidad técnica con alguna necesidad de uno o varios grupos sociales, en caso contrario habrá fracasado o, al menos, será un proyecto suspendido;
2. Los proyectos de innovación tecnológica están constituidos por etapas, cada una de las cuales es condición necesaria y suficiente para acceder a la siguiente. En consecuencia, la innovación tecnológica es concebida como un proceso lineal -o semilineal- y gradual, pues cada etapa va satisfaciendo sus fines precisos. Con cada estadio del proceso se enriquece y mejora el valor del producto susceptible a la innovación;
3. Dado que concibe a los proyectos de innovación como constituidos por etapas -cada una con sus propios fines-, la TIIT tiende, para efectos de análisis y de una correcta planeación estratégica, no sólo a fragmentar o atomizar todo el proceso donde se desempeñan más que individuos, roles. Congruente con esta posición, los análisis empíricos que la TIIT realiza de proyectos singulares de innovación son fundamentalmente sincrónicos: la "historia" de éstos suele iniciarse justo ahí donde la planeación comienza a incidir sobre ellos; el conocimiento histórico tiene únicamente un valor informativo o referencial; y
4. A pesar de que reconoce el carácter contingente y conflictivo de los proyectos de innovación tecnológica, la TIIT considera que estos rasgos son accidentales, por tanto, pueden ser eliminados o modificados -fundamentalmente mediante cuatro estrategias organizacionales- para propiciar el éxito de los proyectos.[18]

Los mismos autores hacen referencia a cuatro estrategias organizacionales que siguen las instituciones con la finalidad de ejecutar los proyectos. Antes de mencionarlas, es necesario señalar que en lugar de hablar de instituciones es más adecuado hacer referencia a los actores u organizaciones públicas y privadas,

[18] *Ibíd.,* pp. 58-62. (subrayado propio).

nacionales, regionales o globales que participan en los proyectos de innovación. Así, las cuatro estrategias organizacionales son las siguientes:

1. Transformar y adaptar las estructuras organizacionales ya establecidas a las situaciones siempre novedosas que supone la innovación; sin embargo, ésta es cada vez más irrelevante en virtud de sus altos costos y lentitud, inaceptables ante un entorno tan competitivo y cambiante;
2. Erigir nuevas estructuras organizacionales, pero ante todo una: las unidades de gestión tecnológica; éstas tienen por objetivo vincular a los emisores con los receptores de tecnología; los gestores son coordinadores y en ocasiones los líderes de los proyectos de innovación; representan el espacio institucional de socialización y reproducción de la aún joven comunidad gestora y administradora de la innovación tecnológica;
3. Establecer formas o sistemas organizacionales (por ejemplo, la organización matricial) que permiten la toma ágil y expedita de decisiones, así como el libre y abierto flujo de información y que inhiban el conflicto y reduzcan la incertidumbre. No es de extrañar que para la TIIT es incluso posible administrar el conflicto con sólo ubicar a la autoridad que, en una decisión en debate, tiene la última palabra; y
4. Administrar sabiamente los recursos humanos y permitir el desempeño adecuado de los llamados roles críticos para la innovación.[19]

Para ilustrar esto, basta recordar la creación de Bletchley Park, en el norte de Londres, Inglaterra, durante la Segunda Guerra Mundial, como un espacio creativo habilitado para el desarrollo de un dispositivo capaz de descifrar mensajes encriptados de las radiocomunicaciones alemanas. Como resultado de la colaboración de más de 10 mil especialistas en diversas áreas del conocimiento como matemáticas, ingeniería y lingüística, donde dos terceras partes del personal eran mujeres, se creó la máquina BOMBE de Alan Touring, capaz de descifrar los mensajes emitidos por los alemanes a través del dispositivo ENIGMA. Posteriormente, hacia 1944, se crearía Colossus, con dos versiones, Mark I y II. La segunda versión contribuyó a descifrar el tráfico de información en tiempo real para

[19] *Ibíd.,* pp. 61, 62.

informar sobre la invasión alemana a Normandía el 6 de junio de 1944, hecho que muestra el éxito del proyecto de *Bletchley Park*.[20]

Bajo las estrategias mencionadas, también subyace la idea de que existe una relación metonímica entre tecnología y progreso. Es decir, para muchos analistas y organizaciones, tanto públicas como privadas, se ha implantado la idea de que los avances tecnológicos y científicos se inscriben en un enfoque lineal de la historia, donde la acumulación de conocimientos a través de los años y su transmisión de generación en generación modela e impacta de manera positiva a la vida en sociedad, generando entornos tecnológicos que redundan en bienestar social.

Sobre este particular, vale la pena citar a Gabriel Pérez Salazar, en su artículo Hacia una tecnología socialmente significativa, donde expone de manera clara los principales supuestos de la TIIT:

> Hay algunos enfoques que ubican a la tecnología como la variable independiente por antonomasia, es decir, aquella a partir de la cual se originan casi todos los cambios sociales. La principal lógica que opera en este sentido se deriva de la evolución que tuvieron las economías de los países centrales durante el siglo XIX y la primera mitad del siglo XX. A muy grandes rasgos, en tales naciones tuvieron lugar una serie de innovaciones que impactaron a fondo a todos los sectores de la sociedad, a partir de los cambios en los medios de producción. El desarrollo de la máquina de vapor aplicada a la fabricación de bienes de consumo y de producción en gran escala, es cierto, favoreció el surgimiento de una sociedad de masas, aunque es muy discutible si las mejoras en los niveles de vida observados en tales contextos fueron la consecuencia del desarrollo científico y tecnológico o si las nuevas formas de organización social impulsaron los cambios observados en los niveles de ingreso en dichos contextos.[21]

Gabriel Pérez señala algo que es fundamental para distinguir a las dos grandes rutas analíticas para estudiar fenómenos vinculados a la innovación: por un lado, el desarrollo científico y tecnológico como pilares del progreso social y, por otro, los cambios de las comunidades políticas, particularmente en su forma de

[20] Charles Severance, *Alan Turing and Bletchley Park*, Revista Computer, vol. 45, junio de 2012, pp. 6-8.
[21] Gabriel Pérez Salazar, *Hacia una tecnología socialmente significativa,* en Santos, M. J. y De Gortari, R. (coords.), Computadoras e Internet en la biblioteca pública mexicana, México, UNAM – IIS – Pearson, 2009, pp. 3,4.

organizar las diversas actividades encaminadas a la satisfacción de sus necesidades.

Es en este punto donde se plantea, en la presente investigación, la interrogante acerca de qué debe considerarse primero para el análisis de los grandes cambios de la sociedad internacional: por un lado, si dar prioridad analítica a las transformaciones en la base política, económica y social en torno a la producción de bienes materiales o, por el otro, tomar como variable independiente las diversas formas de innovar apoyado en los conocimientos y las tecnologías vinculadas a procesos específicos y su impacto en la base organizacional.

La TIIT privilegia el papel de la tecnología como promotora y artífice del cambio social, hecho que evidencia su carácter determinista. Desde esta perspectiva, la tecnología determina a la sociedad y sobre esta base se han erigido una parte importante de los discursos de los gobiernos, organizaciones internacionales y demás actores de la sociedad internacional.

Un elemento a destacar es que la tecnología es observada como una variable independiente, a la cual ya se ha hecho referencia, cuyo carácter no queda del todo claro, tal como señala Gabriel Pérez Salazar al citar a Trevor Pinch y a Wiebe E. Bijker, íconos de los estudios sobre innovación tecnológica:

> Pinch y Bijker (1989) señalan que la tecnología muchas veces es vista como una "caja negra", esto es, como un dispositivo cuyo funcionamiento interno se desconoce. Es posible sugerir que dicha cualidad fortalece la valoración simbólica de la tecnología, alcanzando tales atributos mágicos. Dentro del discurso de la modernidad, la tecnología parece convertirse en un tótem al que se debe reverenciar y del cual hay que esperar su benevolente respuesta.[22]

Esta noción de "caja negra", como si la tecnología tuviera una serie de atribuciones inexpugnables, es muy notable en los discursos oficiales, basta citar la presentación de la Estrategia Digital Nacional de México, dada a conocer por el presidente Enrique Peña Nieto en noviembre de 2013, donde Alejandra Lagunes Soto Ruiz, coordinadora de dicho programa, en la presentación de la estrategia plantea lo siguiente:

[22] *Ibíd.,* p. 6.

> Esta estrategia surge en respuesta a la necesidad de aprovechar el potencial de las Tecnologías de la Información y la Comunicación (TIC) como elemento catalizador del desarrollo del país. La incorporación de las TIC en todos los aspectos de la vida cotidiana de las personas, organizaciones y gobierno, tiene múltiples beneficios que se traducen en una mejora en la calidad de vida de las personas. La evidencia empírica ha mostrado que la digitalización impacta en el crecimiento del Producto Interno Bruto, la creación de empleos, la innovación, la transparencia y la entrega efectiva de servicios públicos, entre otros aspectos [...]
>
> Con la convicción de que el camino de la digitalización es el rumbo hacia un mayor desarrollo para nuestro país, la Coordinación de Estrategia Digital Nacional de la Oficina de la Presidencia de la República dedicará sus esfuerzos para que los objetivos de este documento se materialicen, por el bien de México y de todos los mexicanos.[23]

Si bien las TIC podrían ser un elemento catalizador –entre otros elementos- en el desarrollo, no lo determinan y no suponen tampoco, necesariamente, múltiples beneficios que se traduzcan en la mejora de la calidad de vida de las personas. Además, existen diversos niveles a partir de los cuales la digitalización y la diseminación de tecnologías de información y comunicación (TIC) en la sociedad, pueden condicionar, mas no determinar, la vida de las personas en una sociedad en particular. Estos niveles, tomando como referencia lo que en la actualidad se denomina *brecha digital*, se refieren al acceso, uso y apropiación tecnológicas, donde el elemento cultural es fundamental.[24]

La TIIT se constituye como un discurso hegemónico que es promovido a través de un número importante de instituciones y organizaciones; sin embargo, desde hace varias décadas, se ha consolidado también una propuesta que cuestiona los postulados de ésta. A dicha propuesta, Rodrigo Díaz y Martha Lee la llaman Tradición Interpretativa de la Innovación Tecnológica (TIIN).

La evolución de los principales enfoques teóricos sobre la innovación tecnológica pasa por ambos enfoques, la TIIT versus la TIIN que, a pesar de analizar

---

[23] Gobierno de México, *Estrategia Digital Nacional*, Gobierno de la Republica, México, 2013, consultado en http://www.presidencia.gob.mx/edn/#descargas [diciembre 2017]

[24] Para introducirse en el estudio de la brecha digital, cómo se caracteriza y los niveles desde los cuales puede ser abordada, se sugiere revisar el siguiente texto: OECD, Understanding the digital divide, OECD Publications, 2001, en: https://www.oecd.org/sti/1888451.pdf [consultado el 14 de noviembre de 2017]

un mismo cúmulo de fenómenos globales relacionados con la tecnología, tienen perspectivas que parten de polos muy distintos.

A continuación se expondrán los principales fundamentos de la TIIN, sus orígenes, desarrollo y evolución, además, se presentarán los principales enfoques teóricos de la innovación tecnológica que la articulan y que han dado lugar a una amplia variedad de rutas críticas que han abierto nuevas puertas a la interpretación de los complejos procesos globales, propios del estudio de las Relaciones Internacionales.

1.2 La tradición interpretativa de la innovación tecnológica.

Desde finales de la década de los sesenta del siglo XX, diversos estudiosos del desarrollo de la ciencia y la tecnología como Wiebe Bijker, Trevor Pinch, Bruno Latour, María Josefa Santos, Rosalba Casas, Michael Callon y Gabriel Pérez, entre otros, se han dado a la tarea de explorar el contenido de la "caja negra" de la tecnología, desentrañar sus diversos significados y avanzar hacia una comprensión más profunda de los procesos de innovación.

Es importante ofrecer un panorama general de esta tradición, y para ello resulta de gran utilidad fijar la atención en el texto de Rodrigo Díaz y Martha Lee, ya que logra dos cosas fundamentales: primordialmente, ofrece un panorama amplio que la describe a partir de varias premisas, los supuestos principales que de manera afortunada logran dar cuenta de su complejidad y, para ahondar, brinda ejemplos claros y sencillos que la explican con mayor claridad.

De acuerdo con Díaz y Lee, el ejemplo de la evolución de la bicicleta como artefacto sociotécnico a finales del siglo XIX ilustra cómo la innovación tecnológica va más allá de la lógica del mercado y la exitosa satisfacción de una necesidad de un grupo social, así lo mencionan:

> [...] Un proyecto exitoso puede dejar de serlo ante nuevas necesidades del mercado; necesidades que estimularán a su vez el desarrollo de un nuevo proyecto con nuevos objetivos y con sus propias estrategias de planeación. Los cambios tecnológicos se resuelven entonces en una suerte de continuum constituido por procesos discretos de demandas y ofertas tecnológicas que satisfacen necesidades del mercado o, más precisamente, de algunos grupos

> sociales. [...] Con otras palabras, la TIIT concibe "el surgimiento de una nueva tecnología en un sistema social dado como un proyectil que, lanzado del exterior, golpea un medio más o menos resistente. A partir de la crítica a esta imagen -donde las tecnologías parecen provenir del exterior de la sociedad- surgirá la que proponemos llamar la tradición interpretativa de la innovación tecnológica (TIIN).[25]

La bicicleta es un ejemplo que utilizan Díaz y Lee al cuestionar los supuestos de la TIIT. A partir de la categoría de "grupos públicos de interés", explican el curso de la innovación tecnológica de acuerdo a experiencias e intereses de grupos sociales específicos, que tienen significados distintos de un mismo objeto. Al respecto, Dave Horton et. al. comentan los siguiente:

> El ciclismo, entonces, representa muchas cosas, que varían de acuerdo al tiempo y al espacio. A nivel global, en algunos lugares es una respuesta a los problemas donde hay muchos automovilistas, mientras que en otros es una forma de movilidad para alejarse de la búsqueda del progreso y generar mayores automovilistas; en otros aún sigue siendo un modo de movilidad económica y accesible. Donde algunas personas abandonan sus automóviles por bicicletas (por lo menos algunos días), otras abandonan sus bicicletas por automóviles (generalmente casi todos los días), mientras otras, debido al alto costo o a prohibiciones culturales, aún siguen luchando por andar en bicicleta algún día. Mientras en algunas sociedades europeas el ciclismo es un deporte nacional que despierta pasiones, pero una práctica poco común (Italia, Francia y España), en otras es una manera ordinaria y común de desplazarse (Dinamarca, Países Bajos y Suecia).
>
> Claro que existe desigualdad entre los ciclistas en sociedades y contextos históricos específicos. Ambos niveles, ciclismo y actitudes hacia éste, varían regularmente de manera dramática de acuerdo al género, clase social, etnia o edad. Así, por ejemplo, en muchas sociedades, el ciclismo es practicado y entendido de manera distinta por las mujeres, para las cuales en algunas sociedades ni siquiera está permitido. En sociedades con altos niveles de ciclismo, tanto hombres como mujeres lo practican.
>
> El carácter de la variable social del ciclismo puede ser confundido y confundir. Por ejemplo, mientras se asume que los altos niveles de ciclismo están asociados con la falta de automóviles, en Reino Unido las personas en hogares que cuentan con automóvil son más propensas a realizar viajes en bicicleta que las que no tienen automóvil. Asimismo, sociedades ciclistas como los Países Bajos y Dinamarca, también tienen niveles altos de propietarios de vehículos motorizados. En algunos lugares el ciclismo es entendido como una práctica

[25] Rodrigo Díaz y Martha Lee, *La innovación tecnológica: dos aproximaciones…, Op. Cit.,* p. 63 (subrayado propio).

> de los pobres y en otros como una práctica de ricos. De manera similar, el ciclismo es típicamente entendido como una actividad que requiere aptitudes físicas y mentales; más aún, el ciclismo es adoptado como una práctica que beneficia a las personas con alguna discapacidad. Incluso, una forma de analizar el panorama social de la movilidad es que el exceso de automovilistas niega el derecho de los ciclistas, incluyendo los placeres y beneficios.[26]

A pesar de que Rodrigo Díaz y Martha Lee ilustran la participación de los grupos públicos de interés en los procesos de innovación tecnológica, con los cambios que sufrieron las bicicletas a finales del siglo XIX, la cita anterior evidencia de manera más clara la diversidad de grupos, concepciones, actitudes y experiencias actuales en torno a un mismo artefacto.

En el mismo sentido, se puede ver cómo la innovación tecnológica es un proceso incierto y conflictivo, relacionado con grupos públicos de interés, y no precisamente con etapas autocontenidas que pueden ser organizadas y administradas desde y hacia un punto u objetivos centrales específicos.

En suma, se puede afirmar que la TIIN concibe la innovación como un proceso holístico y multifuncional, apoyado fundamentalmente por las premisas que se exponen a continuación:

- Existen diversos significados de un mismo objeto tecnológico;
- Se analizan procesos y no etapas;
- Tanto conflictos como intereses, así como las negociaciones, son consideradas en los procesos de innovación;
- Un artefacto técnico no puede ser descontextualizado;
- Los períodos y la interacción de los conocimientos para innovar no son parte de una acumulación lineal temporal;
- Ninguna disciplina aislada puede explicar la innovación tecnológica; y
- El proceso está constituido por actores humanos y no humanos.[27]

A pesar de ofrecer mayores elementos y premisas de análisis más profundas, los mismos autores concluyen que la TIIN "por sí sola tampoco presenta una

[26] Dave Horton, Paul Rosen y Peter Cox, *Cycling and society*, Reino Unido, Ashgate Publishing Company, 2007, pp. 5,6.

[27] Rodrigo Díaz y Martha Lee, *La innovación tecnológica: dos aproximaciones…*, *Op. Cit.,* p. 64 (subrayado propio).

alternativa suficiente para lograr una visión comprensiva del origen, causas, trayectorias y destinos de las nuevas tecnologías, en particular, su principal insuficiencia es minimizar el carácter instrumental de la innovación". A partir de esta idea, surge la inquietud de explicar desde las Relaciones Internacionales cómo se construyen y transforman las tecnologías de información y comunicación en el marco de la globalización, así como indagar cuáles son las tendencias globales actuales.

Para lograr lo anterior, es importante conocer cuáles son las principales escuelas y enfoques teóricos que articulan la TIIN. Díaz y Lee ofrecen un panorama general pero no profundizan en éste; ni siquiera logran articular un marco explicativo tan acabado como en el caso de la tradición instrumental de la innovación tecnológica. Sin embargo, resultaba necesario prestar atención a los planteamientos que hacen en torno a esta tradición porque logran exponer, de manera general, cómo se han articulado otras propuestas.

Por ello, a continuación, se presentarán los principales exponentes de los estudios sobre ciencia, tecnología y sociedad: la construcción social de la tecnología y la teoría del actor red; sus principales postulados, así como las rutas críticas que orientan los análisis sobre la innovación tecnológica desde la perspectiva interpretativa de dichas escuelas.

1.3 Los estudios CTS

Bajo el nombre de *estudios de ciencia, tecnología y sociedad* (CTS), se agrupan los distintos trabajos que permiten comprender la forma en que la ciencia y la tecnología permean espacios sociales distintos, constituyéndose como un campo disciplinar que ha contribuido sustantivamente al análisis de la innovación desde una perspectiva interpretativa y como un esfuerzo teórico para explicar el carácter social, político, filosófico, económico e histórico de la ciencia y la tecnología.[28]

Los estudios CTS no comprenden una sola corriente o teoría predominante, son una confluencia de investigaciones y estudios de disciplinas heterogéneas cultivados principalmente por epistemólogos, historiadores, filósofos, sociólogos y antropólogos, desde mediados de la década de los sesenta del siglo pasado. Entre estos se encuentran trabajos llevados a cabo desde sociologías de la ciencia, sociologías de la tecnología, historiografías de la ciencia y la tecnología, políticas de la ciencia y la tecnología, antropología cognitiva y comparativa, antropología del uso y la construcción de tecnologías, psicología de la ciencia, filosofía de la ciencia y la técnica, teorías y modelos de gestión y distribución del desarrollo y la innovación científicos, entre otros. Al respecto, Tomás Sánchez-Criado y Florentino Blanco ahondan al hablar de su carácter analítico:

> El propósito es hacer una reflexión analítica y empírica sobre las relaciones entre: los métodos de la ciencia y su normatividad, las formas particulares de 'socialización' científica (realizando estudios de los científicos al estilo de cualquier otro grupo o 'tribu' humana), la generación de sus productos, su distribución y apropiación por parte de otros, las condiciones de construcción de formas de argumentación, regímenes de percepción y prueba y el despliegue de redes de comercio científico… En general, las tecnologías y los hechos científicos son tratados como productos de procesos de construcción ligados a determinados parámetros teórico-metodológicos que hacen 'visibles' determinadas cuestiones y no otras, no como entidades puras y ahistóricas (SIC) listas para la observación sin mediación de ningún elemento. El interés es observar las formas de mediación ejercidas e

[28] María Josefa Santos Corral (Coord), *Perspectivas y desafíos de la educación, la ciencia y la tecnología*, México, UNAM, 2003, p. 141.

intentar tratar de otra manera las relaciones entre Ciencia, Conocimiento, Prácticas, Tecnologías y Políticas.[29]

Los estudios CTS encuentran su fundamento en el cuestionamiento del carácter instrumental y determinista de los estudios previos sobre ciencia y la tecnología, donde la noción de éstas dos se articulaba en una relación metonímica con la idea de progreso. Por lo que la relación ciencia-tecnología-sociedad constituye una ruptura fundamental con la tradición optimista que entendía a la tecnología como una actividad liberadora y neutral, no susceptible de ser juzgada.

Dicha visión comenzó a desplomarse cuando surgieron diversos fenómenos dentro de la sociedad internacional, que se ligaron a los desarrollos tecnológicos asumidos como inhumanos y peligrosos. Por ejemplo, la Guerra de Vietnam, la contaminación ambiental y el armamentismo creciente, fueron algunos de los catalizadores de diversas protestas sociales que, a su vez, fueron retomadas por científicos e investigadores sociales para, desde una óptica más realista, cuestionar el modelo lineal de desarrollo científico y tecnológico. Paralelamente, se concibieron tecnologías alternativas no agresivas con el ambiente y más adecuadas a las estructuras sociales básicas y comunitarias.

Así, los estudios de CTS surgieron como campo académico explícito de enseñanza e investigación en Estados Unidos a partir de movimientos sociales que les dieron fondo:

- grupos de desobediencia civil que cuestionaban la tecnología fuera de control que había envenenado el suelo, los árboles, el agua, etcétera;
- manifestaciones en contra de la energía nuclear; y
- grupos de activistas preocupados por la investigación en biología molecular e ingeniería genética.

Al tiempo que, en Europa, surgían preocupaciones similares que llevaban a resultados análogos:

[29] Tomás Sánchez-Criado y Florentino Blanco, *Constructivismos ante el Reto de los Estudios de la Ciencia y la Tecnología*, publicado en AIBR, Revista de Antropología Iberoamericana, edición electrónica, No. Especial, noviembre-diciembre 2005, Madrid, Madrid, p. 2, consultado en http://www.aibr.org/antropologia/44nov/articulos/nov0519.pdf [mayo 2018]

- En Gran Bretaña, el estudio de Derek J. de Solla, "Price, Little Science, Big Science… and Beyond", publicado en 1963, impulsó los debates sobre lo que parecía ser un crecimiento exponencial potencialmente desastroso del financiamiento de la tecnología por parte del Estado, lo que promovió la idea de hacer ciencia de la ciencia;[30]
- Dinamarca empieza a reivindicar estudios sobre evaluación tecnológica desde el plano de la cultura política; y
- En Holanda se establecen tiendas de ciencia, donde ingenieros y científicos suministraban información y opinión experta a cualquier grupo, comunidad, sindicato u organización que quisiera ésta para usarla en su trabajo.[31]

Para entender cabalmente el proceso de formación de los estudios CTS, a estas preocupaciones sociales hay que agregar la influencia de los trabajos desde una perspectiva weberiana, marxista, pero, sobre todo, del campo de la sociología normativa que concibió a la ciencia como un sistema social y como una institución, con normas y valores propios. Con respecto a los cada vez más estrechos vínculos entre ciencia, tecnología y sociedad, Rosalba Casas señala lo siguiente:

> En ocasiones es difícil separar los estudios sociales de la ciencia, de los de la tecnología y la innovación, sobre todo durante la última década en que se observa una tendencia a considerarlas de manera integral. Esto, desde nuestra perspectiva, se debe a la adopción de nuevas prácticas en la producción de conocimiento, en la que éste es concebido como un proceso lineal en el que los vínculos entre ciencia, tecnología e innovación se dan de manera interactiva y por tanto los análisis de estas actividades en el futuro dejarán de estar tan marcadamente separados como lo estuvieron en el pasado. De aquí se desprende el planteamiento de que la diferenciación disciplinaria en este campo será cada vez menos operativa, por lo que se requiere avanzar hacia la investigación interdisciplinaria y por ende hacia la consolidación del campo de los estudios sociales de la ciencia y la tecnología que integren los diferentes

[30] Texto completo: Derek J. de Solla, *Price, Little Science, Big Science… and Beyond*, Columbia University Press, Nueva York, 1986, 301 pp., consultado en: http://www.andreasaltelli.eu/file/repository/Little_science_big_science_and_beyon_.pdf [11 de enero de 2016].

[31] Stephen Cutcliffe, *Ideas máquinas y valores: los estudios de ciencia tecnología y sociedad,* Anthropos-UAM, España, 2003, pp. 150-200 [subrayado propio]

> enfoques que hasta ahora se han desarrollado, muy ligados a ciertas disciplinas.[32]

No obstante, resulta conveniente diferenciar los enfoques teóricos de la ciencia con los de la innovación tecnológica, teniendo presente que ambas actividades, como se ha mencionado reiteradamente, se encuentran imbricadas. En relación al desarrollo de los estudios sobre la ciencia, Casas señala lo siguiente:

> En el terreno teórico, los estudios contemporáneos de la ciencia tienen una ecología diversificada; hay nichos weberianos, marxistas y durkheimnianos que coexisten y que han llegado a constituirse en tradiciones sociológicas que se encuentran vigentes: a) el sistema social de la ciencia; b) el paradigma kuhniano; c) los estudios marxistas de la ciencia que son, de acuerdo con Restivo, la alternativa tradicional más obvia al paradigma mertoniano-kuhniano; d) la teoría del conflicto, que se basa en las teorías de Marx, Weber y Durkheim, y que construye la explicación de la ciencia sobre las bases establecidas de la teoría de la estratificación y la organización en la sociología en general y, e) la construcción social de la conjetura, que de acuerdo con Restivo, tiene sus raíces clásicas en el trabajo de Marx y especialmente en el de Durkheim.[33]

En efecto, en las ciencias sociales frente a la ciencia como quehacer e institución, se encuentran numerosos exponentes que desde diversos enfoques teóricos han procurado analizar cómo ha sido la evolución de ésta y cuáles son los retos que enfrenta en espacios de tiempo o contextos específicos.

En el campo de la Sociología, se genera uno de los primeros enfoques para el estudio social de la ciencia que ha tenido una fuerte influencia y que la concibió como un sistema social y como una institución. El objeto central de este enfoque fue la identificación de la ciencia como un objeto social con valores y normas. Este hecho representa un giro cognitivo muy importante, ya que se buscó desde un inicio estudiar el contenido de la caja negra del conocimiento científico. Aquí se destacan las aportaciones de Robert Merton, quien desde la perspectiva funcionalista procuró conocer los diversos roles de la comunidad científica y los intercambios que se generan entre los grupos que la integran.

---

[32] Rosalba Casas, *Los estudios sociales de la ciencia y la tecnología: enfoques, problemas y temas para una agenda de investigación*, en Santos Corral, María Josefa (Coord), "Perspectivas y desafíos de la educación, la ciencia y la tecnología", UNAM, México, 2003, p. 143.
[33] *Ibíd*., p. 144.

Robert Merton fue el mayor exponente de esta nueva forma de concebir la actividad científica y, junto con otros colegas (Ellul y Munford), explicaban el funcionamiento de la ciencia en su ámbito institucional y organizacional. La ciencia operaba dentro de un conjunto de normas a partir de las cuales los científicos desarrollaban un conocimiento objetivo de la naturaleza y su funcionamiento. Por otro lado, la escuela sociológica francesa pone énfasis en tres conceptos clave: 1) la ruptura y distinción entre naturaleza y sociedad; 2) el problema de las redes; y 3) la definición de actores, tanto humanos como no humanos.

En América Latina, se dieron propuestas en los años setentas que intentaban incluir el contexto social, ya fuera centrándose en aspectos de tipo institucional de la investigación científica o analizando la historia de hallazgos o inventos significativos y su repercusión al interior de una disciplina, también se iniciaron estudios dedicados a reseñar las grandes obras ingenieriles de la región. Pero el centro de los estudios CTS durante esa y la siguiente década se conformó alrededor de las políticas científicas y tecnológicas basadas en las plataformas internacionales que se adoptaron en la región en busca del despegue económico, promovidas por CEPAL, UNESCO y OEA, entre otras.[34]

Destaca también el proyecto Bariloche, que entre 1974 y 1976 se propuso discutir el modelo prospectivo del club de Roma. Las formulaciones de Jorge Sábato sobre el papel de las relaciones CTS en la dinámica del desarrollo y propuestas de un modelo de ciencia no dependiente; las concepciones de Oscar Varasavsky sobre estilos tecnológicos y proyectos nacionales y, por último, los trabajos de Jorge Katz en el campo de la economía del cambio tecnológico.[35]

En la década de los noventa del siglo XX emergen nuevas preocupaciones y nuevos enfoques para analizar la forma en que se produce y transfiere el conocimiento científico. John Michael Ziman discute las distintas formas en que se produce el conocimiento científico y Michael Gibbons desarrolla una propuesta que

[34] Javier Jiménez Becerra, *Origen, desarrollo de los estudios CTS y su perspectiva en América Latina*, FLACSO, Publicado en "Ciencia, política y poder. Debates contemporáneos desde Ecuador", Edición electrónica, noviembre 2010, Ecuador, pp. 3-4, consultado en https://www.researchgate.net/publication/259043117_Origen_desarrollo_de_los_estudios_CTS_y_su_perspectiva_en_America_Latina [abril 2018]

[35] *Ibíd*., pp. 4-5.

sostiene que existe una nueva forma de producción de conocimiento, que se vincula con su posible aplicación y las consecuencias de ésta. Convendría señalar que la década de los noventa representa un parteaguas en la historia de la ciencia y la tecnología, sobre todo por el contexto en el que se realizan las aportaciones: un espacio cada vez más complejo e interconectado por la diseminación de las tecnologías de información y comunicación, por una parte, y por la otra, debido a los grandes cambios políticos a nivel internacional.

Otros sociólogos destacados que van más allá del funcionalismo mertoniano son :

- Mulkay, quien sitúa al conocimiento científico como dependiente del contexto social, modelado por el entorno, pero también por los intereses de los científicos (stablishment);
- Bloor aboga por un programa fuerte, todas las pretensiones del conocimiento falsas y/o verdaderas deben de ser explicadas por las mismas razones sociales no racionales, donde no solo la conducta de los científicos, sino también el contenido de la explicación científica es construido;
- Collins muestra cómo los científicos usan una amplia gama de creencias negociadas y mediatizadas socialmente para llegar a un consenso; y
- Bruno Latour hace análisis etnográfico y del discurso siguiendo los métodos antropológicos de campo. Observa la ciencia en acción y encuentra que todos los hechos científicos son construidos socialmente, a partir de argumentos y persuasiones que llevan a la construcción de una red que sirve para esconder los hechos científicos de su carácter social.[36]

Todos estos elementos fueron definiendo un campo de trabajo de carácter crítico respecto a la tradicional imagen esencialista de la ciencia y la tecnología, buscando comprender la dimensión social del desarrollo, adaptación y difusión científico tecnológico. A partir de esto se puede establecer que la innovación tecnológica es un proceso inherentemente social, donde elementos no epistémicos o técnicos como por ejemplo valores morales, convicciones religiosas, intereses

[36] María Josefa Santos y Marco Antonio Lopátegui, *La Construcción Global de la Ciencia y la Tecnología Bajo la Lupa de los Enfoques CTS*, en Castañeda, Dávila y Morales (Coord), "El futuro de las ciencias sociales en un entorno social globalizado", UNAM, México, 2017, p. 259.

profesionales o presiones económicas, desempeñan un papel decisivo en la génesis y consolidación de las ideas científicas y los artefactos técnicos.

Esta nueva relación ciencia-tecnología-sociedad se concentra en diversos planos, tanto en los campos de estudio académico y como en el activismo social, en los niveles de reflexión ética y en las nuevas tendencias educativas sobre el tema.

Como lo mencionan Santos y Díaz, "podemos dar un paso más y considerar a la tecnología como un símbolo en sí misma y, como cualquier símbolo, la tecnología estructura nuestros mundos social y natural"; por lo que se pueden dar distintas rutas en múltiples investigaciones de las Ciencias Políticas y Sociales, desde las Relaciones Internacionales hasta la Administración Pública, pasando por las Ciencias de la Comunicación, la Ciencia Política y la Sociología, que consisten en estudiar las diversas interpretaciones que el símbolo tecnología provoca en los grupos sociales y cómo se convierte en un elemento básico en nuestros campos de batalla globalizados.[37]

Asimismo, los trabajos CTS están ligados a dos grandes tradiciones, la europea y la norteamericana. La primera, más vinculada a los trabajos de filosofía de la ciencia, de la sociología del conocimiento científico y de la historia de la tecnología, centró su eje explicativo en el proceso de construcción social de la tecnología, mientras que la segunda, ligada desde sus inicios con la relación sociedad-economía-tecnología, se ubicó en el análisis de las consecuencias socioeconómicas de las innovaciones tecnológicas y su influencia en nuestras formas de vida e instituciones.

Con el fin de tener una visión más puntual, se esboza la revisión de los planteamientos teórico-metodológicos de los dos esquemas explicativos de mayor relevancia, de entre el cúmulo de estudios de los estudios CTS: la Construcción Social de la Tecnología, como una propuesta de análisis que explica el surgimiento, consolidación, adopción y evolución de una tecnología y; la Teoría de Actor Red,

[37] Josefa Santos y Rodrigo Díaz, *El análisis del poder en la relación tecnología y cultura: una Perspectiva Antropológica*, en Santos Corral, M. J. (coord.), "Perspectivas y desafíos de la educación, la ciencia y la tecnología", México, IIS-UNAM, 2003, pp. 381.

que permite seguir las redes sociales de los actores que son clave en los procesos de innovación tecnológica.

1.3.1 La Construcción Social de la Tecnología

Los programas de desarrollo industrial y los documentos de las organizaciones internacionales, entre los años cincuenta a ochenta del siglo pasado, intentaban implantar la idea de que las innovaciones tecnológicas, por sí mismas, llevarían el desarrollo a los países. Esto provocó el interés de los estudios CTS por el cuestionamiento en las relaciones que se habían pensado entre la sociedad, la ciencia y la tecnología, a través de lo que se conoce como el modelo lineal del desarrollo.

La discusión resultó en varias propuestas, entre las más destacadas está el giro interpretativo conocido como construcción social de la tecnología, a partir del cual se planteó demostrar la naturaleza socialmente contingente en la construcción del conocimiento científico y la creación de tecnologías, sistemáticamente organizado a partir de actividades aparentemente muy desordenadas.

Javier Jiménez explica que este desprendimiento del constructivismo presume que la tecnología está influenciada por componentes socioculturales, "se hace énfasis en que la tecnología contiene elementos sociales y que los diversos intereses de los grupos humanos desempeñan un papel importante en el momento de tomar una decisión sobre ella; decisión que guarda relación con su diseño, desarrollo, apropiación e implementación."[38]

La propuesta concreta aparece en una obra de 1987: *The Social Construction of Technological Systems. New Directions in the Sociology and History of Technology*, editado por Trevor J. Pinch, Wiebe E. Bijker y Thomas P. Hughes.[39] En ésta se compilaron ensayos escritos por reconocidos investigadores de lo que se ha denominado la concepción interpretativa de la innovación tecnológica, particularmente de sus dos corrientes de mayor reconocimiento, la construcción social de la tecnología (en adelante COST) y la Teoría del Actor Red.

[38] Javier Jiménez Becerra, *Origen, desarrollo de los estudios CTS…, Op. Cit.,* p. 6.
[39] Trevor J. Pinch, Wiebe E. Bijker y Thomas P. Hughes, *The Social Construction of Technological Systems. New Directions in the Sociology and History of Technology*, MIT Press, Estados Unidos, 198, 470 pp.

Para ilustrar sus observaciones a partir de las categorías de análisis de la COST, Bijker y Pinch realizan una reevaluación de la historia de la bicicleta aplicando nuevas herramientas metodológicas. La historia breve, popular y heroica de la bicicleta cuenta que se desarrolló en Estados Unidos y se resumía en la evolución del artefacto, que poco a poco va pasando de diseños pobres e inapropiados a uno que finalmente se consolida como el mejor gracias a sus ventajas técnicas.

Se trata del diseño que tiene dos ruedas del mismo tamaño, neumático de caucho, cadena de transmisión y un marco que los une; éste ha cambiado muy poco en los últimos cien años. Como en toda historia mítica, el héroe de ésta es un fabricante único, Alexander Pope, quien, contra viento y marea, logró apropiar el conocimiento de diseño, fabricación y comercialización de la bicicleta de fuentes europeas y consolidar su negocio. En esta versión tradicional y determinista de la historia, el paso significativo por la bicicleta de rueda alta es un mero paso en la "evolución natural" del diseño de las bicicletas.[40]

Pero los promotores de la COST deconstruyen la versión lineal antes mencionada y asumieron el reto de "abrir la caja negra" para entender cómo el diseño mismo de la bicicleta es el resultado de procesos de negociación y de interpretaciones entre grupos sociales. Para ello adaptan los logros de un programa sociológico de análisis del desarrollo de la ciencia. Le llamaron Empirical Programme of Relativism (EPOR) y tenía el propósito de estudiar cómo se construye socialmente el conocimiento científico y poder relacionar el contenido de la ciencia misma con los contextos en que se produce y transfiere.[41]

Para aplicar este análisis, la propuesta de la COST distingue cinco herramientas:

1. Existen **grupos sociales relevantes** asociados con el desarrollo de un artefacto tecnológico que compartían un significado del artefacto, un

[40] Andrés Valderrama, *Teoría y crítica de la construcción social de la tecnología*, en Revista Colombiana de Sociología, No. 23, Bogotá, 2004, p. 217.

[41] Trevor Pinch, *La construcción social de la tecnología: una revisión*, en Santos,M. J. Y Díaz Cruz, R. (compiladores), "Innovación tecnológica y procesos culturales. Nuevas Perspectivas Teóricas", Fondo de Cultura Económica, México, 1997, p. 25, consultado en https://es.scribd.com/document/140890763/Pinch-T-1997-La-construccion-social-de-la-tecnologia-una-revision [agosto 2016]

significado que podía ser usado para explicar las trayectorias particulares del desarrollo e implementación que tomaba dicho artefacto.[42]

2. Hay una **flexibilidad interpretativa**, según la cual existen significados radicalmente diferentes respecto a un artefacto tecnológico, en relación con los diversos grupos sociales asociados al mismo.[43] Esta premisa se refiere a la amplia variedad de usos que se le puede dar a un mismo objeto tecnológico y que va más allá de lo que conciben los diseñadores.
3. El tercer componente es el **mecanismo social de cierre**, a partir del cual se afianzan las controversias iniciadas, según el cual se limita la flexibilidad interpretativa de un artefacto y se imponen las visiones más aceptadas,[44] ya sea por la demostración de la ventaja técnica *per se*, por la propaganda de la funcionalidad del artefacto o por la influencia de los grupos sociales con mayor poder, entre otros factores.
4. El cuarto es el **marco tecnológico**, que se refiere al conjunto de conceptos y técnicas empleados por una comunidad para la solución de problemas,[45] es decir, que dentro del contexto en el que una tecnología se desarrolla hay toda una serie de conocimientos científicos, técnicas y estructuras sociales que alimentan la consolidación y permanencia de cierta innovación tecnológica.
5. En quinto lugar, hay **distintos grados de inclusión** dentro del marco tecnológico: quienes están más incluidos tienden a operar dentro de la lógica del marco y quienes están menos centrados, en algunos casos, tienden a producir cambios radicales.[46]

Con base en la propuesta analítica de la COST, Pinch y Bijker examinaron el caso de la bicicleta con los siguientes resultados.

---

[42] *Ibíd*., p. 26.
[43] *Ibíd*., p. 27.
[44] Andrés Valderrama, *Teoría y crítica de la construcción…*, *Op. Cit., p. 219.*
[45] Wiebe Bijker, *Of Bicycles, Bakelite and Bulbs. Toward a Theory of Sociotechnical Change*. Cambridge, The MIT Press, 1997, p. 111.
[46] Andrés Valderrama, *Teoría y crítica de la construcción…*, *Op. Cit.,* p. 219

Identificaron los grupos sociales relevantes que rodearon el desarrollo del artefacto en cuestión: los hombres, las mujeres, los niños, los viejos, los fabricantes de bicicletas, colegios de ingenieros, entre otros. Cada grupo tenía varias características que lo hacían más o menos relevante para que el diseño de la bicicleta permitiera un uso socializado, por ejemplo, las mujeres de la época usaban vestidos largos que dificultaban que montaran bicicletas de ciertos diseños o medidas, mientras que otros grupos podían hacer mayor uso de bicicletas que tuvieran, por ejemplo, ruedas muy altas.[47]

Se aplicó el concepto de la flexibilidad interpretativa en relación con los diversos grupos sociales asociados al artefacto. Así, distinguieron que la rueda alta en el diseño de la bicicleta tenía un significado de poder y virilidad, puesto que sólo podían utilizarla hombres adultos y sanos, mientras que para personas de mayor edad, niños y mujeres, resultaba complicado socializar su uso. Por eso, grupos de diseñadores, ingenieros y fabricantes de bicicletas, con el interés de difundir el artefacto, diversificaron el diseño atendiendo a las necesidades de los grupos sociales, presentando adaptaciones a la seguridad y accesibilidad en su uso. [48] Esto permitió que otros grupos sociales se fueran apropiando de dicha tecnología y le dieran nuevos significados, por ejemplo, una alternativa de movilidad y de utilidad para la salud.

Después de un proceso de diferentes propuestas técnicas en los diseños, de socialización del producto entre los grupos más relevantes y de resignificación para la sociedad, con la popularización en el mercado del modelo “Facile”, que mostraba un diseño más seguro y accesible para casi cualquier usuario, finalizaron algunas controversias y se afianzaron otras, definiendo diversos mecanismos de cierre.[49]

En este caso fue el grupo social de los fabricantes, quienes, a través de la publicidad, penetraron entre los consumidores para convencerlos de que el modelo “Facile” (que tenía dos ruedas de 40 o 42 pulgadas, del mismo tamaño y cadena de trasmisión y llanta neumática) superaba los contras que otros diseños de bicicletas tenían. Otro mecanismo de cierre fue la controversia por redefinición o

[47] Trevor Pinch, *La Construcción Social …*, *Op. Cit*., p. 26.
[48] Andrés Valderrama, *Teoría y crítica de la construcción…*, *Op. Cit.,* p. 220
[49] *Ibíd*., p. 221

desplazamiento del problema, solucionado por el neumático de caucho, que en un principio no tenía aceptación entre los diseñadores por la estética y la estabilidad, pero al ser probado se demostró que ofrecía ventajas en la velocidad, por lo que el neumático se constituyó no en una solución a la estética o la estabilidad, sino en una gran ventaja en la velocidad del vehículo, provocando que se olvidaran las otras cuestiones, logrando cerrar la controversia por la redefinición del problema.[50] Así se terminaba con las controversias técnicas sobre la utilización el artefacto y el éxito comercial del modelo "Facile" afianzó su socialización, al darse la apropiación de la bicicleta entre varios grupos sociales de hombres, mujeres, personas mayores y niños.

El marco tecnológico en el que se desarrolló la bicicleta contribuye a un análisis más acabado, puesto que se explica que dicho artefacto no apareció por una invención individual, sino que el contexto tanto técnico como social, permitió que se desarrollara. La bicicleta no es un único artefacto, más bien tiene diversos componentes que no existieron en otro contexto, como la rueda neumática, y su necesidad de uso no se produjo antes del incremento de producción industrial y del crecimiento de las ciudades, lo que obligaba a tener más opciones de movilidad.[51] Se tuvieron que dar un conjunto de factores técnicos y una serie de fenómenos en las estructuras sociales que alimentaron la consolidación y permanencia de la bicicleta.

Por último, al analizar el rol de los diferentes grupos sociales en la consolidación de la bicicleta, no se debe dar por sentado que unos tenían mayor grado de inclusión que otros, y que su capacidad de influir tanto en el diseño como en la producción, la comercialización y el consumo del producto los hacía más o menos relevantes, y a la vez, los obligaba a impulsar cambios menos o más radicales. Por el contrario, los grupos sociales de hombres adultos, blancos y sanos tenían un mayor grado de inclusión dentro del marco tecnológico de la bicicleta de rueda alta e influían en que así se mantuviera el diseño, mientras que los grupos con menor grado de inclusión tendían a considerar soluciones radicales con mayor

[50] *Ibíd*., p. 222.
[51] Trevor Pinch, *La Construcción Social …, Op. Cit*., p. 27.

facilidad, como modificar el tamaño de las ruedas e introducir el material de los neumáticos.[52]

De acuerdo a la COST, las innovaciones tecnológicas no siguen una trayectoria "natural", sino que son dependientes de los contextos en los cuales se desarrolla, envuelve a muchas más personas que un solo y único inventor; se rodea de la influencia de grupos sociales enteros en interacción continua sobre ciertos períodos de tiempo; asimismo, se revelan las tensiones y las relaciones de poder de las sociedades en las que se desarrolla cierta tecnología.

La COST establece premisas puntuales, generalizaciones teóricas y matices políticos, para llegar a entender la relación ciencia-tecnología-sociedad. De esta manera, se abrió la "caja negra" para encontrar respuesta a la inquietud sobre cómo llega un artefacto a ser lo que finalmente es, no sólo en términos de su diseño sino en cuanto al significado simbólico, de función y de uso que le otorga una sociedad.

Para el momento en que apareció como una propuesta teórica-metodológica, a mediados de los ochenta del siglo XX, la COST, de Bijker y Pinch, era una respuesta radical a las visiones lineales, acumulativas y deterministas de la ciencia y la tecnología.

1.3.2 La Teoría del Actor Red

En la corriente de estudios CTS, que buscaban alternativas de explicación sobre los procesos de innovación y la forma en que interactuaban la ciencia, la tecnología y la sociedad, Michael Callon fue el principal exponente de la Teoría del Actor Red. A mediados de los ochenta, como muchos investigadores, también buscaba explicar "los mecanismos de poder de la ciencia y la tecnología, revelando los modos en los que los laboratorios simultáneamente reconstruyen y relacionan los contextos sociales y naturales sobre los que actúan."[53]

Este enfoque supone que los centros de investigación y desarrollo, privados y públicos, producen cambios en la sociedad, por lo que es necesario caracterizar el modo en que lo hacen, lo que implica examinar lo que ocurre en su interior, así

[52] Andrés Valderrama, *Teoría y crítica de la construcción…*, *Op. Cit.,* p. 222

[53] Michael Callon, *The sociology of an actornetwork: The case of the electric vehicle*, en Callon, Law and Rip (Editores), "Mapping the dynamics of Science and Technology", Macmillan, Reino Unido, 1986, p. 20.

como los mecanismos que les permiten actuar sobre la sociedad en toda su extensión. El análisis incluye la caracterización de estrategias, intereses y relaciones de poder entre los diversos actores.

Callon establece que los científicos y los desarrolladores de tecnología están produciendo cambios constantemente, mediante la creación de nuevas variaciones y asociaciones entre las entidades que componen la sociedad. Para dar cuenta de este proceso, Callon propone la definición de tres conceptos que permitirían cumplir con dicho propósito: de actor-mundo, de traducción y de actor-red. Ahora bien, la asociación se da porque el actor-mundo crea asociaciones de entidades heterogéneas, a través de procesos de traducción entendidas, en principio, en tres sentidos: hablar por, ser indispensable y desplazar.[54]

El conjunto de los actores-mundo y los procesos de traducción (hablar por, ser indispensable y desplazar) constituye lo que Callon denomina el actor-red. Esto es, una entidad compuesta por múltiples entidades cuyas asociaciones están en permanente negociación. Así, un actor-mundo es una red, cuyos nodos son identificables: municipios, ministerios, celdas de combustión, etcétera; y sus enlaces son las relaciones entre estos.

Cada nodo visto por dentro, es una red en sí mismo: las celdas aglutinan componentes, mecanismos, investigadores, etcétera. Callon denomina simplificación cuando varios elementos se componen en una red en sí misma y se convierten en nodo. El conjunto de personas, instituciones y lugares geográficos puede ser simplificado en el gobierno o instancia local que impulsa los cambios. Asimismo, según Callon, existe una yuxtaposición de actores cuando cada nodo también se define, dentro del actor-red, en relación a otros nodos.[55]

Posteriormente, Bruno Latour profundizó en los conceptos de la Teoría del Actor Red, al explicar que los desplazamientos se verifican a través de actores cuya mediación es indispensable para que ocurra cualquier acción, “en vez de una oposición rígida entre el contexto y el contenido, las cadenas de traducciones se

[54] Andrés Valderrama, *Teoría y crítica de la construcción…*, *Op. Cit.,* p. 225.
[55] Ibíd., p. 26.

refieren al trabajo mediante el que los actores modifican, desplazan y trasladan sus distintos y contrapuestos intereses."[56]

El planteamiento de Latour implica una extensión de la genealogía a las relaciones entre humanos y no-humanos, lo que hace que la palabra 'actor' sea extensible a cualquier entidad que actúe en un sentido semiótico, es decir, que influya, transforme o modifique las interacciones durante el proceso de innovación y que pueda ser observada empíricamente en el proceso de producir dicha modificación (por ejemplo, un electrón o un chip). Según Latour, las controversias no se dan sólo en el plano de las teorías o problemas técnicos sino en todos los puntos efectivos de interacción, donde se producen conflictos. Su planteamiento consiste en analizar todas las instancias por las que pasa la consolidación de una tecnología.[57]

En ese proceso se podrían incluir desde los esfuerzos de un director de un laboratorio por conseguir financiación para sus experimentos, hasta las formas de argumentación científica o realizaciones técnicas que se ponen en juego para convencer a otros colegas y generar aliados, así como los actores no-humanos para producir lo que se quiere constituir (materias primas, insumos, maquinaria). Ninguno de estos elementos mencionados puede ser concebido como interno o externo, sino que toda la cadena de traducciones para consolidar una innovación tecnológica es crucial para su existencia, para que devenga en una finalización del producto (algo parecido al cierre propuesto por la COST).

Para aplicar la teoría del actor red a un fenómeno concreto, Michael Callon expone el caso del vehículo eléctrico en Francia. Cuando se dio la crisis energética mundial de principios de la década de 1970 en dicho país, los ingenieros de Electricité de France (EDF) -una élite técnica acomodada en las alturas de una de las organizaciones estatales de mayor poder- vislumbraban que la era industrial estaba llegando a su fin y se avecinaba un cambio sustancial en la sociedad,

[56] Bruno Latour, *La esperanza de Pandora. La realidad de los Estudios de la Ciencia*, traducción de Tomás Fernández Aúz, editorial Gedisa, España, 2001, p. 370.

[57] Bruno Latour, *La ciencia en acción. Cómo seguir a los científicos e ingenieros a través de la sociedad*, traducción de Eduardo Aibar, Roberto Méndez, Estela Ponisio, editorial Labor, España, 1992.

querían participar y ser motores del cambio. EDF se asume como el actor-mundo, Callon así lo expresaba:

> EDF no es un actor que se enfrenta con tecnologías nuevas y poco familiares o con el conocimiento localizado en la sociedad. Tampoco es una construcción imaginaria que puede ser considerada como irreal por un sociólogo experimentado. Tampoco es un mundo simple. Es lo que proponemos llamar un actor-mundo, un mundo donde EDF, su primer motor, es una parte. EDF compone una lista de entidades y una lista de lo que hacen, piensan, quieren y experimentan. Estas entidades no son solamente humanas, sino que también incluyen electrones, catalizadores, electrolitos y acumuladores de plomo. Estas entidades actúan, reaccionan y se cancelan mutuamente del mismo modo que las entidades tradicionales.[58]

La lectura en EDF los llevaba a concluir que la sociedad estratificada, donde el automóvil de gasolina jugaba un rol de estatus característico, estaba viendo sus últimos días. Esto se evidenciaría en la concepción y uso de un nuevo modo de movilización. Se trataba del vehículo eléctrico, más limpio pero menos potente, que reemplazaría por completo el automóvil de combustión interna.

Para conseguir ese cambio, los ingenieros de EDF tenían que alcanzar varios objetivos técnicos y no técnicos. Por un lado, tenían que lograr que los acumuladores de zinc/ aire, los acumuladores de plomo y las celdas de combustión fueran efectivas y baratas. Por otro lado, debían movilizar a los ministerios implicados que darían los subsidios y estímulos necesarios para que los municipios de Francia adoptaran medidas favorables a los vehículos eléctricos. Asimismo, tenían que convencer a los consumidores de que la alternativa de los vehículos eléctricos era la más atractiva por cuanto se alineaba con los objetivos sociales propuestos por los principales movimientos sociales de renovación. Incluso consideraban que una compañía del tamaño de Renault debía renunciar a sus intenciones de ser la productora de automóviles más grande y poderosa de Europa y asumir el rol de ser sólo una ensambladora de los vehículos eléctricos diseñados por la Compagnie Générale d'Electricité (CGE).[59]

[58] Michael Callon, *The sociology of an actornetwork…, Óp. Cit.*, p. 22.
[59] Andrés Valderrama, *Teoría y crítica de la construcción…, Op. Cit.,* pp. 223-224.

Con base en la teoría, EDF traduce a Renault las celdas y los consumidores asignándoles identidad, intereses, roles y un curso de acción. Se atribuye la responsabilidad de ser quien hable por estas entidades en un futuro: EDF es vocero de la Renault que acepta ensamblar y renuncia a su poder, es vocero de los consumidores que optan por el vehículo eléctrico y es vocero de las celdas de combustible baratas y eficaces. En suma, EDF determina la identidad de los elementos y regula su comportamiento y evolución, así explica Callon el modo en que un grupo proyecta un mundo futuro, lo convierte en actores y roles, y procede a convencer a las entidades actuales para que asuman su parte.

No obstante, las entidades se resisten a seguir el guion asignado: Renault no quiere reducir su poder, las celdas no logran ser baratas y eficaces y los consumidores quieren seguir comprando carros de gasolina. Por lo que se intenta crear una "geografía de puntos obligatorios de paso", es decir, una configuración de cosas que obligue a las entidades presentes a acudir a EDF para seguir existiendo. Por eso se debe instalar al vehículo eléctrico en el centro de un problema a resolver, como el problema de la contaminación o el del transporte, o ambos. Pero antes se debe resolver un problema técnico: aumentar la vida útil de los acumuladores de zinc/aire o de plomo o de las celdas y para ello tiene que recurrir a grupos de investigación y desarrollo. De este modo, EDF trata de construir una situación donde ella misma es un punto de paso obligado. Solo cuando suceda esto, los actores dependerán de los avances y logros de los laboratorios de EDF:

> Para que todo tenga efecto es necesario lograr que las diferentes entidades acepten los roles asignados. Esto requiere de un gran esfuerzo: hay que desplazar a los ministerios para que adopten una política; a Renault para que quiera ensamblar vehículos eléctricos; a los acumuladores para que sean baratos, eficaces y durables. Estos desplazamientos se logran haciendo circular una gran cantidad de inscripciones: memorandos, documentos, estudios, reportes... comunicaciones que van y vienen, que invitan, que producen reacciones y que, en últimas, producen desplazamientos en las entidades. Cuando estos desplazamientos coinciden con lo esperado por el centro de circulación, en este caso EDF, se dan los cambios deseados.[60]

[60] Ibíd., p. 225.

Todas esas entidades son actores mundo y el conjunto de los actores-mundo y los procesos de traducción son los actores red. En este caso, el rol de Renault se define en relación a los roles y acciones de EDF, CGE, los ministerios, los consumidores, los acumuladores, etcétera.

Según Callon, su modelo amplía considerablemente el espectro de relaciones sociales para dar cuenta de un cambio: hay relaciones contractuales, de poder y de dominación que describir y analizar; pero también se requiere entender cómo son las relaciones entre celdas de combustión y motores eléctricos y, para ello, hay que entender, describir y analizar corrientes eléctricas, fuerzas electromagnéticas, contextos de validación, evaluación de pares y procesos de validación de prototipos. Esta visión permite, además, concebir los aparatos no como unidades creadas de una vez y para siempre, sino como asociaciones de elementos dinámicos que, serán tan durables como lo sean los elementos y las asociaciones que existen entre ellos. Callon finaliza aseverando que 'el vehículo eléctrico es como el actor-mundo que lo sustenta y es sustentado por el mismo, es un logro científico, político y económico, es una combinación de elementos'.[61]

Los conceptos actores-mundo, actores-red y los procesos de traducción, simplificación y yuxtaposición son la propuesta de la teoría para dar cuenta de las diferentes formas en que la ciencia y la tecnología operan en el mundo, en interacción y dinamismo social. La propuesta de Callon señala que 'no sólo se extiende el repertorio de entidades y procesos de traducción, sino que la composición de este repertorio tampoco obedece reglas definitivas'.[62]

A partir de la revisión de las propuestas analíticas de los estudios CTS, y más puntualmente de la COST y la Teoría del actor red, se pueden dilucidar distintas reflexiones. Se logró discernir la llamada "caja negra", para descubrir que ésta no existe en realidad, sino que era necesario tener un enfoque que volteara su atención al examen de toda una serie de elementos interactivos que permiten, o no, el desarrollo y consolidación de una tecnología, más que de una realización técnica; y que el contexto social, las relaciones de poder, el mercado, entre otros factores,

[61] Michael Callon, *The sociology of an actornetwork…, Óp. Cit.,* p. 23.
[62] *Ibíd.,* p. 33.

están inmiscuidos en un proceso de innovación tecnológica que parecía que sucedía como por arte de magia e impactaba a la sociedad. Los elementos siempre estuvieron allí, pero no se les incluía en los análisis de la tradición instrumental de la innovación tecnológica, metiendo en esa "caja negra" todo lo que lo rodeaba.

La innovación tecnológica es un proceso complejo, con múltiples actores, tiempos de acción e interacciones, no una serie de eventos acumulativos y lineales como lo dictaba la TIIT. Se deconstruye la idea mítica del inventor, como personaje único y determinante para lograr la introducción de una tecnología, ya terminada y aceptada, en la vida de las sociedades. Se reconoce la existencia de diversas alternativas que sucedieron, se intentó que sucedieran o que no pudieron suceder, por la interacción de los actores y factores, y se esclarece el porqué de la consolidación de lo que sí logró permanecer.

Después de revisar la COST y la Teoría del Actor Red, se afianza la intención del presente trabajo, que el investigador, el analista y el lector abandonen de antemano las distinciones analíticas entre ciencia, tecnología y sociedad y acepten el reto de observar que los procesos e interacciones son dinámicos, heterogéneos y diversos.

Esto no implica que la forma de abordar los temas sea caótica, sino que se tengan premisas bien identificadas, a partir de las cuales examinar los casos; que el acercamiento teórico-metodológico tenga una estructura que permita realizar conclusiones prácticas sobre los fenómenos observados, como lo demostraron claramente los ejemplos en que se aplicaron ambas propuestas, representativas de los estudios CTS.

1.4 Caracterización de la innovación desde las Relaciones Internacionales.

Como se ha explicado desde el inicio de la presente investigación, existen diversas formas de abordar a la innovación tecnológica, por eso se presentó una revisión de la evolución de los estudios CTS y, como parte de las ciencias sociales, la disciplina de Relaciones Internacionales también tiene su visión particular.

El entendimiento sobre la innovación de los internacionalistas se enmarca tanto en la parte formal, desde el andamiaje teórico y las premisas de conflicto/cooperación internacional; y desde el objeto material, es decir, en cómo se contextualiza la innovación dentro de los fenómenos sucedidos en la sociedad internacional, en el múltiple entramado de relaciones políticas, económicas y sociales, existentes entre sus actores.

Marcel Merle, si bien no fue el primer analista que introdujo al factor técnico como parte importante del análisis de la sociedad internacional, sí en cambio es de los más reconocidos por su señalamiento sobre la influencia que tenían los "descubrimientos científicos" en las relaciones internacionales y que expresó de la siguiente manera:

> Desde finales del siglo XVIII, la irrupción de la técnica ha producido inmensas transformaciones en todos los niveles de la vida de las sociedades. Indiscutiblemente, ha sido el progreso técnico, fruto de los descubrimientos científicos, el que ha engendrado […] el fenómeno bien conocido de la "aceleración de la historia", mediante la acción que ha ejercido sobre la producción de bienes, el nivel de vida, el género de vida y la vida misma (a causa de las transformaciones de la medicina y de la cirugía). Pero no se observó suficientemente que los efectos combinados de la revolución científica y técnica también se ejercían a nivel de las relaciones internacionales. A este particular, el progreso técnico ha intervenido en dos formas principales: la aceleración de las comunicaciones y la transformación de la producción y de los intercambios.[63]

Asimismo, señalaba que los "progresos técnicos" llevarían a un desarrollo de las comunicaciones tal que los intercambios culturales se exacerbarían, impactando la influencia de la tecnología en la cultura, sobre todo, las transmisiones culturales de las potencias hacia países subdesarrollados. "El impacto de la técnica sobre la difusión y sobre el contenido de la cultura es bien conocido. Si no se atienden las implicaciones internacionales de estas transformaciones, es porque se olvida que los hechos políticos, comenzando por el hecho nacional, son en buena medida

[63] Marcel Merle, *Sociología de las Relaciones Internacionales*, versión española de Roberto Mesa, Alianza editorial, 1991, p. 173.

hechos culturales."[64] Es decir, concebía a la inversa la relación tecnología-cultura de lo que lo hacen los estudios CTS, sobre todo los enfoques constructivistas.

La aportación de Merle fue precisamente centrar la atención en la necesidad de observar 'suficientemente los efectos de este factor a nivel de las relaciones internacionales. De igual forma que en sus apuntes, resalta la aceleración de las comunicaciones y la forma en que los sistemas productivos se iban a revolucionar, así como de la influencia que tendría la tecnología en las transacciones comerciales.

Su visión puede ser encuadrada en la tradición instrumental, al darle una carga valorativa al "progreso técnico" y su influencia determinante 'en la vida misma', pero es entendible ya que Merle analizaba un contexto sociohistórico internacional enmarcado en las décadas posteriores a la Segunda Guerra Mundial, donde las dos grandes potencias promovían la idea de que una innovación tecnológica les daría la delantera en ciertos sectores estratégicos. Basaba su análisis en autores como Marshall McLuhan, cuya visión imperaba por la necesidad, en ese momento, de controlar y orientar las decisiones en el ambiente tecnológico durante la Guerra Fría. Lo que sucedía con Merle y sus contemporáneos es explicado por Santos y Lopátegui:

> Aunque en la mayoría de las ocasiones sólo quedan enunciados los cambios culturales que asumen las formas organizacionales alrededor de estas hipermodernas propuestas socio-técnicas, esto es, los cambios culturales se dan por hechos, no son problematizados, estos trabajos parten de un supuesto básico: los cambios culturales y sociales de las nuevas organizaciones están determinados por el uso intensivo de las tecnologías de telecomunicaciones, y son estas tecnologías, a veces combinadas con otras (como la biotecnología), las ruedas sobre las que van corriendo los nuevos procesos sociales del cambio global.
>
> Desde este enfoque determinista emerge el concepto de sociedad de la información, por mencionar alguno entre muchos otros conceptos que se montan, como ya lo hemos mencionado, sobre las ruedas de la tecnología el andamiaje explicativo para dar cuenta de los cambios observados en las sociedades a nivel global desde mediados del siglo XX.
>
> Obras como La nueva sociedad: anatomía del orden industrial de Peter Drucker (1950); La producción y distribución del conocimiento en los Estados Unidos de Fritz Machlup y La Galaxia Gutemberg de Marshal McLuhan (1962); Sociología

[64] *Ibíd.,* p. 177.

> de las Relaciones Internacionales de Marcel Merle (1974); El advenimiento de la sociedad Post-industrial de Daniel Bell (1976); La informatización de la sociedad de Simon Nora y Alain Minc (1981); Neuroamante de William Gibson (1984); The information society and cultural industries theory de Jean-Guy Lacroix y Gaëtan Tremblay (1997); La era de la información de Manuel Castells (1996); Historia de la sociedad de la información de Armand Mattelart (2001); junto con una amplia variedad de publicaciones y diversos informes de la Unión Internacional de Telecomunicaciones; el Consejo Económico y Social de las Naciones Unidas, la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura; el Banco Mundial; la Organización para la Cooperación y el Desarrollo Económicos; la Unión Europea; la Comisión Económica para América Latina; et. al., conforman un vasto universo de ideas que dan cuenta de los grandes cambios observados desde una perspectiva global y que dibujan una realidad más compleja que los estados capitalistas anteriores por tres cuestiones fundamentales: el nuevo entorno tecnológico, la unificación de los mercados y la universalización de valores y formas de concebir y hacer política.[65]

Para dichos autores, el enfoque determinista se explicaba en un contexto histórico y analítico predominante, basado en el andamiaje explicativo para dar cuenta de los cambios observados en las sociedades a nivel global desde mediados del XX. Como lo mencionan, la visión también fue promovida desde las organizaciones internacionales, actores de los que es importante mencionar su visión sobre la innovación.

Destaca la descripción que ofrece Naciones Unidas, la gran referencia sobre los temas importantes de la agenda global, misma que resalta 'el impacto de la innovación' en el sistema internacional, tal como se refiere a continuación:

> La innovación es el conductor central del crecimiento económico, del desarrollo y de mejores empleos. Es uno de los factores claves que les permite a las firmas competir exitosamente en el mercado global, y es el proceso mediante el cual se encuentran las soluciones a los desafíos sociales, ambientales y económicos. Es la fuente de las mejorías en la calidad de nuestras vidas diarias. Para poder aumentar la capacidad productiva, empleos y trabajos decentes, y para poder erradicar la pobreza de forma inclusiva, sustentable y mediante un crecimiento económico equitativo, debe haber un apoyo considerable a la innovación y acceso equitativo a sus beneficios.[66]

---

[65] María Josefa Santos y Marco Antonio Lopátegui, La Construcción Global…, *Óp. Cit*., pp. 262-263.

[66] Naciones Unidas, *Science, technology and innovation and intellectual property rights: The vision for development*, En Sitio Oficial de Naciones Unidas, mayo 2012, p. 5, consultado en

La referencia destaca los efectos de la innovación, pero carece de un sustento real que demuestre puntualmente la relación causa-efecto de sus impactos esperados, porque no señala elementos que incluyan a todos los componentes, actores y factores, que intervienen en los procesos de innovación. Asimismo, el fundamento de la definición descansa sobre una idea determinista con claros visos de instrumentalidad.

Cabe recordar una definición más amplia, como la de la OCDE –ya referida en el primer apartado-, donde se considera que la innovación implica la introducción de nuevos productos, procesos y métodos o su mejoría, con lo cual aporta nuevos ingredientes a la descripción que concierne a esta investigación, y al igual que la ONU, considera el impacto que esto tiene para las naciones.[67] No obstante, a pesar de que sugiere otras características, su visión es aún incompleta.

La Organización de los Estados Americanos (OEA) también considera que "la innovación supone un cambio o una mejora a la idea original, proceso, producto o servicio. Su meta es producir cambios positivos, que usualmente se traducen a un incremento al valor para la sociedad".[68] Aunque se destaca la idea de que el fin último de la innovación es 'incrementar el valor para la sociedad', sigue estando muy limitada su percepción de que la innovación tecnológica tiene por antonomasia un efecto positivo siempre.

Por otra parte, la Comisión Económica para América Latina (CEPAL) da un viraje respecto a las otras organizaciones y plantea un enfoque más complejo, ya que integra los elementos que contribuyen a entender el fenómeno de la innovación en varias dimensiones. En la publicación "Innovación para el Desarrollo: Reflexiones desde América Latina y el Caribe" se señala que:

-Innovación puede ser:

- Introducción de nuevos procesos, productos y servicios;
- Mejora tecnológica y modernización

---

http://www.un.org/millenniumgoals/pdf/Think%20Pieces/11_ips_science_innovation_technology.pdf [abril 2018]

[67] OCDE*, La Estrategia de Innovación…, Óp. Cit.*, p. 22.

[68] OEA, *Innovación y competitividad*, En Sitio Oficial de la OEA, 2008, consultado en http://portal.oas.org/Portal/Topic/CienciaTecnolog%C3%ADaeInnovaci%C3%B3n/Programas/Innovaci%C3%B3nyCompetitividad/tabid/1535/Default.aspx [abril 2018]

- Cambio en los modelos de negocio y en la organización empresarial
- Cambio en la gestión y comercialización

-Al mismo tiempo:

La innovación es un proceso que se da en un contexto donde interactúan diferentes agentes (como son las empresas, los institutos de investigación, las universidades, etc.).

El proceso de generación, difusión y aplicación de nuevas tecnologías o innovaciones no es determínista, ni lineal. Las políticas públicas y las instituciones de apoyo a la tecnología e innovación desempeñan un papel fundamental.[69]

La concepción de este organismo regional retoma a los factores involucrados en la innovación, desde un enfoque similar a la tradición interpretativa de la innovación tecnológica, además, señala que ésta no debe ser un proceso ni determinante ni rígido y que incluye a otros actores y grupos sociales interesados.

Esta discrepancia con las otras organizaciones consultadas está relacionada con los debates académicos que han nutrido en el tema de la innovación tecnológica a las organizaciones regionales, a las políticas públicas y a los indicadores en América Latina en las últimas décadas.

En la región, a finales del siglo pasado, hubo cuestionamientos relativos a la innovación tecnológica debido, principalmente, a los procesos de liberalización y globalización sucedidos en América Latina, generando un cambio en el rol del Estado respecto a la ciencia y la tecnología, pasando de ser la principal fuente de gestión de los proceso de producción, financiación de la ciencia y la tecnología, a tener un papel más bien de regulador, dejando a las empresas como los actores principales y provocando también que la comunidad científica o las instituciones de investigación dependieron de las instancias privadas. Así lo explica Leonardo Vaccareza:

> El Estado se mantiene en un segundo plano como facilitador de vínculos, divulgador de experiencias, organizador de información y de transparencia del mercado de conocimientos y se priorizan los temas de la economía del cambio tecnológico que resaltaba la necesidad de estudios empíricos sobre las actividades científicas y tecnológicas que permiten o hacen posible la innovación local, con una preocupación por la investigación y el desarrollo de

[69] Alicia Bárcena, *Innovación para el Desarrollo: Reflexiones desde América Latina y el Caribe*, en Sitio Oficial de CEPAL, 2011, p. 6, consultado en http://www.cepal.org/noticias/paginas/8/33638/innovacionparaeldesarrollo.pdf [abril 2018]

> procesos productivos de bienes y servicios que se enmarcaron en los llamados estudios de la relaciones Universidad-Empresa y Universidad-Sector productivo.[70]

En dicho contexto, durante las décadas de los ochenta y noventa, los mismos analistas internacionales asintieron a la visión constructivista como una propuesta analítica profunda, lo que los llevó a preguntarse por la necesidad de incluir en este enfoque elementos del contexto internacional, como la transnacionalización y los crecientes procesos de globalización, derivando en desarrollos conceptuales complementarios, como el nuevo abordaje al concepto de redes trasnacionales sobre los procesos técnicos y organizacionales en distintos tipos de procesos de innovación. Javier Jiménez señala los más relevantes:

> En este campo podemos destacar los trabajos de Rosalba Casas, en México, y de manera complementaria, los trabajos de Charum y Parrado en Colombia, sobre la utilidad del conocimiento científico como proceso de construcción social que formula la necesidad de caracterizar a los usuarios del mismo.
> En Argentina, Kreimer propuso el concentrarse en el estudio de la conformación de tradiciones científicas en contextos periféricos, asumiendo que estas tradiciones socio cognitivas sólo pueden ser analizadas considerando al mismo tiempo las restricciones del contexto y la estructura de las relaciones internacionales. Adicionalmente propuso el concepto de integración subordinada, para mostrar los mecanismos por los cuales las agendas de investigación en nuestra región dependen de las agendas de laboratorios y grupos pares localizados en el primer mundo, en una especie de división internacional, donde los investigadores más prestigiosos de la periferia trabajan en tareas rutinarias y segmentadas cuya unidad conceptual se localiza en el primer mundo. Por su parte Thomas propone los conceptos de resignificación de tecnologías, dinámica, trayectoria sociotécnica y estilo sociotécnico como herramientas que nos permiten captar la complejidad de proceso locales de usos de conocimientos y artefactos tecnológicos.
> Por último, Renato Dagnino en Brasil, junto con Thomas, generaron el concepto de adecuación sociotécnica, herramienta conceptual que permite comprender los procesos de creación y utilización de las tecnologías y que además hace posible orientar y mejorar las políticas de ciencia, tecnología e innovación en Latinoamérica.[71]

[70] Leonardo Vaccarezza, *El campo CTS en América Latina y el uso social de su producción*, CTS: Revista iberoamericana de ciencia, tecnología y sociedad, Vol. 1, Nº. 2, 2004, pp. 211-21.
[71] Javier Jiménez Becerra, *Origen, desarrollo de los estudios CTS…, Op. Cit.,* pp. 17-18.

El mismo autor continúa con la revisión de los trabajos más relevantes por parte de los analistas internacionales en la región y los espacios académicos donde se lograron concretar interacciones para los estudios CTS, como el inicio de las jornadas latinoamericanas de estudios sociales en ciencia y tecnología, organizadas en Argentina, Venezuela y México en 1995, 1996 y 1998 respectivamente, donde se consolidó como un encuentro regular bianual cuya última jornada se llevó a cabo en Río de Janeiro, en 2008.[72]

También se creó la red de indicadores de Ciencia y Tecnología Iberoamericana e Interamericana (RICYT), que se logró con el apoyo del Programa Iberoamericano de Ciencia y Tecnología (CYTED), la UNESCO y la Organización de Estados Iberoamericanos (OEI) en 1995, aportando a la elaboración de indicadores, la descripción de las características de la internacionalización de la ciencia y la tecnología de los países iberoamericanos, generando también un manual Latinoamericano de Indicadores de Innovación Tecnológica en 2002. En los últimos 20 años los estudios CTS en la región adquirieron una identidad propia a causa del contexto antes descrito, promoviéndose centros, programas y grupos de investigación.[73]

En la actualidad, los internacionalistas siguen mirando al factor científico-tecnológico como un elemento importante para desarrollar un análisis integral sobre la realidad global. Fausto Quintana señala que la sociedad internacional se encuentra en pleno proceso de una revolución científico-tecnológica, mismo que ha trastocado todos los puntos de las relaciones entre sus actores en una realidad compleja:

> Es necesario señalar, en el marco de una empresa disciplinaria, que si bien el objeto de estudio, es decir, la esencia y la naturaleza de las relaciones internacionales, se basa en relaciones de poder y cooperación en un modelo de desarrollo capitalista, la sociedad mundial está inmersa en una profunda revolución científica-tecnológica que ha intensificado los intercambios comerciales y financieros; incrementado los flujos migratorios; generado problemas ambientales; mejorado las armas y, por ende transformado las estrategias de guerra; y acentuado los cambios culturales a través del desarrollo de las tecnologías de la información y las comunicaciones,

[72] *Ibíd.,* p.19.
[73] *Ibídem*.

> consolidando un sistema mundial que sólo puede definirse en términos de complejidad.[74]

Asimismo, Quintana señala que este fenómeno científico-tecnológico "ha trastocado en lo más específico, particular y, por qué no decirlo, metafísico de las estructuras sociales" y destaca ejemplos de las innovaciones en ingeniería genética, la revolución energética, las mejoras en la industria de la microelectrónica y su impacto en las telecomunicaciones, la nanotecnología y el reforzamiento de la definición del mundo como una sociedad del conocimiento y la información, concluyendo que es necesario que la disciplina de Relaciones Internacionales se consolide en su análisis.[75]

Al respecto, Lourdes Marquina considera que existe una sociedad internacional cada vez más interconectada, basada en una serie de transformaciones en las relaciones entre los actores de la sociedad internacional, donde se da relevancia a las innovaciones tecnológicas y a los esfuerzos de cooperación internacional que intentan coadyuvar en la solución de las problemáticas globales. Retoma el hecho de las diferencias de poder entre los actores y señala la importancia del sector privado como 'conductor del cambio tecnológico'. Esto lo expresa de la siguiente manera:

> Si consideramos que en el escenario internacional actual participan en forma activa pero con pesos de poder diferenciados, no sólo los Estados sino otros actores internacionales como las empresas transnacionales, los organismos internacionales/regionales y demás organizaciones tanto públicas como privadas que actúan a escala global, es necesario avanzar en la comprensión de estas nuevas relaciones que establecen los actores internacionales para la atención de las problemáticas que enfrenta la sociedad internacional en su conjunto.
>
> La descentralización del poder político hacia actores no estatales se ha visto favorecida por el término de la Guerra Fría, el desarrollo y convergencia de las tecnologías de la información y el proceso de globalización de la economía mundial, lo cual ha abierto espacios de poder a las empresas transnacionales para erigirse como una autoridad en ciertos asuntos internacionales relacionados con la economía, como la conducción del cambio tecnológico, en

[74] Fausto Quintana Solórzano, *El reto de la incorporación de nuevos temas en el estudio de Relaciones Internacionales*, en Revista de Relaciones Internacionales, UNAM, No. 109, enero-abril de 2011, p. 146.
[75] *Ibíd*., p. 147

> virtud de que el conocimiento altamente especializado que se requiere para ello, está en sus manos y no en las de los Estados.[76]

Aquí se da otro viraje analítico, al referirse a la descentralización del poder político hacia los actores no gubernamentales, de los cuales, los más relevantes son las empresas trasnacionales, que llevan décadas siendo los principales inversores en la consolidación de los procesos de innovación tecnológica.

Como ejemplo destaca la visión de Google, el gigante de las telecomunicaciones y el marketing. Susan Wojcicki, vicepresidenta sénior de publicidad de Google, señala que la empresa busca siempre "garantizar que no se queda anclada en el pasado mientras avanza hacia el futuro", por lo cual deben mantenerse en constante innovación, invirtiendo en productos nuevos y en mejorar los que ya tienen, mientras aprenden en el proceso. También señala los 8 principios de la innovación que ha ido estableciendo dicha empresa a medida que evolucionaba y sobre los cuales se siguen guiando: 1) tener una misión importante; 2) pensar a lo grande, pero comenzar por lo pequeño; 3) esforzarse por innovar de forma continua, no por lograr la perfección instantánea; 4) buscar ideas en cualquier parte; 5) compartirlo todo; 6) estimular la innovación con la imaginación y alimentarla con datos; 7) ser una plataforma; 8) no dejar de fracasar. Se destaca que la nueva visión empresarial a pesar de ser determinista, ya no es tan lineal e incorpora elementos más allá de la innovación misma o de los equipos para el desarrollo científico-tecnológico.[77]

La trasnacional de la electrónica Samsung, considerada entre las 10 empresas más innovadoras del mundo, tiene una visión parecida a las revisadas por los teóricos de la innovación. Según las declaraciones de BK Yoon, Presidente de Samsung Electronics, su innovación "se basa en un enfoque centrado en productos, procesos y personas. Para crear los mejores productos, tenemos el

[76] Lourdes Marquina, *Gobernanza global del comercio en Internet*, Primera edición, INAP, México, 2012, p. 53
[77] Susan Wojcicki, Los ocho pilares de la innovación, en Sitio Oficial de Google (acerca de), diciembre de 2012, consultado en https://www.thinkwithgoogle.com/intl/es-es/insights/los-ocho-pilares-de-la-innovacion/ [marzo 2018]

mejor proceso, y para crear el mejor proceso, necesitamos a los mejores profesionales".[78]

Esto implica que centran su atención en el desempeño del personal que integra los equipos de innovación tecnológica. Asimismo, la cabeza de Samsung delinea cuatro megatendencias globales: la movilidad, la urbanización, el envejecimiento y las nuevas amenazas como el cambio climático; señala que estos factores están alterando todo, 'desde la forma en que vivimos y trabajamos hasta la forma en que estructuramos y organizamos las sociedades y los gobiernos',[79] por lo que Samsung se esfuerza en la innovación tecnológica, ya que la ven como la clave para lidiar con estas megatendencias, por lo que han instalado decenas de centros de innovación para "desarrollar y acelerar tecnologías disruptivas a través de innovación abierta, inversiones y adquisiciones, trabajando en colaboración con empresarios y socios estratégicos."[80]

La empresa trasnacional que tiene tal vez la visión más completa y menos lineal de la innovación es Microsoft, donde se señala que la innovación se refiere a la creación de innovadores productos, soluciones y servicios. Pero, a diferencia de otras empresas, Microsoft ahonda en explicar que innovación difiere de la "mejora" o "invención", ya que el cambio estructural es inherente a la innovación, por lo que es extremadamente difícil la innovación al no poder ser forzada o trucada, además de señalar que el proceso de la innovación tecnológica está arraigado en la cultura, y que no es una actividad separada de ese contexto.[81]

Para las empresas, la innovación tecnológica se convierte en un hito, que implica una revolución constante a la que se incorpora cada vez mano de obra más especializada, trabajadores de conocimiento que trascienden espacios físicos y cuyas capacidades les permiten gestionar nuevas formas de organización

[78] Naider, *El tigre de la innovación ¿Por qué es Samsung una compañía tan innovadora?*, en Sitio Oficial de Naider, mayo 2017, consultado en http://naider.com/por-que-es-samsung-una-compania-tan-innovadora/ [mayo 2018]
[79] Ibídem.
[80] Samsung, *Samsung: Innovando para el futuro*, en Sitio Oficial de Samsung, 26 de julio de 2017, consultado en https://news.samsung.com/ar/articulo-sobre-innovacion-parte-1-samsung-innovando-para-el-futuro [marzo 2018]
[81] Romi Mahajan, Administración de TI: La singularidad en la innovación, en Sitio oficial de Microsoft, consultado en https://technet.microsoft.com/es-es/library/hh641413.aspx [marzo 2018]

empresarial que se reflejan en cada vez más cortos lapsos para innovar en tecnología y aumentar los niveles de productividad.[82]

Tomando en cuenta la participación de las empresas trasnacionales, consideramos muy relevante incluir su visión sobre la innovación tecnológica. Estos actores de la sociedad internacional la definen a partir de los fenómenos productivos, organizacionales, comerciales y sobre todo, como lo menciona IBM, el incremento de las ganancias que pueden percibir las organizaciones lucrativas a partir de la influencia de la innovación.[83]

Este recorrido conceptual da cuenta de la forma en que los internacionalistas abordan el tema de la innovación tecnológica a partir de herramientas teórico-metodológicas propias, así como la influencia de los fenómenos internacionales y sus actores en el análisis de los temas de ciencia, tecnología y sociedad.

Es a partir de la disciplina de Relaciones Internacionales que se puede entender a los procesos de innovación tecnológica como parte de toda una serie de fenómenos que ocurren en las sociedades a nivel internacional, regional y local. Y que se constituyen distintas tendencias de innovación a nivel global, dependiendo de qué actor las promueva, en la cual participan una multiplicidad de actores y factores que establecen agendas, objetivos y mecanismos de difusión y asimilación de la misma, de acuerdo al contexto tecnológico, social, político y económico de cada sociedad en particular.

Asimismo, es notable la influencia de los fenómenos internacionales de la segunda mitad del siglo XX en la concepción y promulgación de la innovación, al ubicar su promoción en el entorno de los fenómenos políticos y económicos después de la Segunda Guerra Mundial con la promesa de la transformación, progreso y desarrollo social a partir de la ciencia y la tecnología.

No obstante, es necesario seguir generando, consolidando y ampliando el desarrollo conceptual que se ha ido produciendo, lo que parece prioritario en la medida en que enfrentamos un entorno global más complejo, donde la simple

---

[82] Google, *En qué creemos*, en línea, Sitio oficial de Google Google (acerca de), consultado en https://www.google.com.mx/intl/es/about/company/philosophy/ [marzo 2018]

[83] IBM, *The Net Result: Social Inclusion in the Information Society,* Special Report IBM, Reino Unido, 1997, p. 9, consultado en http://www.local-level.org.uk/uploads/8/2/1/0/8210988/netresult.pdf [marzo 2018]

introducción de modelos y conceptos traídos de las discusiones de moda (incubadoras de empresas, redes sociales, cibercultura, por mencionar algunos) no permiten dar cuenta del contexto. La disciplina de Relaciones Internacionales, por las singularidades de su objeto de estudio y sus metodologías, tiene que ser referente de la reflexión sobre la influencia de las dimensiones globales en los procesos de innovación tecnológica.

Asimismo, persiste el reto de avanzar hacia la sensibilización social e incluso académica del valor del pensamiento CTS como crítica social y como alternativa para crear maneras de inclusión de la sociedad civil en estos debates. Esto es considerado por Javier Jiménez como un reto fundamental para los países de regiones como América Latina "en la medida en que la mayoría de los movimientos sociales y políticos han tenido un discurso bastante optimista frente a la ciencia y la tecnología, que se sigue insistiendo en la necesidad de la adopción acrítica de los modelos tecnológicos y científicos del primer mundo como senda para el progreso".[84]

El presente capitulo ha tenido el propósito de hacer un recorrido crítico de la evolución teórica e histórica en los estudios CTS, para explicar cómo fue que durante el siglo XX se consolidó la creencia de que existe una relación metonímica entre tecnología y progreso. Todo relacionado con los contextos políticos, económicos y sociales enmarcados en dos guerras mundiales y un sinnúmero de fenómenos en todo el globo, como la división internacional del trabajo, el enfrentamiento ideológico, la carrera armamentista y la carrera espacial, los movimientos sociales trasnacionales, diferentes procesos de integración regional formales e informales, el desarrollo de las telecomunicaciones y el ascenso de la información y el conocimiento a los procesos productivos, entre otros.

Se buscaba poner en el centro de los debates sobre la innovación tecnológica, la idea de hacer propuestas más críticas e integrales, como la TIIN y las visiones constructivistas de la COST y la Teoría del Actor Red. Así como la necesidad de retomar los grandes temas de las ciencias sociales y, puntualmente, de la disciplina de Relaciones Internacionales, como las guerras, la pobreza, el

[84] Javier Jiménez Becerra, *Origen, desarrollo de los estudios CTS…, Op. Cit.,* p. 18.

medio ambiente, la migración, la seguridad internacional, el crimen organizado trasnacional, terrorismo, desarme, el ciberespacio y, como lo analizaremos ampliamente, la ciberseguridad. Tópicos de carácter global, presentes en las agendas de los actores de la sociedad internacional y que se ubican en la amalgama ciencia-tecnología-sociedad. Como lo mencionan Santos y Lopátegui:

> Estos fenómenos han sido redibujados, de alguna manera, por los avances en ciencia y tecnología, particularmente en las comunicaciones internacionales, las neurociencias, la biotecnología, las ciencias de la información y la nanotecnología, espacios de conocimiento humano que han conquistado logros muy importantes gracias al contexto social y cultural en el que se han desarrollado.[85]

Con esto se cumple el objetivo del presente capitulo, al realizar un análisis crítico de los fenómenos implicados en la innovación tecnológica a partir de los estudios CTS, para superar la hegemonía del enfoque instrumental de la innovación tecnológica y construir así propuestas teórico-metodológicas más complejas e inclusivas. Se enfatizó especialmente en no separar las innovaciones de sus contextos socio-culturales e históricos, así como de las formas teórico-metodológicas y retóricas de hacerlos relevantes.

En lo subsecuente, la propuesta es dejar de observar a la innovación con una visión no sólo optimista o pesimista de la ciencia y la tecnología, sino desde un enfoque crítico e interdisciplinar. La revisión en la presente investigación ha intentado transformar el análisis y la interpretación a través de los estudios CTS desde la perspectiva del internacionalista, brindando la oportunidad de construir puentes hacia un análisis y discusión interdisciplinaria, sin el peso del determinismo tecnológico, lo que implica comprender las diversas problemáticas nacidas de la ciencia y la tecnología en el complejo contexto global.

Manteniendo este enfoque, en los capítulos subsecuentes se abordará el fenómeno de la ciberseguridad, entendiéndola desde un enfoque multifactorial donde se debe recurrir a la inclusión de los diferentes actores sociales y al entendimiento del fenómeno complejo que implica comprender lo que es el ciberespacio y los riesgos a la seguridad que se reproducen en dicho entorno.

[85] María Josefa Santos y Marco Antonio Lopátegui, La Construcción Global…, *Óp. Cit.,* p. 265.

2. La ciberseguridad como reto en la sociedad internacional.

Para comprender la importancia de la ciberseguridad a nivel internacional es necesario comenzar por la revisión del concepto del ciberespacio y su papel en la interacción humana a nivel global, pues ha alcanzado una relevancia tal que los actores de la sociedad internacional han detectado la necesidad de protegerse ante los riesgos de posibles ciberataques. Para ello se tienen que crear mecanismos, instrumentos de política y de gobernanza desde una perspectiva diferente a la que se ha seguido para abatir las amenazas que tradicionalmente han existido.

Una vez comprendido lo que implica la ciberseguridad, se describen los principales riesgos que se presentan en el ciberespacio y cuáles son sus tipologías, de las cuales destaca su carácter internacional. Para ello es necesario conocer las formas en que se ha abordado a la ciberseguridad a nivel global y extraer las lecciones necesarias para realizar, posteriormente, una evaluación de la estrategia de ciberseguridad en México.

2.1 El ciberespacio en la sociedad global.

2.1.1 Caracterización del ciberespacio.

El concepto ciberespacio parte de la palabra compuesta por el prefijo “ciber” y su relación con “espacio”, como un entorno o lugar donde se sitúan e interactúan diversos tipos de entes y elementos fiscos y no físicos.[86]

El prefijo “ciber” proviene de la ciencia denominada Cibernética, que tomó su nombre del griego *kybernētikḗ* (timonear) que significa 'arte de gobernar una nave'.[87] Dicho termino fue utilizado desde hace cientos de años para referirse a la intención de los seres humanos de fabricar máquinas que pudieran dirigir y automatizar su funcionamiento. André-Marie Ampère en 1834, utilizó el término en una clasificación de las ciencias políticas, en su intento por crear un sistema para

[86] Spanish Oxford Dictionaries, *Espacio (definición),* diccionario en línea, consultado en https://es.oxforddictionaries.com/definicion/espacio [agosto 2017].

[87] Real Academia Española, *Cibernético, ca (definición),* diccionario en línea, consultado en http://dle.rae.es/srv/fetch?id=98YYoXW [agosto 2017].

coordinar todo el conocimiento humano como el arte de gobernar en el sentido político.[88]

Posteriormente, sería propuesto (en su acepción en ingles *cybernetics*) por el prestigiado físico y matemático Norbert Wiener (1894-1964), en un congreso sobre la inhibición cerebral realizado en 1942, para nombrar a la disciplina que llevaría ese nombre. La Cibernética, como ciencia, estudia los sistemas de comunicación y de regulación automática de los seres vivos y los aplica a sistemas electrónicos y mecánicos que se parecen a ellos.[89]

En su obra "Cibernética o el control y la comunicación en los animales y las maquinas", Wiener explicaría la fascinación del hombre como ente creador y su intención de lograr desarrollar herramientas autónomas a partir de una instrucción o programación inicial:

> En cada estadio de la ciencia desde Dédalo o el héroe de Alejandría, la habilidad del artesano para producir un simulacro activo de un organismo viviente ha intrigado siempre al pueblo. Este deseo de producir y estudiar los autómatas ha sido siempre expresado en los términos de la técnica viviente de la época. En los días de la magia, existía el extraño y siniestro concepto del Golem, esa figura de arcilla sobre la que el Rabino de Praga infundía el soplo de la vida con la blasfemia del Inefable Nombre de Dios. En el tiempo de Newton el autómata consistía en la caja con el reloj de música con las pequeñas efigies rígidas en lo alto haciendo piruetas. En el siglo XIX el autómata es la glorificada máquina de vapor quemando algún combustible en lugar del glucógeno de los músculos humanos. Finalmente, el autómata del presente abre las puertas por medio de las fotocélulas o apunta las armas al lugar en el que un rayo del radar coge a un avión o computa una ecuación diferencial.[90]

Así se exponía la idea de crear maquinas autónomas, que puedan ser programadas para que tengan un grado de automación y sistematización, con la capacidad de seguir reproduciendo su funcionamiento e incluso –como se ha desarrollado en los últimos tiempos con la inteligencia artificial- retroalimentarse y reprogramarse en términos más eficaces que los iniciales.

---

[88] Juan José Ríos, *Derecho e Informática en México*, Instituto de Investigaciones Jurídicas UNAM, México, 1997, p. 35, consultado en https://archivos.juridicas.unam.mx/www/bjv/libros/1/147/5.pdf [agosto 2017]

[89] Spanish Oxford Dictionaries, *Cibernética (definición),* diccionario en línea, consultado en https://es.oxforddictionaries.com/definicion/cibernetica [agosto 2017].

[90] Norbert Wiener, *Cybernetics or control and communication in the animal and the machine*, The MIT press, second edition, Cambridge, Massachusetts, 1948, p. 39.

A partir de estos principios se plantea seguir desarrollando herramientas con las cuales se proporcionaría un entorno alternativo de interacción, ya sea máquina-maquina o máquina-hombre. Además, alimentado por sus trabajos de cálculo matemático de las posiciones y trayectorias de los aviones de combate durante la Segunda Guerra Mundial, Wiener ya hacía conjeturas sobre el uso de la cibernética en la industria militar y los sistemas de seguridad.[91]

El libro de Wiener fue muy relevante en su época -después del fin de la Segunda Guerra Mundial- y la Cibernética cobró auge en los círculos académicos y centros de innovación. Esto provocó que se popularizara el término cibernética en las siguientes tres décadas, relacionada con los avances informáticos y de comunicación,[92] lo que propiciaría, a partir de entonces, que el prefijo "ciber" fuera utilizado para identificar tendencias relacionadas con la informática y la comunicación.

Ahora bien, el término ciberespacio encuentra su origen en la literatura de ciencia ficción, acuñado por William Gibson, en una primera referencia en su obra "Quemando Cromo", pero explicado en el clásico "Neuromancer", publicado en 1984, donde el autor utilizó la palabra "cyberspace" de la siguiente manera:

> El ciberespacio. Una alucinación consensual experimentada diariamente por billones de legítimos operadores, en todas las naciones... Una representación gráfica de la información abstraída de los bancos de todos los ordenadores del sistema humano. Una complejidad inimaginable. Líneas de luz clasificadas en el no-espacio de la mente, conglomerados y constelaciones de información. Como las luces de una ciudad que se aleja.[93]

Descrito como un mundo virtual o imaginario para representar gráficamente algo abstracto, como los bancos de datos o canales de información formados por redes que interactúan a través de nodos repartidos en todo el mundo, un entorno de interacción entre humanos que utilizan a las maquinas como intermediarios e intérpretes,[94] Gibson daría origen a un concepto cuyos alcances nunca sospechó,

---

[91] Ibídem.

[92] Sergio Rajsbaum y Eduardo Morales, *Norbert Wiener y el origen de la cibernética*, en revista Ciencia, edición de enero-marzo de 2016, Academia Mexicana de Ciencias, México, consultado en https://www.revistaciencia.amc.edu.mx/images/revista/67_1/PDF/Presentacion.pdf [marzo 2018]

[93] William Gibson, *Neuromante*, Editorial Minotauro, 1984, p. 35.

[94] Ibíd., p. 37

pues el ciberespacio se ha convertido en un lugar que trasciende cualquier entendimiento físico y no físico, y el término ha sido retomado, a partir de ese origen, por académicos, gobiernos, empresas e instituciones internacionales.

Georgina Contreras señala que el ciberespacio es un entorno virtual de interacción, que existe como espacio relacional ya que "su realidad se construye a través del intercambio de información; es decir, es espacio y es medio"; y profundiza en su explicación al señalar que va más allá de una acumulación de datos:

> En ocasiones, se entiende el Ciberespacio como una gran acumulación de información. Esto es cierto, pero no es lo básico. No dejaría de ser simplemente una gran base de datos en la que los usuarios se limitarían a localizar información y saldrían como de cualquier biblioteca. A diferencia de otros medios -el Ciberespacio es también medio-, permite la convivencia, la construcción de relaciones de diversos tipos y grados. Es, en efecto, espacio en todos los sentidos, aunque sea virtual.[95]

De esta manera, para Contreras se puede entender al ciberespacio como un entorno hecho por el propio usuario y sus diversos componentes, pero que forzosamente existe mientras sus componentes estén conectados, ya que 'una red sin interacción entre sus miembros deja de ser una red; la red existe porque existen relaciones entre sus integrantes.

En la "Declaración de Independencia del Ciberespacio", escrita por el filósofo y ciberactivista John Perry Barlow, lo definió como un lugar virtual "formado por transacciones, relaciones y pensamiento en sí mismo, que se extiende como una onda estacionaria en la telaraña de nuestras comunicaciones" y se señala que no tiene localización física al estar 'en todas partes y a la vez en ninguna, pero no está donde viven los cuerpos físicos".[96] En un sentido parecido, la Real Academia Española lo define como el "ámbito artificial creado por medios informáticos."[97]

Para el reconocido filosofo de la cibercultura, Pierre Levy, el ciberespacio es un medio de comunicación 'que emerge de la interconexión mundial, dado por las

---

[95] Georgina Contreras Santos, *Ciberespacio y Educación*, Organización de Estados Iberoamericanos, IBERCIENCIA, Comunidad de Educadores para la Cultura Científica, publicada el 31 de marzo de 2015, consultada en https://www.oei.es/historico/divulgacioncientifica/?Ciberespacio-y-Educacion [abril 2017]

[96] John Perry Barlow*, A Declaration of the Independence of Cyberspace*, 8 de febrero de 1996, Davos, Suiza, consultado en https://homes.eff.org/~barlow/Declaration-Final.html [agosto 2015]

[97] Real Academia Española, *Ciberespacio,* Diccionario en línea, consultado en http://dle.rae.es/?id=98Wdd57&o=h [agosto 2017].

infraestructuras materiales de las redes de ordenadores y demás artefactos electrónicos, las correspondientes TIC y las informaciones y comunicaciones digitales contenidas y mediadas por dichos dispositivos', pero cuya concepción no designa solamente "la infraestructura material de la comunicación numérica, sino también el oceánico universo de informaciones que contiene, así como los seres humanos que navegan por él y lo alimentan".[98]

Luis Joyanes Aguilar, especialista español en ciberseguridad, nos otorga el concepto que ya dimensiona los actuales alcances del ciberespacio y que tan común se ha hecho para las colectividades: la interacción a través de las redes sociales digitales:

> En el espacio donde se navega por Internet, se realizan conversaciones por Skype o en las redes sociales, o estamos cuando consultamos el correo electrónico, chateamos o visitamos un periódico digital [...]
> […] el ciberespacio es el nuevo campo donde pasamos gran parte de nuestras vidas los más de 1.000 millones de habitantes que hoy día tenemos acceso a Internet; este campo, es un gran campo social donde disfrutar, trabajar, pensar, vivir…, pero también es un nuevo campo de batalla, debido a los riesgos y amenazas que su uso masivo plantea.[99]

Esta perspectiva se acompaña de la idea de que, al igual que los entornos físicos de interacción social, en el ciberespacio también se reproducen los riesgos que lo convierten en un "nuevo campo de batalla".

A través de autores cuyo enfoque se encuentra en diversos campos (literatura, ingeniería, comunicación, sociología, seguridad, etcétera) es posible concluir que el ciberespacio trasciende prácticamente todos los ámbitos del conocimiento y los diversos sectores sociales de análisis y de aplicación. También se puede caracterizar al ciberespacio como un entorno de interacción humana que no tiene una identificación física, es intangible y no tiene localización geográfica, que se genera a través de medios informáticos donde se ha construido una red de comunicación e intercambio de información por medio de la cual se relaciona la sociedad desde hace medio siglo- Esta definición envuelve el conjunto de sistemas

---

[98] Pierre Levy, *Cibercultura. Informe Al Consejo De Europa*, Anthropos Editorial, Universidad Autónoma Metropolitana, México, 2007, p. 1, consultado en https://Antroporecursos.Files.Wordpress.Com/2009/03/Levy-P-1997-Cibercultura.Pdf [diciembre 2017]

[99] Luis Joyanes Aguilar, *El estado del arte de la ciberseguridad*, Instituto Español de Estudios Estratégicos, Madrid, febrero 2011, pp. 30.

de comunicación electrónicos en la medida en que transporta informaciones provenientes de fuentes digitales.[100]

Es de suma importancia, asimismo, identificar que la visión de los principales autores aporta también para entender la construcción social del ciberespacio, es decir, en cada una de sus concepciones hay una imbricación entre tecnología y sociedad. Contreras señala que el ciberespacio solo existe en tanto las personas interactúan dentro en él, mientras que Levy mencionaba que las personas lo alimentan y Joyanes lo refirió como un campo social donde vive y convive la gente.

Es decir, el ciberespacio lo crea la sociedad, en un contexto donde las realizaciones técnicas (como Internet o la inteligencia artificial) han permitido su construcción y evolución. De tal manera que cualquier política, estrategia o plan a desarrollar relacionado con el ciberespacio tiene que considerar el componente social.

Relacionado al punto anterior, resulta necesario establecer una aclaración para liberar de la confusión en la que cientos de escritores, *influencers*, periodistas y hasta académicos han caído, la de tratar como sinónimos al ciberespacio y a Internet, como si fueran lo mismo. Esto no es así en la medida en que Internet es una red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación,[101]mientras que el ciberespacio es un entorno de interrelación social. La diferencia es sutil pero significativa.

Lawrence Lessig, reconocida jurista y activista del ciberespacio, en su obra El Código 2.0, establece que muchos 'han utilizado alguna vez Internet y algunos, además, han estado en el ciberespacio" y explica que Internet no es más que el medio por el que se envían correos electrónicos y publican páginas web, una herramienta con la que se ordenan libros en Amazon o se consultan los horarios del cine, mientras que el ciberespacio es algo más, ahí se interna la gente, atraída por

[100] Pierre Levy, *Cibercultura, sociedad de la información y conocimiento*, en "Cibercultura. La cultura de la sociedad digital", Barcelona, Anthropos-UAM, 2007, p. 70

[101] Real Academia Española, *Internet*, consultado en http://dle.rae.es/srv/fetch?id=LvskgUG [agosto 2017]

la mensajería instantánea, los juegos online y gran cantidad de actividades de toda índole, a partir de la cual se crea y se está en comunidad.[102]

Esta aclaración, además, refuerza la idea de construcción social del ciberespacio y, por lo tanto, de todas las implicaciones de éste a nivel global, lo que involucra dilemas tan variados como el acceso al mismo, el debate de su regulación (o autorregulación) y, por supuesto, los riesgos a la seguridad que se presenten en dicho entorno.

La idea de ciberespacio se asimiló, aunque gradualmente, de forma relativamente rápida en prácticamente cada sector de la sociedad, de tal manera que el propio concepto se mantiene en construcción, al grado que personajes como el propio William Gibson[103] o John Perry Barlow[104] han reconocido en entrevistas que sus descripciones originales han sido superadas. Por lo que es necesario que las ciencias sociales mantengan análisis constantes de los temas relativos al ciberespacio.

2.1.2 El ciberespacio en la sociedad internacional.

En la sociedad internacional cada vez son más relevantes los asuntos vinculados al ciberespacio, tanto para las organizaciones internacionales como para los estados y las empresas. Ello plantea la necesidad de reforzar el acceso y la búsqueda de seguridad en el ciberespacio.

Desde las organizaciones internacionales, se busca que el ciberespacio sea alcanzado por los diferentes estratos de las sociedades nacionales, ya que -al igual que en el caso de las innovaciones tecnológicas- existe la idea del impacto positivo de la conectividad. La Unión Internacional de Telecomunicaciones (UIT) utiliza el

---

[102] Lawrence Lessig, *El Código 2.0*, Cambridge, Basic Books, Reino Unido, 2006, p. 43-44, consultado en http://www.articaonline.com/wp-content/uploads/2011/07/El-c%C3%B3digo-2.0-Lawrence-Lessig.pdf [diciembre 2017]

[103] Laura Fernández, "*Me quedé corto cuando definí el ciberespacio. Nunca pensé que serviría para cotillear",* entrevista a William Gibson para Vanity Fair, publicada el 27 de abril de 2012, consultada en https://www.revistavanityfair.es/poder/articulos/el-futurismo-de-william-gibson/16450 [diciembre 2017]

[104] The Economist [redacción], *How John Perry Barlow views his internet manifesto on its 20th anniversary*, entrevista a John Pery Barlow para The Economist, publicada el 8 de febrero de 2016, consultado en https://www.economist.com/international/2016/02/08/how-john-perry-barlow-views-his-internet-manifesto-on-its-20th-anniversary [diciembre 2017]

concepto ciberespacio "para describir sistemas y servicios conectados directa o indirectamente a Internet, a las redes informáticas y a las de telecomunicaciones".[105] Asimismo, ahonda en promover la importancia de trabajar en estrategias que coadyuven en el mejor funcionamiento de las redes, ya que consideran que 'la vida moderna de las organizaciones depende del momento oportuno y el rendimiento adecuado del ciberespacio.

La Unión Europea considera que el ciberespacio es un entorno virtual "por donde circulan los datos electrónicos de los ordenadores del mundo."[106] También lo reviste de importancia al considerarlo un elemento que coadyuva en la búsqueda de la libertad y la democracia para las sociedades:

> En nuestra vida diaria, los derechos fundamentales, las interacciones sociales y las economías dependen de que las redes de información y comunicación trabajen sin contratiempos. Un ciberespacio abierto y libre ha promovido la inclusión política y social en todo el mundo; ha derribado las barreras entre países, comunidades y ciudadanos, permitiendo la interacción y el intercambio de información e ideas a través del globo; ha provisto un foro para la libertad de expresión y un ejercicio fundamental de los derechos y ha empoderado a las personas en su búsqueda por sociedades más democráticas y justas.[107]

Para la Unión Europea, resulta necesario que exista un ciberespacio libre y abierto, pero en sus documentos también reconoce y advierte que mientras más acceso y apertura se logre, 'se incrementan los riesgos de seguridad debido a las actividades maliciosas de sectores y actores que intentan satisfacer sus intereses a costa de la violación de los derechos de protección de información de instituciones gubernamentales, empresas e individuos'.[108]

Por su parte, la *Homeland Security* de Estados Unidos considera que el ciberespacio es "una red interdependiente de infraestructura de tecnologías de información, e incluye Internet, redes de telecomunicaciones, sistemas informáticos, inserción de procesadores y controladores en industrias prioritarias. El uso común

---

[105] ITU, *ITU National Cybersecurity Strategy Guide*, 2012, Ginebra, Suiza, p. 5, consultado en http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf [agosto 2015]
[106] Comisión Europea*, Glosario y Acrónimos en sociedad de la información*, Sitio oficial European Comission, consultado en http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c. [agosto 2017]
[107] Unión Europea*, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Comunicado conjunto al Parlamento Europeo, el Consejo, el Comité Económico y Social Europeo y la Comunidad de Regiones, Bruselas, 2013, p. 2
[108] *Ibídem*.

del término también refiere al ambiente virtual de información e interacción entre las personas."[109]

Los estadounidenses tienen una de las visiones más completas al respecto, para ellos es un entorno estratégico, ya que consideran que el ciberespacio se encuentra globalmente conectado y que está presente en casi todas las facetas de las sociedades modernas, siendo un componente de la economía nacional, la infraestructura civil, la seguridad pública y la seguridad nacional.' Por esas razones, son importantes la regulación, los protocolos y la creación de escudos de defensa del ciberespacio.[110]

Para el gobierno mexicano, el ciberespacio es "un entorno digital global constituido por redes informáticas y de telecomunicaciones, en el que se comunican e interactúan las personas y permite el ejercicio de sus derechos y libertades como lo hacen en el mundo físico."[111] Además, reconoce su complejidad debido a su 'naturaleza global y la concurrencia de diferentes soberanías y marcos jurídicos' en el ciberespacio y que las actividades que se realizan ahí también tienen impacto en el mundo físico.[112]

La revisión conceptual destaca la importancia del ciberespacio como un entorno que ha llegado a un estadio tal que, acompañado del desarrollo de las aplicaciones informáticas y las tecnologías de la información y la comunicación, tiene un alcance global. Lo que implica un fenómeno cuyos problemas trascienden y tienen repercusiones reales en las relaciones entre cada actor de la sociedad internacional.[113]

---

[109] National Security Presidential Directive, *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure*, Sitio Oficial de la Presidencia de Estados Unidos, p. 11, consultado en https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf [julio 2017]

[110] Ibíd., p. 4.

[111] Gobierno de la República, *Estrategia Nacional de Ciberseguridad*, en www.gob.mx, México, publicada en noviembre de 2017, p. 27, consultado en https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf [diciembre 2017]

[112] Ibíd., p. 8.

[113] Andrés Jiménez, *La delincuencia organizada en el ciberespacio, en el marco de la sociedad de la información y el conocimiento: la estrategia de ciberseguridad en México (2013-2015),* FCPyS-UNAM, México, 2016, p. 37, consultada en http://132.248.9.195/ptd2016/octubre/0751124/Index.html [diciembre 2017]

Inés Cisneros lo recordaba al hablar de los postulados de las teorías de la información y de la cibernética, que indicaban la capacidad de la mente humana para actuar como 'una maquina capaz de inquirir, manipular información y la idea de crear circuitos artificiales que precisamente imitaran esa cualidad de la mente'; ideas que también influyeron en el desarrollo de una infinidad de redes de comunicación donde hoy interactúan todos aquellos que están conectados.[114]

Armand Mattelart también señaló que los fenómenos globales de internacionalización y deslocalización de la producción empujaron la creación de infraestructura en telecomunicaciones a través de las cuales se fue formando la red global[115] que hoy día forma parte de la estructura por medio de la cual se ha construido el ciberespacio como entorno de interacción humana. Asimismo, de manera crítica, se puede identificar la visión instrumental que permea en los Estados, las organizaciones internacionales y las empresas sobre las cualidades y oportunidades en el ciberespacio.

México participa también del ciberespacio lo que hace necesario evaluarlo contextualmente desde postulados no deterministas, reconociendo que los riesgos que se producen en los entornos sociales físicos también se reproducen en el ciberespacio, entre ellos: la desigualdad de acceso, la desigualdad de desarrollo tecnológico, la inequidad en el aprovechamiento de sus oportunidades económicas y las distintas regulaciones que permiten la sobre traslación de datos.[116] Así se puede entender que México se encuentra también en un proceso constante de crecimiento en el nivel de interconexión global, cuyas características de deslocalización y velocidad en la generación y transmisión de información constituyen un riesgo a la seguridad en el ciberespacio y una potencial amenaza global.

Por consiguiente, una vez caracterizado el ciberespacio y su entendimiento e influencia a nivel global, es tiempo de revisar cuáles son los riesgos, amenazas y necesidades de protegerlo a través de diversas estrategias, acuerdos, programas y

---

[114] Inés Cisneros, Inés Cisneros, et. al; *¿Sociedad de la información o sociedad del conocimiento?*, p. 2, consultado en http://tecnologiaedu.us.es/edutec/paginas/43.htm [abril 2017]
[115] Armand Mattelar, *Historia de la Sociedad de la Información…Op. Cit., p. 108*
[116] Ibíd., pp. 168-169

políticas de seguridad en dicho entorno, que permitirán comprender la importancia de abordar, evaluar y generar de manera integral a la ciberseguridad.

2.2 Los retos a la seguridad en el ciberespacio.

El 27 de abril del año 2007, la República de Estonia sufrió uno de los primeros ataques cibernéticos a gran escala en el mundo. Después de retirar el monumento conocido como “El soldado de Bronce”, considerado un símbolo de la era soviética en dicho país, comenzaron los problemas: las páginas *web* gubernamentales comenzaron a colapsarse; el acceso a la banca *online* se bloqueó; la gente buscaba noticias en Internet, pero las páginas se habían caído.[117] En algún lugar, una red de terminales furtivas estaban perpetrando un “Ataque Distribuido de Denegación de Servicio” (DDoS por sus siglas en inglés).[118] Los ciberataques proliferaron de forma exponencial durante dos semanas, de los mil paquetes de información a la hora inicial del 27 de abril se llegó a los 4 millones de paquetes de información por segundo para el 9 de mayo. Los daños además de calcularse en 120 millones de dólares (sin contar las pérdidas de los bancos, mismas que nunca se hicieron públicas),[119] incluyeron un sinnúmero de emergencias no atendidas, servicios públicos no realizados, la pérdida de confianza de la población y una gran cantidad de disturbios sociales. A pesar de las investigaciones que señalaron al *Kremlin* de estar detrás, no hubo pruebas contundentes y sigue sin saberse quién perpetró los ciberataques. [120]

En enero de 2010, en una planta nuclear en Natanz, Irán, las centrifugadoras usadas para enriquecer uranio estaban fallando. El fenómeno se repitió cinco meses después, pero esta vez los expertos pudieron detectar la causa: un malicioso virus informático. Era de tipo "gusano" y se le llamó Stuxnet, mismo que tomó el control de 1.000 máquinas que participaban en la producción de materiales nucleares y les

---

[117] Néstor Ganuza, *La situación de la ciberseguridad en el ámbito internacional y en la OTAN*, Instituto Español de Estudios Estratégicos, Madrid, febrero 2011, p. 174.

[118] Más adelante se explicará en que consiste éste y otros de los tipos de ataques cibernéticos más comunes.

[119] Néstor Ganuza, *La situación de la ciberseguridad… Óp. Cit., p. 182.*

[120] Bestor Cram y Mike Majoros, *Weapons of mass disruption (Amenaza cibernética*), Documental en línea, producido por Nothern Light Productions, trasmitido por Odisea Channel, Washington D. C., 2011, dirección URL: https://www.youtube.com/watch?v=nWXQacWRn5I [consultado en enero de 2015]

dio instrucciones de autodestruirse. El virus se fue infiltrando en la red informática de las máquinas, hasta que encontró el software que las controlaba y se insertó en él, tomando el control. Primero, hizo que las centrifugadoras giraran peligrosamente rápido, durante unos 15 minutos, antes de volver a la velocidad normal; luego, aproximadamente un mes después, las desaceleró durante unos 50 minutos. Esto se repitió en distintas ocasiones durante varios meses, hasta que la tensión provocada por las velocidades excesivas causó que las máquinas infectadas, unas 1000, se desintegraran. Alrededor del 20 por ciento de las centrifugadoras en la planta de Natanz quedaron fuera de servicio.[121]

Durante el proceso electoral presidencial de Estados Unidos del 2016, hubo diversos ataques cibernéticos a los sistemas electorales en 39 estados, incluyendo intrusiones a las bases de datos de los votantes, sistemas de software y a los correos electrónicos del partido Demócrata. En Illinois, investigadores del FBI encontraron evidencia de que los intrusos cibernéticos intentaron borrar o alterar los datos de los votantes, accedieron al software diseñado para ser utilizado por los trabajadores electorales el día de las elecciones, y en al menos un estado, accedieron a una base de datos de financiamiento de campaña. El alcance y la sofisticación preocuparon tanto a la administración de Barak Obama que se quejaron directamente con Moscú. La Casa Blanca contactó al Kremlin para ofrecer documentos detallados sobre lo que acusaban, era el papel de Rusia en la intromisión en las elecciones y para advertir que los ataques podrían derivar en un conflicto más amplio. Los funcionarios rusos han negado públicamente haber participado en dichos ataques cibernéticos y el presidente Vladimir Putin declaró que criminales dentro del país podrían haber estado involucrados sin haber sido contratados por el gobierno ruso. Hasta el momento no se tiene identificado a los

[121] BBC [Redacción*], El virus que tomó control de mil máquinas y les ordenó autodestruirse*, BBC, sección IWonder, 11 de octubre 2015, consultado en http://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet [agosto 2017]

autores de las intromisiones cibernéticas durante el proceso electoral de ese país con la inteligencia cibernética más avanzada del mundo.[122]

Estos ejemplos muestran al menos cuatro puntos: lo ciberataques son capaces de afectar el mundo físico ya sea en infraestructura o servicios; su influencia va más allá de los temas informáticos o de comunicación, pueden provocar problemas políticos y sociales; los ciberataques se han vuelto más sofisticados y la proliferación de dispositivos móviles y su conexión a la red hará que el número de posibles ataques continúe creciendo y aumente su exposición a las amenazas; y que es cada vez más difícil identificar el origen o a los responsables de los ataques.

De acuerdo a datos de la UIT, en 2017 prácticamente la mitad del mundo utilizó Internet (3.500 millones de usuarios) y, según una estimación de Cisco Systems, habrá más de 12 mil millones de dispositivos conectados a Internet para 2020.[123] La transformación digital se está construyendo con elementos como la nube, *big data*, analíticos, movilidad y redes empresariales, pero también se conforma de sistemas cognitivos, internet de las cosas, realidad virtual, robótica, e impresión 3D, entre otras tecnologías. Esto ha provocado una penetración en la vida cotidiana, académica, empresarial y gubernamental, en los espacios públicos y privados, cada vez más profunda, de las innovaciones tecnológicas y aplicaciones que día a día se van desarrollando.[124]

Este nivel de penetración en la vida cotidiana implica que existen peligros latentes en el ciberespacio, prácticamente las 24 horas del día, representando riesgos para al menos la mitad de la población directamente, y de forma indirecta para poblaciones enteras si se ataca alguna infraestructura o servicio básico.

La compañía global de ciberseguridad, Symantec, ha descubierto que los correos electrónicos maliciosos se convirtieron en el arma preferida para una amplia

---

[122] Michael Riley y Jordan Robertson, *Ciberataque ruso en elecciones de EU es más grande de lo que se creía*, en Bloomberg, publicada 13/06/2017, consultado en http://www.elfinanciero.com.mx/mundo/ciberataque-ruso-en-elecciones-de-eu-es-mas-amplio-de-lo-que-se-creia [abril 2018]

[123] UIT*, Global Cybersecurity Index 2017*, en uit.org, Unión Internacional de Telecomunicaciones-ABI research, 2017, p. 1, consultado en https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

[124] Alejandro Nájera, *Inversión en ciberseguridad fundamental en la transformación digital*, en Info Security México, publicado 7 de abril 2018, consultado en https://infosecuritymexicoblog.com/2017/11/21/inversion-en-ciberseguridad-fundamental-en-la-transformacion-digital/

gama de ataques cibernéticos, desde grupos de ciberespionaje, patrocinados por el estado, hasta pandillas de *ransomware* de envío masivo; para 2017, uno de cada 131 correos electrónicos enviados era malicioso, la tasa más alta en cinco años, y a través de estos ataques se secuestran los datos de los usuarios con una demanda promedio de rescate que supera los mil dólares.[125]

Estas cifras sólo son muestra de que cada vez hay más personas interactuando en ese gran campo social llamado ciberespacio, en un entorno de reproducción de relaciones sociales donde el flujo de información logra multiplicarse sin distinción de lugar, desde cualquier punto en el globo.[126] Concebir cómo este entorno ha ido redefiniendo las formas de relación entre los actores de la sociedad internacional, permite reconocer la importancia, pertinencia y vigencia de aplicar medidas regulatorias y parámetros de seguridad y protección en el ciberespacio.

La consultora IDC estima que para el año 2018, ya más del 75% de las cadenas de valor de fabricación utilizan procesos, recursos, productos y servicios que están conectados digitalmente para mejorar su capacidad de respuesta y productividad.[127] La UIT ha señalado en diversos informes que los ciberataques aumentaron un 30 por ciento entre 2011 y 2012, afectando a 550 millones de personas en todo el mundo y ocasionando pérdidas económicas de más 110,000 millones de dólares. Para el 2016, se estimó que el cibercrimen le costaba al mundo hasta $575,000 millones de dólares al año, lo que representa 0.5 por ciento del Producto Interno Bruto global.[128]

En América Latina y el Caribe, este tipo de delitos cuestan alrededor de $90,000 millones de dólares al año. Con relación al informe de 2014 Tendencias de Seguridad Cibernética en América Latina y el Caribe, patrocinado por la Organización de Estados Americanos (OEA), se estima que los costos inherentes a la comisión de los delitos informáticos alrededor del mundo ascendieron a 113,000 millones de dólares y en México representaron 3,000 millones dólares.[129]

---

[125] UIT, *Global Cybersecurity Index 2017…, Óp. Cit*., p. 1.
[126] Julio Linares y Francisco Ortiz, *Autopistas Inteligentes…, Óp. Cit.,* p. 134
[127] ITU, *Global Cybersecurity Index 2017…,* Op. Cit., p. 1.
[128] Gobierno de la República*, Estrategia Nacional de Ciberseguridad…, Óp. Cit*., p. 5.
[129] Ibídem.

La tendencia de la digitalización conlleva a que más personas se internen en el ciberespacio, que más servicios estén conectados a Internet, e incluso que dependan de sistemas de información para su funcionamiento, lo que implica que se incrementen los riesgos. Para intentar contrarrestar las vulnerabilidades, la ciberseguridad se está volviendo cada vez más relevante en la agenda de los tomadores de decisiones a nivel global, y las doctrinas relacionadas con la ciberseguridad se han establecido en casi todos los países del mundo.

Para muchos analistas, los peligros han llegado a su quinto dominio, y éste es el ciberespacio, como un "lugar" donde se libran batallas, después de las dimensiones físicas: la tierra, el mar, el aire y el espacio,[130] de tal manera que los conflictos que se producen en las relaciones de los grupos sociales en los otros entornos, también se reproducen en el ciberespacio. Lo cual, aunado a la penetración ya mencionada, concientiza sobre los riesgos reales para la vida cotidiana de las sociedades.

Por lo anterior, se tiene que entrar de lleno en la ciberseguridad, partiendo su análisis desde perspectivas distintas a las tradicionales (utilizadas para hablar de problemas de seguridad en general), y situarse en una nueva categoría que requiere otras dimensiones para su eficacia. El ciberespacio tiene una característica principal, que es la capacidad de comunicación, de acceso y de intercambio de información con otros, lo que es una espada de doble filo; los mismos procesos y las mismas tecnologías pueden dar lugar a un nuevo negocio o a una nueva amenaza, alcanzando miles de millones de potenciales clientes o de potenciales víctimas.[131]

El tema de la ciberseguridad, por las razones mencionadas, ha cobrado importancia desde hace prácticamente una década en los gobiernos, sobre todo en los ministerios de seguridad; en las organizaciones internacionales de cooperación en defensa como la OTAN; y en las instituciones internacionales tanto públicas

---

[130] The Economist (redacción*), Cyberwar. War in the fifth domain*, en linea, The Economist, Reino Unido, 1 de junio de 2010, consultado en http://www.economist.com/node/16478792 [febrero 2015]

[131] Gonzalo Sánchez, *Temas candentes de la Ciberseguridad. Un nuevo espacio lleno de incógnitas*, por el CEO de PWC España, publicado por PWC España, 2015, consultado en https://www.pwc.es/es/publicaciones/gestion-empresarial/assets/temas-candentes-ciberseguridad.pdf [abril 2016]

como privadas, como la UIT; que miran con inquietud el crecimiento de personas que acceden a la red global y la posibilidad de atentados con alcances que van desde aquellos muy focalizados contra empresas o sectores, hasta ataques a países y regiones enteras. La ciberseguridad surge como una nueva visión para las vulnerabilidades derivadas de la utilización del ciberespacio, que requiere soluciones concordantes con su configuración y con los problemas que estas plantean.[132] Por lo que, es importante saber qué es la ciberseguridad y qué implica, y así caracterizar los esfuerzos que se pueden y deben realizarse para hacer estrategias efectivas al respecto.

Asegurar el ciberespacio es difícil porque éste es utilizado por la sociedad, en primera instancia, para interactuar, por lo que lo que suele promoverse es la conectividad, más que la seguridad. Por ello cualquier estrategia de ciberseguridad debe implicar la protección "tanto a los datos como a las personas, enfrenta múltiples amenazas, en particular el ciberdelito y el espionaje industrial en línea, los cuales están creciendo rápidamente.[133]

Para la Unión Europea -como la instancia multilateral que más ha trabajado el tema- la ciberseguridad se refiere a las medidas de salvaguarda que se pueden usar "para proteger el dominio cibernético, tanto en el ámbito civil como militar, de aquellas amenazas que están asociadas o que pueden dañar las redes interdependientes y la infraestructura de la información." La ciberseguridad se esfuerza por preservar la disponibilidad e integridad de las redes y la infraestructura, así como la confidencialidad de la información contenida en ellos.[134]

En el gobierno mexicano se ha asimilado esta dimensión integral de la ciberseguridad al concebirla en su estrategia nacional como el "conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas

---

[132] Andrés Jiménez, *La delincuencia organizada en el ciberespacio…*, *Óp. Cit*., *p.42.*

[133] The Economist [redacción], *Defending the digital frontier, Special report on cyber-security*, publicado el 10 de julio de 2014, consultado en https://www.economist.com/special-report/2014/07/10/defending-the-digital-frontier [enero 2018]

[134] Comisión Europea, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace Brussels*, Unión Europea, Bruselas, publicado el 7 de febreo de 2013, p. 3, consultado en https://ec.europa.eu/digital-single-market/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security [diciembre 2017]

asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicación."[135]

Asimismo, ha reconocido el aumento de 'riesgos, amenazas y ataques informáticos sofisticados, el surgimiento de nuevas formas y técnicas para aprovechar vulnerabilidades, el incremento de conductas delictivas que se cometen a través de las TIC, así como la naturaleza global del ciberespacio y la concurrencia de diferentes soberanías y marcos jurídicos', circunstancias que hacen de la ciberseguridad un tema sumamente complejo y delicado.[136]

Entonces, la ciberseguridad, en sentido más claro y conciso, se puede caracterizar como el conjunto de acciones destinadas a mantener márgenes de seguridad y certidumbre dentro del ciberespacio, protegiéndolo hasta donde sea posible, de ataques a los intereses de las organizaciones legales y legítimas, que incluye toda una serie de medidas para garantizar la protección del dominio cibernético.[137]

Richard Alan Clarke, quien fuera encargado del combate al terrorismo del gobierno de Estados Unidos, alerta sobre los posibles alcances de una ciber amenaza en su libro: "*Cyber War: The Next Threat to National Security and What to Do About It Paperback*". Según su perspectiva, existe la probabilidad de que se desate una ciberguerra, con alcances aún más destructivos que las anteriores dos guerras mundiales; todo a partir un colapso de 15 minutos en los que, por medio de ciberataques, se revelarían secretos militares, se harían explotar oleoductos y refinerías de petróleo, se caerían los sistemas de control de tráfico aéreo, se descarrillarían trenes de pasajeros y de mercancías, se perderían millones de datos financieros y los satélites podrían ser sacados de orbita afectando las comunicaciones, advirtiendo que en esa ciberguerra "la identidad del atacante podría ser un misterio".[138]

---

[135] Gobierno de la República*, Estrategia Nacional de Ciberseguridad…, Óp. Cit*., p. 28.
[136] Ibíd., p. 3.
[137] Andrés Jiménez, *La delincuencia organizada en el ciberespacio…, Óp. Cit*., p. 191
[138] Richard A. Clarke y Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It Paperback*, Harper Collins, Estados Unidos, 2010, p. 6

En la UIT también se reconoce que los ciberataques son particularmente difíciles de controlar y sus consecuencias aún pueden ser incalculables o de magnitudes desconocidas debido a la velocidad con la que suceden, el alcance que pueden tener, los pocos elementos jurídicos y la insuficiente concertación y coordinación política que hay al respecto para activar protocolos de seguridad y defensa en el ciberespacio.[139] La UIT menciona tres características que hacen del ciberespacio un entorno con dificultades únicas para resguardar la seguridad:

> Primero, debido al alcance global de las redes, los actores amenazantes pueden lanzar peligrosos ataques desde muy lejos de sus víctimas y generalmente desde lugares donde no existe reglamentación sobre delitos cibernéticos o donde hay una endeble jurisdicción. En segundo lugar, la rápida velocidad de conexión da a las victimas muy poco tiempo para defenderse de los ataques, por lo que, en el mejor de los casos, los Estados y las organizaciones solo se dan cuenta del ataque cuando éste ya está en proceso, en el peor, las víctimas ni siquiera se dan cuenta de la crisis en sus sistemas […]. En tercer lugar, mientras que los países persiguen sus intereses nacionales a través de un sistema internacional basado en leyes, el ciberespacio no ha aceptado normas o principios proporcionales a los tradicionales en el sistema internacional. Por ejemplo, mientras que un país requiere la aprobación de Naciones Unidas para participar en cualquier actividad que refiera a la seguridad de la comunidad internacional, cualquier actor puede configurar en el ciberespacio y hacer prácticamente lo que le plazca. Actores como las organizaciones criminales, insurgentes y terroristas no se preocupan de las normas internacionales y no temen ninguna represalia debido a la dificultad para atribuir algún ataque a algún individuo o grupo criminal determinado. La falta de la aceptación de normas en el ciberespacio está reduciendo la confianza en el uso de las TIC, por eso cada vez tienen mayor relevancia las Resoluciones de Naciones Unidas concernientes a la ciberseguridad.[140]

Entender estos riesgos es lo que ha provocado que los actores internacionales compartan el interés de mantener a salvo de estos ataques a las redes trasnacionales y las estructuras de información que forman el ciberespacio, ya que “una pequeña escaramuza en el ciberespacio podría ser precursora de un

---

[139] Henning Wegener, *Un concepto de ciberespacio*, en “La búsqueda de la Paz en el Ciberespacio”, UIT, Ginebra, 2011, p. 92, consultado en https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-S.pdf [marzo 2015].

[140] Frederick Wamala, *The ITU National Cybersecurity Strategy Guide*, Unión Internacional de Telecomunicaciones, Ginebra, septiembre 2011, p. 14, consultado en http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf [abril 2015]

importante ciberconflicto y desencadenar una escalada regional que tendría repercusiones internacionales".[141]

Aunque estas posturas son muy preocupantes, hasta el momento -y sin tomar a la ligera ese tipo de advertencias- los ataques cibernéticos no se han enfocado en provocar un caos a nivel global, antes bien, se han centrado en agresiones focalizadas o de escala local, que tienen intereses bien definidos de tipo económico o político, ya que los embates de mayor magnitud registrados no han sido dirigidos a la sociedad en general. Por ejemplo, en el caso de Estados Unidos, aunque la intromisión electoral puede decirse que afectó la vida política de todo un país, no estaba enfocada en atacar directamente a la población general, el ciberataque tenía un tinte político específico y estaba dirigido al gobierno, los partidos políticos y a sus instituciones electorales.

Según un análisis del Ministerio de Defensa de España, "más de nueve décimas partes del tráfico de Internet son submarinas, viajan bajo la superficie del mar a través de cables de fibra óptica y éstos son críticos en algunos lugares, por ejemplo alrededor de Nueva York, el Mar Rojo o el estrecho de Luzón en Filipinas."[142] Eso significa que a pesar de que personajes como Richard Clark u organizaciones como la UIT teman o se anticipen a ataques mundiales, se considera que un ataque de magnitudes globales es muy difícil que ocurra debido a que las redes tienen diferentes caminos y corren a través de diferentes tipos y niveles de subestructuras, de tal manera que la infraestructura en telecomunicaciones al ser frágil en algunos puntos del globo, interrumpiría la transmisión de la amenaza cibernética antes de que ésta recorriera el globo entero.

William J. Lynn III, ex subsecretario de Defensa de Estados Unidos, en su artículo "Defending a New Domain. The Pentagon's Cyberstrategy" para *Foreing Affairs*, señala algunos principios básicos que deben tomar en cuenta las estrategias de ciberseguridad: 'el ciberespacio debe ser reconocido como un territorio de dominio igual que la tierra, mar y aire en lo relativo a la guerra; la defensa del ciberespacio debe ir más allá del mundo de las redes militares y de defensa del

[141] John Bumgarner, *US Cyber Consequences Unit*, Jane's Defence Weekly, Chief Technology Officer, 29 de septiembre de 2010, p. 92, consultado en www.jdw.janes.com [junio 2015]
[142] Luis Joyanes Aguilar, *El estado del arte de la ciberseguridad… Op. Cit*., p. 22.

gobierno (dominios .mil y .gov), para abarcar las redes civiles y comerciales (dominios .com, .net, .info, .edu, etc.); una estrategia de defensa ciberespacial debe realizarse con los aliados internacionales para una política efectiva de 'alerta compartida' ante las amenazas, mediante el establecimiento de 'ciberdefensas' con países aliados; y los departamentos de defensa y seguridad gubernamentales deben contribuir a mantener e incrementar las capacidades tecnológicas con base en los últimos avances de hardware y software en TIC.'[143]

Dicha visión abarca más dimensiones e involucra a todos los sectores sociales, pero dependiendo de la sociedad donde se aplique la estrategia de ciberseguridad se tienen diferentes necesidades y condiciones para enfrentar los riesgos. Como lo indica James Forsyth, analista en seguridad y defensa, cada Estado enfrenta su propio dilema de ciberseguridad y por necesidad también tendrá que cooperar con otros estados:

> Hoy, cada país enfrenta su propio dilema de ciberseguridad distinto al de otros, tanto dentro como fuera de la red se crean vulnerabilidades que complican la vida cotidiana, pero aunque sean problemas nacionales, no por otra razón que la supervivencia, los estados no tendrán más remedio que trabajar juntos para modular estas vulnerabilidades.[144]

Según Forsyth, ante la dificultad de localizar el origen de los atacantes y el alcance que pueden tener, debe existir una cooperación y coordinación entre actores públicos y privados, nacionales y trasnacionales, aunque cada nación presente diferentes problemas de ciberseguridad. Asimismo, destaca que tienen que ser los Estados los que promuevan y lideren tales esfuerzos.

En la estrategia de ciberseguridad de México se marca que diversos países han desarrollado estrategias de ciberseguridad con sus propias circunstancias y particularidades, en razón de su capacidad económica, social y política, pero que sin importar los diferentes grados de avance de los países y las estrategias deben dejar en claro la intención de generar beneficios "a los individuos, organizaciones

---

[143] Wiliam Lynn III, *Defending a New Domain. The Pentagon's Cyberstrategy*, en Revista *Foreign Affairs*, publicada por el Council on Foreign Relations, septiembre-octubre 2010, Estados Unidos, consultado en https://www.foreignaffairs.com/articles/sunited-states/2010-09-01/defending-new-domain [abril 2015]

[144] James Forsyth, *Structural Causes and Cyber Effects. Why International Order is Inevitable in Cyberspace?*, Strategic Studies Quaterly-The Air University, Alabama, 2014, p. 123, consultado en http://www.au.af.mil/au/ssq/digital/pdf/winter_14/forsyth.pdf [junio 2015]

privadas, academia e instituciones de gobierno con acciones concretas en ciberseguridad."[145]

Cisco Systems, empresa líder en telecomunicaciones y protección informática, publicó en su informe 2014 *Midyear Security* que, a pesar de los múltiples ataques y amenazas que sufren los gobiernos, año con año lo más rentable para los ciberdelincuentes es "el fraude por clics, los ataques que se disfrazan de antivirus y los timos lucrativos."[146] Asimismo, explica que la ciberdelincuencia se ha vuelto más eficiente al aprovecharse de las innovaciones tecnológicas relativas al Internet móvil[147], las redes sociales digitales, los juegos en línea y los avisos publicitarios, a través de ataques multivector que combinan diferentes soportes como el correo electrónico, descarga de videos, juegos y películas.[148]

Esta información revela que, sin restar la importancia a la defensa y la seguridad nacional, hoy día la mayoría de los ciberataques no están relacionados a ciberterroristas o están destinados a atacar los sistemas de defensa de manera sincronizada, sino que tienen objetivos económicos y buscan invadir "sitios web legítimos a través de los cuales se gestionan ataques de *spam* o *bots*"[149] con el fin de realizar fraudes a empresas o robar datos de los usuarios promedio.

Estas circunstancias, lejos de causar tranquilidad, hacen tomar conciencia sobre los cercanos que son los riesgos para la población en general, alertan sobre la necesidad de realizar estrategias integrales de ciberseguridad, que envuelvan una gran coordinación en la que se circunscriba a actores públicos y privados, ya que la ciberdelincuencia es cada vez más ávida, sutil y sofisticada. De esta manera se tiene un concepto amplio donde se caracteriza lo que es y todo lo que envuelve la ciberseguridad, misma que va más allá del ciberterrorismo o la guerra cibernética entre Estados.

---

[145] Gobierno de la República*, Estrategia Nacional de Ciberseguridad…, Óp. Cit*., p. 23.
[146] Cisco Systems, *2014 Midyear Security Report*, sitio web Cisco Systems Company, San Francisco, 2014, consultado en http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html [marzo 2015]
[147] Este tipo de innovaciones se refiere a los teléfonos inteligentes, geolocalizadores, *google glasses* o el 'Internet de los objetos', entre otras tecnologías que revisaremos en el siguiente capítulo.
[148] Cisco Systems, *2014 Midyear Security Report…, Op. Cit*.
[149] Luis Joyanes Aguilar, *El estado del arte de la ciberseguridad… Op. Cit*., p. 40.

No obstante, la importancia que tiene el tema y la conciencia que se debe tomar al respecto de los riesgos en el ciberespacio, la ciberseguridad no puede partir de la sensación de pánico ni se debe dar un sentido alarmista a la sociedad, porque eso podría provocar una pérdida de confianza en las redes informáticas y de comunicación o en las múltiples formas en que los servicios digitales aportan al aumento de la producción global y a la eficiencia de los intercambios de datos personales, comerciales y financieros.[150] El Estado debe enfocarse en brindar confianza a los usuarios de que el ciberespacio mantiene márgenes amplios de seguridad, disponibilidad, integridad de las redes[151], confidencialidad, transparencia y certidumbre legal.[152]

Se puede concluir que una estrategia de ciberseguridad efectiva debe contener políticas y estándares respecto a la seguridad y las operaciones en el ciberespacio, así como incluir 'toda una gama de reducción de amenazas, reducción de vulnerabilidades, disuasión de ataques, colaboración internacional, respuesta oportuna a incidentes, aumento de la resiliencia y políticas de recuperación ante ataques consumados'.[153]

Asimismo, estos objetivos se lograrán si se generan las normas jurídicas respectivas, si se realizan operaciones de respuesta inmediata en las redes, si se coordinan acciones diplomáticas y medidas de protección en el ámbito militar y llevarse a cabo misiones permanentes de inteligencia dentro de la infraestructura mundial de la información y las comunicaciones.[154]

En el último capítulo se podrán revisar a fondo los pilares sobre los que se debe plantear una estrategia de ciberseguridad integral, por ahora se han esbozado algunas características del fenómeno de la seguridad en el ciberespacio y la importancia que ha cobrado en la agenda global en los últimos años, debido sobre todo a los riesgos y ataques perpetrados hacia prácticamente todos los sectores de la población. Ahora es momento de hacer una descripción de los principales tipos

[150] Frederick Wamala, *The ITU National Cybersecurity Strategy Guide…, Op. Cit.,* p.15
[151] European Commission, *Cybersecurity Strategy of the European Union…, Op. Cit.,* p. 3
[152] Ibid., p. 13
[153] National Security Presidential Directive, *Cyberspace Policy Review…, Op. Cit.*, p. 2
[154] Ibídem.

de incidentes que ocurren en el ciberespacio, para conocer de manera puntual a qué se enfrenta la sociedad en general para salvaguardar su seguridad en dicho entorno.

2.3 Principales amenazas a la ciberseguridad.

Después de hacer una revisión de porqué es importante la ciberseguridad, nos ha quedado claro que el ciberespacio, si bien presenta oportunidades de interacción ilimitadas, tiene también posibilidades de daños incalculables. En ese espacio se puede contactar a cualquier proveedor de cualquier producto o servicio; ordenar tanto un ramo de flores como una tonelada de armas, reservar un hotel de cualquier ciudad del mundo o solicitar una prostituta de cualquier nacionalidad, comprar un kilogramo de carne o encargar 100 gramos de cocaína.[155]

Estas características del ciberespacio lo ponen en un plano totalmente distinto a cualquier otro entorno susceptible de ser atacado, por lo que deben conocerse los principales tipos de conductas ilegales que se presentan en él, para reconocerlas cuando se presenten y también saber los retos que representa el enfrentarlas, ya que hay diversas causas por las que un ataque cibernético suele no sólo cumplir su cometido, sino también quedar impune.

Es importante establecer desde un principio que, prácticamente todas las formas conocidas para mantener la seguridad en otros entornos no sirven ni se pueden reproducir en el ciberespacio. Lo que hace necesario crear estrategias específicas para enfrentar los ciberdelitos. En su libro “La mentada estrategia”, Alejandro Hope y Jaime López Aranda abordan esta cuestión de la siguiente manera:

> […] los delitos no serán iguales. Lo que en mayor medida es posible es que el delito tenga un tinte menos violento en términos de pérdidas humanas, pues se ira sofisticando a efecto de hacer frente a los medios de combate al crimen. Veremos menos capos cargando balas y más *geeks* con paquetería para hackear y borrar rastros cibernéticos.
> Tendremos delitos en los cuales lo importante no será mostrar el musculo sino el cerebro. El crimen se mudará de las calles al ciberespacio: el robo de

[155] Andrés Jiménez, *La delincuencia organizada en el ciberespacio…, Óp. Cit., p.58.*

> identidad, el robo de activos electrónicos, la extorsión y el chantaje serán los delitos más frecuentes.[156]

Asimismo, Hope y López aprecian que los esfuerzos en México por combatir el crimen cibernético son hasta el momento insuficientes, al considerar que se ha avanzado en la materia, pero se sigue 'priorizando el gasto en compra de equipo convencional y no en la profesionalización y desarrollo de nuevas tecnologías en combate al crimen'.[157] Lo cual no sólo es propio de México, sino, como menciona Bruce Bagley, en general de los países en desarrollo, han sido incapaces de atender los problemas de sus poblaciones e impedir la propagación de organizaciones trasnacionales, más complejas y preparadas desde el punto de vista tecnológico.[158]

Al respecto, la revista *Time* publicó el artículo "*Why The Deep Web Has Washington Worried*", una investigación sobre las principales formas de operación ilegal en Internet, en donde apunta que existen más de 800 mil cuentas de usuarios diarias (dichas cuentas se abren y se cierran en lapsos de horas y hasta minutos) que contratan servicios de grupos organizados, especializados en encriptar y desencriptar información de solicitudes de todo tipo de productos y servicios ilegales, por medio de los cuales se accede a miles de sitios web, que se abren y se cierran, se muestran y se ocultan en cuestión de horas, dando como resultado más del 90% del uso total de Internet de usuarios de todo el mundo. La cifra resulta impactante ya que implica que 9 de cada 10 usuarios de Internet en el mundo, lo hacen ocultando información y que al menos la mitad de dicha información se descubre por los piratas informáticos.[159]

Estos datos son muestra clara de la tendencia creciente de las actividades ilegales en el ciberespacio y de crímenes que, aunque se llevan a cabo en su forma tradicional, también han evolucionado de acuerdo a los elementos técnicos que tiene a su alcance, puesto que cerca del 50% de tráfico de servicios y productos

---

[156] Alejandro Hope y Jaime López Aranda, *La mentada estrategia. Dos ensayos y treinta y nueve preguntas sobre seguridad, justicia, violencia y delito*, primera edición, Senado de la República, México, julio 2015, p. 91.
[157] Ibídem.
[158] Bruce Bagley, *La globalización y la delincuencia organizada…, Óp. Cit.,* p. 187.
[159] Newton-Small, Jay, *Why The Deep Web Has Washington Worried*, en Revista "Time", Vol. 182, No. 20, Time Inc., Nueva York, 11 de noviembre de 2013., p. 26-30.

ilegales se negocian en el ciberespacio.[160] Esto reviste la importancia de construir estrategias integrales de ciberseguridad, pero también resalta la necesidad de conocer -previo a la estrategia- y tener muy claro qué es un crimen o actividad ilegal en el ciberespacio y cuáles son las características de los principales tipos de cibercrímenes.

La referencia principal sobre las conductas delictivas en el ciberespacio la ofrece la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), cuya explicación señala que no existe una definición de delito cibernético aceptada globalmente, sino que depende, en gran medida, de la intención con que se emplee dicha expresión.

Según esta instancia de Naciones Unidas, existen delitos explícita y casi exclusivamente del ciberespacio, "un número limitado de actos contra la confidencialidad, la integridad y la disponibilidad de los datos o sistemas informáticos se hallan en la base del delito cibernético,"[161] pero también existen otros actos realizados para obtener beneficios económicos o para perjudicar a otros, que tradicionalmente han existido y que no necesariamente necesitan del ciberespacio para realizarse, pero están relacionados durante su planeación o ejecución con el mismo, como el robo de identidad, la falsificación de documentos o el fraude, lo que "impide llegar fácilmente a definiciones jurídicas de esa expresión en un sentido general".[162]

Symantec, empresa líder en seguridad informática y antivirus, describe las actividades ilícitas cibernéticas como "cualquier delito cometido en el que se haya utilizado un equipo, una red o un dispositivo de hardware; el equipo o el dispositivo

[160] Ibídem.

[161] Naciones Unidas, *Estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno*, por el Grupo de expertos encargado de realizar un estudio exhaustivo del delito cibernético, Oficina contra la Droga y el Delito de Naciones Unidas, Viena, 23 de enero de 2013, p. 2, consultado en https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_S.pdf [agosto 2015]

[162] Ibídem.

pueden ser el agente, el facilitador o la víctima del crimen; el delito puede tener lugar en el equipo únicamente o en otras ubicaciones también."[163]

Por su parte, en el Convenio sobre la Ciberdelincuencia del Consejo Europeo si se ha intentado llegar a una definición más concreta, señalando que el crimen cibernético se refiere a delitos que abarcan desde 'actividades criminales contra datos hasta las infracciones de contenidos, *copyright* (derechos de autor), fraude electrónico, el acceso no autorizado a contenido encriptado por el gobierno o las empresas, la pornografía infantil y el *cyberstalking* (acoso en Internet).[164] Aunque, para los alcances del ciberespacio, tal definición puede resultar insuficiente para los analistas de la ciberseguridad.

En México, Miguel Ángel Davara, uno de los primeros especialistas en normatividad informática, definía los delitos cibernéticos como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software". [165] No obstante, es importante señalar que a Davara no le parecía adecuado hablar de delito cibernético, porque dicho concepto de conducta ilegal no está tipificado en la legislación penal mexicana; en ningún ordenamiento jurídico federal o general existe, o al menos no definido como tal.

Fue en 1999 que se incorporó a la legislación penal en México, el concepto de delitos informáticos y estaban incluidos en algunas "figuras lesivas genéricas", es decir, su concepción resulta insuficiente para el alcance que han tenido las conductas delictivas en el ciberespacio. Como señala Jorge Cassou, "este fenómeno que tomó por sorpresa a muchos gobiernos, y que a pesar de los intentos

---

[163] Symantec, *¿Qué es el crimen cibernético?*, en Norton.com, Symantec Inc., Estados Unidos, 2015, consultado en http://mx.norton.com/cybercrime-definition/promo [agosto 2015]

[164] Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, en Agencia Española de Protección de Datos, Budapest, 23 de noviembre de 2001, p. 4-5, consultado en https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF [julio 2015]

[165] Miguel Ángel Davara, *Fact Book del Comercio Electrónico*, Ediciones Arazandi, Segunda Edición, Pamplona, 2002, p. 45

por lograr un consenso entre los diversos países a fin de tipificar los delitos informáticos ha sido lento en comparación con las actividades delictivas."[166]

A pesar de no estar en los ordenamientos jurídicos como tal, en la Estrategia Nacional de Ciberseguridad de México sí se conceptualiza a los delitos cibernéticos[167] como las acciones delictivas que utilizan como medio o como fin a las tecnologías de la información y comunicación y que se encuentran (dichas actividades) tipificados en algún código penal u otro ordenamiento nacional.[168] Esto resulta confuso al buscar un ámbito de aplicación legal, sin embargo, permite caracterizar la forma en que se entienden a las conductas delictivas en el ciberespacio. Los retos jurídicos son parte de uno de los pilares en lo que se debe trabajar como parte de una estrategia de ciberseguridad efectiva.

Sin tipificación, el delito cibernético como tal no existe en algunas legislaciones nacionales –como lo es en el caso de México-, incluso no hay algún acuerdo internacional que lo defina de manera general. No obstante, es posible describir una serie de actividades ilegales cibernéticas que pueden ser ajustadas a tipificaciones tanto nacionales como internacionales, referentes a delitos tanto del orden doméstico, como trasnacional. Es decir, existen actividades y conductas ilegales que, al igual que las actividades criminales tradicionales, pueden adoptar muchas formas y se producen en prácticamente cualquier lugar, pero cuyos métodos, funciones y objetivos se operan en el ciberespacio.[169]

Para fines prácticos de análisis, aun sin una definición jurídica de los delitos cibernéticos, se les puede describir por sus implicaciones y concebir de acuerdo a sus alcances dentro de toda una infinidad de actividades que se generan en el ciberespacio. Por lo tanto, con base en la información emitida por expertos en ciberseguridad, organizaciones internacionales y gobiernos, a continuación se desglosa una serie de características de las actividades criminales que se cometen en el ciberespacio.

---

[166] Jorge Cassou Ruiz, Delitos informáticos en México https://www.ijf.cjf.gob.mx/publicaciones/revista/28/Delitos_inform%C3%A1ticos.pdf

[167] También se les llamará ciberdelitos o cibercrimen para referirse a las actividades ilegales que se engloban en su ámbito de aplicación para, desde o a través del ciberespacio.

[168] Estrategia

[169] Andrés Jiménez, *La delincuencia organizada en el ciberespacio…, Óp. Cit., p.61.*

- Son actividades ilegales que se producen dentro del ciberespacio; sea porque se usa dicho espacio virtual o algún punto de la infraestructura mundial de redes para perpetrarse.[170]
- Ofrecen muchas posibilidades de anonimato, puesto que en milésimas de segundo y sin una presencia física pueden llegar a consumarse, lo que representa una dificultad adicional para ubicar a los responsables.[171] Es particularmente difícil encontrar a los culpables y proceder en su contra, debido a la falta de procedimientos judiciales y a la falta de regulación jurídica.[172] Asimismo, presentan grandes dificultades para su comprobación, esto por su propio carácter técnico.[173]
- Para perpetrar un ciberataque se requiere de personas que puedan operar a un determinado nivel de conocimientos técnicos sobre aplicaciones informáticas y redes de comunicación.[174] Además, por el acceso y apropiación de las generaciones actuales, puede haber muchos menores de edad involucrados, a los que en caso de ser descubiertos se les dan consideraciones especiales por su capacidad jurídica; de hecho, en al menos de la mitad de los casos castigados, los culpables eran menores de 21 años.[175]
- Se realizan con el fin de obtener algún tipo de beneficio y a costa del perjuicio de otros usuarios del ciberespacio –sean personas físicas o morales-, el daño puede ser de tipo económico, pero también puede ser político y social (esto es más claro en el caso del acoso cibernético o la difamación).
- Algunas son actividades que por sí mismas podrían no ser ilegales o producir un perjuicio a otros usuarios de manera directa o inmediata,

[170] Naciones Unidas, *Estudio exhaustivo del problema del delito cibernético…, Óp. Cit.*
[171] Estrada Garavilla Miguel, *Delitos Informáticos*, en Universidad Abierta Université de Freibourg, 2013, consultado en https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf [agosto 2015]
[172] Miguel Ángel Davara, *Fact Book del Comercio Electrónico…, Óp. Cit*.
[173] Juan Téllez, *Derecho Informático…*, *Óp. Cit*., p. 104.
[174] Julio Téllez, *Derecho Informático*, 2ª. Ed, Mc Graw Hill, México, 1996, p.103-104.
[175] Juan Téllez, *Derecho Informático…*, *Óp. Cit*., p. 104.

pero se utilizan como una parte de una red más grande de actividades delictivas, como la utilización de *bots* o los fraudes por *clics*.[176]

- Suelen perpetrarse de manera oportunista sobre aplicaciones informáticas o temas cuya tendencia tiene gran alcance dentro de las redes digitales.[177] Esto puede provocar que también existan crímenes imprudenciales, debido al engaño que alguien promueve o al desconocimiento que muchos usuarios aun demuestran al internarse en el ciberespacio.[178]

Los crímenes cibernéticos son eminentemente trasnacionales. Esto se puede determinar por los siguientes elementos:

- Generalmente, aunque tenga un objetivo focalizado, suelen darse ataques simultáneamente contra distintos puntos en el globo, se perpetran en más de un Estado. Esto se relaciona directamente con la capacidad intrínseca del alcance global del ciberespacio, no existen barreras físicas, en cuestión de segundos se puede enviar una amenaza con la capacidad de expandirse lejos del país de .[179]
- Aun cuando se cometa contra objetivos ubicados en un solo país, una parte sustancial de su preparación, planificación, dirección o control se realiza en otro; esto es común en los delitos cibernéticos, puesto que las bases de los operadores suelen tener una ubicación geográfica determinada, aunque, de hecho, esta puede no ser permanente.[180]
- Suelen entrañar la participación de delincuentes ubicados en distintos países, muchas veces ni siquiera se conocen físicamente entre sí, pero se comunican a través del mismo ciberespacio, ahí negocian, se

[176] Néstor Ganuza, *La situación de la ciberseguridad… Óp. Cit.,* p. 179.

[177] Bestor Cram y Mike Majoros, *Weapons of mass disruption (Amenaza cibernética)…, Op. Cit*.

[178] Miguel Estrada Garavilla, *Delitos Informáticos*…, Op. Cit., p. 6

[179] Naciones Unidas, *12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal*, Oficina contra la Droga y el Delito de Naciones Unidas, Salvador (Brasil), 12 a 19 de abril de 2010, p. 4, consultado en https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050385s.pdf [agosto 2015]

[180] Álvaro Bunster, *El crimen organizado frente al derecho*, en "Boletín Mexicano de Derecho Comparado", IJJ-UNAM, año XXIX, num. 87, México, 1998, p. 458, consultado en http://biblio.juridicas.unam.mx/revista/pdf/DerechoComparado/87/art/art1.pdf [agosto 2015]

organizan y ejecutan todas las actividades ilegales. Asimismo, utilizan elementos técnicos ubicados en otras latitudes, como computadores, terminales o servidores infectados previamente; esto sucede en ataques masivos, para despistar el origen del ciberataque se utilizan dominios y direcciones desde distintas ubicaciones;[181]

- Aunque algunas veces hay atacantes que actúan de forma aislada, las actividades ilegales cibernéticas se insertan, en su mayoría, en operaciones criminales mayores o relacionadas con grupos delictivos organizados, cuyos alcances de actividad criminal trascienden fronteras.[182]
- Los grupos dedicados al delito cibernético suelen tener una estructura más flexible y abierta, que permite la incorporación de nuevos miembros por un período de tiempo limitado y a pesar de estar en distintos países, los grupos que cometen delitos cibernéticos con frecuencia son mucho más pequeños que los grupos delictivos organizados tradicionales.[183]

Entre las características de dichas actividades, también deben señalarse que la naturaleza de éstas se determina por el móvil o la razón con la que se ejecuta, por lo que los distintos tipos de ciberdelitos se pueden clasificar de la siguiente manera, basados en su objetivo:

- Motivos económicos/financieros. Son los delitos cibernéticos más comunes y pueden ser a pequeña o a gran escala, dirigidos contra miles de víctimas o contra un blanco específico de gran importancia. Se pueden presentar como operaciones bancarias, timos comerciales y robos de identidad. Dentro de este también entran todos los relacionados con amenazas, secuestro y comercio ilegal a través del ciberespacio, siempre y cuando su fin único y último sea el de obtener dinero de las víctimas.[184]

[181] Oscar Lira Arteaga, *Cibercriminalidad*, Instituto Nacional de Ciencias Penales, primera edición, México, 2010, p 86, consultado en http://biblio.juridicas.unam.mx/libros/7/3169/15.pdf [septiembre 2015].
[182] Naciones Unidas, *Convención de Naciones Unidas sobre Delincuencia…, Op. Cit.,* articulo 3, p. 6
[183] Naciones Unidas, *12º Congreso de las Naciones Unidas sobre…, Op. Cit.,* p. 11.
[184] Andrés Jiménez, *La delincuencia organizada en el ciberespacio…, Óp. Cit., p.65.*

- *Hacking* Político. Son ataques por medio de los que se saturan los sistemas de información de los gobiernos, se interceptan mensajes cifrados entre agencias gubernamentales para hacerse públicos o se viralizan en las redes sociales críticas al gobierno relacionadas con la agenda pública en momentos de coyuntura política (la intromisión en las elecciones de Estados Unidos son un ejemplo).[185]
- Terrorismo. Los grupos terroristas emplean el ciberespacio como una herramienta más para realizar sus actividades. Lo pueden utilizar para establecer sus comunicaciones, para distribuir su propaganda, para robar cuentas bancarias, desactivar sistemas de seguridad y defensa u obtener información necesaria para sus fines. Generalmente los grupos terroristas no cuentan con el personal capacitado, pero contratan los servicios de grupos criminales del ciberespacio.[186]
- Servicios de Inteligencia. Son amenazas contra información clasificada de los gobiernos o de empresas estratégicas, de la industria militar o energética. El tiempo, los recursos técnicos y la cantidad de agentes que deben coordinarse para este tipo de objetivos revela un nivel de organización y sofisticación superior, asimismo, suelen ser los servicios mejor pagados en el mercado negro.[187]
- Espionaje industrial. Los delincuentes cibernéticos son contratados por compañías o gobiernos que tienen interés en disponer de información crítica sobre los desarrollos tecnológicos e innovaciones industriales de sus rivales o competidores.[188]
- Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos. Engloba las conductas de acceso ilícito,

[185] Bestor Cram y Mike Majoros, *Weapons of mass disruption (Amenaza cibernética)…, Op. Cit*.
[186] Javier Candau Romero, *Estrategias nacionales de ciberseguridad. Ciberterrorismo*, en "Ciberseguridad. Retos y amenazas a la seguridad en el ciberespacio", Instituto Español de Estudios Estratégicos, Madrid,cfebrero 2011, p. 264.
[187] Juan Salomón Clotet, *El ciberespacio y el crimen organizado…, Op. Cit*., p. 133
[188] Javier Candau Romero, *Estrategias nacionales de ciberseguridad. Ciberterrorismo…, Op. Cit*., p. 265

interceptación ilícita, interferencia de datos, interferencia de sistemas y el abuso de dispositivos.[189]

- Delitos relacionados con las infracciones de la propiedad intelectual y de los derechos afines. Se encuentra toda clase de robo, uso o reproducción ilegal de contenidos a través del ciberespacio.[190]
- Delitos sociales. Comprende las conductas que se engloban con la tenencia y distribución en el ciberespacio de contenidos como pornografía infantil, xenofobia, racismo, discursos de odio, violencia de género, entre otros.[191]
- Ataques personales. Estas son actividades que tienen como fin el ataque especifico entre particulares, suele darse con amenazas o difamaciones, con infinidad de fines y perjuicios, generalmente del orden civil, los más comunes se dan a través de las redes sociales con maltrato psicológico y *stalking* (acecho constante).

Toda esta gama de características de los delitos cibernéticos fortalece la importancia de establecer criterios y acciones específicas de acción para contrarrestar los riesgos en el ciberespacio y para tener más herramientas, es necesario conocer también el *modus operandi* de los ciberdelitos más comunes. Para ello se va a nombrar los más comunes a nivel internacional, qué son, cómo funcionan, en qué casos se utilizan y algunos datos sobre su nivel de incidencia.

Bots* y *botnets. Un *bot* es un programa malicioso que tiene cargada una programación inicial con la que el criminal cibernético que lo creó, lo puede hacer actuar de forma automática dentro del equipo o red en el que se inserta. Ffunciona como un robot (de ahí toma su nombre) y permite que un atacante tome el control de un equipo infectado. Los *bots* suelen propagarse por Internet en busca de equipos desprotegidos a los que puedan infectar, cuando encuentran un equipo sin protección, lo infectan rápidamente e informan a su creador. Cada máquina reclutada por el virus se pone en contacto sigilosamente con el cibercriminal a la

[189] Consejo de Europa, *Convenio sobre la Ciberdelincuencia…, Óp. Cit.,* artículos 4-11.
[190] Ibídem.
[191] Ibídem.

espera de sus órdenes, su objetivo es permanecer ocultos hasta que se les indique que realicen una tarea.[192]

A los equipos infectados por *bots* se les llama zombis, debido a que han dejado de manejarse por sí mismos y cumplen las órdenes de quien lo infectó. Los *bots* no trabajan en solitario, sino que forman parte de una red de equipos infectados denominada "*botnet*" (red de bots). Algunas *botnets* contienen decenas e incluso centenares de miles de zombis a su servicio y muchos de los equipos se infectan sin que sus dueños se enteren.[193]

Según *Symantec*, existen aproximadamente 9000 variaciones distintas de tres de los *bots* más frecuentes (*Spybot, Gaobot y Randex*), lo que supone la aparición de un mínimo diario de 50 nuevos *bots* con motivaciones criminales en Internet buscando equipos desprotegidos. Son las armas más polivalentes de los criminales cibernéticos, ya que los creadores de las *botnets* alquilan sus redes ilícitas a otros a cambio de cierta cantidad de dinero o usan los *bots* ellos mismos para cometer distintos tipos de crímenes, como ataques *DDoS*, robos de identidad o *spam*, entre otros.[194]

Sutxnet. Es un programa de *software* dañino del tipo gusano (entra al sistema, se instala, penetra y contamina los sistemas operativos) que aprovecha la vulnerabilidad de los sistemas operativos ; se instala de manera camuflada pero ya tiene un comando programado para comenzar a atacar. Puesto que las infraestructuras a las que va dirigido no están conectadas a Internet, *Stuxnet* se introduce en los sistemas directamente por puertos USB o entradas de memoria, luego se multiplica a sí mismo y se expande por todas las terminales de la red local recogiendo información y dañando los controladores.[195]

Penetra los sistemas industriales y toma el control de instalaciones como plantas nucleares, plantas eléctricas o represas, entre otras operaciones industriales, entonces puede modificar códigos y no permitir que los operadores lo

---

[192] Symantec, *Bots y botnets: Una amenaza creciente*, en Norton.com, consultado en http://mx.norton.com/botnet [septiembre 2015]

[193] Symantec, *¿Qué es el crimen cibernético?, Óp. Cit.*

[194] Ibídem.

[195] Luis Joyanes Aguilar, *El estado del arte de la ciberseguridad… Op. Cit.,* p. 27.

noten, de tal manera que se logra manipular equipamiento físico.[196] *Stuxnet* apareció en enero de 2010, en el caso mencionado previamente de la planta nuclear en Natanz, Irán. Fue la primera vez que un ataque cibernético logró dañar la infraestructura del "mundo real". Durante el análisis del gusano, se descubrió que el código altamente avanzado de *Stuxnet* había sido diseñado con una mentalidad bélica.[197]

Ataques DDoS. Los ataques de denegación de servicio (DDoS Distributed Denial of Service) consisten en el envío de un gran número de peticiones a un servidor de manera que los usuarios legítimos del servicio no puedan acceder a esos recursos, es decir, saturan el servidor y hacen que “caiga de la red” el sitio atacado. Generalmente se perpetran con la ayuda de miles de equipos infectados con *bots*.[198] Estos aprovechan las vulnerabilidades relacionadas con la implementación de un protocolo TCP/IP y son eficaces contra cualquier tipo de equipo que cuente con *Windows* (95, 98, NT, 2000, XP, etc.), *Linux* (Debian, Mandrake, RedHat, Suse, etc.), *Commercial Unix* (HP-UX, AIX, IRIX, Solaris, etc.) o cualquier otro sistema operativo. Existen dos tipos de DDoS: las denegaciones de servicio por saturación, que saturan un equipo con solicitudes para que no pueda responder a las solicitudes reales; y las denegaciones de servicio por explotación de vulnerabilidades, que aprovechan una vulnerabilidad en el sistema para volverlo inestable. Ambos envían paquetes IP o datos de tamaños o formatos atípicos para saturar los equipos de destino y los vuelven inestables.[199]

La amenaza DDoS suele ser utilizada por grupos terroristas para hacer caer sitios y servicios web de los gobiernos y así ejercer presión por medio del caos que implica la no disponibilidad de los recursos de los gobiernos en el ciberespacio.

---

[196] Symantec, *Stuxnet*, en Symantec.com, *Symantec* Inc., Estados Unidos, 2015, consultado en http://www.symantec.com/es/mx/page.jsp?id=stuxnet [septiembre 2015]

[197] BBC [Redacción*], El virus que tomó control de mil máquinas y les ordenó autodestruirse*, BBC, sección IWonder, 11 de octubre 2015, consultado en http://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet [octubre 2015]

[198] Cyberseguridad.net, *Ataques de denegación de servicio (DoS) (Ataques Informáticos III)*, en Cyberseguridad.net, España, 29 de junio de 2012, consultado en http://cyberseguridad.net/index.php/197-ataques-de-denegacion-de-servicio-dos-ataques-informaticos-iii [septiembre 2015]

[199] CCM Benchmark Group, *Introducción a los ataques por denegación de servicio*, en ccm.net, consultado en http://es.ccm.net/contents/22-ataque-por-denegacion-de-servicio [septiembre 2015]

También tienen fines económicos, pues se han convertido en la principal arma de los extorsionadores del ciberespacio, al ser utilizados por grupos de la delincuencia organizada como amenaza a empresas y gobiernos. Son bastante lucrativos y demandados en el mercado cibernético ilegal y provocan pérdidas millonarias a las organizaciones cada año.[200]

***Phishing*.** Es un engaño en línea donde se utilizan *spam*, sitios de Internet falsos, llamadas falsas, mensajes de correo electrónico o mensajes instantáneos que aparentan provenir de fuentes reales y confiables, como bancos, escuelas o instancias de gobierno, con los que engañan a los usuarios para que proporcionen información confidencial, como los datos de la tarjeta de crédito o de cuentas bancarias, de tal manera que toda esa información queda en manos del delincuente. Una vez que el cibercriminal tiene los datos de la víctima puede vaciar sus cuentas y realizar pagos a crédito, causando enormes daños económicos.[201]

Durante el año 2005, los ataques de los *phishers* (ladrones de identidad) se hicieron mucho más complejos. Comenzaron a utilizar software de actividades ilegales junto con sus sitios web falsos, y aprovecharon vulnerabilidades conocidas de los exploradores de Internet para infectar los equipos de las víctimas. Así que con sólo hacer clic en el vínculo de un correo electrónico de *phishing* que conduce a un sitio web falso, es posible robar la identidad del usuario y el *phisher* ya no necesita que el usuario introduzca su información personal.[202]

Pharming. Los *pharmers* utilizan sitios web falsos y el robo de información confidencial para perpetrar estafas en línea, pero, en muchos sentidos, es mucho más difícil detectarlos, ya que no necesitan que la víctima acepte un mensaje "señuelo". El *pharming* redirige a sus víctimas a un sitio web falso, incluso si escriben correctamente la dirección web de su banco o de otro servicio en línea en el navegador de Internet. El sistema de nombres se basa en los servidores DNS para efectuar la conversión de los nombres de los sitios *web* basados en letras, que son fáciles de recordar por parte de los usuarios, en dígitos comprensibles por los

[200] Cyberseguridad.net, *Ataques de denegación de servicio…, Op. Cit.*
[201] Pandasecurity, *Phishing*, en Pandasecurity.com, consultado en http://www.pandasecurity.com/mexico/homeusers/security-info/cybercrime/phishing/ [septiembre 2015]
[202] Symantec, *¿Qué es el crimen cibernético? ..., Op. Cit.*

equipos para conducir a los usuarios al sitio web de su elección. Cuando un *pharmer* logra lanzar un ataque de envenenamiento de la caché del DNS con éxito, modifica las normas de circulación del tráfico en una sección completa de Internet, de esta manera el ataque *pharming* tiene una potencial de víctimas nunca antes visto.[203]

Fraudes de Tarjeta de Crédito. Consiste en crear sitios Web, aparentemente auténticos, de venta de bienes inexistentes o de valor inferior al real, de entradas falsas a conciertos, espectáculos o eventos deportivos, donde el pago se realiza con tarjeta de crédito. Otra modalidad es penetrar con *bots* páginas reales de servicios de pago por tarjeta de crédito, y cuando el usuario realiza el pago, la transacción se orienta a las cuentas de los criminales.[204]

Extorsiones. Los cibercriminales obtienen datos personales por medio de *bots* o de la violación a bases de datos escolares, gubernamentales o comerciales y utilizan esta información para contactar a las víctimas; les hacen creer que un presunto miembro de la delincuencia organizada (esto podría ser cierto o no) las ha estado vigilando y los tienen en la mira, y amenazan con secuestrar o hacer daño a su salud, o a la de sus familiares, en caso de no atender a sus solicitudes de dinero. El contacto con la victima puede ser por teléfono móvil, teléfono fijo, correo electrónico, redes sociales o servicio de mensajería instantánea.[205]

Fraude publicitario o fraude por *clics*. Consiste en conseguir anunciantes y patrocinadores reales de alguna supuesta empresa de entretenimiento o publicitaria, o de cualquier giro, del que se crea un sitio en Internet. El trato es que los anunciantes sólo pagarán por las ocasiones en que el sitio sea visitado y su publicidad sea vista, por lo que se establece un medidor de entradas, es decir, cada que alguien dé *clic* en la página o en el anuncio, se genera un costo para el patrocinador. El sitio y los anuncios son legales, pero a través de *botnets* se programa que el sitio sea visitado constantemente. A efectos prácticos, en las estadísticas se verá que los *clics* provienen de cientos o miles de direcciones IP

[203] Symantec, *¿Qué es el crimen cibernético? ..., Óp. Cit.*
[204] Cyberseguridad.net, *Las estafas más habituales en la red*, en Cyberseguridad.net, publicado el 26 de enero de 2015, consultado en http://cyberseguridad.net/index.php/408-las-estafas-mas-habituales-en-la-red [septiembre de 2015]
[205] Cyberseguridad.net, *Las estafas más habituales en la red*..., Op. Cit.

diferentes, repartidas por todo el mundo y por tanto parecerá que son usuarios legítimos y no una estafa, de esta forma el anunciante deberá pagar el porcentaje convenido.[206]

Estafa sentimental. Funciona a través de sitios de citas en línea o de mensajería instantánea donde se crean perfiles de usuarios falsos, generalmente operados a través de *bots*. El estafador demuestra interés en la victima y obtiene datos e información confidencial, además propone realizar algún encuentro personal, para lo cual la víctima debe pagar transporte, hospedaje y dinero para viáticos; el usuario ficticio nunca llega a la cita. A veces se hace pasar por una persona con problemas de salud o financieros y solicita préstamos a la víctima. En el peor de los casos, puede utilizar la información personal que ha obtenido a través de la mensajería para chantajear o extorsionar a la víctima.[207]

Delitos contra la propiedad intelectual. Son todos aquellos relacionados con la reproducción, transmisión, distribución y consumo no autorizados por el autor de diversas creaciones intelectuales, tanto informáticas como culturales a través del ciberespacio. Los tipos más comunes de piratería de obras protegidas por el derecho de autor atañen a los libros, la música, las películas, los videojuegos y los programas informáticos. Las descargas ilícitas se llevan a cabo mediante redes de intercambio de archivos, servidores ilícitos, sitios web y ordenadores pirateados.[208]

La piratería cibernética se puede presentar con la falsificación, que implica la duplicación, distribución y/o venta ilegales de material con propiedad registrada; piratería de software, que se produce cuando se descarga software de Internet de manera ilegal, lo mismo sucede cuando se compra sin las licencias de los fabricantes en soportes como DVD; piratería de usuario final, la cual se da cuando un individuo reproduce copias de software o de contenidos multimedia sin autorización.[209] A pesar de que dichas prácticas son cada vez más complejas y

---

[206] Luis Joyanes Aguilar, *El estado del arte de la ciberseguridad… Op. Cit*., p. 28.

[207] Ibídem.

[208] UNESCO, *Observatorio Mundial de Lucha Contra la Piratería*, en unesco.org, consultado en http://portal.unesco.org/culture/es/ev.php-URL_ID=39412&URL_DO=DO_TOPIC&URL_SECTION=201.html [septiembre 2015]

[209] Symantec, *Tipos de piratería*, en Symantec.com, consultada en https://www.symantec.com/es/mx/about/profile/antipiracy/types.jsp [septiembre 2015]

tienen repercusiones negativas en las industrias culturales e informáticas (se estima que el 24% del tráfico total de Internet a nivel mundial infringe los derechos de propiedad intelectual), también se aduce el argumento de que frenar dicho fenómeno limitaría el derecho de acceso a la información, el conocimiento y la cultura.[210]

Contenidos ilegales. Esta es una serie de delitos que no precisamente son exclusivos del ciberespacio pero que, con la capacidad de propagación del mismo, suele ser utilizado para dichos fines, relacionados con delitos tradicionales, ahora en soportes cibernéticos y que provocan la violación de los derechos a terceros.[211] Diversas organizaciones gubernamentales y civiles se han mostrado sumamente interesadas en proteger el ciberespacio de contenidos, además de urgir a los gobiernos a trabajar en regulaciones jurídicas y reformas penales contra quienes cometan tales crímenes.

Explotación sexual comercial. Es la explotación de las personas para relaciones sexuales remuneradas; pornografía (que incluye la infantil y adolescente); turismo sexual; utilización de cualquier persona, sobre todo vulnerable, en espectáculos sexuales, donde exista además un intercambio económico o pago de otra índole para la persona explotada o para intermediario.[212]

La Policía Cibernética de México señala que la explotación sexual a través de Internet ocupa el tercer lugar en la lista de delitos cibernéticos, sólo antecedida por los fraudes y las amenazas; además, informa que los sitios en la red se incrementan a ritmos acelerados y afirman que muchas de las páginas que promocionan dicha explotación provienen de Rusia y que no son sencillas de localizar.[213]

Pornografía infantil. Es la representación, producción, distribución, posesión y consumo de imágenes de menores de edad en actividades sexuales,

---

[210] UNESCO, *Observatorio Mundial de Lucha Contra la Piratería*…, *Op*. *Cit*.

[211] Consejo de Europa, *Convenio sobre la Ciberdelincuencia*…, *Op. Cit.,* artículos 4-11.

[212] UNICEF, *Explotación sexual comercial,* en UNICEF.org, Adaptado de la Declaración del Congreso Mundial contra la Explotación Sexual Comercial de los Niños (Suecia, 1996), Nueva York, 2006, consultado en http://www.unicef.org/spanish/protection/files/Explotacion_sexual_comercial.pdf [septiembre 2015]

[213] ECPAT International, *Monitoreo global de las acciones en contra de la explotación sexual comercial de niños, niñas y adolescentes*, Saladaeng Printing Co.Ltd, México, 2006, pp. 12, 13, consultado en http://www.derechosinfancia.org.mx/Global%20Monitoring%20Report-MEXICO.pdf [septiembre 2015]

reales o simuladas, explícitas o sugeridas. Se inserta dentro de toda una gama de abusos y explotación sexual de menores con fines de lucro, se cataloga como delito trasnacional y se propaga tanto por Internet como por dispositivos de almacenamiento como DVD, CD, *Blue-ray* y en formatos impresos. La distribución a través de Internet ofrece una alta probabilidad de anonimato tanto por parte del distribuidor como del consumidor. Naciones Unidas informa que la producción y distribución de pornografía infantil por Internet representan un negocio de entre 2000 y 3000 millones de dólares anuales, por lo que la demanda de niños para estos sitios aumenta constantemente, además de que estos sitios se multiplican a un ritmo alarmante, el Fondo de las Naciones Unidas para la Infancia (UNICEF) calcula que existen más de cuatro millones y cuentan con una audiencia de 750.000 opredadores en todo momento.[214]

Ciberacoso y *ciberbulliyng*. Se considera ciberacoso a las amenazas, hostigamiento, humillación u otro tipo de molestias realizadas por un adulto contra otro adulto en el ciberespacio y toma el atributo de *ciberbullying* si el acoso se da entre menores de edad.[215] En el ciberespacio, los agresores disponen de muchas ventajas con respecto al acoso tradicional, ya que las víctimas son mucho más vulnerables por la facilidad espacio-temporal, además de que los ataques se pueden generalizar o compartir a otros. Cuando se da a través de dispositivos móviles o Internet no se sabe quién o quiénes están implicados, si el agresor es uno solo o varios, además de la posibilidad de la invasión de la intimidad a distancia y de mantener el anonimato.[216]Algunos estudios en Europa, México y Brasil señalan que hasta 83% de los alumnos han lidiado como actores o espectadores con el *ciberbullying*. Una encuesta en la ciudad de México reveló que el 16% de estudiantes de secundaria se han considerado víctimas de *ciberbullying*, y que los principales medios de agresión son el teléfono celular y el Internet.[217]

---

[214] Naciones Unidas, *Pornografía infantil: Relatora especial urge a adoptar legislación y proteger a víctimas*, en Centro de Noticias ONU, 16 de septiembre de 2009, consultado en http://www.un.org/spanish/News/story.asp?NewsID=16500#.Vp1iKCrhDIU [septiembre 2015]

[215] Ciberacoso.net, *Qué es el ciberacoso*, en ciberacoso.net, consultado en http://www.ciberacoso.net/definicion.html [septiembre 2015]

[216] Andrés Jiménez, *La delincuencia organizada en el ciberespacio…*, *Óp. Cit*., *p. 78.*

[217] Guillermo Cárdenas Guzmán, *Ciberacoso*, en revista "Cómo ves" en línea, UNAM, México, 2012, consultado en http://www.comoves.unam.mx/numeros/articulo/197/ciberacoso [septiembre 2015]

Extremismos religiosos, racismo, xenofobia y violencia de género. Los discursos que incitan al odio y la violencia han hallado en Internet su mejor medio de difusión, sobre todo los relacionados con los extremismos religiosos, racismo, xenofobia y violencia de género. Puesto que permiten un alcance internacional y ventajas contra los agresores, como el anonimato o incluso cuando son firmados por personajes o asociaciones que se caracterizan por tener pensamientos extremistas, estos apelan a la libertad de expresión para protegerse.[218]

Asociaciones civiles, instituciones internacionales y grupos de expertos sobre ciberseguridad han recomendado a los países crear leyes que castiguen la incitación a la violencia a través del ciberespacio por opiniones sobre temas de cualquier índole. Esto es un dilema importante por la delgada línea de la libertad de expresión y la cantidad de opiniones que se vierten en las redes. Aunque existen políticas de contenidos que las mismas empresas han puesto en marcha; por ejemplo, *Facebook* e *Instagram* tienen aplicaciones por medio de las cuales se pueden denunciar este tipo de contenidos y ser inhabilitadas las publicaciones y/o los usuarios que incurran en ellos.[219]

Una observación que debe recalcarse sobre las actividades ilegales más comunes en el ciberespacio es que la mayoría ya se cometían en el mundo real desde hace mucho tiempo, pero que se han adaptado a las características y funcionalidades del ciberespacio. Robo, extorsión, fraudes, ataques terroristas, agresiones políticas, acoso, pornografía infantil, etcétera, han tenido un aumento exponencial una vez que se han generado herramientas técnicas para propagarse a través del ciberespacio. Día tras día, van adquiriendo mayor incidencia social, su alcance es cada vez mayor y por eso, como se describió en muchos de los diferentes cibercrímenes, “el interés por regularlos y generar mejores prácticas de defensa ante tales amenazas sigue creciendo entre las organizaciones internacionales, los Estados, las empresas y la sociedad civil organizada.”[220]

Conocer los tipos y modus operandi de toda la gama de amenazas que se presentan en el ciberespacio, permite resaltar la importancia de protegerlo de la

[218] Andrés Jiménez, *La delincuencia organizada en el ciberespacio…, Óp. Cit., p. 78.*
[219] Ibídem.
[220] Oscar Lira Arteaga, *Cibercriminalidad…, Op. Cit.,* p. 17.

manera más integral posible; asimismo, con los datos presentados en el presente apartado, se puede concluir que los criminales pueden operar desde puntos geográficos difíciles de ubicar, además de que generalmente traspasan las fronteras nacionales a través de movimientos sincronizados dentro del ciberespacio. Esta afirmación, de que los factores de riesgos son trasnacionales y deslocalizados, da cabida a las herramientas teóricas y metodológicas de los internacionalistas para plantear, generar y evaluar estrategias de ciberseguridad efectivas.

2.4 La dimensión internacional de la ciberseguridad.

Una vez examinados, la concepción del ciberespacio a nivel global, las implicaciones de la ciberseguridad y las características de los peligros que se presentan en el quinto entorno, podemos mostrar la relevancia y alcance internacional que se debe otorgar a la ciberseguridad.

Para ello, tenemos que asumir que el ciberespacio rebasa el ámbito tecnológico en la medida en que su construcción y operación incluye otra serie de variables, sean éstas sociales, políticas, económicas, culturales, jurídicas, incluso de relaciones interpersonales. Por tanto, el ciberespacio debe ser protegido de incidentes, actividades maliciosas y un mal uso; toda una serie de amenazas que sólo es posible enfrentar si hay una concientización de toda la sociedad y si todos los actores trabajan en conjunto para fortalecerse y ofrecer los márgenes más amplios de libertad y seguridad posibles en el ciberespacio. Tratando siempre de respetar y proteger los derechos fundamentales de los individuos y las organizaciones para que puedan interactuar en el ciberespacio de manera confiable.

Naciones Unidas ha reconocido que los crímenes cibernéticos son fundamentalmente internacionales y señala que ello tiene una relación directa con el creciente desarrollo de la conectividad global. Como se mencionó anteriormente, hoy día la mitad de la población mundial puede conectarse al ciberespacio y más del 60% lo hace desde dispositivos móviles.[221] Conocer estas cifras da cuenta de

[221] Naciones Unidas, *13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal*, Oficina de Naciones Unidas contra la Droga y el Delito, Doha, 12 a 19 de abril de 2015, consultado en

los riesgos potenciales a la ciberseguridad; baste mencionar que algunos elementos de la ciberdelincuencia como las *botnets* pueden constituir redes globales de miles de dispositivos infectados con programas informáticos maliciosos controlados a distancia por delincuentes y que existen miles de sitios de Internet y redes sociales digitales que se utilizan para realizar actos ilegales.

Para enviar un correo electrónico con un contenido ilegal a destinatarios de distintos países, basta con tener una computadora fija o un dispositivo móvil y utilizar el programa malicioso a través de un servicio de correo electrónico prestado por un proveedor que es trasnacional o que no está en el país del origen del atacante. Estos elementos refuerzan la dimensión transnacional del delito cibernético, lo que conlleva muchas dificultades.[222]

Sin embargo, sigue existiendo una resistencia a trabajar de modo coordinado a nivel internacional para dar fiabilidad al ciberespacio. A pesar de que en todos los países se acepta que existe un aumento de los riesgos a la seguridad a través del ciberespacio, la mayoría de los Estados carecen de estrategias de ciberseguridad y la mayoría de las regiones no tienen tácticas de prevención y respuesta regional a las amenazas cibernéticas.

Un estudio de la Oficina de las Naciones Unidas contra la Droga y el Delito que incluyó a los Estados miembros, organizaciones internacionales, representantes del sector privado e instituciones académicas, reveló que las autoridades reconocen que se han incrementado las actividades criminales cibernéticas, además de exponer la preocupación de que los delincuentes cibernéticos ya ni siquiera necesitan habilidades técnicas complejas, especialmente en los países en desarrollo donde, por ejemplo, han aparecido subculturas de jóvenes dedicados a los crímenes cibernéticos, ligados a los grupos organizados en sus últimos años de la adolescencia.[223]

La magnitud y complejidad del ciberespacio demandan una estrategia internacional para su plena consolidación y desarrollo, como forma de arraigar y

---

https://www.unodc.org/documents/congress//Documentation/A-CONF.222-12_Workshop3/ACONF222_12_s_V1500666.pdf [octubre 2015]

[222] Andrés Jiménez, *La delincuencia organizada en el ciberespacio…, Óp. Cit., p. 84.*

[223] Naciones Unidas, *12º Congreso de las Naciones Unidas sobre…, Op. Cit.,* p.5.

hacer viable un entorno que otorgue confianza a los internautas de que sus derechos y libertades no serán vulnerados, sin importar el nivel, tipo o alcance de interacción que tenga.[224]

Los retos para la comunidad internacional son complejos y requieren de un entendimiento integral, pero a la vez enfocado en el plano global. El elemento transnacional de la ciberseguridad plantea un gran desafío para la prevención, defensa, investigación, resolución y castigo de los crímenes cibernéticos. No existen protocolos de seguridad regional sobre una pronta respuesta a amenazas cibernéticas: Al respecto sólo la OTAN ha fortalecido su capacidad, pero no ha podido diseñar métodos de seguimiento eficientes. En la mayoría de los países del mundo, no existe una instancia permanente que esté disponible para actuar de forma inmediata, que coordine la información entre países o que proporcione atención a las solicitudes y denuncias internacionales sobre ataques cibernéticos.[225]

Cuando se recibe un ciberataque, hay poco tiempo disponible para llevar a cabo las investigaciones, pues las pruebas de la agresión cometida suelen suprimirse automáticamente al cabo de poco tiempo. Los procedimientos oficiales prolongados pueden obstaculizar seriamente la neutralización de las amenazas y la captura de los culpables, por consiguiente, el establecimiento de procedimientos para responder rápidamente a los incidentes y a las solicitudes de cooperación internacional se considera de importancia vital.[226]

Estos factores para aplicar una estrategia internacional de ciberseguridad están relacionados con diversos obstáculos que parecen ser difíciles de superar. El más importante es la soberanía nacional, según el cual no pueden realizarse investigaciones en territorios extranjeros sin el permiso de las autoridades locales, la cooperación estrecha entre los Estados involucrados es crucial para la investigación de los delitos cibernéticos, pero para evitar intromisiones a la

---

[224] José María Molina Mateos, *Globalización, ciberespacio y estrategia especial. Consideración a la estrategia de la información,* boletín electrónico del Instituto Español de Estudios Estratégicos, Ministerio de Defensa [España], publicado el 12 septiembre de 2014, España, consultado en http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO100-2014_Globalizacion-CIberseguridad-Estrategia_JMMolinaMateos.pdf [enero 2018]

[225] Andrés Jiménez, *La delincuencia organizada en el ciberespacio…, Óp. Cit., p. 84.*

[226] Naciones Unidas, *12º Congreso de las Naciones Unidas sobre…, Op. Cit.*, p.8.

soberanía, la colaboración es condicionada y la coordinación es obstruida constantemente por motivos jurídicos, políticos o burocráticos.[227]

Otro factor es que la respuesta y seguimiento de los delitos cibernéticos implican cuestiones de privacidad en el marco de la normativa internacional de derechos humanos. Estas normas estipulan que las leyes deben ser suficientemente claras para dar una indicación adecuada de las circunstancias en que las autoridades están facultadas para realizar una diligencia de investigación y especifican que deben existir garantías suficientes y eficaces contra el abuso a los derechos de la privacidad de las personas. Pero, cuando las investigaciones son transnacionales, los distintos niveles de protección tornan imprevisible el acceso de las fuerzas del orden extranjeras a los datos y dan lugar a posibles lagunas jurisdiccionales.[228]

También se deben tomar en cuenta las diferentes legislaciones a favor de la protección de usuarios del ciberespacio o en contra de ciberdelitos, que tampoco ha sido una prioridad en la mayoría de los países del mundo, sobre todo en los países en desarrollo y los menos desarrollados, donde se obstaculizan las medidas legislativas al respecto debido a la desinformación, abuso y limitada inclusión de los diferentes sectores sociales implicados en las normas de ciberseguridad.[229]

Otro elemento de suma importancia, tal vez el más complejo y complicado de sortear sin voluntad política y estrategias efectivas de coordinación, es la relación entre las organizaciones gubernamentales y los proveedores privados de servicios de informática y telecomunicaciones. Las empresas no sólo son las propietarias y operadoras de la mayor parte de la infraestructura crítica, tecnología de codificación, software y servicios de telecomunicaciones, sino que son también las que poseen las bases más densas de datos sobre cibernautas, tienen información de los suscriptores, facturas, registros de conexión, información sobre la ubicación y el contenido de sus comunicaciones. En conjunto representa un riesgo quizá, el más importante para prevenir, responder y localizar ataques cibernéticos. Además, son

[227] Naciones Unidas, *Estudio exhaustivo del problema del delito cibernético…, Op. Cit*, p.7.
[228] Naciones Unidas, *Estudio exhaustivo del problema del delito cibernético…, Op. Cit*, p.9.
[229] Naciones Unidas, *12º Congreso de las Naciones Unidas sobre…, Op. Cit*., p.5.

las grandes corporaciones las que actúan como líderes en la creación de capacidades técnicas para la protección del ciberespacio.[230]

Además, es vital que exista colaboración entre los gobiernos y el sector privado para facilitar el intercambio de recursos en ciberseguridad y permitir el intercambio de la información sobre las vulnerabilidades y las amenazas cibernéticas en tiempo real. No obstante, las obligaciones jurídicas nacionales y las políticas de retención y divulgación de datos del sector privado varían enormemente según el país, la industria y el tipo de bases de datos que maneje; por eso, organizaciones del sector privado han expresado su preocupación por establecer esquemas legales y procedimentales para compartir la información, a la vez que demandan el cumplimiento voluntario de las solicitudes directas de las fuerzas del orden en determinadas circunstancias.[231]

A pesar de lo mencionado anteriormente, no todo el panorama es oscuro. Aun con las dificultades de orden técnico, legislativo y político, muchos países y regiones ya están llevando a cabo esfuerzos importantes de ciberseguridad. No existe un consenso dominante sobre cómo tratar el fenómeno, ya que todos tienen sus propios dilemas en el uso del ciberespacio, dependiendo las condiciones propias de cada país tales como; el mayor o menor potencial técnico, la capacidad de los sistemas legislativos para lograr consensos de forma más rápida y flexible y, la relevancia del país en el escenario internacional.

Si bien en algunos países la agenda de ciberseguridad es muy importante mientras que en otros se posterga su discusión, es posible localizar tendencias globales sobre la agenda, que han sido consultadas por México para establecer la suya y con ello la estrategia de ciberseguridad nacional. De estas se pueden mencionar algunas con el fin de conocer las actividades más destacadas a nivel internacional y así contribuir a un análisis nutrido de la experiencia de las instancias más adelantadas en la materia, con el objetivo de establecer parámetros adecuados para evaluar la estrategia de ciberseguridad en México.

---

[230] UIT, *ITU National Cybersecurity Strategy Guide*, 2012, Ginebra, Suiza, p. 108, consultado en http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf [agosto 2015]
[231] Naciones Unidas, *Estudio exhaustivo del problema del delito cibernético…, Op. Cit*, p.9.

Como ya se ha mencionado, los analistas más destacados del ciberespacio, los gobiernos y las organizaciones internacionales reconocen que los desafíos institucionales, técnicos y jurídicos que plantea la ciberseguridad son de carácter global, por lo que las estrategias deben ser no sólo integrales en cuanto a los actores y sectores incluidos, sino que además deben existir amplios y eficientes marcos de colaboración internacional. En consecuencia, se han generado diversos espacios por todo el mundo que buscan realizar un esfuerzo significativo para incluir la ciberseguridad como un tema importante de la agenda global.

En el marco de Naciones Unidas, la Cumbre Mundial sobre la Sociedad de la Información (CMSI) fomentaba una visión centrada en las personas. En sus primeras dos etapas (Ginebra 2003 y Túnez 2005) se reconoció que los riesgos de una ciberseguridad inadecuada y la proliferación del ciberdelito eran reales y significativos. De tal manera que, en la Agenda de Túnez para la Sociedad de la Información, los gobiernos y los líderes mundiales le dieron a la UIT la responsabilidad de implementar la Línea de Acción C5 de la CMSI, dedicada a la creación de confianza y seguridad en el ciberespacio.[232]

Como respuesta, la UIT presentó la Agenda sobre Ciberseguridad Global (Global Cybersecurity Agenda, GCA) en 2007. Para acompañar a la GCA, se creó un Grupo de expertos de Alto Nivel (GEAN) que se encargaría de ofrecer asesoramiento y orientación en materia de estrategias para promover la ciberseguridad. Este grupo de expertos se integró por especialistas de instituciones como *AT&T, Intel, Microsoft,* Interpol y *Verisign*, así como de altos representantes de los sectores público, académico y privado del mundo entero y está presidido por el Juez Stein Schjolberg (Noruega), que lleva trabajando en la legislación de la ciberdelincuencia desde hace más de 30 años.[233]

---

[232] UIT, *El ciberdelito: guía para los países en desarrollo*, en División de Aplicaciones TIC y Ciberseguridad, Departamento de Políticas y Estrategias Sector de Desarrollo de las Telecomunicaciones de la UIT, publicado en abril de 2009, consultado en http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf [noviembre 2015]

[233] UIT, *Expertos de alto nivel determinan una hoja de ruta para la ciberseguridad*, en uit.int, Sala de prensa de la UIT, consultado en http://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=06&ipage=05&ext=html [octubre 2015]

La GCA es un marco mundial para el diálogo y la cooperación internacional a fin de coordinar la respuesta a los retos cada vez mayores que plantea la ciberseguridad y mejorar la confianza y la seguridad en la sociedad de la información y el conocimiento. Se basa en trabajos, iniciativas y asociaciones que tienen como objetivo el de proponer estrategias globales que aborden los retos actuales relativos a la creación de confianza y seguridad en el ciberespacio.[234]

Por su parte, el Foro para la Gobernanza de Internet (IGF, por sus siglas en inglés) incluye los de "Mejores Prácticas" en temas de ciberseguridad. México fue anfitrión de la reunión del IGF en 2016, en la cual se abordó la ciberseguridad como un fenómeno multifactorial que es y será pieza clave para el desarrollo sostenible.[235]

Durante la Reunión Ministerial de Economía Digital de 2016, de la Organización para la Cooperación y Desarrollo Económico (OCDE), los países participantes se comprometieron a colaborar en ciberseguridad, específicamente en tres factores:

- Reducir barreras para el comercio electrónico nacional e nternacional.
- Desarrollar estándares técnicos globales que permitan la interoperabilidad y un Internet seguro, estable, abierto y accesible.
- Desarrollar con los tomadores de decisiones, estrategias para la privacidad y protección de datos enfatizando la transparencia en el sector público.[236]

En la Organización de Estados Americanos se acordó la creación de un Grupo de Trabajo sobre Medidas de Fomento a la Confianza en el Ciberespacio, que busca crear herramientas que consideren los avances internacionales logrados por el GEG de la ONU, o en otros foros ajustándolos a las necesidades e intereses de la región.[237]

---

[234] UIT, *El ciberdelito: guía para los países en desarrollo…*, Óp. Cit., p. 13

[235] Estrategia, p. 10

[236] OCDE, *Declaración Ministerial sobre la Economía Digital: Innovación, Crecimiento y Prosperidad Social, s*itio oficial, centro de información de la OCDE, publicado el 23 de junio de 2016, consultado en: http://www.oecd.org/centrodemexico/medios/declaracion-ministerial-sbore-la-economia-digital.htm [abril 2018]

[237] Estrategia, p. 11

En el Foro Económico Mundial se definió a la resiliencia y seguridad cibernética como condiciones clave para el desarrollo tecnológico y económico. En 2016, el Consejo de la Agenda Global en Ciberseguridad publicó su libro blanco orientado a señalar los obstáculos existentes en el sector público y privado, que dificultan la colaboración y la adopción de mejores prácticas en materia de ciberseguridad. Asimismo, identificó en su Informe de Riesgos Globales 2017 al robo masivo de datos y ciberataques en el escenario de riesgo para dicho año.[238]

Es posible notar en todos estos esfuerzos, que se está marcando una tendencia internacional en esta materia preocupada por los incidentes y ataques cibernéticos que están aumentando en frecuencia, grado de afectación y sofisticación. Los gobiernos, las empresas y las ONG, a nivel global, reconocen la necesidad de contar con marcos, medidas y capacidades de seguridad de la información y ciberseguridad más robustas, así como de la cooperación e intercambio de información, para hacer frente al creciente número de riesgos en el ciberespacio.[239]

Sin embargo, y a pesar de que hay diversos esquemas de colaboración en temas relacionados con el ciberespacio y foros de análisis a nivel bilateral, regional y multilateral, no existe, hasta el momento, un tratado, convenio o acuerdo vinculante sobre las acciones relativas a la ciberseguridad que son responsabilidad de los Estados, y ello supone un reto al momento de establecer parámetros a nivel internacional para realizar o evaluar estrategias nacionales.

El referente general al que se puede acudir con mayor claridad es la UIT, la organización internacional que ha tomado la batuta de promover, evaluar y guiar los esfuerzos en ciberseguridad a nivel global. Así, a través de congresos, foros, índices y documentos elaborados por grupos de expertos en el tema, la UIT ha emitido recomendaciones para servir como marco de referencia de estrategias de ciberseguridad.

La UIT lleva casi dos décadas trabajando en la creación de capacidades para promover la seguridad en el ciberespacio, proporcionando asistencia técnica,

[238] World Economic Forum, *Global Agenda Council on Cybersecurity*, White Paper, abril 2016, consultado en: http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf [abril 2016]
[239] Estrategia, p. 12

realizando proyectos, utilizando tecnologías avanzadas y especializadas en la materia y organizando foros de creación de capacidades sobre ciberseguridad, a fin de ayudar a los gobiernos a determinar si disponen de una capacidad nacional suficiente en materia de ciberseguridad. También ha divulgado publicaciones sobre ciberseguridad y ciberdelito y ha creado diversas herramientas sobre mitigación de *botnets*, legislación de la ciberdelincuencia, equipos encargados de incidentes informáticos (CIRT) y ha promovido una cultura de la ciberseguridad.[240]

Como ya se mencionó, la Agenda sobre Ciberseguridad Global (GCA) publicada por la UIT es el documento que mayor tendencia ha marcado en la última década sobre el tema a nivel global. La Agenda tiene por objeto establecer un vínculo entre iniciativas existentes y crear un marco global para facilitar la obtención de consensos, eso es lo que la convierte en la iniciativa más importante sobre ciberseguridad a nivel global. Es única e innovadora porque cada actor o grupo de interesados puede dedicarse a su propio mandato y garantizar la cooperación en los temas que le parezcan prioritarios. Por ejemplo, en el marco de la GCA, la Interpol ya comparte ideas con la UNODC, y esa colaboración aumenta las probabilidades de éxito en la lucha contra los crímenes cibernéticos trasnacionales. Esto permea la visión general de los grupos de expertos de la UIT, que consideran a la colaboración sistemática en materia de ciberseguridad como la única opción.[241]

La GCA está basada en los siguientes 5 pilares, específicos en su concepción, que son lo suficientemente amplios y flexibles para adaptarse a los diferentes Estados y organizaciones internacionales:

1. Medidas legislativas. La primera recomendación está relacionada con la creación de iniciativas para elaborar una legislación modelo sobre ciberdelincuencia, que sea globalmente aplicable y se adapte a las legislaciones nacionales y regionales existentes. El GEAN reconoció que la Convención sobre la Ciberdelincuencia del Consejo Europeo (citada anteriormente) es una referencia válida, cuyos principios se pueden utilizar

[240] UIT, *Trabajar juntos para proteger la Sociedad mundial de la información: Agenda de la UIT sobre ciberseguridad global*, en itu.int, Sala de prensa de la UIT, consultado en http://www.itu.int/net/pressoffice/backgrounders/itu/5-es.aspx#.VqUrXyrhDIU [octubre 2015]
[241] UIT, *Trabajar juntos para proteger la Sociedad mundial de la información…, Óp. Cit.*

como directrices. Insta a los países a considerar en sus legislaciones penales que amenazas como el correo indeseado (spam), el robo de identidad y los ataques DDoS sean tipificados como delitos. Además, las legislaciones deben ser suficientemente flexibles para tener en cuenta los avances tecnológicos, se señala la importancia de que los gobiernos y las empresas del sector privado colaboren para asegurarse de que la policía y el poder judicial dispongan de las herramientas apropiadas para proteger al público contra las actividades delictivas, pero siempre preservando los derechos humanos y la privacidad.[242]

2. Medidas técnicas y de procedimiento. Son medidas clave para promover la adopción de métodos mejorados que aumenten la gestión de la seguridad y el riesgo en el ciberespacio, incluidos los esquemas, protocolos y normas de acreditación. Incluyen la promoción de la ciberseguridad, establecer métodos de evaluación y la gestión de las redes, el control de los protocolos de Internet, las medidas de seguridad y control de identidad digital, así como la creación de sistemas de protección para las tecnologías emergentes.[243]
3. Estructuras organizacionales. La GCA promueve la creación de estructuras organizacionales nacionales, regionales e internacionales apropiadas para proteger la ciberseguridad y luchar contra la ciberdelincuencia. Su función consiste en integrar las actividades de varios organismos, ahorrar valiosos recursos e impedir la duplicación de esfuerzos. El GEAN recomienda un "marco organizacional de ciberseguridad" flexible que los países puedan adaptar a sus circunstancias particulares. Los centros regionales de vigilancia, aviso y respuesta a incidentes deberían prestar servicio en varios países.[244]
4. Creación de capacidades. Se centra en la elaboración de estrategias para la creación de saberes que contribuyan a hacer visible el problema, transferir los conocimientos e impulsar la ciberseguridad en la agenda política internacional. La creación de capacidades en el campo de la ciberseguridad

[242] UIT, *Expertos de alto nivel determinan una hoja de ruta para la ciberseguridad…, Óp. Cit.*
[243] Ibídem.
[244] Ibídem.

exige recursos financieros, técnicos y humanos específicos, así como una cooperación internacional. En 2007 y 2008, la UIT organizó ocho foros regionales sobre ciberseguridad para proporcionar información y facilitar el intercambio de prácticas idóneas y estudios de casos prácticos. La UIT también trabajó sobre planteamientos integrados de ciberseguridad nacional para coordinar los esfuerzos nacionales y publicó una guía de estrategias para los países. Se promueve la colaboración público-privada y la capacitación de un núcleo reducido de miembros de los poderes públicos en las regiones que necesitan asistencia internacional.[245]

5. Cooperación internacional. Esta iniciativa se enfoca, a su vez, en 4 puntos cruciales:

- Coordinación de los trabajos. Creación de una red que coordina y armoniza las iniciativas sobre ciberseguridad, mediante acuerdos o memorandos de entendimiento. El GEAN considera que de esta manera se coordinan las labores de varias organizaciones, se evita la duplicación de esfuerzos y se mejora la colaboración con los organismos internacionales, regionales y nacionales.
- Supervisión de iniciativas de ciberseguridad. La GCA sirve como compilador de información y se dedica a divulgarla. Por otra parte, al recibir la información sobre las iniciativas de ciberseguridad en el mundo, tiene los elementos necesarios para supervisar y evaluar los avances.
- Intercesión. Al tener a los expertos la información suficiente y la responsabilidad de liderar las iniciativas, la UIT puede ser el foro donde se diriman las querellas que puedan surgir sobre ciberseguridad.
- Foros mundiales. Es necesario promover la organización de foros mundiales en la UIT (y a través de otras organizaciones) para facilitar el desarrollo, la disponibilidad y la utilización de capacidades de ciberseguridad en todo el mundo.[246]

[245] UIT, *Trabajar juntos para proteger la Sociedad mundial de la información…, Óp. Cit.*
[246] Ibídem.

Además de establecer estos parámetros, la UIT desprendió de la GCA el Índice Global de Ciberseguridad (GCI), un reporte que mide el avance de los países en los pilares mencionados. México, junto a otros 76 países, se le identifica en una etapa de "maduración", en tanto que sólo 21 países son ubicados en etapa de "líderes" en ciberseguridad. De acuerdo a los resultados del GCI 2017, México se encuentra ubicado en el lugar 28, de 193 países, con una calificación de 0.66 en una escala de 0 a 1, lo cual indica que ya se están realizando labores por implementar una estrategia de ciberseguridad efectiva. Sin embargo, falta mucho por ejemplo, en 10 de los 25 indicadores apenas se están iniciando o madurando los esfuerzos, por ello la necesidad de abordar este tema desde el ámbito académico.[247]

Es posible aseverar que la ciberseguridad es un tema transversal que debe ser abordado en México, para diseñar y construir los cimientos en torno al uso y aprovechamiento de las TIC, que permita que la paz y la seguridad en México, también que se puedan construir desde el ciberespacio y coadyuvar así en el desarrollo de capacidades, aprovechamiento de oportunidades y el crecimiento económico, político y social de la población.

A manera de resumen, en este capítulo se presentó un estado del arte del ciberespacio, para entender su origen y evolución dentro de la sociedad internacional, así como comprender por qué es importante mantenerlo abierto, libre y protegerlo de amenazas.

Se analizaron los riesgos del ciberespacio y las diversas actividades ilegales que se presentan en el mismo. Asimismo, se revisaron las características de los ciberataques y se pudo destacar que éstos tienen un carácter trasnacional y deslocalizado. Esto es, que pueden ser realizados desde cualquier punto del mundo sin limitar sus efectos a fronteras físicas, ello es muy complicado detectarlos, y a que se propaguen a gran velocidad.

[247] ITU, *Global Cybersecurity Index 2017*, en uit.org, Unión Internacional de Telecomunicaciones-ABI research, 2017, consultado en https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Se puede establecer que la ciberseguridad no es un concepto cerrado, ni limitado en su margen de acción, sino que es todo un conjunto de estrategias, planeaciones, estructuras, acciones y evaluaciones que están destinadas a mantener márgenes de seguridad y certidumbre dentro del ciberespacio, protegiéndolo de ataques a los individuos y a cualquier organización pública o privada.

También se percibió que la ciberseguridad no es un fin en sí misma, sino que todas las actividades relacionadas con ella tienen el objetivo de construir confianza en el ciberespacio y la meta de asegurar que no se dañen los intereses de los internautas, la infraestructura de la información y los canales de comunicación.

Comprender la circunstancia y alcances de la ciberseguridad permite definirla como un fenómeno que tiene que ser abordado desde la perspectiva no solo tecnológica, sino también social, política, económica, jurídica y cultural a niveles local, nacional, regional y global.

Con base en todos estos elementos y tomando en cuenta la propuesta de estudios CTS mencionada en el primer capítulo, se tiene un panorama amplio y las herramientas metodológicas suficientes para someter a consideración una evaluación de la Estrategia Nacional de Ciberseguridad de México.

En el siguiente capítulo se lleva a cabo una evaluación de dicha Estrategia, se revisa el estatus de la ciberseguridad en México en la actualidad, cuáles son las principales incidencias para los cibernautas mexicanos y las necesidades de las instituciones públicas y privadas para su protección, las medidas con las que se pretende dar confianza al ciberespacio, así como la efectividad de las acciones ejecutadas tanto a nivel nacional como internacional.

3. Revisión crítica de la Estrategia Nacional de Ciberseguridad en México.

En el primer capítulo se revisaron las premisas fundamentales de los estudios CTS y se consideró que este enfoque permite abordar los fenómenos tecnológicos de manera integral. En el capítulo 2 se explicó cómo se ha construido el ciberespacio a nivel global, así como los riesgos que pueden surgir en este entorno de interacción social y las implicaciones para la ciberseguridad. En este capítulo se analiza la Estrategia Nacional de Ciberseguridad bajo el enfoque CTS, para proceder posteriormente a elaborar un diagnóstico y evaluación.

Para lograr dicho objetivo, en este capítulo se expone la forma en que la visión crítica de los estudios CTS permite dar un viraje al diagnóstico y evaluación de la estrategia de ciberseguridad mexicana, y permite brindar una perspectiva integral, global y alejada del determinismo tecnológico.

Para ello, a partir del documento sobre la Estrategia Nacional de Ciberseguridad en México, se examinan los fundamentos y principios en los que se sustenta, los objetivos que persigue, los ejes que la guían y el marco institucional que enmarca su aplicación.

3.1 Visión crítica de la ciberseguridad.

En el primer capítulo, se realizó un recorrido crítico de la evolución histórica y teórica de los estudios CTS, se explicó por qué se consolidó la creencia de una relación metonímica tecnología-progreso durante el siglo XX, en un contexto marcado por dos guerras mundiales y un sinnúmero de fenómenos políticos, sociales, económicos, ideológicos y culturales en todo el globo. Se presentó un análisis que debatía a la tradición instrumental de la innovación tecnológica (TIIT) para exponer ideas más críticas e integrales respecto a los fenómenos tecnológicos. Por ello, se evocó a la tradición interpretativa de la innovación tecnológica (TIIN) y a las visiones constructivistas más reconocidas: la construcción social de la tecnología (COST) y la teoría del actor-red (TAR).

Asimismo, se hizo referencia a la contribución de la disciplina de las Relaciones Internacionales para estudiar los tópicos de carácter global, presentes en la agenda de los actores de la sociedad internacional y que se ubican en la

amalgama ciencia-tecnología-sociedad; particularmente, el análisis del ciberespacio y la necesidad de mantener la seguridad en dicho entorno. Se dio cuenta de la forma en que los internacionalistas abordan los fenómenos tecnológicos a partir de herramientas teórico-metodológicas propias, así como la influencia de los actores y factores internacionales en el análisis de dichos temas.

En este capítulo se parte de una visión crítica de la ciencia, la tecnología y la sociedad, necesaria para examinar la ciberseguridad en México. Esto implica examinar dicho fenómeno de forma transversal apoyado en el análisis de la Estrategia Nacional de Ciberseguridad publicada en México en el año de 2017 (ENCS) para posteriormente realizar su diagnóstico y evaluación.

3.1.1 Enfoque integral para analizar el fenómeno de la ciberseguridad.

La disciplina de Relaciones Internacionales permite comprender los fenómenos tecnológicos como parte de una compleja serie de procesos que ocurren en las sociedades a nivel internacional, regional y local, y que se constituyen a su vez como distintas tendencias a nivel global, dependiendo del actor que las promueva. En estas dinámicas complejas, participan una multiplicidad de actores y factores que establecen agendas, objetivos y mecanismos de difusión y asimilación de acuerdo al contexto tecnológico, social, político y económico de cada sociedad en particular y del contexto histórico internacional. Por lo tanto, existe la necesidad de seguir formando, consolidando y ampliando los marcos conceptuales para las Ciencias Sociales, específicamente para las Relaciones Internacionales, ya que como se ha mencionado el entorno global es cada vez más complejo.

La hegemonía del enfoque instrumental de la innovación tecnológica en los planteamientos oficiales sobre procesos donde se implica a la ciencia y a la tecnología, se puede superar a partir de la construcción de propuestas teórico-metodológicas más complejas e inclusivas. Por esta razón, se ha enfatizado en la necesidad de no separar los fenómenos tecnológicos de sus contextos socio-culturales e históricos, así como de las formas teórico-metodológicas y retóricas que los hacen relevantes.

Dejar de observar a los fenómenos tecnológicos con una visión no sólo optimista o pesimista de la ciencia y la tecnología, sino desde un enfoque crítico e interdisciplinar –sin el peso del determinismo tecnológico- permitió que se abordara el fenómeno de la configuración global del ciberespacio y de la ciberseguridad, entendiéndola desde un enfoque multifactorial donde se debe recurrir a la inclusión de los diferentes actores sociales y al entendimiento de la complejidad que implica comprender qué es el ciberespacio y los riesgos a la seguridad que se reproducen en dicho entorno.

Después de presentar en el segundo capítulo un estado del arte del ciberespacio y la ciberseguridad, es posible entender su origen y evolución en la sociedad internacional, así como percibir su relevancia y por qué es importante mantenerlo abierto, libre y protegido de amenazas. Lo anterior permitió establecer que el ciberespacio no es un concepto cerrado, ni limitado en su margen de acción; y que la ciberseguridad no es un fin en sí misma, sino que todas las actividades relacionadas a la misma tienen el objetivo de construir la confianza en el ciberespacio y la meta de asegurar que no se dañen los intereses de los internautas, la infraestructura de la información y los canales de comunicación.

También se analizaron los elementos implicados en la ciberseguridad y su importancia a nivel internacional. Para comprenderla, se exploró previamente el concepto del ciberespacio y cómo se ha configurado en un entorno de interacción humana a nivel global, alcanzando una relevancia tal, que los actores de la sociedad internacional han detectado la necesidad de protegerse ante los riesgos a la seguridad, en un plano diferente a las amenazas que tradicionalmente han existido.

Al caracterizar el ciberespacio, se encontró que este es un entorno donde las personas interactúan en una gran cantidad de actividades de toda índole, construyendo una comunidad. Esta idea refuerza la noción de que el ciberespacio es construido socialmente, más allá de los medios técnicos que permiten la comunicación y almacenamiento de los datos que lo hacen posible. Eso explicaba, en gran medida, por qué dicho entorno fue asimilado de forma relativamente rápida en prácticamente cada sector de la sociedad, pero también cómo ha evolucionado,

lo que justificaría la presencia del análisis de las ciencias sociales en temas relativos al ciberespacio.

La ciberseguridad ha cobrado importancia a nivel global. Tanto para las organizaciones internacionales, como para los Estados y las empresas, es necesario reforzar el acceso y la búsqueda de seguridad y confianza en el ciberespacio. Esto implica un fenómeno cuyos problemas trascienden y tienen repercusiones reales en las relaciones entre cada actor de la sociedad internacional. Asimismo, de manera crítica, se ha podido identificar la visión instrumental de la tecnología que permea en los actores internacionales sobre las cualidades y oportunidades en el ciberespacio.

Por consiguiente, la evaluación de la Estrategia Nacional de Ciberseguridad en México partirá de postulados no deterministas, al reconocer que los fenómenos que se presentan en los entornos sociales y físicos también se reproducen en el ciberespacio, como la desigualdad de acceso, las diferencias del desarrollo tecnológico, la restricción de acceso a la información, la censura a la libertad de expresión y la falta de acciones y recursos humanos, técnicos, institucionales, legales y económicos para salvaguardarse y mitigar los riesgos dentro de la arquitectura mundial de redes.

La ciberseguridad incluye un conjunto de acciones destinadas a construir y sostener márgenes de seguridad, certidumbre y confianza dentro del ciberespacio, protegiéndolo hasta dónde es posible, de ataques a los derechos y patrimonio de los individuos y de las organizaciones sociales, públicas y privadas. No obstante, muchos actores sociales no le han dado la importancia debida al espacio donde diariamente se relaciona prácticamente la mitad de la población mundial (hay 3.500 millones de usuarios de internet en el mundo según la UIT)[248] y en donde se tiene muy poco control y restricciones sobre el tiempo y el espacio para interactuar. No obstante, en países como México ya se esbozan esfuerzos para brindar confianza y ampliar los márgenes de seguridad, disponibilidad, integridad de las redes, confidencialidad, transparencia y certidumbre legal a los cibernautas.

[248] UIT, *Global Cybersecurity Index 2017…, Óp. Cit.*

Por lo tanto, una estrategia de ciberseguridad integral y efectiva debe construirse a partir de la participación de todos los sectores sociales, puesto que la sociedad en su conjunto es amenazada por los peligros cibernéticos. La confianza se consolidará si se generan las normas jurídicas respectivas, se realizan operaciones de respuesta inmediata en las redes, se coordinan acciones diplomáticas y medidas de protección en el ámbito militar y se establecen misiones permanentes de inteligencia dentro de la infraestructura mundial de la información y las comunicaciones. Sólo así se podrán generar políticas y estándares depurados sobre seguridad y las operaciones en el ciberespacio, así como establecer toda una gama de acciones que coadyuven en la reducción de amenazas, reducción de vulnerabilidades, disuasión de ataques, colaboración internacional, respuesta oportuna a incidentes, aumento de la resiliencia y políticas de recuperación ante ataques consumados.

De acuerdo a la revisión previa, a pesar de no tener una tipificación en el marco jurídico mexicano, a las actividades ilegales cibernéticas se les ha descrito por sus implicaciones en el espacio virtual o porque usan algún punto de la infraestructura mundial de redes para perpetrarse. Entre sus características se destaca que ofrecen muchas posibilidades de anonimato, una gran dificultad para ubicar a los responsables, la falta de procedimientos judiciales y de regulación jurídica al respecto, dificultades de comprobación por las herramientas técnicas para borrar algunos rastros, así como su alcance trasnacional que presenta desafíos jurisdiccionales, económicos y diplomáticos.

Al conocer los tipos de incidencias y los *modus operandi* de las amenazas en el ciberespacio, se reconoció la importancia de protegerlo de la manera más integral posible, por los desafíos de enfrentarse a criminales que pueden operar desde puntos geográficos difíciles de ubicar y de alcance global. El hecho de que los factores de riesgo tengan dicho alcance, invita a los internacionalistas a generar un enfoque integral, comparativo y multidisciplinar al momento de plantear, generar y evaluar estrategias de ciberseguridad efectivas.

Ahondando en uno de los puntos más claros del fenómeno estudiado en la presente investigación, la relevancia y alcance internacional de la ciberseguridad es

el meollo para establecer criterios de diagnóstico y evaluación de una estrategia nacional. Recalcando que no se trata de un fenómeno solamente tecnológico, sino de algo más complejo, que incluye otra serie de variables sociales, políticas, económicas, culturales, jurídicas, incluso de relaciones interpersonales y psicológicas. Por consiguiente, es claro que todos estos factores no podrán afrontarse si no hay una concientización de la sociedad y del trabajo conjunto de los actores para fortalecerse y ofrecer los márgenes más amplios posibles de libertad y seguridad en el ciberespacio.

Comprender la relevancia y los alcances de la ciberseguridad ha permitido precisarla como un fenómeno multidimensional, pero también en los niveles locales, nacionales, regionales y globales. Asimismo, se observa que la ciberseguridad es un tema transversal, que debe ser el fundamento en México al diseñar y construir los cimientos en torno a la apropiación de las TIC, para que éstas, lejos de sostener una esperanza de progreso nacional por sí mismas, permitan tener un uso que coadyuve a la creación de oportunidades y desarrollo en los diversos sectores educativos, productivos y gubernamentales.

Con base en los elementos anteriores, se retoma la propuesta de los estudios CTS mencionada en el primer capítulo, que tiene un panorama amplio y las herramientas metodológicas suficientes para someter a consideración una evaluación de la Estrategia Nacional de Ciberseguridad de México.

3.1.2 La ciberseguridad a través de los estudios CTS.

El enfoque de la presente investigación se sustenta en la TIIN, que tiene una amplia variedad de rutas críticas que han abierto nuevas puertas a la interpretación de los complejos procesos globales, propios del estudio de las Relaciones Internacionales. Dicha propuesta cuestiona los postulados de la tradición instrumental y su idea determinista de la tecnología. La TIIN lleva más de 50 años desarrollándose, dándose a la tarea de expugnar la llamada “caja negra” de la tecnología, desentrañando sus diversos significados y avanzando hacia una comprensión más profunda de sus procesos.

El panorama general examinado en el primer capítulo presentó un cuadro amplio que la describe a partir de varias premisas que logran dar cuenta de su complejidad. Asimismo, se ha explicado desde las Relaciones Internacionales cómo se ha ido construyendo y transformando el ciberespacio en el marco de la globalización y cuáles son las tendencias globales actuales de la ciberseguridad.

La TIIT concibe a la tecnología en un sistema social dado, como un proyectil que, lanzado del exterior, golpea un medio más o menos resistente. Pero la investigación ha dado cuenta de que los fenómenos tecnológicos van más allá de la lógica del mercado y la exitosa satisfacción de una necesidad de un grupo social. En un sentido inverso, se observa cómo la tecnología pende de procesos contingentes y conflictivos, relacionados con grupos públicos de interés, y no precisamente con etapas autocontenidas que pueden ser organizadas y administradas desde y hacia un punto u objetivos centrales específicos.

En el análisis de la ciberseguridad en México, se mantienen los principios que la TIIN sostiene al abordar los fenómenos tecnológicos, como procesos holísticos y multifuncionales, para alcanzar una visión comprensiva del origen, causas, trayectorias y destinos del ciberespacio y minimizar el carácter instrumental de las tecnologías implicadas. Para lograrlo, fue importante conocer los principales enfoques teóricos que articulan la TIIN, para ello se examinaron a los principales exponentes de los estudios sobre ciencia, tecnología y sociedad y sus principales postulados, así como las rutas críticas que orientan sus análisis.[249]

Bajo el nombre de estudios de ciencia, tecnología y sociedad (CTS), se han agrupado los distintos trabajos que permiten comprender la forma en que los fenómenos tecnológicos permean espacios sociales distintos, desde una perspectiva interpretativa y como un esfuerzo teórico para explicar el carácter social, político, filosófico, económico e histórico de la ciencia y la tecnología.

Los estudios CTS son el resultado de una confluencia de investigaciones y estudios de disciplinas heterogéneas cultivadas principalmente por epistemólogos, historiadores, filósofos, sociólogos y antropólogos. Encuentran su fundamento en el

[249] *Cfr.* Tula Molina, Fernando; Giuliano, Héctor Gustavo, "La teoría crítica de la tecnología: revisión de conceptos", *Redes*, vol. 21, núm. 41, diciembre, 2015, pp. 179-214, Universidad Nacional de Quilmes, Buenos Aires, Argentina, disponible en: https://www.redalyc.org/pdf/907/90748415006.pdf.

cuestionamiento del carácter instrumental y determinista de los estudios previos sobre ciencia y la tecnología, donde la noción de estas dos se articulaba en una relación metonímica con la idea de progreso. Por lo que la relación ciencia-tecnología-sociedad constituye una ruptura fundamental con la tradición optimista que entendía a la tecnología como una actividad liberadora.

El conjunto de estos elementos fue definiendo un campo de trabajo de carácter crítico, buscando comprender la dimensión social del desarrollo, adaptación y difusión científico-tecnológica, por lo que no existe una sola corriente o teoría predominante de los estudios CTS. Sin embargo, los distintos postulados han podido establecer que los fenómenos tecnológicos son procesos inherentemente sociales, donde elementos no epistémicos o técnicos, como los valores morales, usos sociales, convicciones políticas, intereses profesionales o presiones económicas, desempeñan un papel decisivo en la génesis y consolidación de las ideas científicas y los artefactos técnicos.

Se revisaron los dos esquemas explicativos de mayor representación de los estudios CTS: la COST, como una propuesta de análisis que explica el surgimiento, consolidación, adopción y evolución de una tecnología; y la TAR, que permite seguir las redes sociales que tejen los actores que son clave en los fenómenos tecnológicos. El propósito era tener una mayor comprensión de las aportaciones teórico-metodológicas de esta visión crítica de los fenómenos tecnológicos, sin considerar conveniente aplicar cada una de las categorías de análisis de ambos postulados en la presente tesis.

No obstante, la propuesta para evaluar y ofrecer una perspectiva de la Estrategia de Ciberseguridad Nacional en México, está cimentada en la base del giro interpretativo de la tecnología, a partir del cual se ha planteado la naturaleza socialmente contingente en la construcción del conocimiento científico y la creación de tecnologías, sistemáticamente organizadas a partir de actividades aparentemente desordenadas.

De la COST, de manera implícita se retoma la deconstrucción de la versión lineal y de sus cinco herramientas metodológicas principales, la más relevante para el objeto de estudio de la presente tesis, es la inclusión de los grupos sociales

relevantes asociados con el desarrollo de las medidas de ciberseguridad. Estos grupos son los ministerios de defensa, las empresas que poseen infraestructura en telecomunicaciones, individuos que exigen seguridad, libertad y confidencialidad al interactuar en el ciberespacio, instituciones que manejan datos de usuarios, asociaciones civiles que promueven el respeto a los derechos de todos los internautas y gobiernos que buscan brindar mayor confianza a sus ciudadanos, entre otros grupos.

También se retoma la flexibilidad interpretativa, a partir de la cual la ciberseguridad puede tener diversos significados y utilidades para los individuos y los sectores sociales, dependiendo de los riesgos a los que se expongan; por ejemplo, para los gobiernos lo más importante es la defensa y seguridad nacional en el ciberespacio, para las empresas la ciberseguridad debe proteger sus recursos económicos y para los individuos la ciberseguridad debe centrarse en la protección de sus derechos al internarse al ciberespacio.

Finalmente, el marco tecnológico distinto también por las condiciones de nuestro país, los niveles de conexión, los usos de la infraestructura y los recursos económicos y educativos con los que cuenta la población en general y el personal capacitado para operar las redes (ingenieros, técnicos, investigadores, policías) respecto a otros más avanzados en materia de ciberseguridad. Los cuales con la cooperación internacional, pueden coadyuvar a fortalecer las capacidades técnicas y ser aplicadas para proteger el ciberespacio.

De acuerdo a la COST, la ciberseguridad no sigue una trayectoria natural progresiva, sino que tiene que ser constantemente evaluada y estar pendiente de los contextos técnicos, como nuevo software, alcances o *modus operandi* de los criminales cibernéticos, en los cuales se desarrolle. Asimismo, se deben contemplar las relaciones de poder, las tensiones internacionales, las capacidades económicas y la colaboración entre entes públicos y privados donde se está aplicando.

De la TAR, se incluye la caracterización de estrategias, intereses y relaciones entre los diversos actores que pueden intervenir en la construcción de una estrategia de ciberseguridad. Así, el ciberespacio es un sistema-red, cuyos nodos son identificables: la infraestructura crítica, las capacidades técnicas, las redes

globales de comunicación, los individuos que se conectan desde dispositivos fijos o móviles; y sus enlaces son las relaciones entre éstos en un entorno virtual.

Los actores-mundo son los Estados, las empresas, las organizaciones civiles, las medidas legales, los grupos criminales, los centros de respuesta a incidentes, cuya conjunción se da a partir del proceso de traducción, que son las estrategias de ciberseguridad. Las cadenas de traducción serán las medidas legales, la cooperación internacional, la colaboración público-privada, los mecanismos de creación de capacidades técnicas y las estructuras organizacionales en las que se relacionan.

El conjunto de los actores-mundo y las estrategias de ciberseguridad como procesos de traducción constituyen una parte importante de la constante construcción del ciberespacio como sistema-red; convirtiéndolo en una entidad que no obedece reglas definitivas, compuesto por múltiples entidades cuyas asociaciones están en permanente y creciente interacción y construcción.

A partir de la revisión de las propuestas analíticas de los estudios CTS, y más puntualmente de la COST y la TAR, se puede afirmar que el ciberespacio no es sólo un fenómeno técnico, sino que está compuesto por una serie de elementos interactivos que permiten, o no, su desarrollo y consolidación en el imaginario social y que dentro de éste se reproducen todo tipo de relaciones dadas en el contexto social, como la delincuencia, con sus características concretas.

En esta investigación se considera que un análisis integral de la ciberseguridad debe estar influenciado por elementos sociales y que los diversos intereses de los grupos humanos desempeñan un papel importante en el momento de tomar una decisión sobre ella. Por lo tanto, una estrategia efectiva para brindar confianza en el ciberespacio debe estar compuesta en su diseño, desarrollo, apropiación e implementación, por los distintos sectores sociales y por los elementos no humanos suficientes que posibiliten su ejecución eficaz.

En consonancia con los postulados de los estudios CTS, se propone al lector de esta investigación que abandone las distinciones analíticas entre ciencia, tecnología y sociedad, y acepte el reto de observar que los procesos e interacciones en este fenómeno son dinámicos, heterogéneos y diversos. No obstante, esto no

significa que la forma de abordar los temas sea caótica, sino que hay premisas bien identificadas, a partir de las cuales examinar los casos; de manera que el acercamiento al fenómeno de la ciberseguridad tenga una estructura que permita realizar conclusiones concretas.

Asimismo, la disciplina de Relaciones Internacionales imprime su sello al dar cuenta de un fenómeno tecnológico que se puede dilucidar como parte de toda una serie de fenómenos que ocurren en las sociedades a nivel internacional, regional y local. Que se constituyen distintas tendencias a nivel global, en este caso la ciberseguridad, en las que participan una multiplicidad de actores y factores que establecen agendas, objetivos y mecanismos de difusión y asimilación de la misma, de acuerdo al contexto tecnológico, social, político y económico de cada sociedad en particular. Los internacionalistas, entonces, pueden ser referentes –dentro de las ciencias sociales- de la reflexión sobre la influencia de las dimensiones globales en las estrategias de ciberseguridad.

Por ello se insiste en el reto de avanzar hacia la sensibilización social de los temas relacionados con la tecnología, promover la idea de hacer propuestas más críticas e integrales, así como la necesidad de retomar los grandes temas de las ciencias sociales. De manera puntual de la disciplina de Relaciones Internacionales, como las guerras, la pobreza, el medio ambiente, la migración, la seguridad internacional, el crimen organizado trasnacional, el terrorismo, el ciberespacio y la ciberseguridad, entre otros. Tópicos de carácter global, presentes en las agendas de los actores de la sociedad internacional y que se ubican en la amalgama ciencia-tecnología-sociedad.

En el siguiente apartado se aborda desde la institucionalidad, cómo conciben los creadores de la Estrategia al fenómeno de la ciberseguridad y cuáles son las medidas con las que se pretende dar confianza al ciberespacio. El objetivo es conocerla en la letra documental para, posteriormente, hacer un diagnóstico de la ciberseguridad en el país durante el último sexenio y también evaluar la efectividad de las acciones ejecutadas, tanto a nivel nacional como internacional en el último año.

3.2 Documento de la Estrategia Nacional de Ciberseguridad (2017).

La Estrategia Nacional de Ciberseguridad es el documento que establece la visión del Estado mexicano en la materia y se presentó el 13 de noviembre de 2017, en el marco de la Tercera Semana Nacional de Ciberseguridad, en la Ciudad de México.[250] Es un instrumento marco, donde no están especificadas cada una de las acciones, pero se despliegan una serie de principios, objetivos y recomendaciones con la intención de tener en el ciberespacio un entorno confiable y resiliente.

La ENCS es un documento de 30 páginas, compuesto de 9 apartados que, al examinarlos, se pueden dividir en 3 partes. La primera parte, que consta de 5 subapartados, muestra el contexto y los fundamentos sobre los que se asienta la visión del Estado mexicano respecto al tema de la ciberseguridad y la necesidad de haber creado dicho instrumento institucional. Los siguientes 2 apartados abordan la estrategia, despliegan los principios, ejes y objetivos, asimismo, explican el marco institucional para la ejecución de dichas medidas. La última parte es complementaria; en ella se brinda un glosario para entender a cabalidad la terminología utilizada y se anexa la información con las reuniones a través de las cuales se llevó a cabo el proceso colaborativo entre los distintos actores sociales para desarrollar la ENCS.

A continuación, se exploran las dos partes relevantes de la ENCS. Se revisan las bases, justificación y contextos que se tomaron en cuenta para que se generara dicha estrategia. También se examina su margen de acción, al conocer sus principios, ejes, estructura, objetivos y marco institucional. El propósito es conocer en forma y fondo lo que dice la Estrategia y cuáles son las medidas con las que se pretende dar confianza al ciberespacio.

[250] OEA, *México presentó Estrategia Nacional de Ciberseguridad desarrollada con apoyo de la OEA*, Organización de Estados Americanos, comunicado de prensa, publicado el 13 de noviembre de 2017, consultado en http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-082/17 [marzo 2018]

3.2.1 Fundamentos y contextos de la ENCS

En este apartado se muestran las secciones más significativas del documento de la ENCS, a partir de una síntesis que permite hacer observaciones pertinentes para explicar la visión plasmada por sus creadores.[251]

La primera parte de la ENCS se compone de los siguientes subapartados:

1. Resumen ejecutivo.
2. Justificación.
3. Introducción.
4. Contexto internacional.
5. Contexto nacional.

En el **Resumen ejecutivo** se plantea, a grandes rasgos, cómo se dio el proceso de estructuración de la ENC, a partir del reconocimiento de tres fenómenos:

> A. La importancia de las tecnologías de la información y comunicación (TIC) como un factor de desarrollo político, social y económico de México; en el entendido de que cada vez más individuos están conectados a Internet y que tanto organizaciones privadas como públicas desarrollan sus actividades en el ciberespacio.
>
> B. Los riesgos asociados al uso de las tecnologías y el creciente número de ciberdelitos.
>
> C. La necesidad de fomentar una cultura general de ciberseguridad. (p.2)

En primer lugar, se puede observar que, de acuerdo al punto A, la ENCS está permeada por una visión determinista y optimista de la tecnología, pues describen a las TIC como "un factor de desarrollo político, social y económico de México", es decir, como un ente externo que por sí solo puede impactar en el desarrollo de todo un país. Por otro lado, también es notable que hay una conciencia de los riesgos que existen asociados al uso de dichas tecnologías y la necesidad de construir no sólo medidas institucionales, sino de generar una cultura de la ciberseguridad.

A continuación, se expone la razón por la cual era necesario crear una estrategia de alcance nacional:

[251] Todos los fragmentos son extraídos directamente del documento "ESTRATEGIA NACIONAL DE CIBERSEGURIDAD, MÉXICO 2017", ya citada anteriormente. Para especificar la referencia, será señalado el número de página del fragmento, entre paréntesis, al final de la cita.

> El aumento de riesgos, amenazas y ataques informáticos sofisticados, el surgimiento de nuevas formas y técnicas para aprovechar vulnerabilidades, así como el incremento de conductas delictivas que se cometen a través de las TIC, son circunstancias que hacen de la ciberseguridad un tema complejo. A lo anterior se suma la naturaleza global del ciberespacio y la concurrencia de diferentes soberanías y marcos jurídicos. (p.2)

Al caracterizar la complejidad del fenómeno de la ciberseguridad, se da un paso importante, puesto que eleva su importancia para no ser abordada desde enfoques simplistas ni como un ámbito que debe tomarse a la ligera.

Se explica la estructura de la ENCS, que define objetivos y ejes transversales, plasma los principios rectores, identifica a los diferentes actores involucrados y da claridad sobre la articulación de esfuerzos entre individuos, sociedad civil, organizaciones privadas y públicas en materia de ciberseguridad; además señala el modelo de gobernanza para la implementación, seguimiento y evaluación de la Estrategia. (p.2)

Se describe la forma en que el Gobierno de la República tomó el rol central para promover espacios de diálogo, discusión y aprendizaje, mediante foros y talleres en un proceso de colaboración denominado “Hacia una Estrategia Nacional de Ciberseguridad”, que tuvo lugar en los meses de marzo a octubre de 2017. Después de los debates y propuestas de los sectores participantes, se enumeran las necesidades que debía atender la estrategia:

- ✓ Articular el desarrollo de las acciones de ciberseguridad que sirvan a individuos, empresas e instituciones públicas del Estado mexicano.
- ✓ Colaboración y cooperación entre los diferentes sectores como pieza clave para el desarrollo, seguimiento y evaluación de la Estrategia.
- ✓ Conocer la dimensión de los riesgos y amenazas en el ciberespacio, el estado que guarda la ciberseguridad en el país, la construcción de un diagnóstico nacional, así como obtener evidencia para mejorar la toma de decisiones en materia de ciberseguridad.
- ✓ Contemplar el escenario global como parte de la problemática y la diplomacia como vía para entablar diálogos y acuerdos que permitan hacer frente a los riesgos, amenazas y ciberdelitos.

- ✓ Desarrollar capital humano especializado en materia de ciberseguridad.
- ✓ Promover el uso responsable de las TIC y reforzar una cultura de ciberseguridad que contemple acciones de concientización, educación y formación. (p.3)

Estas conclusiones, van en consonancia con la visión crítica e integral que se ha ido planteando en la presente investigación, aunque faltan elementos articuladores y líneas de acción concretas. Además, se resalta que, aun sin una estrategia institucional de ciberseguridad en México, se han impulsado en los últimos años esfuerzos en la materia con actores separados –tanto públicos como privados- actuando cada uno por su lado.

El resumen ejecutivo señala que el éxito de la ENCS radica en la colaboración de las diferentes partes interesadas y en la corresponsabilidad ante la adopción y uso de las TIC. Esta última aseveración está estrechamente relacionada con la reducción de la brecha digital y sus tres dimensiones, de acceso, uso y apropiación, y cabe ser críticos para mencionar que en todo el documento nunca se habla de apropiación de las TIC.

El resumen ejecutivo concluye con la siguiente aseveración: “Este es un documento vivo que pretende actualizarse constantemente conforme la dinámica social lo requiera”.(p.4) Este es, quizá, su mayor acierto, y es que significa que el documento es un marco que está abierto a la interpretación y actualización, dependiendo de las necesidades y recursos; pero también es un arma de doble filo, al implicar que puede ser descartado fácilmente por gobiernos posteriores que no tengan la misma visión que se plasmó en la ENCS de 2017.

En la **Justificación** se explica que la ENCS se fundamenta en el Plan Nacional de Desarrollo 2013-2018, en el Programa Nacional para la Seguridad Pública 2014-2018 y el Programa para la Seguridad Nacional 2014-2018. No se ahonda en señalar los puntos o líneas estratégicas a las que pertenece la ENCS, pero en la presente investigación se despliega a continuación:

En la tercera línea de acción de la “Estrategia 1.2.3” del Plan Nacional de Desarrollo, se formula el impulso de “iniciativas de ley que den sustento a las actividades de inteligencia civil, militar y naval, para fortalecer la cuarta dimensión

de operaciones de seguridad: ciberespacio y ciberseguridad."[252] Dicha línea de acción está relacionada con el objetivo 1.2 "Garantizar la Seguridad Nacional", que se propone fortalecer la inteligencia del Estado Mexicano para identificar, prevenir y contrarrestar riesgos y amenazas a la Seguridad Nacional, perteneciente a la meta número uno del gobierno "México en Paz".[253] Dichos objetivos y líneas de acción se incluyeron en la elaboración del Programa para la Seguridad Nacional 2014-2018 (PSN) y del Programa Nacional de Seguridad Pública 2014-2018 (PNSP).

En el PSN, la ciberseguridad recibe una alta prioridad -solo después de los desastres naturales y la delincuencia organizada trasnacional- ya que se reconoce que el "incremento de los ataques en contra de la infraestructura crítica, los intereses económicos, las redes de información y las capacidades de defensa de las naciones demuestra que existen gobiernos, grupos criminales y organizaciones terroristas dispuestas a explotar el ciberespacio con propósitos hostiles."[254]

De esta manera, se considera que la ENCS no sólo estaba fundamentada en políticas de Estado, sino que tenía una alta prioridad; sin embargo, no se dieron las condiciones ni los canales necesarios para construir la estrategia desde la primera parte del sexenio, por lo que será importante que el gobierno actual (2018-2024) preste atención en el tema de la ciberseguridad desde el inicio, esta vez con un marco ya establecido, como lo es la ENCS.

La justificación prosigue mencionando que las TIC ya han alcanzado un uso generalizado en las actividades cotidianas de individuos, organizaciones privadas y públicas, y vuelven a mencionar que son impulsoras del desarrollo político, social y económico. De nueva cuenta se privilegia el significado de la tecnología por sí misma.

Para ello, se presentan una serie de datos sobre los ciberataques reportados a nivel global (algunos de ellos ya mencionados en el capítulo 2 de la presente investigación). Señala que los ciberataques aumentaron un 30 por ciento entre 2011

---

[252] Gobierno de la República*, Plan Nacional de Desarrollo 2013-2018,* Gobierno de la República, México, 2013, p. 107, consultado en http://pnd.gob.mx/ [mayo 2018].
[253] Ibíd., pp. 103-107.
[254] Gobierno de la República, *Programa para la Seguridad Nacional 2014 - 2018 del Estado mexicano*, en dof.gob.mx, Gobierno de la República, México, publicado el 30 de abril de 2014, p. 17, consultado en http://www.dof.gob.mx/nota_detalle.php?codigo=5342824&fecha=30/04/2014&print=true [mayo 2018]

y 2012, afectando a 550 millones de personas en todo el mundo; que el cibercrimen le cuesta al mundo hasta US$575,000 millones al año, lo que representa 0.5 por ciento del producto interno bruto global. En América Latina y el Caribe, este tipo de delitos representa un gasto de alrededor de US$90,000 millones al año. En México se estima que los costos inherentes a la comisión de dichos delitos representaron 3,000 millones dólares. (pp. 6-7) Estos datos son significativos tomando en cuenta que en México, los internautas han pasado a ser 70 millones en 2018, lo que significa que más del 50% de la población está en condiciones de sufrir algún ataque a través del ciberespacio (o de cometerlo…).

Estos datos, asociados a las bases institucionales y las políticas de Estado, justifican la creación de la ENCS y se recalca que sólo la suma de los esfuerzos de todos los involucrados en materia de ciberseguridad permitirá “diseñar y construir los cimientos en torno al uso y aprovechamiento de las TIC en un ambiente libre, responsable y confiable que permita el desarrollo de capacidades, aprovechamiento de oportunidades, el crecimiento económico, político y social de la población”. (p.7)

En la **Introducción** se reconoce que las actividades que se realizan en el ciberespacio también tienen impacto en el mundo físico, por lo que resultaba apremiante tener un referente en materia de ciberseguridad, con la finalidad de contribuir al fortalecimiento de las instituciones públicas y al cumplimiento y respeto de los derechos humanos.

Se explica que, dada la complejidad y naturaleza transfronteriza de las dinámicas de la era digital, es necesario abordar la ciberseguridad de forma integral, colaborativa, holística y transversal. En este sentido, la presente investigación ha propuesto una visión multidisciplinaria e inclusiva. La ENSC resalta la meta de que cualquier esfuerzo que aborde dicho fenómeno evolucione en el tiempo, pero siempre apostando al esfuerzo conjunto de todos los sectores sociales.

Se subraya que la ENCS busca contribuir al desarrollo sostenible de México, y se despliegan los principios rectores que sustentan la Estrategia:

A. Perspectiva de derechos humanos.

B. Enfoque basado en gestión de riesgos.

C. Colaboración multidisciplinaria y de múltiples actores.

Entrando en materia, se aborda brevemente el **Contexto internacional** en materia de ciberseguridad, describiendo los diferentes escenarios y mecanismos internacionales, tanto vinculantes, como no vinculantes, que guardan relación con el tema y en los que ha participado el Estado mexicano en la última década. Con el propósito de hacer conciencia sobre la gran relevancia que ha tomado la ciberseguridad como asunto global en la agenda internacional.

Se señala que la globalización y la hiperconectividad exigen soluciones centradas en la colaboración internacional de manera precisa, eficaz y eficiente. Por lo que, ante la complejidad de la sociedad en la era digital y los retos que representa el uso y aprovechamiento de las TIC en la sociedad de la información, es importante plantear el tema de la ciberseguridad desde la óptica del contexto internacional. En seguida se enuncia una serie de instancias internacionales, gubernamentales y no gubernamentales, donde se han centrado en debatir y afrontar el tema de la ciberseguridad en todas sus aristas.

Se despliegan instancias globales como la Organización de las Naciones Unidas (ONU), a través la Cumbre Mundial sobre la Sociedad de la Información (CMSI) de 2003 y 2005; el Grupo de Expertos Gubernamentales (GEG) que fue creado para analizar las amenazas, retos y dimensiones de la ciberseguridad; la Comisión de Prevención del Delito y Justicia Penal (CCPCJ); el Foro para la Gobernanza de Internet (IGF) que desde 2014 incluye los Foros de Mejores Prácticas en temas de ciberseguridad; y la UIT que ha desarrollado el Índice Global de Ciberseguridad (GCI), para medir el compromiso de los países en el tema, donde se señala que México está en una etapa de “maduración”.

También aparecen diversas instancias que, sin tener un alcance global, tienen una gran relevancia al insertarse en esquemas multilaterales. Así se menciona a la OCDE, en la que México, junto con otros 40 países, se ha comprometido a reducir las barreras para el comercio electrónico nacional e internacional y a desarrollar estándares técnicos globales que permitan la interoperabilidad y un Internet seguro, estable, abierto y accesible; el Banco Interamericano de Desarrollo (BID) que, en conjunto con la OEA y el Centro Global de Capacitación de Seguridad Cibernética (GCSCC) de la Universidad de Oxford,

publicaron un documento sobre ciberseguridad para la región; el Foro para la Gobernanza de Internet (LACIGF); el Foro Económico Mundial (WEF); el Consejo de la Agenda Global en Ciberseguridad; y la Corporación para la Asignación de Nombres y Números en Internet (ICANN), entre otras. (p.12)

Asimismo, se enumeran algunas instancias regionales donde se trabajan de manera puntual y más a profundidad la cooperación técnica e institucional entre los países miembros, como el Comité Interamericano contra el Terrorismo (CICTE); la Agenda Digital para América Latina y el Caribe (eLAC); la Alianza del Pacífico; y La Reunión Regional Preparatoria de América Latina y el Caribe para el Foro para la Gobernanza de Internet (LACIGF).

Se destacan algunos datos sobre la tendencia internacional en esta materia, indicando que los incidentes y ataques cibernéticos están aumentando en frecuencia, grado de afectación y sofisticación; señalando que la UIT ha informado que los ciberataques aumentaron un 30 por ciento entre 2011 y 2012, afectando a 550 millones de personas en todo el mundo y ocasionando pérdidas económicas de 110,000 millones de dólares. Por lo que “los gobiernos y las empresas a nivel global reconocen la necesidad de contar con marcos, medidas y capacidades de seguridad de la información y ciberseguridad más robustas, así como de la cooperación e intercambio de información, para hacer frente al creciente número de ataques informáticos, amenazas y riesgos en el ciberespacio”. (p.12)

En el apartado del **Contexto nacional,** se señala el estado del desarrollo digital del país, el sector de telecomunicaciones y usuarios de Internet, así como algunas referencias necesarias que se han elaborado en México respecto a la ciberseguridad. Se indica que el uso generalizado y los diferentes factores económicos, políticos y socioculturales han propiciado que, según datos del INEGI, casi el 60 por ciento de la población mexicana, con edad de seis años o más, se declare usuaria de Internet, que el 68.5 por ciento de los cibernautas mexicanos tiene menos de 35 años y que el 47 por ciento de los hogares del país tienen conexión a Internet. Asimismo, que Internet se utiliza principalmente como medio de comunicación para la obtención de información en general y para el consumo de contenidos audiovisuales.

Dentro de los ordenamientos del gobierno en turno, se menciona que en el marco del Plan Nacional de Desarrollo 2013-2018, dentro del Programa para un Gobierno Cercano y Moderno 2013-2018, se estableció la Estrategia Digital Nacional cuya finalidad es impulsar la digitalización de México, a través de acciones como: gobierno digital, datos abiertos, inclusión y habilidades digitales, servicios de salud y educación a través de las TIC, el uso de TIC en servicios financieros, entre otras. Se subraya la importancia de fortalecer la ciberseguridad para que todos los servicios públicos, principalmente los digitales y los derechos de las personas se realicen sin barreras, de manera confiable y con resiliencia, con miras a fortalecer la confianza en el uso de las TIC y en la relación entre instituciones públicas, sector privado y la sociedad en general.

Se refiere al documento “Evaluación de la Ciberseguridad en México: Brechas y Recomendaciones en un Mundo Hiper-Conectado”, estudio realizado en el año 2017 por el sector privado, donde obtuvieron las siguientes conclusiones:

- La necesidad de contar con una Agencia de Ciberseguridad Nacional que coordine la estrategia que se estaba definiendo.
- La importancia de redefinir el marco jurídico para la ciberseguridad, que garantizara la protección a datos personales y estimulara la compartición de información.
- Garantizar la protección de infraestructura crítica, sobre todo la ciberresiliencia bajo un enfoque de gestión de riesgo.
- El desarrollo de habilidades y competencias para el nuevo ecosistema digital, definiendo claramente las nuevas habilidades que serán necesarias, ampliando, desarrollando y reclutando el mejor talento posible.

Asimismo, se mencionan algunos datos sobre la labor de la Policía Federal, a través de la División Científica, al informar que han logrado atender más de 51,000 denuncias ciudadanas y más de 200,000 incidentes cibernéticos; que se han desactivado cerca de 17,000 sitios fraudulentos y emitido más de 2,000 alertas de ciberseguridad dirigidas a instituciones públicas y privadas. (pp. 14-15)

Por último, y no menos importante, en el contexto nacional se resalta que la ENCS es de naturaleza transversal, que se articula con otros programas y estrategias y se desprende de lo señalado en el propio Plan Nacional de Desarrollo 2013-2018, en apego a los valores y principios que establece la Constitución Política de los Estados Unidos Mexicanos. Como se muestra en el siguiente esquema:

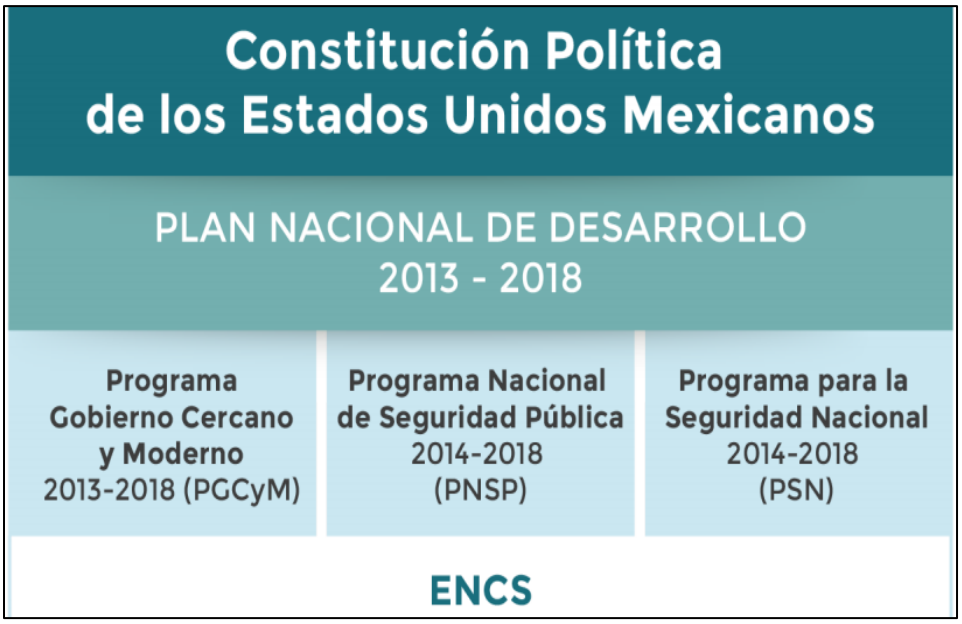

Ilustración 1. Estrategia Nacional de Ciberseguridad, p. 15.

Al revisar esta primera parte de la ENCS, se pudieron conocer –de la letra misma del documento- las bases, justificación y contextos tomados en cuenta para que se generara dicha estrategia. Se desmenuzaron las partes más significativas, a modo de síntesis y se realizaron algunas observaciones pertinentes para explicar la visión plasmada por sus creadores, con el propósito de conocer en fondo y forma lo qué dice la Estrategia.

Los primeros cinco apartados del documento mostraron el contexto y los fundamentos sobre los que se asienta la visión del Estado mexicano respecto al tema de la ciberseguridad y la necesidad de haber creado dicho instrumento institucional. A continuación se hace referencia a la parte toral, donde se describen puntualmente cuáles son los principios, ejes y objetivos de la ENCS.

3.2.2 Principios, objetivos, ejes y marco institucional de la ENCS.

El apartado “Estrategia Nacional de Ciberseguridad” es la sección de mayor importancia, ya que en ella se describen la visión, los principios, los objetivos estratégicos y los ejes transversales que la guían.

Visión. En 2030, México será una nación resiliente ante los riesgos y amenazas en el ciberespacio, que aprovecha con responsabilidad el potencial de las TIC para el desarrollo sostenible en un entorno confiable para todos.

Objetivo general. Fortalecer 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. (p. 16)

Principios

La ENCS contempla los siguientes principios rectores:

A. Perspectiva de derechos humanos.

Contemplar en las diferentes acciones en materia de ciberseguridad la promoción, respeto y cumplimiento de los derechos humanos; entre otros, la libertad de expresión, el acceso a la información, el respeto a la vida privada, la protección de datos personales, la salud, educación y trabajo. Cabe mencionar que todos estos encuentran su fundamento en la Constitución Política de los Estados Unidos Mexicanos y los Tratados Internacionales suscritos por México.

B. Enfoque basado en gestión de riesgos.

Contar con la capacidad de manejar escenarios de incertidumbre por medio de enfoques preventivos y correctivos, con la intención de minimizar el impacto de las cambiantes amenazas y riesgos del ciberespacio.

C. Colaboración multidisciplinaria y de múltiples actores.

Enfoque basado en la colaboración multidisciplinaria de las diferentes partes (actores y sectores): 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. Este será el reto mayor por la dificultad de articular de manera eficiente a todas las partes. (p.16)

La ENCS plasma las acciones generales que ha de desarrollar el Estado mexicano en su conjunto: sociedad civil, academia, sector privado e instituciones públicas, para que se obtenga el máximo beneficio de las TIC en un entorno confiable y resiliente que se traduzca en beneficios para todos. A continuación, se despliega su estructura.

Para lograr el objetivo general, se plantean cinco objetivos estratégicos, cuyo desarrollo requiere de ocho ejes transversales, mismos que están articulados, son interdependientes y contribuyen a alcanzar cada uno de los objetivos estratégicos. A su vez, todas las acciones de cada eje transversal serán desarrolladas sobre los tres principios rectores. A continuación, se muestra la representación gráfica de la estructura de la ENCS:

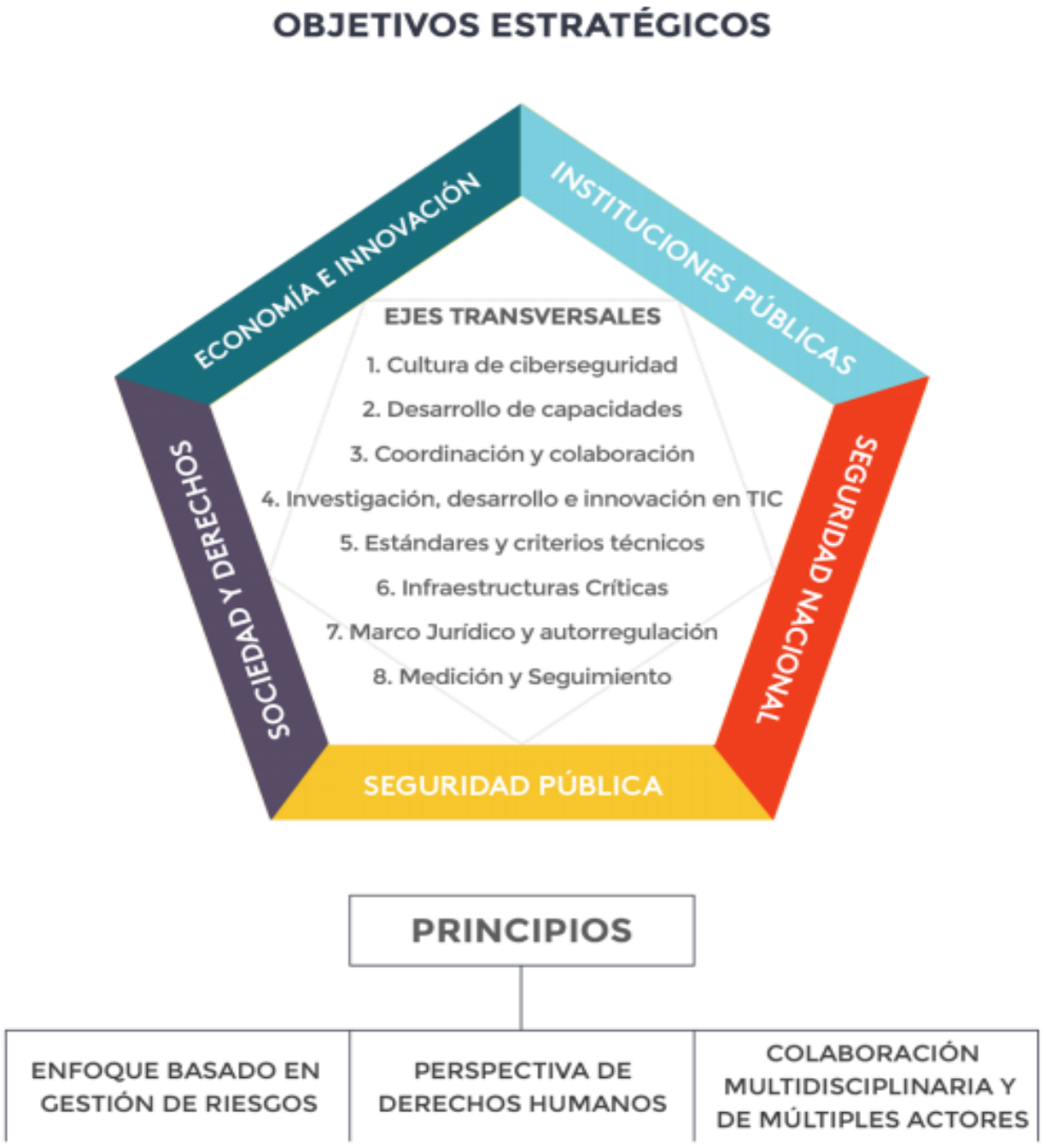

Ilustración 2. Estrategia Nacional de Ciberseguridad, p. 17

Objetivos

Los objetivos estratégicos son los cinco entornos a proteger y de los cuales se derivan las acciones generales que buscarán beneficiar a la sociedad civil, al sector privado, las instituciones públicas y las comunidades académicas y técnicas.

I. Sociedad y derechos.

Generar las condiciones para que la población realice sus actividades de manera responsable, libre y confiable en el ciberespacio, con la finalidad de mejorar su calidad de vida mediante el desarrollo digital en un marco de respeto a los derechos humanos como la libertad de expresión, vida privada y protección de datos personales, entre otros.

II. Economía e innovación.

Fortalecer los mecanismos en materia de ciberseguridad para proteger la economía de los diferentes sectores productivos del país y propiciar el desarrollo e innovación tecnológica, así como el impulso de la industria nacional en materia de ciberseguridad, a fin de contribuir al desarrollo económico de individuos, organizaciones privadas, instituciones públicas y sociedad en general.

III. Instituciones públicas.

Proteger la información y los sistemas informáticos de las instituciones públicas del país para el funcionamiento óptimo de éstas y la continuidad en la prestación de servicios y trámites a la población.

IV. Seguridad pública

Incrementar las capacidades para la prevención e investigación de conductas delictivas en el ciberespacio que afectan a las personas y su patrimonio, con la finalidad de mantener el orden y la paz pública.

V. Seguridad nacional

Desarrollar capacidades para prevenir riesgos y amenazas en el ciberespacio que puedan alterar la independencia, integridad y soberanía nacional, afectando el desarrollo y los intereses nacionales. (p. 18)

Ejes

De la mano de los objetivos, se plantean ocho ejes transversales, los cuales constituyen la columna vertebral de la ENCS, mismos que también servirán como base para el desarrollo del plan de implementación correspondiente.

1. Cultura de ciberseguridad:

Es el conjunto de valores, principios y acciones en materia de concientización, educación y formación, que se llevan a cabo por la sociedad, academia, sector privado e instituciones públicas, que inciden en la forma de interactuar en el ciberespacio de forma armónica, confiable y como factor de desarrollo sostenible. La cultura de ciberseguridad abonará al cumplimiento de los cinco objetivos estratégicos, mediante el desarrollo de políticas públicas, estrategias, programas, proyectos, acciones e iniciativas que:

- Contribuyan a la promoción, cumplimiento y protección de los derechos de individuos y organizaciones públicas y privadas, con énfasis en la protección de niñas, niños y adolescentes en el ciberespacio y sus derechos.
- Favorezcan el máximo aprovechamiento y uso responsable de las tecnologías de la información y comunicación, la convivencia armónica y el desarrollo de actividades en el ciberespacio.
- Incentiven la innovación y la economía para el desarrollo sostenible.
- Fortalezcan la prevención de riesgos y conductas delictivas que afectan a individuos, organizaciones privadas y públicas.
- Incrementen la confianza y continuidad de los servicios y trámites digitales públicos y privados.
- Contribuyan a la prevención de riesgos que pudieran afectar a las infraestructuras críticas de información y operación. (p.19)

2. Desarrollo de capacidades:

Es el conjunto de acciones encaminadas a la generación y fortalecimiento de las capacidades organizacionales, de capital humano y recursos tecnológicos en materia de ciberseguridad, que permitan a los actores contar con los recursos para

la gestión de riesgos y amenazas en el ciberespacio, así como el incremento de la resiliencia nacional. Ayudan en el cumplimiento de los objetivos mediante el desarrollo de políticas públicas, estrategias, programas, proyectos, acciones e iniciativas que:

- Incentiven el desarrollo de capital humano mediante la formación de:
  i. Especialistas y profesionales de la ciberseguridad.
  ii. Líderes profesionales de la ciberseguridad como conductores de estrategias y políticas.
  iii. Profesionales de la investigación y desarrollo para la industria y el comercio de la ciberseguridad.
  iv. Profesionales de la investigación y persecución de los delitos que se cometen a través de las TIC, así como de la procuración e impartición de justicia.
- Establezcan la organización que deberá prevalecer en lo público y privado a fin de:
  i. Posicionar a la ciberseguridad a nivel estratégico en las organizaciones públicas y privadas.
  ii. Establecer los mecanismos de participación ciudadana en materia de ciberseguridad.
- Generen la infraestructura tecnológica necesaria para:
  i. El desarrollo tecnológico nacional de ciberseguridad para el fortalecimiento gradual de la ciberseguridad en México.
  ii. Incrementar las capacidades técnicas para la identificación y gestión de incidentes cibernéticos a nivel nacional. (p. 19-20)

3. Coordinación y colaboración:

Es el conjunto de acciones orientadas a coordinar y establecer los canales de colaboración entre las distintas instituciones públicas, academia, sociedad civil y organizaciones privadas en materia de ciberseguridad, en los diferentes ejes transversales, con la finalidad de consolidar el ecosistema de ciberseguridad y obtener la capacidad resiliente necesaria para establecer los mecanismos

preventivos, proactivos y reactivos que brinden confianza y tranquilidad a la población en el uso y aprovechamiento de TIC. El desarrollo de acciones de coordinación y colaboración apoyará el cumplimiento de los objetivos a través de la implementación de acciones que:

- Fortalezcan la cooperación y colaboración internacional.
- Identifiquen los mecanismos de coordinación y cooperación entre los distintos actores involucrados a nivel nacional.
- Definan y apliquen el modelo de gobernanza de ciberseguridad entre sociedad civil, sector privado, academia e instituciones públicas para compartir información y mejores prácticas en materia de ciberseguridad.
- Establezcan protocolos y canales de comunicación que fortalezcan la confianza, reciprocidad, y estimulen la responsabilidad social de todos los actores. (p.20)

4. Investigación, desarrollo e innovación en TIC:

Es el conjunto de acciones orientadas a establecer los mecanismos para fomentar la investigación, desarrollo e innovación en el uso y aprovechamiento de las tecnologías en materia de ciberseguridad con la finalidad de favorecer el desarrollo de capital humano e innovación tecnológica en la materia e impulsar el mercado nacional de ciberseguridad que favorezca el desarrollo de capacidades y la madurez del ecosistema nacional. Estas permitirán consolidar los cinco objetivos estratégicos a través de la generación de nuevos modelos y tecnología orientados a minimizar los riesgos y vulnerabilidades inherentes a las tecnologías mediante:

- Establecimiento de políticas, programas, acciones e iniciativas que detonen y consoliden el ecosistema de ciberseguridad en México, entre academia, sociedad civil, sector privado y sector público para detonar innovación en TIC relacionadas a ciberseguridad.
- Promoción de investigación científica y tecnológica que impulse el desarrollo de capacidades en materia de ciberseguridad.

● Impulso del mercado nacional en materia de ciberseguridad que favorezca la autonomía tecnológica a nivel nacional y detone la economía nacional en dicho sector. (p. 21)

En este eje, es preciso detenerse para reflexionar sobre la visión determinista y optimista de la Estrategia que además le atribuye propósitos que están fuera de su alcance. 'Lograr la autonomía tecnológica a nivel nacional y detonar la economía nacional en dicho sector' no son objetivos realistas para un documento de 30 páginas con indicaciones generalizadas sobre un sector específico como la ciberseguridad. El desarrollo del sector es posible a través de una política de Estado, de programas de investigación, desarrollo e innovación. No se depende de una estrategia de ciberseguridad, sino de un conjunto de factores, diagnósticos, líneas, con un presupuesto asignado, personal especializado, la participación de universidades, de institutos de investigación, mecanismos de vinculación, entre otras estructuras legales e institucionales y con recursos económicos, humanos y técnicos suficientes para consolidarla.

5. Estándares y criterios técnicos:

Es el conjunto de acciones enfocadas al desarrollo, adopción y fortalecimiento de los estándares, criterios técnicos y de normalización en materia de ciberseguridad, que permitan la homologación y aplicación de las mejores prácticas y procesos en el uso y adopción de las TIC en un entorno de ciberseguridad, los cuales coadyuvaran en el cumplimiento de los cinco objetivos estratégicos mediante:

● Establecimiento de criterios, normas y metodologías para la generación, uso y adopción de hardware y software con la finalidad de fortalecer el ecosistema de ciberseguridad y disminuir riesgos y vulnerabilidades inherentes a la tecnología.

● Definición de los marcos de referencia para fortalecer la ciberseguridad de organizaciones privadas y públicas, academia y sociedad en general.

● Promoción de la participación de la comunidad académica, técnica y científica en el desarrollo y fortalecimiento de estándares, metodologías y normalización en materia de ciberseguridad.

● Identificación y, en su caso, fomento del uso de estándares y mejores prácticas internacionales en materia de ciberseguridad. (p. 21)

6. Infraestructuras críticas:

Conjunto de acciones encaminadas a establecer las acciones y mecanismos necesarios para minimizar la probabilidad de riesgos y vulnerabilidades inherentes en el uso de las TIC para la gestión de infraestructuras críticas, así como para fortalecer la capacidad de resiliencia para mantener la estabilidad y continuidad de los servicios en caso de sufrir un incidente de ciberseguridad.

Estas medidas ayudarán al cumplimiento de los objetivos mediante el desarrollo de políticas, programa de desarrollo de capital humano y acciones orientadas al establecimiento de políticas y acciones que se llevarán a cabo en el marco de la Ley de Seguridad Nacional y demás instrumentos aplicables y aplicables en materia de seguridad nacional y en colaboración con las instancias de seguridad nacional. (p. 22)

7. Marco jurídico y autorregulación:

Impulsar y establecer acciones y mecanismos necesarios para la adecuación del marco jurídico nacional vinculado a la ciberseguridad y de autorregulación; por parte de los concesionarios, permisionarios, distribuidores de servicios de TIC, incluida la modificación a efecto de brindar certeza jurídica al actuar de los intermediarios de Internet, y la sociedad en general, que permita el uso y aprovechamiento de las TIC y sana convivencia en el ciberespacio.

Las acciones orientadas a la adecuación del marco jurídico nacional y el desarrollo de mecanismos de autorregulación en la era digital son vitales para el avance de la digitalización en el mundo y clave para la prevención de riesgos y amenazas, la investigación y sanción de los delincuentes en la era digital; sumado a que es clave para fortalecer la confianza entre sociedad, sector privado e instituciones públicas. Lo anterior contribuirá al cumplimiento de los 5 objetivos estratégicos a través de:

● El desarrollo de capacidades de operadores jurídicos y tomadores de decisiones en instituciones públicas y privadas, así como de la sociedad civil; sobre el ecosistema digital, la gobernanza de Internet y la ciberseguridad para analizar y proponer modificaciones o armonización legislativa acorde a las necesidades de la sociedad de la información que permita afrontar los riesgos y amenazas en materia de ciberseguridad.

● La certeza jurídica para que las instituciones públicas y privadas puedan desarrollar sus tareas en un entorno de cooperación, donde las instancias de procuración de justicia que incrementen su eficacia en la investigación, prevención, persecución y en la sanción a las personas ciberdelincuentes.

● El análisis y establecimiento de mecanismos y procedimientos de autorregulación que favorezca la construcción de confianza entre individuos, sector público y organizaciones privadas con apego a derecho.

● La homologación y armonización de códigos penales y leyes complementarias en relación a ciberdelitos, así como de las herramientas jurídicas con las que cuentan las instancias de procuración de justicia para la persecución de los mismos. (p. 22)

8. Medición y seguimiento:

Es el conjunto de políticas y acciones encaminadas al fomento y desarrollo de mecanismos homologados de medición que permitan dar seguimiento a los resultados obtenidos de la implementación de la ENCS y su impacto en el desarrollo social y económico del país, con la finalidad de identificar las áreas de oportunidad para su mejora continua. Estas acciones coadyuvarán al cumplimiento de los objetivos mediante la generación de estadísticas e indicadores que permitan:

● La colaboración conjunta de actores para la elaboración de metodología que permita la construcción de diagnóstico nacional sobre riesgos y amenazas en el ciberespacio.

● El establecimiento de estadísticas centralizadas relacionadas con la implementación y el impacto de la ciberseguridad y de la Estrategia en los sectores económicos, políticos y sociales.

● La obtención de datos para la mejora continua y actualización de la Estrategia Nacional de Ciberseguridad. (p. 23)

De esta manera, se despliegan los ocho ejes transversales, de los cuales también se desprenden líneas de acción más puntuales, pero no tan específicas. La eficacia y funcionalidad de cada uno de estos ejes, en la práctica, se examina en el último capítulo. De hecho, poder corroborar si estas acciones se pueden llevar a cabo y qué resultados arrojan, es parte medular de la evaluación que se realizará del ENCS en la presente investigación.

Alcance y futuro

Se explica que la ENCS es un documento pensado para evolucionar conforme a las necesidades de la sociedad en torno a la ciberseguridad, con la finalidad de tener la capacidad de adaptación y mejora continua frente a los retos, riesgos, amenazas y vulnerabilidades inherentes a las futuras tecnologías y la nueva dinámica social en el corto, mediano y largo plazo.

Es un documento que reafirma la visión de que la ciberseguridad es un habilitador para ampliar el potencial de la digitalización del país y pieza clave para el desarrollo sostenible de México y el mundo. Este enfoque nuevamente demuestra su base instrumental, el determinismo y hasta el discurso esperanzador de la digitalización de la sociedad mexicana.

Por eso, se subraya que existen riesgos y amenazas en el ciberespacio, que también evolucionan las técnicas de generación de malware y conductas delictivas de forma incluso más rápido de lo que puede reaccionar una política pública, o la regulación. Por ello debe haber una preparación constante para conocer y atemperar los posibles riesgos inherentes al uso de dichas tecnologías. (p. 24)

Se concluye la explicación de la estructura, señalando que la ENCS es un documento vivo que marca la ruta para el desarrollo de la ciberseguridad en México, con un enfoque integral, transversal, holístico y con la colaboración de las diferentes partes interesadas, es decir: sociedad civil, instituciones públicas, sector privado y comunidades técnicas y académicas.

Marco Institucional

En el documento de la ENCS se contempla un marco institucional, el cual será parte del modelo de gobernanza de la ciberseguridad, y que da cuenta de cómo el Gobierno de la República coordinará el tema de ciberseguridad por medio de las dependencias competentes, para que en el futuro se establezcan los canales de cooperación y participación de los múltiples actores interesados.

A nivel nacional existen diferentes esfuerzos en materia de ciberseguridad, tanto de instituciones públicas como privadas, además de esfuerzos de comunidades técnicas y académicas y de la sociedad civil.

El Gobierno de la República, en el marco de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE)[255], en el mes de octubre de 2017, mediante acuerdo adoptado por unanimidad en la Comisión, acordó la creación de la Subcomisión de Ciberseguridad, presidida por la Secretaría de Gobernación a través de la CNS (Policía Federal /División Científica). (p. 25)

Entre los integrantes de esta subcomisión se encuentran diversas dependencias y entidades de la Administración Pública Federal, con la finalidad de que la Estrategia Nacional de Ciberseguridad cuente con un desarrollo integral, holístico y transversal desde el Ejecutivo Federal y permita la vinculación con las diferentes partes interesadas, es decir: sociedad civil, sector privado, comunidades técnica y académica e instituciones públicas de los distintos poderes y de los diferentes órdenes de gobierno, incluida cualquier institución pública con autonomía.

[255] De conformidad con el artículo Tercero, fracción III y Décimo Noveno del Acuerdo que tiene por objeto crear en forma permanente la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, publicado en el Diario Oficial de la Federación el 09 de diciembre de 2005, y el Acuerdo Tercero del Acta de la 18ª Sesión Ordinaria de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, del 11 de octubre de 2017, se creó la Subcomisión de Ciberseguridad, integrada por las siguientes autoridades: 1. División Científica de la Policía Federal, quien la preside. 2. Jefe de la Unidad de Innovación y Estrategia Tecnológica de la Oficina de la Presidencia de la República. 3. Unidad de Gobierno Digital de la Secretaría de la Función Pública, y 4. Los titulares de las Unidades de Tecnologías de la Información y Comunicaciones de la Secretarías de Gobernación, de Economía, de Educación Pública, y de Hacienda y Crédito Público, así como el titular de la Unidad de Tecnología de la Información y Comunicaciones de la Procuraduría General de la República. La Subcomisión de Ciberseguridad cuenta con los siguientes invitados permanentes: SEDENA, SEMAR, SAT, CNBV, PROFECO, CONDUSEF, IPN, CONACYT, CENACE, SRE, SSA, STCNS-OPR, y SE SIPINNA.

Entre otras tareas, la Subcomisión de Ciberseguridad se encargará de:

● Aprobar y dar a conocer la Estrategia;

● Dar seguimiento y coordinar la implementación de la ENCS en colaboración con las diferentes dependencias y entidades de la APF;

● Impulsar los esquemas de colaboración y cooperación interinstitucional en materia de ciberseguridad; y

● Fomentar la colaboración y cooperación con los diferentes actores interesados: sociedad civil, sector privado, comunidades técnicas y académicas. (p. 25)

Implementación de la ENCS

La Subcomisión de Ciberseguridad establecerá los grupos de trabajo para el desarrollo de cada uno de los ejes transversales, que de manera directa impactarán en los diferentes objetivos estratégicos. Los grupos de trabajo permitirán integrar esfuerzos, acciones y propuestas de los diferentes actores, acorde a las capacidades y atribuciones de cada una de las partes.

Rol de la Subcomisión de Ciberseguridad

La Subcomisión será el vínculo formal con el Consejo de Seguridad Nacional, a través del Comité Especializado en Seguridad de la Información. Las acciones necesarias para dar cumplimiento al objetivo estratégico de seguridad nacional deberán ser aprobadas en el seno del Consejo de Seguridad Nacional, y su implementación estará a cargo del Comité Especializado en Seguridad de la Información, en coordinación con la Subcomisión de Ciberseguridad, en el ámbito de su competencia. (p. 26)

En la última parte del documento de la ENCS, se muestran un par herramientas complementarias.

Se brinda un **glosario** que ayuda a entender a cabalidad la terminología utilizada. Su importancia radica en que se conceptualizan diversos términos técnicos y específicos, propios del rubro de la ciberseguridad.

Finalmente, se anexa la información del proceso colaborativo denominado **"Hacia una Estrategia Nacional de Ciberseguridad"**, donde se explica que en el desarrollo del documento de la ENCS queda plasmada la participación y apoyo de diferentes actores en México: sociedad civil, sector privado, comunidad técnica y académica, e instituciones públicas de los tres poderes y de los diferentes órdenes de gobierno. Se detallan los temas de las reuniones con las que se fueron concretando los esfuerzos conjuntos, mismas que tuvieron lugar entre los meses de mayo a noviembre del año 2017, en distintas sedes institucionales, ubicadas en la Ciudad de México y el Estado de México. (p. 30)

Al revisar la ENCS, se pudieron identificar los fundamentos y la justificación sobre la que está basada. Fue reconocible la idea instrumental de la visión de sus creadores. Los tomadores de decisiones siguen dándole atribuciones especiales al fenómeno tecnológico, en este caso, a los efectos relacionados con las TIC. No obstante, también es posible identificar un enfoque holístico, una conciencia de que la ciberseguridad es un tema transversal y de alcance global, que no puede ser abordado de manera excluyente y desarticulada.

Una vez reconocida la institucionalidad del documento escrito como una herramienta colectiva y oficial con alcance de futuro, se pudo estimar la forma en cómo conciben sus creadores el fenómeno de la ciberseguridad y cuáles son las medidas con las que se pretende dar confianza al ciberespacio.

Con el examen del texto documental, es posible apreciar que éste no es solo una guía práctica o un código de acciones para seguir, sino un instrumento marco, en el que si bien no están especificadas cada una de las acciones, en cambio se establece una serie de principios, objetivos y recomendaciones.

El propósito último de este capítulo fue abordar en forma y fondo lo qué dice la Estrategia y, una vez conocidos estos elementos, hacer tanto un diagnóstico como una evaluación de la ciberseguridad más enfocados en lo que –en el supuesto institucional- debería derivar la ENCS, comparando la realidad de los datos y los estándares internacionales, es decir, el ser *versus* el deber ser.

En este capítulo, se expuso la forma en que la visión crítica de los estudios CTS permite dar un viraje al diagnóstico y evaluación de una estrategia de

ciberseguridad para ofrecer una perspectiva integral, global y alejada del determinismo tecnológico. Se estableció que una estrategia efectiva para brindar confianza en el ciberespacio debe estar influenciada en su diseño, desarrollo, apropiación e implementación, por los distintos sectores sociales y por los elementos no humanos para su ejecución eficaz.

En consonancia con los postulados de los estudios CTS, se planteó el reto analítico de observar que los procesos e interacciones del fenómeno son dinámicos, heterogéneos y diversos, bajo premisas bien identificadas de manera que el acercamiento al fenómeno de la ciberseguridad bajo la lupa CTS tenga una estructura que permita realizar conclusiones prácticas.

A lo largo del capítulo se realizó un recorrido del documento publicado el 13 de noviembre del 2017 de la Estrategia Nacional de Ciberseguridad en México, donde el enfoque previamente explicado permitió conocer los fundamentos y contextos en que fue concebido, así como los principios que observa, los objetivos que persigue, los ejes que la guían y el marco institucional.

Después de su examen a nivel documental se puede afirmar que la ENCS se inserta en la visión instrumental que ha permeado sobre la tecnología en los programas y políticas gubernamentales, ya que se atribuye el predominio de la innovación y al desarrollo científico y tecnológico por encima de otros factores, y la inexpugnable facultad de impactar al entorno social, como si la tecnología surgiera como un elemento externo a la sociedad. En el caso de la ENCS, se señalan en reiteradas ocasiones como beneficios inherentes al desarrollo y efectos de una buscada inserción de las TIC en la sociedad.

No obstante lo anterior, también se pudo identificar la conciencia de que la ciberseguridad debe ser abordada de manera integral e incluyente. De igual manera fue posible reconocer que las instancias que lideraron el proceso de construcción de la ENCS entienden que el fenómeno es transversal y tiene alcance global.

Respecto al documento de la ENCS, se puede concluir que ésta es un marco general, no un manual de acciones y estándares, por lo que resulta ser flexible en su aplicación, pero también permite muchas generalidades, incluso ambigüedades,

que podrían poner en riesgo su ejecución pensando en el largo plazo, como política de Estado de alcance transexenal.

Establecidas estas consideraciones, en el último capítulo se lleva a cabo una observación puntual sobre la ENCS. Al mismo tiempo que se presenta un diagnóstico del fenómeno de la ciberseguridad en México y se hace una evaluación a la Estrategia basada en dos parámetros: el primero, se refiere al contexto internacional y, el segundo, se remite a la revisión de las actividades realizadas con base en sus ejes transversales y los resultados obtenidos en la consecución de los objetivos plasmados en dichos ejes.

4. Diagnóstico y evaluación de la Estrategia Nacional de Ciberseguridad en México (2012-2018).

Una vez explicado el enfoque con el que se debe abordar el fenómeno de la ciberseguridad y revisada la Estrategia en forma y fondo, se presentan los elementos necesarios para entrar en el estudio de caso y realizar el diagnóstico y la evaluación, focalizados en lo que –en el supuesto documental- debería derivar la ENCS, comparado con los estándares internacionales y la realidad de los datos, es decir, el ser *versus* el deber ser.

En este capítulo, se lleva a cabo un análisis sobre la situación actual de la ciberseguridad y una evaluación de la Estrategia. A través del estatus general de la ciberseguridad durante el sexenio del presidente Enrique Peña Nieto, de manera de comparar el documento de la Estrategia con un marco de referencia global para finalmente examinar los esfuerzos por ejecutar de las acciones planteadas en la misma.

El capítulo se divide en dos secciones. La primera tiene como objetivo conocer las condiciones generales de la ciberseguridad a lo largo del sexenio anterior (2012-2018), para ello se describen las principales incidencias en el tema de la ciberseguridad, las acciones y esfuerzos de los distintos actores y sectores sociales durante el periodo. En la segunda parte, se lleva a cabo la evaluación de la ENCS, observada a partir de dos estándares: primero, bajo una referencia global de buenas prácticas en ciberseguridad; y, segundo, el cotejo de los propios lineamientos de la ENCS, con las actividades realizadas desde su publicación.

La evaluación, además del análisis cualitativo, tiene un valor cuantitativo y, con base en los resultados de la investigación, se presentan algunas consideraciones sobre la ENCS. De esta manera, se cuenta con los elementos suficientes para definir si se encuentra planteada adecuadamente para su correcta aplicación y si efectivamente podrá cumplir su objetivo primordial: fortalecer 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.

4.1 Diagnóstico de la ciberseguridad durante el sexenio de Enrique Peña Nieto: condiciones generales e incidencias.

En el presente apartado se presentan una serie de datos que permiten conocer el estatus general de la ciberseguridad durante el sexenio del presidente Enrique Peña Nieto (2012-2018). Para lograr dicho objetivo, se realizó una investigación sobre las principales incidencias y acciones en general en materia de ciberseguridad durante el periodo referido.

En el año 2018, México reportó 129 163 276 habitantes[256], de los cuales –según la Asociación de Internet Mx- 79.1 millones son internautas.[257] Esto significa que más del 64% de los mexicanos tiene la capacidad de internarse en el ciberespacio. Un número que implica un avance significativo en cuanto a penetración de Internet durante del sexenio que lo precedió, ya que de 45.1 millones de personas que usaban Internet en 2012[258], al 2018, se observó un incremento del 75.5%.

Las principales actividades de los mexicanos son interactuar en redes sociales, utilizar el servicio de correo electrónico, escuchar música y, cada vez más, se realizan compras en línea y trámites gubernamentales. Asimismo, de acuerdo a la Asociación mencionada, el 78% se conectan preferentemente desde dispositivos móviles y los internautas pasan más tiempo conectados que años anteriores, pues en el 2018 alcanzaron las 8 horas con 12 minutos de conexión al día, es decir, una tercera parte del tiempo total de su vida cotidiana se encuentra en línea.[259]

Estos datos en específico son relevantes, ya que nos muestran que en la cotidianeidad del mexicano promedio, cada vez son menos las restricciones para internarse al ciberespacio, por más tiempo y sin distinción de lugar, lo que implica riesgos ante el descuido o la poca conciencia que pudiera tener la sociedad

---

[256] Banco Mundial, *Datos México*, en World Bank Group, consultado en https://datos.bancomundial.org/pais/mexico [septiembre 2018]

[257] Asociación de Internet MX, *14° Estudio sobre los Hábitos de los Usuarios de Internet en México 2018*, Ciudad de México, publicada en mayo de 2018, consultada en https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/14-Estudio-sobre-los-Habitos-de-los-usuarios-de-Internet-en-Mexico-2018/lang,es-es/?Itemid= [octubre 2018]

[258] Ibídem.

[259] Ibídem.

mexicana en temas de protección cibernética. En suma, este hecho deriva en un tema de apropiación tecnológica.

Aunque más de 45 millones de mexicanos siguen desconectados de Internet, la tendencia de penetración es clara y el incremento de conexiones ha sido significativo en los últimos seis años. Ello eleva la importancia de la ejecución efectiva de las acciones en ciberseguridad para proteger a la población en general y brindar confianza para que los cibernautas sigan conectándose al ciberespacio.

También en encuestas sobre la confianza de los usuarios en temas como la banca y el comercio electrónico, se revelaron algunas preocupaciones de los mexicanos. El 87% de los cibernautas desconfían de la seguridad al momento de utilizar sus tarjetas bancarias y hacer compras en línea,[260] por lo que el 93% utiliza alguna herramienta de protección, como antivirus, contraseñas largas y los dispositivos *token,* entre los más utilizados. Sin embargo, el 31% considera que su seguridad en el ciberespacio depende de las empresas o del gobierno y no del usuario a nivel individual.[261]

Si bien los datos anteriores ofrecen un marco general sobre el alcance y la penetración del ciberespacio en México, así como sobre la percepción de los cibernautas sobre el tiempo y tipo de interacción que realizan, el panorama general se complementa al revisar las incidencias más comunes sobre el dominio cibernético en México y algunas de las medidas con las que han respondido las autoridades mexicanas al respecto.

A continuación, se presentan los tipos de ataques, riesgos e incidencias que se han registrado en los últimos años en México. Esto permitirá tener un mapa más articulado de las conductas ilícitas que más se denuncian en este país y la manera en que han reaccionado las instituciones destinadas a la protección del ciberespacio.

---

[260] Asociación de Internet Mx, *Estudio Comercio Electrónico en México 2015*, en asociaciondeinternet.mx, México, 2015, consultado en https://amipci.org.mx/estudios/comercio_electronico/Estudio_de_Comercio_Electronico_AMIPCI_2015_version_publica.pdf [septiembre 2018]

[261] Asociación de Internet Mx, *Banca electrónica 2013*, México, 2013, consultado en https://www.amipci.org.mx/estudios/banca_por_internet/Banca_Electronica_2013_VP.pdf[septiembre 2018]

La Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI), en conjunto con la Asociación Mexicana de Tecnologías de la Información (AMITI) y la Asociación de Internet Mx, presentaron el estudio "Evaluación de la Ciberseguridad en México: Brechas y recomendaciones en un Mundo Hiper-Conectado", donde se señala que "es difícil monitorear la actividad cibernética maliciosa y su impacto en México, porque las organizaciones no las reportan por miedo a dañar su reputación o simplemente porque no están conscientes de que han sido víctimas."[262] No obstante, las incidencias y tendencias en los riesgos a la ciberseguridad en el país han sido reportadas por las autoridades de seguridad a nivel nacional y en varios estudios realizados en los últimos años.

Desde la entrada del pasado gobierno, en el seno de la institución que se responsabiliza de la seguridad al interior del país, la Secretaria de Gobernación (SEGOB), se le asignó a la División Científica de la Policía Federal, el cuidado, vigilancia y atención del ciberespacio.Esta División está bajo el mando de la Comisión Nacional de Seguridad (CNS), instancia que ha informado que en la primera parte del sexenio se atendieron cerca de 60 mil incidentes, relacionados con ataques cometidos principalmente contra los tres niveles de gobierno (53 por ciento), el ámbito académico (26 por ciento) y el sector privado (21 por ciento).[263]

Las denuncias sobre ataques cibernéticos están focalizadas en los siguientes tipos de crímenes: suplantación y robo de identidad (68 por ciento), fraude cibernético (17 por ciento) y ataques a sitios web (15 por ciento).[264] La Policía Federal también informó sobre la identificación y desactivación de 5 mil 549 sitios de Internet apócrifos que usurpaban la identidad de instancias financieras y

[262] CANIETI, *Evaluación de la Ciberseguridad en México: brechas y recomendaciones en un mundo híper-conectado*, Reporte final de Ciberseguridad (iniciativa privada y asociación civil), Ciudad de México, 6 de septiembre de 2017, pp. 45-46, consultado en https://docplayer.es/65552142-Evaluacion-de-la-ciberseguridad-en-mexico-brechas-y-recomendaciones-en-un-mundo-hiper-conectado.html [enero 2018]
[263] CNC, *Fortalece CNS estrategias para la protección del ciberespacio mexicano,* en cns.gob.mx, Comisión Nacional de Seguridad, comunicado de prensa no.32, México, 25 de febrero de 2015, consultado en http://www.cns.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1368028 [agosto 2018]
[264]Ibídem.

gubernamentales con fines de fraude, es decir, se logró neutralizar cerca del 10% de las amenazas.[265]

En 2015, la firma PwC señaló que México era el segundo país más atacado en América Latina y el número de ciberataques creció 40% entre 2013 y 2014, afectando a 10 millones de víctimas.[266] En 2016, *CISCO Systems* señaló que se generaba gran cantidad de malware en el país, ya que Brasil, México y Colombia, en orden descendente generaron 75% del *SPAM* que había afectado a la región.[267]

En un estudio realizado para el sector financiero en México, la firma británica *Control Risks* identificó que los ciberataques más importantes experimentados en este sector estaban dirigidos más a los ciudadanos que a las grandes corporaciones. Señaló que los ciberataques más comunes reportados por instituciones financieras eran de los menos sofisticados, tales como Denegación de Servicio (DDoS), los Troyanos y los programas maliciosos. Estas mismas instituciones reconocieron que el crimen organizado utilizó malware y spam como medio para extorsionar a ciudadanos y falsificar su identidad.[268]

La OEA señaló en un estudio que en México las incidencias que afectaron a la población civil habían crecido 409% a causa del *phishing*. Algunos de los sectores más importantes de México, tales como finanzas, telecomunicaciones, energía y educación han reportado incidentes crecientes a su seguridad cibernética y están dando mayor prioridad a su protección.[269]

PwC identificó en una encuesta que 91% de las compañías en México otorgaban alta prioridad a la ciberseguridad y registraban las inversiones más altas en la región. Dentro de los sectores más proactivos en este tema, están el financiero y las telecomunicaciones, que son los más atractivos para los cibercriminales y los de mayor alcance a nivel global.[270]

---

[265]Ibídem.

[266] PwC Mexico, *Cybersecurity in Mexico*, PwC, Mexico, 2015, consultado en https://www.pwc.com/mx/es/knowledge-center/archivo/20150917-kc-cybersecurity.pdf [junio 2018]

[267] CISCO SystemsInc, *Spam Overview*, CISCO, Estados Unidos, 2016, consultado en: https://www.senderbase.org/static/spam/#tab=4 [junio 2018]

[268] Control Risks, *CyberThreatstotheMexicanFinancial Sector*, 21 de diciembre de 2016, consultado en https://www.controlrisks.com/en/services/security-risk/cyber-threats-to-the-mexican-financial-sector [junio 2018]

[269]Ibídem.

[270]CANIETI, *Evaluación de la Ciberseguridad en México: brechas y recomendaciones…, Óp. Cit.*, p. 47.

Con base en el Reporte de Riesgo Global 2017, del Foro Económico Mundial, los incidentes masivos de fraudes y robo de datos son considerados dentro de los cinco de mayor probabilidad de afectar al mundo. El crecimiento exponencial de la actividad en el ciberespacio se correlaciona con una escalada similar de las acciones criminales en México. Sobre todo, el reporte alertó sobre el incremento en el *hacking* ilegal, el robo de identidad, el fraude asociado a tarjetas de crédito y la explotación en línea de menores.[271]

Un estudio especial del Equipo de Emergencia de Cómputo de EEUU (US-CERT) estimó que 32% de los ataques fueron dirigidos a compañías de energía –basta recordar el ataque a la planta nuclear iraní-. Dado que la energía es parte de la infraestructura crítica y su vulnerabilidad puede impactar a la seguridad nacional; los gobiernos de la región, incluido el mexicano, están poniendo mayor atención en el sector, adoptando mejores estrategias y protocolos.[272]

La Policía Federal ha informado que mantiene "patrullajes en Internet", para detectar a delincuentes que cometen fraudes, intrusiones o realizan actividades ilícitas en la red local e internacional y que constantemente se emiten alertas sobre ciberataques, en especial sobre distintos tipos de extorsión, tanto a través de correo electrónico como por red telefónica, al ser los más comunes en México.[273]

La División Científica ha señalado que el 79 por ciento de las denuncias cibernéticas a nivel nacional provienen de la Ciudad de México, la entidad con mayor penetración de Internet en el país.Sin embargo, esto no implica que no haya incidentes en las entidades con menor número de denuncias, sino que la información sobre cómo denunciar y las campañas de concientización no han llegado a muchos estados de la República. Además, en la capital del país se

---

[271] World Economic Forum, *The Global Risks Report 2017*, 12th Edition, enenero 2017, consultadoenhttp://www3.weforum.org/docs/GRR17_Report_web.pdf [julio 2018]

[272]CANIETI, *Evaluación de la Ciberseguridad en México: brechas y recomendaciones…*, *Óp. Cit*., p. 47.

[273] CNS, *Policía Federal detecta intentos de extorsión cibernética*, en cns.gob.mx, Comisión Nacional de Seguridad, Comunicado de prensa No. 31, México, 23 de febrero de 2015, consultado en http://www.cns.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1368028 [septiembre 2018]

encuentran las centrales de los corporativos de empresas que han recibido ataques, sobre todo del sector financiero y telecomunicaciones.[274]

La CNS informó que durante la administración de Peña se emitieron más de mil alertas preventivas de seguridad cibernética. Se resalta el caso de un ataque *phishing* que utilizaba la imagen de instituciones policiales de distintas partes del mundo con fines de extorsión, pero que la Policía Federal desarrolló el protocolo para desactivarlo, con lo que se evitó riesgos a más de un millón de usuarios y pérdidas de hasta dos mil millones de pesos. Se destacó también la alerta sobre el virus CTB-Locker que obstruye el acceso al contenido de los archivos de la computadora con el fin de extorsionar a la víctima a cambio de recuperarla.[275]

Luisa Parraguez, del Instituto para México del Centro Wilson en Washington, subrayó los riesgos que enfrenta el país por la gran capacidad financiera del crimen organizado. Considera que es difícil que estos grupos no hayan contratado expertos en seguridad para establecer sus propias unidades de contrainteligencia. En un capítulo dedicado al crimen organizado y el cibercrimen en México, describe una larga lista de actividades criminales de estos grupos a través de Internet, como el robo de identidad, fraudes, extorsiones, secuestros, tráfico de órganos y armas, así como la emergencia de grupos de cibervigilantes enfrentados con cárteles de la droga para contrarrestarlos.[276] Desde la perspectiva del documento mencionado de la CANIETI, "toda esta larga cibercriminalidad debe haber sido objeto de investigaciones por parte de instituciones policiacas y militares encargadas de la ciberseguridad en el país".[277] Aunque, hasta el momento, no hay un informe o documento detallado con ese tipo de información.

El hecho de que México sea la economía 15 del mundo y haya registrado crecimiento (1 a 2%) en los últimos años; a lo que se agrega el ser de las economías más abiertas, su cercanía e intercambio comercial con una potencia como Estados

---

[274] CNS, *Policía Federal detecta intentos de extorsión cibernética*, en cns.gob.mx, Comisión Nacional de Seguridad, Comunicado de prensa No. 31, México, 23 de febrero de 2015, consultado en http://www.cns.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1368028 [julio 2018]

[275] Comisión Nacional de Seguridad, *Fortalece CNS estrategias para la protección del ciberespacio…, Óp. Cit.*

[276] Luisa Parraguez, *TheStateofCybersecurity in Mexico: AnOverview*, Wilson Center, enero de 2017, consultado en https://www.wilsoncenter.org/publication/the-state-cybersecurity-mexico-overview [junio 2018]

[277] CANIETI, *Evaluación de la Ciberseguridad en México: brechas y recomendaciones…, Óp. Cit.*, p. 47.

Unidos, y suposición geopolítica estratégica, permite reconocer lo crítico que puede llegar a ser un problema generalizado de inseguridad cibernética en el país.[278]A los factores externos, se le suman las amenazas cibernéticas particulares a nivel interno, como son el crimen organizado, grupos subversivos y activistas anónimos que han adquirido experiencia, herramientas y capacidades avanzadas comparables a las del Estado mexicano. Estas organizaciones han lanzado ciberataques contra el gobierno, empresas (sobre todo del sector financiero y de comunicaciones), a los ciudadanos e inclusive, ataques entre los grupos mismos.[279]

Todos los datos señalados demuestran que México se encuentra en un punto de inflexión donde, por un lado, puede comenzar a ser blanco principal de diversas amenazas y ataques cibernéticos en la región y, por otro, puede ser una oportunidad para fortalecerse en el ámbito para ser un referente y una pieza clave en la configuración de estrategias regionales de ciberseguridad.

En cuanto a las acciones emprendidas a lo largo del sexenio, previas a la construcción del documento de la ENCS, las distintas instancias gubernamentales, desde el poder legislativo, y algunos órganos del ejecutivo –sobre todo relacionados con seguridad y defensa- realizaron esfuerzos, pero sin un objetivo general de largo alcance nacional y sin articulación entre los diversos actores.

En julio de 2014, se promulgó la Ley Federal de Telecomunicaciones y Radiodifusión, como parte de una reforma estructural en el sector. La Ley contiene algunas disposiciones como la retención de datos y el hecho de que las autoridades públicas pueden acceder a datos retenidos sin una orden judicial. Cabe mencionar que una de las bases de este ordenamiento fue el marco jurídico del Convenio de Budapest sobre el Delito Cibernético.[280]

En todas las agencias gubernamentales, las TIC se actualizan regularmente, se realizan copias de seguridad y se adhieren a las disposiciones del Manual Administrativo de Aplicación General de TIC y de Seguridad de la Información (MAAGTICSI), el cual se desarrolló con base a normas internacionales como ISO

[278]Ibíd., p. 45.
[279]Ibídem.
[280]Gobierno de la República, *Reforma en materia de Telecomunicaciones*, Presidencia de la República 2012-2018, consultado en http://reformas.gob.mx/reforma-en-materia-de-telecomunicaciones/que-es[julio 2018]

27001, ITIL (Information Technology Infrastructure Library) y COBIT (Control Objectives for Information and Related Technology), entre otras.[281]

Instituciones gubernamentales y la academia han ofrecido cursos, talleres y conferencias sobre seguridad cibernética, además de también algunas oportunidades de capacitación para empleados, incluyendo programas de certificación a través del sector privado. Recientemente, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) inició una campaña proponiendo leyes más estrictas de protección de datos personales, así como una mayor transparencia y disponibilidad de información al público. Además de su labor de promoción, el INAI publica informes y conduce campañas de sensibilización para los ciudadanos sobre sus derechos como usuarios de las tecnologías de la información y la comunicación.[282]

La División Científica de la Policía Federal es la agencia que ha aplicado las acciones sobre ciberseguridad a nivel federal, bajo tres ejes principales:

I. Prevención de los delitos cibernéticos mediante la difusión de información y orientación a la ciudadanía.
II. Detección oportuna de amenazas y ataques cibernéticos, a fin de reducir, neutralizar o mitigar las afectaciones de la población.
III. Fortalecimiento de las capacidades técnico-científicas para la investigación y persecución de los delitos cibernéticos.[283]

Para instrumentar la Estrategia, dicha instancia comenzó a capacitar personal en Estados Unidos, España, Canadá, Francia, Japón, Singapur y Reino Unido, para especializarse en áreas de ingenierías de cómputo, telecomunicaciones, sistemas y seguridad informática, así como en psicología y derecho informático.[284]

También durante el sexenio de Peña Nieto se creó y fortaleció el Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX), que es el organismo acreditado para atender amenazas de ciberseguridad en México, monitorear la

[281] OEA, *Cybersecurity: Are We Ready in Latin America and the Caribbean?,* 2016, consultadoenhttp://caribbean.cepal.org/content/cybersecurity-are-we-ready-latin-america-and-caribbean [septiembre 2018]
[282]Ibídem.
[283] CNS, *Fortalece CNS estrategias para la protección del ciberespacio…,* Óp. Cit.
[284]Ibídem.

seguridad de la red y los sistemas y coordinar la respuesta sobre incidentes a víctimas de ataques cibernéticos.[285]

A partir de la publicación del Reglamento de la Ley de la Policía Federal y de las atribuciones ahí otorgadas, el CERT-MX se estableció como "el organismo encargado de operar el equipo de respuesta a incidentes de seguridad informática en la infraestructura crítica de México, colaborando con los diferentes órdenes de gobierno y actores sociales."[286] Sus objetivos son proporcionar soporte en la respuesta y defensa en contra de incidentes de seguridad de la información en el dominio .mx e infraestructuras críticas del país; coadyuvar en los esfuerzos de protección mediante la colaboración e intercambio de información entre instituciones de gobierno estatal y federal, la industria y equipos de respuesta; y fortalecer las estrategias de seguridad cibernética de México.[287]

Además, el CERT-MX actúa como la instancia donde se intercambia la información con las policías cibernéticas nacionales e internacionales y cuenta con la capacidad de identificar y atender posibles ataques en agravio de la infraestructura gubernamental o contra la ciudadanía en general y contrarresta amenazas con potencial de tener efectos en otros países.[288]

Entre las acciones de colaboración público-privada, la Policía Federal estableció algunos convenios, entre los más importantes son los acuerdos con Microsoft México y con la Asociación de Bancos de México (ABM). Estos convenios buscaban compartir experiencias y casos de éxito en materia de detección, captación, análisis, clasificación y registro de la información, que resultaran de la vigilancia y monitoreo de conductas que pudieran ser constitutivas de delitos en

---

[285] SSP, *Centro Nacional de Respuesta a Incidentes Cibernéticos CERT-MX*, Secretaría de Seguridad Pública, Coordinación para la Prevención de Delitos Electrónicos,México, 23 de marzo de 2012, p. 7, consultado en http://seguridad2012.politicadigital.com.mx/pdf/03.pdf[julio 2018]

[286]Ibíd., p. 8.

[287]Ibíd., p. 9.

[288]CNS, *Policía federal suma sus capacidades tecnológicas a los esfuerzos internacionales liderados por la ONU para proteger los derechos y el patrimonio de los ciudadanos*, en cns.gob.mx, Comisión Nacional de Seguridad, Comunicado de prensa No. 169, México, 10 de agosto de 2014, consultado enhttp://www.cns.gob.mx/portalWebApp/appmanager/portal/desk;jsessionid=qxLTTzpNmsQGD0nBMtCvbgGJwHpnBGT1SnLGknpbYL4vzZ6JQpWG!432963533?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1348094[julio 2018]

medios electrónicos; así como disminuir la brecha digital que existe entre las instancias públicas y las empresas especializadas en ciberseguridad.[289]

Asimismo, se realizaron diversas acciones a nivel internacional. La Policía Federal participó en diversos paneles y reuniones con expertos en dicho ámbito. Entre las más representativas, asistió a la primera reunión del Grupo de Expertos Gubernamentales sobre Avances en la Información y las Telecomunicaciones en el contexto de la Seguridad Internacional, convocada por la ONU. En dicho encuentro se examinaron y promovieron esquemas de coordinación internacional ante ciberamenazas reales y potenciales, tal como lo estableció la resolución 68/243 de la Asamblea General de las Naciones Unidas; misma que reconoce la necesidad de generar y aplicar normas pertinentes para el ciberespacio, a fin de reducir los riesgos y propiciar su uso en un entorno seguro.[290]

En el ámbito regional, la Policía Federal participó en la *VII Cumbre de la Comunidad de Policías de América* (AMERIPOL), donde se acordó crear un Centro de Ciberseguridad de dicha agrupación, a fin de llevar a cabo evaluaciones de las posibles amenazas en este ámbito, mismas que incluyen el intercambio de análisis, perspectivas de tendencias y alertas tempranas entre las instituciones policiales.[291]

El elemento más importante en cuanto a colaboración internacional en materia de ciberseguridad es el CERT-MX que, al establecerse como punto de contacto internacional opera una serie de protocolos para contrarrestar amenazas que potencialmente pueden afectar a varios países. El CERT-MX pertenece al Foro de

---

[289] CNS, I*mpulsan Policía Federal y Microsoft México seguridad informática y prevención de delitos cibernéticos*, en cns.gob.mx, Comisión Nacional de Seguridad,Boletín de prensa No. 119, México, 5 de agosto de 2014, consultado enhttp://cns.gob.mx/portalWebApp/portal/movil.portal?_nfpb=true&_pageLabel=portal_movil_portal_contenido&content_id=1344173#wlp_portal_movil_portal_contenido [julio 2018]

[290] CNS, *Policía Federal suma sus capacidades tecnológicas a los esfuerzos internacionales liderados por la ONU para proteger los derechos y el patrimonio de los ciudadanos*, en cns.gob.mx, Comisión Nacional de Seguridad, Comunicado de Prensa no. 169, México, 10 de Agosto de 2014, consultado en http://www.cns.gob.mx/portalWebApp/appmanager/portal/desk;jsessionid=qxLTTzpNmsQGD0nBMtCvbgGJwHpnBGT1SnLGknpbYL4vzZ6JQpWG!432963533?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1348094 [julio 2018]

[291] CNS, *Policías de América estrechan lazos de cooperación contra el crimen durante la VII Cumbre AMERIPOL*, en cns.gob.mx, Comisión Nacional de Seguridad, Comunicado de Prensa No.168, México, 9 de agosto de 2014, consultado en http://www.cns.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=true&_pageLabel=portals_portal_page_m3p2_boletin&id=1348081 [julio 2018]

Equipos de Seguridad y Respuesta a Incidentes (Forum of Incident Respond and Security Teams-FIRST) que congrega a los CERT de 69 países y que se mantienen en contacto permanente para intercambiar información, responder a incidentes cibernéticos trasnacionales y emitir alertas sobre amenazas mundiales.[292]

Además, la División Científica de la Policía Federal trabaja de manera permanente con la OEA, con la que se mantiene un intercambio de información a través del Programa de Ciberseguridad de dicha organización, donde se enfatiza la cooperación en capacitación para combatir la ciberdelincuencia.[293]

De esta manera, se proporcionaba un diagnóstico de cómo se encontraba la ciberseguridad tanto a nivel de incidencias como de actividades relativas a la atención de los problemas ocurridos en el dominio cibernético y en la búsqueda de confianza en el ciberespacio, antes de la creación de la Estrategia Nacional de Ciberseguridad, en noviembre de 2017.

En síntesis se puede afirmar que aunque se habían realizado diversos esfuerzos para mantener la seguridad y la confianza en el ciberespacio, antes de la generación y publicación de la ENCS, las instituciones mexicanas actuaron, generalmente, de forma reactiva. No respondían a una estrategia previamente diseñada ni a planes definidos de fortalecimiento institucional o medidas preventivas; las acciones eran desarticuladas, las actividades se organizaban por diversas instancias de seguridad pero no se guiaban por un procedimiento conjunto con otras instituciones que también realizaban actividades en ciberseguridad; no seguían un objetivo fijo, a pesar de buscar mantenerse bajo la institucionalidad y responder con acciones concretas a los problemas en el tema de la ciberseguridad; tampoco se concretaba algún plan, líneas de acción u objetivos particulares, así como metas medibles.

---

[292] Andrés Jiménez, *La delincuencia organizada en el ciberespacio…, Óp. Cit.,p. 132.*

[293] CNS, *Académicos y Policía Federal debaten sobre el estudio e investigación policial en materia de ciberseguridad*, en cns.gob.mx, Comisión Nacional de Seguridad, Comunicado de Prensa No. 705, México, 28 de Octubre de 2015, consultado en http://www.cns.gob.mx/portalWebApp/appmanager/portal/desk;jsessionid=13GWWxdKGR1n095M0Rfj1x1GVhQ1V1qW0nzvYzPVG0cpXR8y9MTX!-1153552922?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1398180 [julio 2018]

Por lo anterior, fue necesario generar y publicar la Estrategia Nacional de Ciberseguridad, como parte de la política pública que pretende funcionar de marco general para guiar y articular las acciones aplicables ante cada incidencia y actividad relacionada a la ciberseguridad sucedida en México. Es por ello que consideramos relevante hacer una evaluación sobre si efectivamente la Estrategia consiguió sus fines.

A continuación, se realiza un examen de la ENCS, que ya fue revisada a nivel documental, pero en el siguiente apartado es observada y comparada al cariz de dos estándares: primero, bajo una referencia global de buenas prácticas en ciberseguridad; y segundo, ante los propios lineamientos de la ENCS, pero cotejándolos con las actividades realizadas desde la publicación de la misma.

4.2 Evaluación de la Estrategia Nacional de Ciberseguridad (2017-2018).

De acuerdo a los datos y actividades examinadas, es posible determinar que se observa un creciente número de incidencias en delitos cibernéticos en México, que existe una preocupación cada vez mayor entre el sector gubernamental, empresarial y de la sociedad civil, así como una mayor relevancia del ciberespacio para los mexicanos en general, que ya pasan la tercera parte del día interconectados.

Estas circunstancias justificaron la creación de la Estrategia Nacional de Ciberseguridad en el año 2017, con la intención de que el Estado mexicano enfrentara los problemas crecientes que representa el fenómeno de la ciberseguridad, de manera institucional y con la participación de los distintos actores sociales, para brindar confianza a los cibernautas mexicanos a nivel individual y colectivo. Al final se hace una evaluación puntual de la Estrategia, tanto de su concepción como de la efectividad de su aplicación.

El análisis anterior generó una calificación que representa, de forma cuantitativa, la evaluación general de la ENCS. Para llegar a este valor numérico, la Estrategia fue evaluada con base a dos pautas:

A. En primer lugar, a partir de la comparación de la ENCS con la Agenda de Ciberseguridad Global (GCA) de la UIT, al ser el marco de referencia que

expresa el estándar más aceptado a nivel global, para construir y evaluar estrategias de ciberseguridad.

B. En segundo lugar, se comparan los ocho ejes que menciona la propia ENCS, con las acciones que se han realizado sobre ciberseguridad desde que se publicó el documento en noviembre de 2017 hasta octubre de 2018, correspondientes a cada uno de dichos ejes.

La UIT, en el Índice Global de Ciberseguridad, ya le ha asignado una calificación a México (que se revisará más adelante). En dicho Índice se utiliza una escala de 0 a 1 para calificar, por lo que se usa la misma escala al evaluar el desempeño basado en los 8 ejes de la ENCS.

Después de ponderar la Estrategia ante ambos elementos, se obtuvieron dos calificaciones, la que la UIT le asignó a México con base en la Agenda de Ciberseguridad Global y la que se le asigno en la presente investigación, con base en el cotejo de las acciones ante los ejes de la propia ENCS. Finalmente, se promedian ambos resultados, para tener un solo valor cuantitativo que refleje la evaluación de la Estrategia Nacional de Ciberseguridad.

4.2.1 Análisis comparativo de la ENCS en el marco de la GCA.

En la medida que es inexistente algún tratado o acuerdo relativo a la ciberseguridad a nivel internacional que sea vinculante o de aplicación obligatoria para el Estado mexicano, no se cuenta tampoco con un referente oficial para medir la efectividad de la ENCS. No obstante, a nivel global, la organización multilateral con el liderazgo más reconocido en el tema de la ciberseguridad, es la Unión Internacional de Telecomunicaciones, misma que cuenta con un documento marco y una serie de indicadores sobre las estrategias y acciones relativas a la ciberseguridad a niveles nacionales e internacionales.

Para evaluar una estrategia de ciberseguridad al nivel de un país, existen varios marcos de referencia, algunos aplicados por el sector empresarial y otros por las organizaciones internacionales; el más sólido y aceptado, tanto en su concepción como en su alcance, es la Agenda de Ciberseguridad Global de la UIT.

Entre los acuerdos de la Cumbre Mundial de la Sociedad de la Información (CMSI) organizada por la UIT,en su segunda fase(Túnez 2005), se reconoció que los riesgos por una ciberseguridad inadecuada y la proliferación del ciberdelito eran reales y significativos, por lo que se asignó a la UIT la responsabilidad de implementar la Línea de Acción C5 de la CMSI, dedicada a la creación de confianza y seguridad en el ciberespacio. Como respuesta, la UIT generó la Agenda de Ciberseguridad Global (Global Cybersecurity Agenda, GCA por sus siglas en inglés) en 2007.[294]

La GCA es "un marco mundial para el diálogo y la cooperación internacional a fin de coordinar la respuesta mundial a los retos cada vez mayores que plantea la ciberseguridad y de mejorar la confianza y seguridad en la sociedad de la información y el conocimiento."[295]La GCA tiene por objeto establecer un vínculo entre iniciativas existentes y crear un marco global para facilitar la obtención de consensos, por lo que la convierte en la iniciativa más importante sobre ciberseguridad a nivel global.

Resulta ser innovadora ya la vez flexible, porque cada actor o grupo de interesados puede comprometerse según sus necesidades y garantizar la cooperación en los temas que le parezcan prioritarios.[296]Las recomendaciones de la GCA están basadas en 5 pilares (explicados en el capítulo 2):

1. Medidas legales.
2. Medidas técnicas y de procedimiento.
3. Estructuras organizacionales.
4. Creación de capacidades.
5. Cooperación internacional.[297]

La UIT también generó el Índice de Ciberseguridad Global (*Global Cibersecurity Index,*GCI por sus siglas en inglés), que es el indicador más

[294]UIT, *Expertos de alto nivel determinan una hoja de ruta para la ciberseguridad*, prensa de la UIT, consultado enhttp://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=06&ipage=05&ext=html [agosto 2018]
[295] UIT, *El ciberdelito: guía para los países en desarrollo*, en División de Aplicaciones TIC y Ciberseguridad, Departamento de Políticas y Estrategias Sector de Desarrollo de las Telecomunicaciones de la UIT, abril de 2009, consultado en http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf[agosto 2018]
[296]UIT*, Trabajar juntos para proteger la Sociedad mundial de la información…, Óp. Cit*.
[297] UIT, *Expertos de alto nivel determinan una hoja de ruta…, Óp. Cit.*

reconocido sobre la ciberseguridad a nivel mundial. El GCI califica la respuesta general de los 194 países miembros de la UIT ante el fenómeno de la ciberseguridad y gira en torno a la GCA y sus cinco pilares, para cada uno de estos se desarrollan preguntas que evalúan el avance de cada miembro y se ponderan las acciones registradas para alcanzar un puntaje general del GCI.[298]

El GCI tiene el objetivo clave de crear capacidades a nivel nacional, regional e internacional, mediante la evaluación del nivel de compromiso de los países sobre seguridad cibernética y, con los datos recopilados, se genera una lista de buenas prácticas que pueden utilizar los países que lo requieran. El GCI está incluido en la Resolución 130 (Busan, 2014) sobre el fortalecimiento del papel de la UIT en la creación de confianza y seguridad en el uso de las TIC.[299]

En 2013-2014 se realizó una primera medición del GCI y con la retroalimentación recibida, se planificó y llevó a cabo una segunda valoración que se publicó en el 2017. Esta nueva versión se formuló en torno a una amplia participación de los Estados miembros, expertos y partes interesadas de la industria como socios contribuyentes como el Banco Mundial, el Red Team Cyber, FIRST, INTERPOL, UNICRI y la UNODC entre otros, quienes brindaron apoyo con el suministro de datos secundarios, activación de respuestas, análisis estadístico y apreciación cualitativa, entre otros.La UIT proporciona soporte en el componente sobre creación de capacidades desde una perspectiva de ciberseguridad basada en datos de GCI.[300]

En el GCI publicado en el año 2017, México se encuentra ubicado en el lugar número 28, con una calificación de 0.66, en una escala de 0 a 1, lo cual indica que ya se están realizando labores por implementar una estrategia de ciberseguridad; sin embargo, aún falta mucho, por ejemplo, 10 de los 25 indicadores para el país se calificaron en etapa de inicio o de maduración.[301]De esta manera, se explica la razón

[298]ITU, *Global CybersecurityIndex 2017,* UIT-ABI research, 2017, p. 7, consultado en https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf [septiembre 2018]
[299]Ibíd., p. 15
[300]Ibídem.
[301]Ibíd., p. 28

de tomar a la GCA –y al derivado GCI- como estándar para evaluar a la ENCS, ya se constituye como un parámetro de reconocimiento global.

A continuación, se aplica el comparativo, basado en los 5 pilares de la GCA.Se muestra de qué manera los principios, objetivos y ejes transversales de la ENCS se relacionan y hasta qué punto son aplicables a los pilares de la GCA.

El primer pilar, **Medidas legales**, concierne a la creación de iniciativas para elaborar una legislación sobre ciberdelincuencia. Se ha instado a los países a considerar en sus legislaciones penales que amenazas como el correo indeseado (spam), el robo de identidad y los ataques DDoS sean tipificados como delitos. Además, las reglamentaciones deben ser suficientemente flexibles para tener en cuenta los avances tecnológicos.La GCA señala la importancia de que los gobiernos y las empresas del sector privado colaboren para asegurarse de que la policía y el poder judicial dispongan de las herramientas apropiadas para proteger al público contra las actividades delictivas, pero siempre protegiendo los derechos humanos y la privacidad.[302]

En el GCI se contemplan tres indicadores para medir el avance jurídico en términos de ciberseguridad. El primero es la existencia de un cuerpo de legislación penal específica en delitos cibernéticos; el segundo es la presencia de regulaciones concretas relacionadas con la ciberseguridad e instituciones que vigilen su cumplimiento (como una procuraduría o agencia de vigilancia); el tercero es la formación, y se refiere a capacitación para la aplicación de la ley y el poder judicial; por ejemplo, tener investigadores forenses digitales especializados.[303]

En la ENCS, se aprecia una visión jurídica importante, que incluye los principios de la GCA. Ya que se señala en varios puntos la importancia de generar medidas legales específicas para la ciberseguridad, siempre respetando los derechos de los usuarios.

En la parte central de la ENC, el principio rector A establece que en las diferentes acciones en materia de ciberseguridad se debe contemplar la promoción, respeto y cumplimiento de los derechos humanos; entre otros, la libertad de

[302] UIT, *Expertos de alto nivel determinan una hoja de ruta para la ciberseguridad*, prensa de la UIT, consultado en http://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=06&ipage=05&ext=html [agosto 2018]
[303] ITU, *Global Cybersecurity Index 2017…, Óp. Cit*., p. 52.

expresión, el acceso a la información, el respeto a la vida privada, la protección de datos personales, la salud, la educación y el trabajo.

Entre los objetivos estratégicos, el I. indica que se buscan generar las condiciones para que la población realice sus actividades de manera responsable, libre y confiable en el ciberespacio, con la finalidad de mejorar su calidad de vida mediante el desarrollo digital en un marco de respeto a los derechos humanos como la libertad de expresión, vida privada y protección de datos personales.

El eje transversal número 7, Marco jurídico y autorregulación, busca impulsar y establecer acciones y mecanismos necesarios para la adecuación del marco jurídico nacional vinculado a la ciberseguridad y de autorregulación. Se plantean como objetivos particulares: desarrollar capacidades de operadores jurídicos y tomadores de decisiones en instituciones públicas y privadas, así como de la sociedad civil; que las instancias de procuración de justicia incrementen su eficacia en la investigación, prevención, persecución y sanción a ciberdelincuentes; que se establezcan mecanismos y procedimientos de autorregulación que favorezcan la construcción de confianza entre individuos, sector público y organizaciones privadas con apego a derecho; así como la homologación y armonización de códigos penales y leyes complementarias en relación a ciberdelitos.

El comparativo de la GCA con el documento de la ENCS resulta en un balance positivo, porque prácticamente los tres parámetros para establecerse en una estrategia efectiva, según los expertos de la UIT, son tomados en cuenta en la Estrategia mexicana. Hay una clara intención de brindar certeza jurídica a los cibernautas mexicanos a nivel individual y colectivo; una base de respeto a los derechos humanos y respeto a la privacidad; también existe el mandato dentro de la ENCS de generar las regulaciones especificas relacionadas con la prevención y el castigo a los delitos cibernéticos; se reconoce la necesidad de crear capacidades en los organismos regulatorios y fomentar una cultura jurídica de la ciberseguridad en las organizaciones públicas y privadas.

Sin embargo, no hay una planeación o plazos para generar una ley general o de alcance federal en el tema cibernético, ya que no existe una propuesta de ordenamiento o estructura jurídica sobre la que se deba basar la autorregulación o

la capacitación para las instancias de procuración de justicia. Por lo tanto, con relación al pilar número 1 de la GCA, se puede conferir una evaluación positiva pero insuficiente del documento de la ENCS. En el GCI, México fue calificado con 0.91 (en escala de 0 a 1) en este primer indicador.

El pilar 2, **Medidas técnicas y de procedimiento**, tiene que ver con la correcta aplicación de los principios de la GCA. Se centra en las acciones clave para promover la adopción de métodos mejorados que aumenten la gestión de la seguridad y el riesgo en el ciberespacio, incluidos los esquemas, protocolos y normas de acreditación.

Entre los puntos a resaltar están: el fomento de la ciberseguridad, que implica establecer un compromiso para elaborar métodos de promoción de prácticas idóneas para la gestión de la ciberseguridad y la infraestructura esencial hacia las instancias gubernamentales, las empresas y la sociedad civil; creación de medidas que permitan mejorar la gestión de las redes, el control de los protocolos de Internet, medidas de seguridad y control de identidad digital, así como la creación de sistemas de protección para tecnologías emergentes; y cooperación y consonancia con criterios comunes para la evaluación de la ciberseguridad.[304]

En la ENCS, el principio B está basado en la gestión de riesgos, lo que significa manejar escenarios de incertidumbre a través de enfoques preventivos y correctivos, para lo cual es necesario establecer medidas técnicas y de procedimiento.

En el eje transversal número 5, se proponen acciones enfocadas al desarrollo, adopción y fortalecimiento de los estándares, criterios técnicos y de normalización en materia de ciberseguridad, que permitan la homologación y aplicación de las mejores prácticas y procesos en un entorno de ciberseguridad.El desarrollo de estándares y criterios técnicos comprende el establecimiento de criterios, normas y metodologías para la generación, uso y adopción de hardware y software con la finalidad de fortalecer el ecosistema de ciberseguridad; la definición de los marcos de referencia para fortalecer la ciberseguridad de organizaciones privadas y públicas, academia y sociedad en general; la participación de la comunidad

[304] UIT, *Expertos de alto nivel determinan una hoja de ruta para la ciberseguridad…, Óp. Cit.*

académica, técnica y científica en el desarrollo y fortalecimiento de estándares, metodologías y normalización en materia de ciberseguridad; y el uso de estándares y mejores prácticas internacionales en materia de ciberseguridad.

Asimismo, en el octavo eje, Medición y seguimiento, se busca valorar los resultados obtenidos de la implementación de la ENCS, con la finalidad de identificar las áreas de oportunidad para su mejora continua. A través de la colaboración conjunta de los actores para la elaboración de metodologías de diagnóstico; la generación de estadísticas centralizadas relacionadas con la implementación y el impacto de la Estrategia en los sectores económicos, políticos y sociales.

El documento de la ENCS supera al segundo pilar de la GCA, en lo relativo a objetivos en medidas técnicas y de procedimiento, ya que fomenta la participación de distintos actores para fortalecer las medidas, señala criterios y estándares técnicos y procedimentales en la defensa y prevención de riesgos en el ciberespacio; incluso se desprende la forma en que intentan diagnosticar y evaluar la efectividad de la propia ENCS, a través de la colaboración para la elaboración de metodologías de medición y construcción de bases de datos.

En este sentido, se puede evaluar de forma satisfactoria al documento de la ENCS con respecto a las recomendaciones de la GCA. No obstante, no se ha especifica qué instancia y a través de qué herramientas técnicas y/o metodológicas se llevarán a cabo las medidas mencionadas, tampoco se indica la temporalidad para la realización de las evaluaciones para saber qué tan periódicamente se revisará la efectividad de la ENCS. Además, falta examinar si efectivamente se han realizado acciones institucionales para el diagnóstico y evaluación de la ciberseguridad en el último año, a partir de la publicación de la Estrategia. En el GCI, México fue calificado con 0.89 en el este pilar.

El tercer fundamento de la Agenda son las **Estructuras organizacionales**. Se destaca la importancia de la institucionalidad y se promueve la creación de estructuras nacionales, regionales e internacionales apropiadas para proteger la ciberseguridad y luchar contra la ciberdelincuencia. Su función consiste en integrar las actividades de varios organismos, ahorrar recursos e impedir la duplicación de esfuerzos. La GCA señala que cada país debe determinar su propia estrategia y sus

estructuras para atender a sus necesidades de ciberseguridad nacional, y promover la asistencia a través de la cooperación regional o multilateral.[305]

Por su parte, la ENCS, señala en su objetivo III que se debe proteger la información y los sistemas informáticos de las instituciones públicas del país para el funcionamiento óptimo de éstas y la continuidad en la prestación de servicios y trámites a la población. Entre sus ejes trasversales 2 y 3, se busca desarrollar capacidades organizacionales por medio de la colaboración a nivel institucional. Se impulsa el establecimiento de una organización que deberá prevalecer en lo público y privado, a fin de posicionar a la ciberseguridad a nivel estratégico en las organizaciones públicas y privadas; así como establecer los mecanismos de participación ciudadana en materia de ciberseguridad.

En el documento de la ENCS, se plantea el fortalecimiento de las capacidades organizacionales y se esboza una estructura que coordine los trabajos entre todos los actores involucrados en la materia, así la colaboración con otras instancias análogas a nivel internacional, aunque en general es ambigua e imprecisa. Por un lado, se habla de una serie de acciones, por otro se menciona la identificación de mecanismos y protocolos de comunicación; es decir, no se indica específicamente la creación de una institución, organismo, agencia o instancia rectora en ciberseguridad a nivel nacional, que tenga una estructura, presupuesto, personal, mecanismos y herramientas propias, para ejercer una coordinación de las tareas en ciberseguridad con el alcance necesario para conjugar y sistematizar las acciones.

Con relación a este pilar de la GCA, la Estrategia es insuficiente, al no señalar una instancia específica a nivel organizacional que coordine los esfuerzos institucionales a gran escala, lo cual podría no sólo hacer más eficientes los recursos sino cargar la responsabilidad a un organismo determinado, con una persona o equipo de personas que asuman el compromiso de dirigir la Estrategia a nivel organizacional. En el GCI, México obtuvo una calificación de 0.48 en el tercer indicador, es decir, por debajo de una media aprobatoria.

El cuarto pilar de la GCA se centra en la elaboración de estrategias para los mecanismos de **creación de capacidad** a fin de aumentar la concientización,

[305] Ibídem.

transferir el *know how* e impulsar la ciberseguridad en la agenda de políticas nacionales.[306] Señala que se debe promover la adopción y apoyo en temas técnicos específicos y crearse un punto focal para gestionar diversas actividades de manera coordinada, a fin de apoyar la colaboración nacional, regional e internacional.

También establece que se debe capacitar a los usuarios finales para que adopten un comportamiento seguro, con el fin de convertirse en ciudadanos cibernéticos responsables y alentar a los proveedores de productos y servicios de TIC a aumentar la seguridad de sus productos y servicios. La GCA hace hincapié en educar a varios niveles a todos los actores y desarrollar la capacidad humana en todos los aspectos que ayuden a construir una cultura global de la ciberseguridad. Para lograrlo, se propone la promoción de campañas publicitarias de sensibilización y el aprovechamiento al máximo de las escuelas, ONG, bancos, proveedores de servicios de Internet (ISP), bibliotecas, centros comunitarios o programas de educación para adultosy así transmitir el mensaje de seguridad cibernética.[307]

A su vez, la ENCS, en tres de sus objetivos estratégicos, señala el propósito de crear y fortalecer capacidades técnicas y procesales. Con el objetivo II, Economía e innovación, se buscan fortalecer los mecanismos en materia de ciberseguridad para proteger la economía de los diferentes sectores productivos del país y propiciar el desarrollo e innovación tecnológica, así como el impulso de la industria nacional en materia de ciberseguridad; en el objetivo IV se señala el incremento de las capacidades en seguridad pública para la prevención e investigación de conductas delictivas en el ciberespacio; y en el objetivo V se promueve el desarrollo de capacidades para prevenir riesgos y amenazas en el ciberespacio que puedan alterar la independencia, integridad y soberanía nacional.

En el eje transversal número 1, Cultura de ciberseguridad, se establece la necesidad de promover un conjunto de valores, principios y acciones en materia de concientización, educación y formación, que incidan en la forma de interactuar en el ciberespacio de forma armónica, confiable y como factor de desarrollo sostenible. Esto se logrará, según la ENCS, a través de la promoción, cumplimiento y

[306]UIT, *Trabajar juntos para proteger la Sociedad mundial de la información*…, Óp. Cit.
[307] UIT, *ITU Global Cybersecurity Agenda* (GCA), High-Level Experts Group (HLEG), Suiza, 2007 , p. 14

protección de los derechos de individuos y organizaciones públicas y privadas; el fortalecimiento de la prevención de riesgos y conductas delictivas que afectan a individuos, organizaciones privadas y públicas; y con la prevención de riesgos que pudieran afectar a las infraestructuras críticas de información y operación.

El segundo eje, Desarrollo de capacidades, impulsa las acciones encaminadas a la generación y fortalecimiento de las capacidades organizacionales, de capital humano y recursos tecnológicos en materia de ciberseguridad. Para ello, se proponen programas para formar especialistas y profesionales de la ciberseguridad; generar líderes de la ciberseguridad como conductores de estrategias y políticas; la capacitación de profesionales de la investigación y la persecución de los delitos que se cometen a través de las TIC; asimismo, se busca generar la infraestructura tecnológica necesaria para el fortalecimiento gradual de la ciberseguridad en México, e incrementar las capacidades técnicas para la identificación y gestión de incidentes cibernéticos a nivel nacional.

Al ponderar lo que la GCA establece como parámetros y lo que la ENCS indica como objetivos, ejes y acciones, en este rubro el documento de la Estrategia tiene un balance muy positivo, puesto que no sólo menciona la necesidad de crear capacidades y fomentar una cultura de ciberseguridad, sino que despliega una serie de acciones a realizarse para lograrlo. En este caso, de forma diferente a la evaluación en los pilares anteriores, el documento de la Estrategia sí propone formas más específicas de crear capacidades a nivel técnico, organizacional, institucional, económico, incluso social. En este rubro, México recibió una calificación de 0.68 en el GCI.

En el quinto pilar, **Cooperación internacional**, la GCA recomienda desarrollar una estrategia para la cooperación, el diálogo y la coordinación en el tratamiento de la ciberseguridad. Según la UIT, esto se logra a partir de las siguientes acciones:

-Armonización. La GCA exhorta a que haya una armonización que traspase las fronteras en cada uno de los pilares, sobre todo en las medidas legales. A través de la creación de redes de trabajo para coordinar las actividades, iniciativas y proyectos a través de acuerdos y memorándums de entendimiento. Las acciones deben armonizarse con las que hacen otros

países a nivel regional, siempre respetando la independencia y la soberanía nacional.

-Coordinación de los trabajos. Los expertos de la UIT consideran que coordinar las labores de varias organizaciones evita la duplicación de esfuerzos y se mejora la colaboración con los organismos internacionales, regionales y nacionales.

-Supervisión. La GCA sirve como compilador de información y se dedica a divulgarla. Al recibir la información sobre las iniciativas de ciberseguridad en el mundo tiene los elementos necesarios para supervisar y evaluar los avances.

-Foros mundiales. Es necesario promover y participar en foros mundiales para facilitar el desarrollode capacidades de ciberseguridad a nivel global.[308]

En la ENCS, la cooperación internacional no es parte de los principios, tampoco de los objetivos estratégicos ni de los ejes transversales. Es decir, a diferencia de otros pilares, el documento de la ENCS no pondera el ámbito internacional como un área de trabajo primordial o fundamental, aun cuando tiene todo un apartado del contexto internacional, donde se reconoce que la ciberseguridad es un fenómeno global que no puede ser atendido integralmente si no existen mecanismos de colaboración internacional.

No obstante, el alcance internacional se menciona en el eje 3, Coordinación y colaboración, donde se indica que se deben establecer los enlaces entre las distintas instituciones en materia de ciberseguridad con la finalidad de consolidar el ecosistema de ciberseguridad y menciona, entre otras, la implementación de acciones que fortalezcan la cooperación y colaboración internacional. En el eje 5, Estándares y criterios técnicos, se recalca que debe fomentarse el uso de estándares y mejores prácticas internacionales en materia de ciberseguridad.

La ENCS no le ha concedido jerarquía al ámbito internacional, a pesar de tener toda una serie de justificaciones y diagnósticos en el propio documento de que la ciberseguridad es un fenómeno global. La relevancia del entorno internacional y la necesidad de colaborar con otros actores de la sociedad internacional para

[308]Ibídem, p. 17

fortalecerse en materia de ciberseguridad justificarían que uno de los principios, de los objetivos estratégicos o alguno de los ejes transversales, se dedicara al fortalecimiento en la cooperación con entes fuera de las fronteras nacionales.

A este pilar, la GCA le otorga un lugar preponderante y despliega una serie de recomendaciones y líneas de acción más específicas para lograr una cooperación internacional exitosa, siguiendo los principios de independencia y soberanía nacionales. Pero en la ENCS no se le confiere la misma importancia, al no definir ejes de acción más específicos para aprender de las mejores prácticas y del intercambio de información y capacidades con otros actores de la sociedad internacional; incluso resulta incongruente, al reconocer a la ciberseguridad como un problema global que requiere de cooperación internacional, para después no desplegar acciones suficientes en dicho ámbito. Esta evaluación concuerda con la recibida por México en el GCI para el quinto pilar, 0.34.

La primera parte de la evaluación de la ENCS, contrasta al documento con el marco general más aceptado sobre la ciberseguridad a nivel global. Al respecto se puede notar que la GCA esgrime principios y recomendaciones generales y flexibles, que pueden ser adaptables a las necesidades y la realidad de México en cuanto a recursos y capacidades jurídicas, políticas, económicas y técnicas. Sin embargo, la ENCS no está basada en la GCA, por lo que era necesario hacer una extracción de conceptos para examinarlos con base en un marco de referencia internacional.

De manera general, se pueden observar fortalezas y debilidades en la ENCS. En el documento rector presentado en noviembre de 2017, es posible resaltar la finalidad de llevar el tema de la ciberseguridad a todos los actores y sectores, así como la firme intención de fortalecer al Estado mexicano en diversos rubros para lograr una sociedad que madure en su cultura de ciberseguridad, con instituciones sólidas que puedan prevenir y responder a los riesgos, así como el fortalecimiento de la ciber resiliencia. Sin embargo, no se presentan líneas de acción más concretas, no se propone específicamente la creación de una estructura organizacional, no se nombra responsable a ninguna instancia o persona de

ejecutarla y evaluarla, no hay una propuesta seria de una ley de ciberseguridad de alcance general y tampoco se establecen indicadores u objetivos medibles.

La ENCS se queda en un documento marco, amplio y en ciertos puntos ambiguo, lo que permite comprender a cabalidad la razón de la calificación de México en el GCI de 0.66, misma que coincide con las observaciones realizadas en el presente apartado, una valoración estimada apenas por encima de la media de lo que serían las mejores prácticas en ciberseguridad a nivel internacional.

4.2.2 Implementación de la Estrategia Nacional de Ciberseguridad.

La calificación asignada a México en el GCI, 0.66, se promedió con la obtenida en la evaluación que se realizó sobre la ejecución de los lineamientos establecidos en el documento de la ENCS.

A continuación, se procede a aplicar un segundo elemento de análisis para evaluar, la implementación de las acciones indicadas en la Estrategia. Para ello se cotejan los 8 ejes transversales mencionados en el propio documento de la ENCS con las actividades, gestiones, operaciones y labores correspondientes a cada uno de dichos ejes. De manera de establecer en los hechos, qué tan efectiva ha sido la aplicación de la Estrategia, desde que se publicó en noviembre de 2017 hasta el cierre de la investigación, octubre de 2018.

Al final del análisis de cada eje transversal se le asigna una calificación, que permite establecer un valor cuantitativo a la evaluación, basado en las diferencias identificadas entre las propuestas de la ENCS y la ejecución de las actividades relativas a dicho eje. La calificación depende de qué tan empatadas sean las actividades con respecto al documento, mientras más alejadas estén entre sí el balance será negativo, mientras más cercanas la evaluación será positiva.

El número para calificar se realiza, al igual que en la GCA, en una escala de 0 a 1, hasta el decimal y el centesimal, por ejemplo 0.66 (decimal y centesimal). Posteriormente, se aplica la fórmula de promedio, suma de la calificación de cada eje transversal y dividido entre 8, para obtener una calificación sobre la implementación de la ENCS. Finalmente, se suma el resultado de la GCA (0.66) con

la calificación de la implementación, se dividide entre 2; el número resultante representa cuantitativamente la evaluación de la presente tesis para la ENCS.

Ejes transversales

1. Cultura de ciberseguridad:

El 28 de febrero del 2018, la Comisión Nacional de Seguridad inauguró la campaña de concientización "Ciberseguridad México 2018" en un evento realizado en la Universidad de Colima. El Comisionado Nacional de Seguridad, Renato Sales Heredia y el Gobernador del Estado de Colima, José Ignacio Peralta Sánchez, destacaron la importancia de la colaboración entre la sociedad civil y las instituciones para que en el ciberespacio también pudiera construirse un México en paz. En el marco de este evento se lanzó la campaña "Cibernauta con Estrella" en redes sociales y se realizó la entrega de 400 becas a niños de entre 6 y 12 años.[309]

En el mismo evento, la Policía Federal fue ambigua, ya que en un mismo evento lanzaron dos campañas con nombres distintos, sin explicar a cabalidad ninguna de las dos. De la denominada campaña de concientización "Ciberseguridad México 2018", no se han desarrollado más actividades de gran alcance; y de la campaña "Cibernauta con Estrella" se han publicado al menos dos videos por mes, en las páginas oficiales de la Policía Federal, de las redes sociales *Facebook*, *Twitter* y *YouTube*, donde se alerta sobre conductas como el acoso cibernético, la protección de los datos personales, supervisión a niños en el uso de Internet, la importancia de no entrar a paginas sospechosas de los servicios bancarios y evitar el fraude electrónico o la extorsión, entre otros temas cotidianos para los cibernautas mexicanos.

En el sitio oficial de la Policía Federal sobre la campaña "Cibernauta con Estrella" se plantea que en las relaciones digitales existen "normas de urbanidad para cibernautas", que se refieren a los aspectos que deben cuidarse para tener un comportamiento educado en los diferentes espacios virtuales, donde se llevan a

[309] CNS, *La Comisión Nacional de Seguridad inaugura campaña de concientización en "Ciberseguridad México 2018"*, prensa de la CNS, boletín 103/18, México, publicada 28 de febrero de 2018, consultada en https://www.gob.mx/cns/prensa/la-comision-nacional-de-seguridad-inaugura-campana-de-concientizacion-ciberseguridad-mexico-2018-164033?idiom=es [julio 2018]

cabo las comunicaciones electrónicas, ya sea a través de Internet o en dispositivos móviles. También se presenta una sección interactiva, donde el usuario puede hacer una prueba de 7 preguntas para saber si es un cibernauta con estrella o no. La PF promueve las denominadas normas de "netiqueta"[310] y enumera las siguientes:

- Evitar hacer a otras personas lo que no te gustaría que te hicieran.
- Comportarse con la misma cortesía en internet que en la vida real.
- Respetar el tiempo de las demás personas.
- Compartir conocimiento útil y relevante.
- Respetar la privacidad e intimidad de las demás personas.
- Evitar aprovecharse de quienes tienen menos conocimientos.[311]

En este rubro, la aplicación de la ENCS es insuficiente, ya que la campaña de concientización en ciberseguridad, a pesar de intentar un acercamiento con el usuario promedio de los servicios de Internet, sobre todo los que se relacionan a través de redes sociales, no ha incluido en su difusión a las empresas y las organizaciones de la sociedad civil.

En la Estrategia se menciona que se deben promover valores y principios para"interactuar en el ciberespacio de forma armónica, confiable y como factor de desarrollo sostenible". A su vez, de los 14 videos que se habian publicado hasta el mes de octubre de 2018 relacionados con esta promoción, cada uno, sumando el alcance de las tres redes sociales donde lanzaron, tuvieron entre 20 mil y 25 mil visualizaciones. En total, los videos de sensibilización han sido vistos alrededor de 315 mil veces. Esta cifra, comparada con los 70 millones de internautas mexicanos, nos indica que menos del 0.5% ha visto el material multimedia de la Policía Federal. De esta manera, se puede determinar que la campaña desplegada para cumplir el primer eje transversal de la Estrategia ha tenido un alcance muy bajo para poder permear en la sociedad mexicana en general.

Asimismo, es posible señalar que no hay información sobre campañas para promover una cultura de ciberseguridad realizadas de manera conjunta entre la

[310] El término ha empezado a utilizarse en países angloparlantes, deriva de la palabra en inglés "net", que significa red y "étiquette", expresión francesa que refiere "normas para comportarse adecuadamente".
[311] Policía Federal, *¡Cibernauta con Estrella!,* en sitio oficial de la PF, México, publicada el 16 de mayo de 2018, consultada en https://www.gob.mx/policiafederal/articulos/cibernauta-con-estrella [julio 2018]

Unidad de Ciberseguridad de la Policía Federal y el sector empresarial, académico o con organizaciones de la sociedad civil, por lo que no se cumplen los puntos que la ENCS plantea desarrollar en su eje transversal número 1. La calificación asignada para el primer rubro de implementación es de 0.20.

2. Desarrollo de capacidades

En noviembre de 2017, la Comisión Nacional de Seguridad, la Policía Federal y la empresa Telmex, firmaron un convenio de colaboración para fortalecer la cooperación entre dichas instituciones en torno a la ciberseguridad. El CEO de la compañía telefónica, Héctor Slim Seade, explicó que se formalizó esta relación para permitir el "intercambio de capacitación, buscar mejores prácticas en materia de ciberseguridad y ciberinteligencia, participación en foros y conferencias especializadas, así como del intercambio de muestras maliciosas para su estudio".[312]

En el mismo evento, la CNS presentó la aplicación móvil "Checauto", que permite a los ciudadanos conocer la situación legal de cualquier vehículo tomando una foto o ingresando las placas, que fue desarrollada en un esquema de colaboración con las áreas técnicas de Telmex. Por su parte la Policía Federal lanzó la aplicación móvil "PF Ciber", con la que los usuarios pueden reportar cualquier incidente cibernético relacionado con el uso indebido e ilegal de la tecnología, así como recomendaciones y medidas de protección de riesgos en la red.[313]

En octubre de 2018, se fortaleció el vínculo con la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), para intercambiar información, generar acciones de capacitación, concientización y prevención de delitos cibernéticos. Se prestó especial atención a la alimentación del portal de fraudes cibernéticos lanzado por la Condusef, al destacarse al fraude como uno de los focos rojos en cuestiones de ciberseguridad.[314]

---

[312] CNC, *PF y TELMEX-SCITUM fortalecen la cooperación entre instituciones públicas y privadas en torno a la seguridad informática*, prensa CNS, México,boletín 707/17, 17 de noviembre de 2017, consultado en https://www.gob.mx/cns/prensa/pf-y-telmex-scitum-fortalecen-la-cooperacion-entre-instituciones-publicas-y-privadas-en-torno-a-la-seguridad-informatica-164392?idiom=es[julio 2018]

[313]Ibídem.

[314] El presidente de Condusef, Mario Di Contanzo, informó que en el primer semestre del 2018 se registraron más de 3.5 millones de reclamaciones por posible fraude, donde los usuarios desconocían movimientos por más de 9 mil millones de pesos, y 2 millones de estas fueron definidas como fraudes cibernéticos.

Entre otras actividades para desarrollar las capacidades, como lo establece la ENCS, la PF informó que se han realizado ejercicios de crisis cibernética bajo la dinámica "*Capture the flag*"; se realizaron 24 conferencias y seis paneles con más de mil personas en temas como: pornografía infantil y trata de personas, infraestructuras críticas, ciberseguridad en PyMes, legislación actual y avances nacionales. Así como talleres y cursos relacionados con la protección de sitios de Internet, capacitación a estudiantes de nivel primaria y secundaria, sobre los principales riesgos y medidas básicas de ciberseguridad para prevenir abusos y delitos en Internet. Cabe destacar la celebración de dos sesiones del Comité de Ciberseguridad con los avances para la implementación del Modelo Homologado de Policía Cibernética.[315]

Todas estas acciones, como lo menciona la ENCS, están encaminadas a la generación y fortalecimiento de las capacidades organizacionales, de capital humano y recursos tecnológicos en materia de ciberseguridad. Para ser un periodo de un año, ya se tienen dos convenios de colaboración técnica, se han lanzado dos aplicaciones móviles y se han realizado numerosos cursos de capacitación, así como foros de divulgación y cooperación.

La PF se erige como instancia articuladora de estos esfuerzos, pero queda pendiente la generación de especialistas en ciberseguridad a nivel de investigación y de liderazgo organizacional, así como la creación de la infraestructura nacional en ciberseguridad que menciona la ENCS. No obstante, la evaluación en este rubro es positiva. Se han realizado múltiples actividades para desarrollar las capacidades, aunque faltaron más acciones de capacitación a nivel internacional; en el primer año, es claro el compromiso de ejecutar las premisas de la Estrategia, por lo que la calificación asignada a este eje transversal es de 0.75.

3. Coordinación y colaboración

En el 2017, la Policía Federal sumó un convenio con Cisco Systems, que contempla realizar acciones conjuntas de proximidad ciudadana y el desarrollo de investigación

[315] Policía Federal, *PF clausura la 4ta. Semana Nacional de Ciberseguridad y suma esfuerzos con la Condusef para generar acciones de prevención*, prensa de la PF, boletín 548, 28 de octubre de 2018, consultado en https://www.gob.mx/policiafederal/prensa/pf-clausura-la-4ta-semana-nacional-de-ciberseguridad-y-suma-esfuerzos-con-la-condusef-para-generar-acciones-de-prevencion?idiom=es [octubre 2018]

tecnológica para la prevención de delitos en transacciones en línea, la seguridad de las empresas y la protección de los menores de edad.[316] En el mismo año, la CNS realizó el Primer Coloquio de Ciberseguridad para Medios de Comunicación, donde se destacó el objetivo de unir a la sociedad con la autoridad, a través de ejercicios de vinculación y proximidad social. Se alentó a los representantes de los medios a fomentar la denuncia ciudadana.[317]

La CNS se reunió con el Agregado Jurídico del Buró Federal de Investigación (FBI), Carlos Cases, con la finalidad de crear un grupo de trabajo entre diversas agencias de Estados Unidos de América con instituciones de seguridad de México, poniendo énfasis en temas como la trata de personas y la ciberseguridad.[318] La PF también realizó el Coloquio de Ciberseguridad para telefónicas y proveedoras de servicios de Internet, donde se buscó generar lazos de coordinación para unificar y expandir medidas preventivas y concientizar a la ciudadanía, aunque no se firmó ningún acuerdo entre las instancias participantes.[319]La Policía Federal, a través del Sistema de Desarrollo Policial (SIDEPOL), participó en un curso sobre Delitos Informáticos y Ciberseguridad internacionales, donde los elementos policiales desarrollaron habilidades específicas para planear, desarrollar y ejecutar operaciones de alto impacto que garanticen resultados exitosos.[320]

---

[316] Policía Federal, *CNS-Policía Federal suma capacidades con Cisco Systems para prevenir y atender delitos cibernéticos en el país,* comunicado de la PF, México, 20 de marzo de 2017, consultado en https://www.gob.mx/policiafederal/prensa/cns-policia-federal-suma-capacidades-con-cisco-systems-para-prevenir-y-atender-delitos-ciberneticos-en-el-pais [agosto 2018]

[317] Policía Federal,*CNS realiza Primer Coloquio de Ciberseguridad para Medios de Comunicación*, comunicado PF, México, 19 de julio de 2017, consultado en https://www.gob.mx/policiafederal/prensa/cns-realiza-primer-coloquio-de-ciberseguridad-para-medios-de-comunicacion [agosto 2018]

[318] Policía Federal, *Policía Federal y FBI suman capacidades, conforman grupo de fuerza para atender delitos de alto impacto*, comunicado PF, México, 8 de noviembre de 2017, consultado en https://www.gob.mx/policiafederal/prensa/policia-federal-y-fbi-suman-capacidades-conforman-grupo-de-fuerza-para-atender-delitos-de-alto-impacto [agosto 2018]

[319] Policía Federal, *Policía Federal pide a empresas de telefonía e Internet coordinar esfuerzos en beneficio de la Ciberseguridad*, comunicado PF, México, 16 de noviembre de 2017, consultado en https://www.gob.mx/policiafederal/prensa/policia-federal-pide-a-empresas-de-telefonia-e-internet-coordinar-esfuerzos-en-beneficio-de-la-ciberseguridad [agosto 2018]

[320] Policía Federal, *PF se capacita para adquirir habilidades que permitan planear, desarrollar y ejecutar acciones que garanticen resultados exitosos*, prensa PF, 30 de julio de 2018, consultado en https://www.gob.mx/policiafederal/prensa/policia-federal-se-capacita-para-adquirir-habilidades-que-permitan-planear-desarrollar-y-ejecutar-acciones-que-garanticen-resultados-exitosos?idiom=es [agosto 2018]

Asimismo, la División Científica y las Unidades de Policía Cibernética de las Procuradurías y Fiscalías Estatales de todo el país conformaron el Comité de Ciberseguridad. Se destacó que dicho comité permitirá construir capacidades sólidas para la operación, coordinación y trabajo vinculado con todas las entidades, incluso con autoridades de carácter internacional, para consolidar el Modelo Homologado de Unidades de Policía Cibernética, a fin de estandarizar la estrategia a nivel nacional y derivar la creación de un Formato Homologado sobre Incidentes Cibernéticos. El Comité sesionó en dos ocasiones durante el año 2018.[321]

La Policía Federal también signó un convenio con la Secretaría de la Función Pública (SFP) para capacitar, formar y actualizar a servidores públicos en materia de ciberseguridad. A estas acciones, se le suman los ya mencionados convenios de colaboración con Telmex y CONDUSEF, para intercambiar información, generar acciones de capacitación, concientización y prevención de delitos cibernéticos.[322]

Cabe destacar que se han realizado la tercera (noviembre 2017) y cuarta (octubre 2018) ediciones de la Semana Nacional de Ciberseguridad de la Policía Federal, donde se reunieron expertos nacionales e internacionales para el intercambio de experiencias y mejores prácticas, participando en ciclos de conferencias, talleres y webinars, con temáticas focalizadas a los esfuerzos que se realizan desde el gobierno, con la participación activa de la academia y la industria, para la preservación de un entorno digital seguro, libre, confiable y resiliente.[323]

En el eje transversal 3 se realizaron actividades diversas sobre coordinación y colaboración, donde las instancias encargadas de aplicar la Estrategia, como la CNS, la Policía Federal y su División Científica, generaron distintos tipos de canales para acercarse a otros niveles de gobierno, otras instancias de la administración

---

[321] Policía Federal*, Reúne CNS a las Unidades de Policía Cibernética del país y realiza la primera Sesión del Comité de Ciberseguridad*, México, 21 de abril de 2018, consultado en https://www.gob.mx/policiafederal/prensa/reune-cns-a-las-unidades-de-policia-cibernetica-del-pais-y-realiza-la-primera-sesion-del-comite-de-ciberseguridad?idiom=es [agosto 2018]

[322]Policía Federal*, Policía Federal y la Secretaría de la Función Pública firman convenio en materia de ciberseguridad*, 25 de noviembre de 2017, consultado https://www.gob.mx/policiafederal/prensa/policia-federal-y-la-secretaria-de-la-funcion-publica-firman-convenio-en-materia-de-ciberseguridad [agosto 2018]

[323] Policía Federal, *Arranca la Tercera Edición de la Semana Nacional de Ciberseguridad de la Policía Federal, Fecha de publicación*, 12 de noviembre de 2017, consultado https://www.gob.mx/policiafederal/prensa/arranca-la-tercera-edicion-de-la-semana-nacional-de-ciberseguridad-de-la-policia-federal [agosto 2018]

pública, empresas del sector de la seguridad cibernética y telecomunicaciones, así como la realización de esfuerzos de alcance internacional. Si bien no se concretó en todos los casos un convenio específico con las instituciones (públicas y privadas) con las que se tuvo vinculación, pero en cambio ha sido notable el esfuerzo por seguir acrecentando los lazos de colaboración con distintos actores y sectores como lo señala la ENCS.

No obstante, falta concretar más acciones en este rubro, a través de estrechar más lazos a nivel internacional, sobre todo a nivel regional, consolidar más acuerdos con organizaciones de la sociedad civil y lograr campañas conjuntas con los medios de comunicación, sobre todo los de mayor cobertura nacional. No obstante, para el tiempo que abarca esta evaluación, las actividades fueron numerosas y reflejaron la intención de incluir a distintos tipos de actores, a través de diversos canales, por lo que es satisfactorio el avance en este rubro. La calificación asignada al tercer eje transversal es de 0.80.

4. Investigación, desarrollo e innovación en TIC

En este rubro se puede incluir el acuerdo entre la Policía Federal y *Cisco Systems*. Dicho compromiso incluye el desarrollo conjunto de investigación tecnológica para la prevención de delitos en situaciones como las transacciones comerciales en línea, la seguridad de las empresas y la protección de los menores de edad, así como sumar la experiencia e infraestructura con que cuenta esta empresa global.[324] También, el convenio signado entre Telmex y la Policía Federal formalizó acciones de intercambio de capacitación, mejores prácticas en materia de ciberseguridad y ciberinteligencia, participación en foros y conferencias especializadas.[325]

La Policía Federal y la CONDUCEF realizaron un ciclo de conferencias en materia de Ciberseguridad con el objetivo de debatir posturas, ideas y experiencias en favor de la economía digital, en la que participó la Secretaría de Economía y la Asociación de Internet MX. Entre las actividades,se tocaron temas relativos a los retos legislativos a favor de la economía digital, el marketing digital, el comercio

[324] Policía Federal, *CNS-Policía Federal suma capacidades con Cisco Systems…, Óp. Cit*.
[325] Comisión Nacional de Seguridad, *PF y TELMEX-SCITUM fortalecen…, Óp. Cit*.

electrónico y la economía digital,también se recalcó la idea de generar un proceso continuo de educación digital hacia la prevención.[326]

De las tres líneas de acción indicadas por la ENCS, las actividades realizadas no cumplen a cabalidad aquéllas. No se establecieron políticas para detonar la innovación, todo se quedó en una lluvia de ideas. No se promovió de forma institucional la investigación a través de un programa especial de desarrollo científico y tecnológico. Tampoco se impulsó el mercado nacional para favorecer la autonomía y detonar la economía nacional en el sector.

Los acuerdos y los ciclos de conferencias revisados no cumplen con ninguno de los objetivos que el eje transversal de la Estrategia menciona, a pesar de los esfuerzos por colaborar. Esto se debe a que lograr un programa o política pública sobre innovación, desarrollo científico y tecnológico o detonador de la economía en el sector, es una cuestión más compleja y profunda. En este rubro, las acciones realizadas no solo son escuetas, sino que la misma propuesta del eje escapa del alcance de la Estrategia misma.

El eje transversal número 4, que refiere a la investigación, desarrollo e innovación en TIC, está cargado de una visión determinista y reduccionista. Una política pública y un programa de investigación, desarrollo e innovación, no puede surgir de una estrategia de ciberseguridad, sino de un conjunto de estrategias, ejes, líneas de acción especificas e institucionales, con un presupuesto asignado, personal especializado, la participación de universidades, de institutos de investigación, mecanismos de vinculación consolidados, entre otras estructuras legales e institucionales y con recursos económicos, humanos y técnicos suficientes para consolidarla y hacerla evolucionar. Es necesario un viraje en la visión de la ENCS, porque el enfoque instrumental de la tecnología detendrá su aplicación al plantear ejes como el número 4, con acciones que distan realmente del objetivo y los alcances de una estrategia de ciberseguridad para un país en desarrollo. La intención de que la ciberseguridad coadyuve a la investigación, desarrollo e

[326] Policía Federal, *Policía Federal y Condusef inauguran ciclo de conferencias en materia de Ciberseguridad*, prensa PF, México, 4 de mayo de 2018, consultado en https://www.gob.mx/policiafederal/prensa/policia-federal-y-condusef-inauguran-ciclo-de-conferencias-en-materia-de-ciberseguridad?idiom=es [agosto 2018]

innovación en las TIC puede ser loable, pero la forma de plantear esta meta tiene un enfoque errado en la ENCS, por lo que la calificación asignada es de 0.10.

5. Estándares y criterios técnicos

El gran proyecto de las instituciones de seguridad para lograr los objetivos del eje 5 de la ENCS, es la consolidación del Comité de Ciberseguridad. Como ya se mencionó, está integrado por la División Científica de la PF y las unidades de Policía Cibernética de las Procuradurías y Fiscalías Estatales de todo el país. Ha sesionado dos veces en el año 2018 y busca consolidar el Modelo Homologado de Unidades de Policía Cibernética, a fin de estandarizar la estrategia para combatir la ciberdelincuencia en todas sus formas.

Este Comité busca implementar mecanismos para registro de incidentes y delitos cibernéticos por entidad federativa, la creación de indicadores, estadísticas y tendencias sobre el surgimiento y comportamiento de las bandas delictivas en la red. Se pretende crear un Formato Homologado sobre Incidentes Cibernéticos que pueda ser utilizado en coordinación y colaboración con jueces, ministros y ministerios públicos, así como la aplicación de metodologías y mejores prácticas en la labor de la Policía Federal en materia de ciberseguridad.[327]

Esta propuesta de homologar el modelo del funcionamiento de las policías cibernéticas de los estados tiene dos aristas: una es que la intención de tener criterios y estándares sobre la aplicación de la Estrategia de forma sistematizada e integral, podría garantizar una mejor ejecución de las acciones; la otra es la disparidad entre las capacidades de cada unidad policiaca, ya que no todas las entidades tienen el mismo nivel de recursos técnicos y humanos o infraestructura, tampoco es equiparable el nivel de acceso a Internet de sus habitantes y la cantidad de incidentes registrados, por lo que homologar modelos de aplicación, lejos de ser una opción para la eficacia, podría alargar la curva de aprendizaje de algunas unidades y obstaculizar la implementación de la ENCS a nivel nacional.

Aunque se han presentado algunas propuestas de cómo se deberían elaborar informes sobre incidentes, aun no se ha aprobado el registro homologado. Asimismo, el avance organizacional del Comité de Ciberseguridad está en proceso

[327] Policía Federal*, Reúne CNS a las Unidades de Policía Cibernética del país…, Óp. Cit.*

de consolidación. Sin embargo, a un año de haberse aprobado su creación,[328] ya se ha tenido la voluntad política y se ha comprobado el compromiso de lograr el Modelo Homologado, al sesionar en dos ocasiones, intercambiar experiencias y presentar ya una propuesta de informe y registro.

A un año de la publicación del documento de la ENCS, hay avances para tener ya definido un posible marco de referencia, un registro homologado y estándares cuantitativos. De continuar los trabajos, podrían consolidarse en el próximo año estas medidas y criterios. Por el momento el avance es satisfactorio a pesar de las desigualdades entre entidades, pero es menester el consolidar las propuestas, por lo que la calificación al eje transversal 5 es de 0.70.

6. Infraestructuras críticas

Este eje transversal se respalda, principalmente, con el Centro Nacional de Respuesta a Incidentes Cibernéticos de la Policía Federal (CERT-MX). La instancia que se encarga de prevenir y mitigar las amenazas de ciberseguridad que ponen en riesgo la infraestructura tecnológica y la operatividad en México. El CERT-MX opera áreas especializadas en temas de prevención e investigación cibernéticas y es la única autoridad acreditada para realizar intercambio de información con policías cibernéticas nacionales y organismos policiales internacionales, con el objetivo de identificar y atender posibles ataques en agravio de infraestructuras críticas.

Mantiene un monitoreo permanente de la red pública de Internet, las 24 horas del día durante los 365 días del año. Se coordina con 421 equipos de respuesta a incidentes cibernéticos de 86 países alrededor del mundo, lo que permite generar y fortalecer líneas de investigación que, en colaboración con las policías cibernéticas de otras naciones, logre la identificación y ubicación de probables responsables de ataques cibernéticos, en colaboración con la PGR.[329]

En materia de prevención, se intercambia información con agencias internacionales sobre nuevas amenazas cibernéticas descubiertas en servicios,

[328] La creación del Comité fue propuesta y votada a favor durante la tercera edición de la Semana Nacional de Ciberseguridad de la Policía Federal, realizada en noviembre del año 2017.

[329] Policía Federal, *Centro Nacional de Respuesta a Incidentes Cibernéticos de la Policía Federal*, sitio oficial PF, México, 17 de mayo de 2018, consultado en https://www.gob.mx/policiafederal/articulos/centro-nacional-de-respuesta-a-incidentes-ciberneticos-de-la-policia-federal?idiom=es [agosto 2018]

protocolos y fabricantes tanto de software como de hardware; ello contribuye a brindar una mejor atención y orientación a la ciudadanía. El CERT-MX ha aprovechado los convenios firmados con *Microsoft*, *Cisco Systems*, la Asociación de Bancos de México y Telmex, para la mitigación y prevención de riesgos.[330]

Como resultados de estas medidas, la Policía Federal informó en octubre del año 2018 que los ataques cibernéticos a infraestructuras críticas de diferentes sectores como el de energía, salud y financiero, son una realidad, pero que en los últimos años se han neutralizado más de 23 mil sitios maliciosos que usurpaban la identidad de instituciones públicas y privadas, evitando que más de 3 mil 500 millones de pesos llegaran a manos de la delincuencia y se atendieron más de 64 mil denuncias ciudadanas brindando asesoría técnica-jurídica.[331]

Un caso de cómo funcionan este conjunto de acciones se presentó en mayo de 2017, cuando, derivado del ataque cibernético registrado en distintos países de Europa, Asia y América Latina, la Policía Federal, a través del CERT-MX, instrumentó las siguientes acciones:

-El 12 de mayo se difundió la alerta cibernética con las recomendaciones técnicas a las dependencias federales, infraestructura crítica y financieras.

-Se activó el Protocolo de Colaboración para la gestión de incidentes vinculados al Ransomware. Se obtuvieron muestras de archivos infectados y una muestra del código malicioso para su análisis en colaboración con la industria.

-Se realizó la verificación de incidentes en instituciones del gobierno federal, de infraestructura crítica y financiera en México, sin que se registrarán afectaciones.

-Se identificaron oficialmente cuatro casos de la infección a equipos de cómputo del Ransomware en el sector privado. Mediante la colaboración internacional, se identificó un posible repositorio del código malicioso en un sitio web comprometido de una empresa mexicana, hospedado en Estados Unidos, y se solicitó su baja.

---

[330] Ibídem.

[331] Policía Federal, *Policía Federal realiza la cuarta edición de la Semana Nacional de Ciberseguridad*, prensa PF, boletín 540, México, 23 de octubre de 2018, consultado en https://www.gob.mx/policiafederal/prensa/policia-federal-realiza-la-cuarta-edicion-de-la-semana-nacional-de-ciberseguridad [octubre 2018]

-Se difundió la actualización de la alerta cibernética incluyendo las recomendaciones técnicas de otros equipos de respuesta internacionales.
-Se mantuvo la coordinación internacional permanente con 320 equipos de respuesta a incidentes alrededor del mundo.[332]

Asimismo, el Centro de Ciberseguridad Industrial en México señala que, en el país, las instituciones tanto públicas como privadas, han aumentado la demanda de servicios privados de consultoría/asesoría en ciberseguridad, el hacking ético, auditorías de seguridad internas, auditorías de seguridad externas, copias de seguridad y la gestión de eventos e información de ciberseguridad.[333]

El eje transversal número 6 establece las acciones y mecanismos necesarios para minimizar la probabilidad de riesgos y vulnerabilidades. Aunque la ENCS no es muy específica sobre las actividades que se deben realizar para la protección de las infraestructuras críticas, la PF ha realizado, a través del CERT-MX, un cúmulo de acciones que han mantenido, hasta el momento, las infraestructuras criticas sin mayores peligros, comparados con los que han sufrido centrales de energía, servicios de salud y centros financieros de otros países.

No obstante, la mayoría de estas medidas son reactivas, aun no existe –o al menos no hay información de ello- algún protocolo específico de reforzamiento de la ciberseguridad para proteger las infraestructuras críticas; no existe un catálogo de soluciones o una lista de proveedores confiables de servicios en ciberseguridad tanto para entidades públicas como privadas, como tampoco se cuenta con una normatividad específica que sustente las acciones del llamado "monitoreo permanente de la red pública", lo que ha generado desconfianza entre las organizaciones civiles, porque se considera que existe un patrullaje que podría estar espiando las actividades de todos los usuarios, violando sus derechos a la privacidad.

---

[332] Policía Federal, *CNS, a través de la División Científica de la PF, instrumenta acciones ante ataque cibernético internacional*, prensa PF, boletín 320, México, 15 de mayo de 2017, consultado en https://www.gob.mx/policiafederal/prensa/cns-a-traves-de-la-division-cientifica-de-la-pf-instrumenta-acciones-ante-ataque-cibernetico-internacional [agosto 2018]

[333] Rafael Bucio y Jocsan Laguna, *La Ciberseguridad Industrial en México*, Centro de Ciberseguridad Industrial, México, consultado en https://www.cci-es.org/detalle-congreso?p_p_id=101&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_101_struts_action=%2Fasset_publisher%2Fview_content&_101_assetEntryId=349146&_101_type=content&_101_urlTitle=mexico [agosto 2018]

Considerando fortalezas y debilidades, en este eje se puede dar una calificación satisfactoria, pero con la perspectiva de que faltan elementos importantes para cumplir con los propósitos que la propia ENCS plantea. Así, su calificación es de 0.70.

7. Marco jurídico y autorregulación

Este eje busca impulsar y establecer acciones y mecanismos necesarios para la adecuación del marco jurídico nacional vinculado a la ciberseguridad y de autorregulación, para brindar certeza jurídica al actuar de los intermediarios de Internet y la sociedad en general. La ENCS no señala la intención de generar una ley o reglamento de gran envergadura que norme las conductas en el ciberespacio o que tipifique los crímenes cibernéticos como una categoría especifica.

Las encomiendas del eje transversal 7 son ambiguas y generalizadas. Señalan cooperación y capacitación jurídica, y la acción más substancial es la homologación y armonización de códigos penales y leyes complementarias con relación a ciberdelitos, así como de herramientas jurídicas con las que cuentan las instancias de procuración de justicia para la persecución de los mismos. Pero ninguna de estas premisas representa un cambio profundo en el impulso de medidas legales, necesarias para brindar certeza jurídica y confianza a los cibernautas.

En México no existe una ley federal, de alcance general o marco jurídico nacional destinado a la regulación del ciberespacio, que promueva la ciberseguridad o que castigue específicamente los ciberdelitos, por lo tanto, es necesario revisar algunas legislaciones de menor alcance. Hay algunos instrumentos jurídicos enfocados en sectores en especial, donde pueden encontrarse normas relacionadas con la regulación de conductas cibernéticas en ciertos sectores.

En el Código Penal Federal pueden remitirse los litigios en los casos de delitos que ya están tipificados en su forma tradicional, cuya práctica se ha extendido al ciberespacio, como el fraude, el abuso infantil, o la trata de personas, pero no se especifican procedimientos jurídicos cuando la ejecución de dichos ilícitos implica

al ciberespacio; la única tipificación específica que se menciona es el acceso ilícito a sistemas y equipos de informática en el Artículo 211 bis 1 a 211 bis 7.[334]

En cuanto a regulaciones específicas en el ámbito de la ciberseguridad, hay dos ordenamientos. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que obliga a los responsables del tratamiento de datos personales a observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad; que aplica al ámbito cibernético por las bases de datos, servicios de mensajería o distintos tipos de formularios que pasan por el ciberespacio y de los que se intenta dar confianza a todos los usuarios que no serán utilizados de manera ilícita o en su perjuicio. Así como la Ley de Firma Electrónica Avanzada, que indica que los documentos electrónicos y los mensajes de datos que cuenten con dicha firma producirán los mismos efectos que los presentados con firma autógrafa y tendrán el mismo valor probatorio que las disposiciones aplicables les otorgan a éstos.[335]

Otro instrumento relacionado con brindar certeza a las operaciones donde se utilizan las TIC es reciente. En el año 2018, se promulgó la Ley para Regular las Instituciones de Tecnología Financiera, como la primera ley que se da para el creciente sector denominado "*fintech*". Esta ley norma a las instituciones de financiamiento colectivo, o el *crowdfunding*, los servicios de fondos de pago electrónico, y los servicios financieros a través de nuevas tecnologías (como los de inversión en criptodivisas) Busca prevenir y mitigar el riesgo de lavado de dinero y financiamiento al terrorismo que borran sus pistas de transacciones electrónicas y prevé un régimen de divulgación de riesgos.[336]

Aunque la ENCS tiene la intención de brindar certeza jurídica a los cibernautas mexicanos a nivel individual y colectivo, no se establece en el documento una planeación o plazos para promulgar una ley general o de alcance federal en el tema

---

[334]Estados Unidos Mexicanos, *Código Penal Federal*, en info4.juridicas.unam, vigente desde 1931, consultado en http://info4.juridicas.unam.mx/ijure/tcfed/8.htm?s [septiembre 2018]

[335] UIT, *Global CybersecurityIndex&CyberwellnessProfiles*, en itu.org, UIT-ABI research, Suiza, abril 2015, p. 318, consultado en http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf [octubre 2018]

[336] El Financiero (Redacción), *10 puntos para entender la nueva Ley Fintech*, en sitio oficial El Financiero, 1 de marzo de 2018, Ciudad de México, consultado en http://www.elfinanciero.com.mx/empresas/diez-puntos-para-entender-la-nueva-ley-fintech [septiembre 2018]

cibernético, no existe una propuesta de ordenamiento o estructura jurídica sobre la que se deba basar la autorregulación o la capacitación para las instancias de procuración de justicia. Frente a ello, una organización como la CANIETI, con especialistas en ciberseguridad, ha señalado en su estudio "Evaluación de la Ciberseguridad en México" (antes mencionado), en sus participaciones en foros de políticas públicas por las TIC y en los grupos de trabajo sobre ciberseguridad, que es necesario impulsar una Ley de Ciberseguridad de alcance nacional.[337]

En años recientes, hubo un intento de promulgar una ley federal que sancionara los ciberdelitos, la llamada "Ley Fayad" que, lejos de ser una respuesta, generó desaprobación, ya que había sido trabajada por la Policía Federal, pero la iniciativa no había sido consultada con actores no gubernamentales.[338] La lección es que el tema de la ciberseguridad tenía que ir más allá de las medidas punitivas, debía ser consultado con el sector privado y la sociedad civil, para evitar forjar una reglamentación que resultara ambigua y contradictoria a los derechos humanos.

Con base en el enfoque de la presente investigación se considera la necesidad de crear una ley acorde a los contextos del país, tomando en cuenta los factores jurídicos, sociales y el aparato judicial y administrativo que aplicará las leyes. Es muy importante que los gobiernos,el sector privado y la sociedad civil colaboren para asegurarse de que los cuerpos policiales y el poder judicial dispongan de las herramientas apropiadas, tanto legales como técnicas, para proteger al público contra las actividades delictivas cibernéticas.

Además, el marco jurídico en ciberseguridad debe estar a la par de la tendencia internacional en la materia, para que haya homologación y

---

[337] Al Momento MX (Redacción), *México en busca de la Secretaría TIC y Ley de ciberseguridad*, 30/01/2018, consultado en almomento.mx/mexico-en-busca-de-la-secretaria-tic-y-la-ley-de-ciberseguridad/ [agosto 2018]

[338] El 22 de octubre de 2015, el Senador Omar Fayad Meneses sometió a consideración del pleno de la Cámara de Senadores la iniciativa de "Ley federal para prevenir y sancionar los delitos informáticos", que constaba de 48 artículos, en los cuales se tipificaban como delitos conductas relacionadas con la interferencia de sistemas informáticos, la depredación sexual en la red, terrorismo cibernético, entre otras. La iniciativa fue rechazada por diversas organizaciones de la sociedad civil, medios de comunicación y cibernautas, al considerar que los criterios que establecía para sancionar eran muy generales y ambiguos, por medio de los cuales podrían presentarse violaciones a la libertad de expresión, así como medidas restrictivas excesivas sobre el uso de los elementos informáticos. Fue revocada en el Senado ante la presión mediática.Omar Fayad, *Iniciativa con proyecto de decreto por el que se expide la Ley federal para prevenir y sancionar los delitos informáticos*, en sil.gobernacion.gob.mx, Senado de la República, México, 27 de octubre de 2015, consultado en sil.gobernacion.gob.mx/Archivos/Documentos/2015/10/asun_3291220_20151027_1445523938.pdf [agosto 2018]

correspondencia al aplicar las leyes nacionales cuando los casos sean trasnacionales (la mayoría lo son). Según el marco de la GCA, las legislaciones también deben ser suficientemente flexibles para tener en cuenta los avances tecnológicos. Asimismo, resulta relevante que México participe de la formulación, apoye y adopte las normas internacionales relacionadas con la ciberseguridad.

En el eje transversal 7 se concluye que hay un escueto trabajo en cuanto a leyes que regulen las conductas ilícitas en el ciberespacio. Tanto a nivel documental como ejecutivo no hay una intención de la ENCS de promulgar una ley de alcance nacional en la materia. Además, no se ha demostrado la capacidad de conducir un debate para generar un marco jurídico en ciberseguridad que cumpla con el objetivo de establecer acciones y mecanismos necesarios para la adecuación del marco jurídico nacional vinculado a la ciberseguridad y de autorregulación. Basado en dicho análisis, este eje tiene una calificación de 0.30.

8. Medición y seguimiento

La División Científica de la Policía Federal es la principal responsable de la generación de mecanismos de medición, establecimiento de estadísticas y la obtención de datos referentes a la ciberseguridad. Le corresponde vigilar, identificar, monitorear y rastrear la red pública de Internet, para prevenir conductas delictivas, así como establecer registros de información obtenida en sus investigaciones e instituir mecanismos y protocolos para garantizar la confidencialidad e integridad de los datos. Es la instancia que se encarga de aplicar la ENCS.[339]

En el marco de la tercera edición de la Semana Nacional de la Ciberseguridad, en noviembre del 2017, la División Científica propuso conformar el primer Comité de Ciberseguridad que fue aprobada por el Consejo Nacional de Seguridad. Con ello, se busca implementar un Modelo Homologado de Policía Cibernética en las 32 entidades, para estandarizar y establecer criterios de medición que apliquen a nivel nacional.[340]El comité celebró dos sesiones en el año 2018, una en abril y otra en

[339] Policía Federal, *División Científica de la Policía Federal*, sitio oficial PF, México, 11 de julio 2018, consultado en www.gob.mx/policiafederal/articulos/division-cientifica-de-la-policia-federal?idiom=es [septiembre 2018]
[340] Policía Federal, *Impulsa Policía Federal la creación del primer Comité de Ciberseguridad a nivel nacional*, prensa PF, 16 de noviembre de 2017, consultado en https://www.gob.mx/policiafederal/prensa/impulsa-policia-federal-la-creacion-del-primer-comite-de-ciberseguridad-a-nivel-nacional [septiembre 2018]

octubre; en la primera se presentaron las propuestas del modelo de policía y en la segunda se mostraron avances del formato de registro de incidentes.

Como se mencionó previamente, uno de sus propósitos principales es implementar mecanismos para la creación de indicadores, estadísticas y tendencias sobre el surgimiento y comportamiento de las bandas delictivas en la red. Se pretende crear un Formato Homologado sobre Incidentes Cibernéticos que pueda ser utilizado en coordinación y colaboración con jueces, ministros y ministerios públicos, así como la aplicación de metodologías y mejores prácticas en la labor de la Policía Federal en materia de ciberseguridad.[341]

En el último eje transversal, se busca dar seguimiento a los resultados obtenidos de la implementación de la ENCS y "medir su impacto en el desarrollo social y económico del país, con la finalidad de identificar las áreas de oportunidad para su mejora continua". De nueva cuenta, se plantean metas que no corresponden a una estrategia de ciberseguridad: ¿cómo podría establecerse una relación entre la aplicación de la ENCS y el desarrollo social y económico del país? Se busca justificar una relación "ciberseguridad-desarrollo" a través de indicadores, algo que no solo es determinista y alejado de la realidad del desarrollo económico y social, sino que también resulta poco viable de generar o aplicar.

La División Científica de la Policía Federal intenta transmitir sus capacidades y experiencia a las policías cibernéticas estatales a través de la homologación de estándares y modelos, por lo que el Comité de Ciberseguridad tiene un papel muy importante tanto para la estructura organizacional que aplique la Estrategia, como para el establecimiento de estándares de medición y seguimiento de resultados. Asimismo, aunque no se tienen los formatos o protocolos para medir el impacto de las acciones que se lleven a cabo, ya existen propuestas que, se proyecta, serán aplicadas el siguiente año.

No obstante, el documento de la ENCS es impreciso y general en la cuestión de cuáles serán los métodos de medición o los estándares mínimos permitidos al aplicar la Estrategia. Por ejemplo, no se plantea un porcentaje de reducción de ataques con relación a otros años, un nivel de cobertura de las campañas de

[341] Policía Federal*, Reúne CNS a las Unidades de Policía Cibernética del país…,Óp. Cit*.

“Cibernauta con estrella”, o alguna meta de cantidad de inversión para desarrollar capacidades en ciberseguridad al año. Es decir, no se proponen –o al menos no se han publicado- metas claras que puedan ser ponderables y comprobadas por medio de la estadística, criterios cuantitativos que permitan medir el alcance de los principios, objetivos y ejes transversales de toda la ejecución de la Estrategia o que contribuyan en revelar las debilidades donde se deban redoblar esfuerzos.

Aunque se han presentado algunas propuestas de cómo se deberían elaborar informes sobre incidentes, aún no se ha aprobado el registro homologado. Los avances deben consolidarse. También, se tienen que publicar los resultados y compararse con las actividades que se realizaban sobre ciberseguridad antes de la Estrategia, para saber cuál ha sido el efecto real de su ejecución.

Este último eje se puede evaluar como escaso por el momento, en espera de que se consoliden las propuestas de medición y seguimiento, así como el señalamiento de que las metas que se pretenden alcanzar deben ser claras y establecer criterios cuantitativos que se puedan comprobar a partir de modelos estadísticos. La calificación que se le otorga es de 0.50.

Concluido el análisis del último rubro, en el siguiente cuadro se muestra el compendio de las calificaciones asignadas a cada eje transversal en la evaluación.

1. Cultura de ciberseguridad	0.20
2. Desarrollo de capacidades	0.75
3. Coordinación y colaboración	0.80
4. Investigación, desarrollo e innovación en TIC	0.10
5. Estándares y criterios técnicos	0.70
6. Infraestructuras críticas	0.70
7. Marco jurídico y autorregulación	0.30
8. Medición y seguimiento	0.50

Después de repasar las acciones relacionadas con cada eje transversal, se aplicó la fórmula de la media aritmética, para obtener la calificación sobre la implementación de la ENCS en el periodo de noviembre 2017 a octubre 2018. Se

sumaron los valores correspondientes a cada eje y ese resultado se dividió entre el total de datos, es decir 8, de la siguiente manera:

0.20 + 0.75 + 0.80 + 0.10 + 0.70 + 0.70 + 0.30 + 0.50 = **4.05**

4.05/8 = **0.50625**

Por lo tanto, la calificación asignada en la presente investigación para la implementación de la ENCS es de **0.50**, en una escala de 0 a 1.

Como se explicó, el análisis genera una calificación que representa, de forma cuantitativa, la evaluación general de la ENCS. Para llegar a este valor numérico, la Estrategia fue evaluada con base en las dos pautas examinadas.

Calificación con respecto a la GCA	0.66
Calificación sobre la implementación de la ENCS	0.500625

Después de ponderar la Estrategia ante ambos elementos, se tienen dos calificaciones, por lo que se vuelve a aplicar la fórmula de la media aritmética. Se suma el valor de ambos elementos y el resultado se divide entre el total de datos.

0.50625 + 0.66 = **1.16625**

1.16625 / 2 = **0.583125**

De este resultado, se toman el decimal y el centesimal. Por tanto, la calificación general que se le asigna es de **0.58**, en una escala de 0 a 1. Ese es el valor numérico que representa el resultado de la evaluación realizada en la presente investigaciónpara la Estrategia Nacional de Ciberseguridad en México.

Así finaliza la evaluación aplicada a la ENCS en el presente capitulo, donde se estableció un análisis comparativo en dos planos, el primero sobre el documento que ostenta la Estrategia contrastado con la GCA y el segundo sobre las actividades realizadas con base en los 8 ejes transversales de la ENCS y sus líneas de acción. Este examen permite establecer algunas consideraciones puntuales.

El resultado final revela que la ENCS tiene una ejecución medianamente satisfactoria, si bien su desempeño no tiene un nivel de desempeño malo, es

insuficiente para lograr el objetivo que la misma Estrategia se plantea, de fortalecer 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.

Tener un valor numérico permite concluir que un 58% de efectividad en su implementación resulta ser un porcentaje de éxito escueto y poco loable para un tema como la ciberseguridad, que ha incrementado en magnitud e importancia en los últimos años en México, en la región y a nivel global.

Es notable el contraste que hay entre la concepción de la propia ENCS, comparada con la GCA, y de las indicaciones propuestas en los ejes transversales, cotejadas con las acciones implementadas. Hay puntos donde la ENCS es más acertada y otros donde hay una distancia considerable entre el ser y deber ser. De esta manera se distingue entre el discurso y los hechos concretos enmarcados en la ENCS, con base en un modelo de análisis comparativo y una visión alejada del reduccionismo y el determinismo tecnológico.

Al examinar cada punto, se generó, en primera instancia, una evaluación individual, que permite identificar qué tan cercana esta la concepción y ejecución de cada eje y ayuda a identificar los rubros donde se ha podido trabajar con certidumbre, aquellos donde se tienen que redoblar esfuerzos y unos más donde, incluso, se deberían replantear los objetivos y las acciones. Un examen bajo este procedimiento coadyuva en la afinación de las recomendaciones y parámetros de medición que permitan una ejecución más adecuada de una política pública con la importancia que pretende tener la ENCS.

Resulta preocupante que en tres ejes el contraste es significativo, la evaluación es sumamente negativa, mientras que sólo en dos puntos se supera el 75% de efectividad en su implementación. Del promedio y la evaluación general se puede determinar que apenas se está por encima de la media, que no se alcanza una calificación satisfactoria; prácticamente, al no tener más del 60% de valoración positiva, se puede considerar que la ENCS esta reprobada.

No obstante, el tener una revisión en lo global y en lo específico de la ENCS, coadyuvará en su mejoramiento, puesto que, en los rubros donde se ha trabajado de manera fluida y eficaz, se pueden afinar o continuar las acciones para consolidar esfuerzos, pero donde se tiene un desempeño negativo será necesario buscar redoblar o incluso replantear metas y procedimientos.

El objetivo general de la presente investigación era realizar un diagnóstico y una evaluación integral sobre la Estrategia Nacional de Ciberseguridad en Méxicodurante el periodo 2017-2018, desde una perspectiva en la que se incluyeron algunos parámetros del enfoque de Ciencia, Tecnología y Sociedad.Para ello se emplearon dos pautas referenciales para evaluarla, lo que se complementó con observaciones puntuales en cada pilar y en cada eje transversal, sobre cómo un enfoque integral –basado en la visión de los estudios CTS- podría dar un viraje sustancial a la ENCS, tanto en su concepción como en su implementación, que se traduciría en la asimilación de la propia Estrategia en la sociedad mexicana.

Es importante reiterar, como se mencionó en el segundo capítulo, que la ciberseguridad es un medio,que permite la construcción de confianza en el ciberespacio; con la meta de asegurar que la infraestructura de la información funcione de forma fiable incluso cuando esté bajo amenaza.En este sentido, la evaluación permite observar que el bajo desempeño en la ejecución de la ENCS se aleja del fin último, que es brindar protección y confianza al mexicano que interactúa en el ciberespacio.

Mantener un ciberespacio protegido, gestionando los riesgos, salvaguardándolo de amenazas y reforzando la resistencia y resiliencia ante ataques, implica que el tema de la ciberseguridad debe ser prioritario en los gobiernos, el sector privado, el ámbito académico, las asociaciones civiles y las familias mexicanas.Sobre todo, cuando casi de 80 millones de mexicanos pasan más de una tercera parte de sus días interactuando en el ciberespacio.

Asimismo, debe señalarse que, si bien la ENCS en México no tiene un porcentaje de desempeño satisfactorio, desde su publicación a la fecha se han realizado acciones más puntuales, se han incluido a más actores y se le ha

destinado mayores recursos, lo cual demuestra una ruta que puede lograr avances significativos en un par de años.

El hecho de que se hayan organizado cuatro ediciones de la Semana Nacional de Ciberseguridad; la suscripción de distintos convenios con asociaciones civiles, instancias gubernamentales y empresas del ramo de la seguridad informática y las telecomunicaciones; los pasos para homologar estándares y criterios de medición; la implementación de acciones enfocadas en la creación de capacidades; entre otras actividades significativas; demuestran que la conciencia sobre la promoción de la ciberseguridad es creciente y ha tomado relevancia en los más altos niveles de los tomadores de decisiones. Se considera que es cuestión de tiempo para que muchos de estos esfuerzos se consoliden, lo que contribuirá a lograr el objetivo de generación de confianza en el ciberespacio.

Sin embargo, hay un último e importante factor que mencionar, la presente investigación se ubica en un periodo de cambio político en México. La evaluación realizada a la ENCS recobra importancia porque revela cómo se ha manejado el tema en todo un sexenio y puede ser referente para el periodo del presidente Andrés Manuel López Obrador (2018-2024), de quien no se ha conocido, hasta el momento, una propuesta concreta en materia de ciberseguridad; por lo que el documento de la ENCS puede tener continuidad, ser descartado o ser tomado como una referencia para la construcción de una agenda de ciberseguridad o una nueva estrategia, construida con mayor apoyo de los diferentes sectores sociales.

En esta tesis se considera que una estrategia integral y efectiva para brindar confianza en el ciberespacio debe estar influenciada en su diseño, desarrollo, apropiación e implementación, por distintos sectores sociales y por elementos no humanos como normas y parámetros técnicos que permitan su ejecución eficaz.Es decir, los diversos intereses de los actores desempeñan un papel importante en la planeación, implementación, y toma de decisiones de la Estrategia.

Conclusiones.

La Unión Internacional de Telecomunicaciones estima que, hacia finales del año de 2018, el 51.2 por ciento de la población del mundo utilizó Internet y, según los datos de *Cisco Systems*, habrá más de 12 mil millones de dispositivos conectados a Internet para 2020. Aun cuando el uso de Internet no necesariamente implica navegar por el ciberespacio, el grado de acceso al primero influye en los alcances del segundo. El nivel de penetración del Internet en la vida cotidiana conlleva a enfrentarse a los posibles peligros del ciberespacio, representando riesgos para, al menos, la mitad de la población y, de forma indirecta, si se atacase alguna infraestructura o servicio básico, para poblaciones enteras.

Siguiendo autores cuyos enfoques se inscriben en diversas disciplinas, además de las relaciones internacionales, en la investigación se concluye que el ciberespacio involucra prácticamente todos los campos del conocimiento e implica un entorno de interacción humana que no tiene barreras físicas, es intangible y no tiene una localización geográfica.

Es de suma importancia reconocer que al ciberespacio lo construye la sociedad, y está configurado por un conjunto de aspectos sociales y técnicos. De tal manera que cualquier política, estrategia o plan relacionado con el ciberespacio tiene que ser socialmente significativo tanto para quienes interactúan en él como para quienes lo atacan. Esta afirmación, refuerza la conciencia sobre sus implicaciones a nivel global, lo que envuelve dilemas tan variados como el acceso, el debate de su regulación y, por supuesto, los riesgos a la seguridad que se presenten en dicho entorno.

Symantec encontró en 2017 que uno de cada 131 correos electrónicos era malicioso y se usaba para una amplia gama de ataques, desde grupos de espionaje, hasta pandillas de *ransomware*. De acuerdo con Grant Gross, reportero tecnológico de la Internet Society, el cibercrimen le costaba al mundo más de $600,000 millones de dólares al año, más del 0.8% del PIB global. Con base en datos proporcionados por Gabriela Chávez para la revista Expansión, se calcula que los costos inherentes a los delitos en el ciberespacio representaron para México $7,700 millones de dólares en 2018.

Concebir cómo este entorno ha ido delimitando algunas formas de relación entre los actores de la sociedad internacional, permite reconocer la importancia, pertinencia y vigencia de aplicar medidas regulatorias y parámetros de seguridad y protección en el ciberespacio. Intentar contrarrestar las vulnerabilidades de la ciberseguridad se está volviendo cada vez más relevante en la agenda de los tomadores de decisiones a nivel global. Lo anterior justifica la necesidad de realizar un diagnóstico y evaluación de la Estrategia Nacional de Ciberseguridad en México.

Antes de abordar como tal la Estrategia, se expusieron las características de una propuesta analítica basada en los estudios en ciencia, tecnología y sociedad, con el propósito de presentar una alternativa a los supuestos reduccionistas y deterministas que le han atribuido gobiernos, organizaciones internacionales, empresas, investigadores, académicos y sociedades enteras al factor tecnológico a durante el último siglo.

Así, en el capítulo 1 se explicó el viraje analítico que aportan los estudios CTS. Se realizó una revisión de los principales enfoques teóricos sobre la innovación tecnológica, recorriendo el significado delo que Díaz y Lee caracterizaron como la Tradición Instrumental de la Innovación Tecnológica (TIIT) y su idea determinista de los fenómenos tecnológicos; se explicó el contraste con la Tradición Interpretativa de la Innovación Tecnológica (TIIN), de la cual se abordan dos enfoques derivados del constructivismo social: la Teoría del Actor Red (TAR) y la Construcción Social de la Tecnología (COST).

En este capítulo se buscó hacer propuestas críticas para abordar el fenómeno de la ciberseguridad como un tópico de carácter global, presente en las agendas de los actores internacionales y que se ubica en la amalgama ciencia-tecnología-sociedad. Además, persiste el reto de avanzar hacia la sensibilización social e incluso académica del valor del pensamiento CTS como crítica social y como alternativa para incluir a la sociedad civil en estos debates.

Asimismo, se caracterizó un enfoque desde la disciplina de Relaciones Internacionales, basado en las propuestas teóricas de los estudios CTS, pero con una perspectiva disciplinaria especifica que envolvía la visión y los fenómenos ocurridos en su objeto de estudio, la sociedad internacional. Se desplegó un

recorrido conceptual sobre la forma en que los internacionalistas abordan el tema, así como la influencia de los fenómenos internacionales y sus actores, en el análisis de los temas de ciencia, tecnología y sociedad. Se precisó la necesidad de hacer de Relaciones Internacionales una disciplina referente en la reflexión sobre la influencia de las dimensiones globales en los procesos de innovación tecnológica.

El objetivo del segundo capítulo fue examinar al fenómeno de la ciberseguridad en sus dimensiones e implicaciones globales. Para entender todo lo que la involucra y su importancia internacional, fue necesario revisar al ciberespacio y cómo se ha configurado en un entorno de interacción social a nivel global.

Se examinó el origen y consolidación del ciberespacio, tanto a nivel teórico como en su influjo en el mundo contemporáneo. Se revisaron los conceptos que le antecedieron (como la cibernética) y se le caracterizó como un espacio socialmente construido. Así se podía entender la existencia de un proceso constante de crecimiento en el nivel de interconexión global, cuyas características de deslocalización y velocidad de la generación y transmisión de información hacen de cada riesgo a la seguridad en el ciberespacio, una potencial amenaza global.

Se reconoció que los riesgos que se producen en los entornos sociales físicos también se reproducen en el ciberespacio, como las amenazas provocadas, tanto por individuos como por organizaciones, cuyo *modus vivendi* se sostiene en actividades ilegales; esto sumaba importancia a la necesidad de realizar una evaluación de la ciberseguridad en México. Se concluyó que asegurar el ciberespacio es particularmente complejo, porque la sociedad que interactúa en él promueve su conectividad, no su seguridad.

La ciberseguridad se describió como el conjunto de acciones destinadas a mantener márgenes de seguridad y certidumbre en el ciberespacio, y se incluye una serie de medidas para robustecer la protección, brindar confianza y desarrollar resiliencia en el dominio cibernético. Asimismo, se determinó que la ciberseguridad no puede partir de la sensación de pánico ni se debe dar un sentido alarmista a la sociedad, sino que el Estado debe enfocarse en brindar confianza a los usuarios de que el ciberespacio con márgenes amplios de seguridad, disponibilidad, integridad de las redes, confidencialidad, transparencia y certidumbre legal.

Se concluye que una estrategia de ciberseguridad efectiva debe contener políticas y estándares respecto a la seguridad y las operaciones en el ciberespacio, así como toda una gama de reducción de vulnerabilidades, colaboración internacional, disuasión de ataques, respuesta oportuna a incidentes y aumento de la resiliencia. Estos objetivos se lograrán si se generan las normas jurídicas respectivas, se realizan operaciones de respuesta inmediata, se coordinan acciones diplomáticas y medidas de protección en el ámbito militar y se llevan a cabo misiones permanentes de inteligencia dentro de la infraestructura mundial de redes.

También se analizaron algunas de las características y *modus operandi* de los ciberdelitos más comunes. Se describieron los más frecuentes a nivel internacional, qué son, cómo funcionan, en qué casos se utilizan y algunos datos sobre su nivel de incidencia. Luego de profundizar en las amenazas cibernéticas, se reforzó la idea de que no se trata de un fenómeno solamente tecnológico, sino de algo más complejo, que incluye otra serie de variables sociales, políticas, económicas, culturales, jurídicas, incluso de relaciones interpersonales.

Por tanto, el ciberespacio debe ser protegido de incidentes, actividades maliciosas y toda una serie de amenazas, que sólo es posible enfrentarlas si hay una concientización de toda la sociedad y si todos los actores trabajan en conjunto para fortalecerse y ofrecer márgenes de libertad y seguridad. Asimismo, se explicó que el elemento transnacional de la ciberseguridad plantea un gran desafío para la prevención, defensa, investigación, resolución y castigo de los crímenes cibernéticos.

Con toda esta complejidad, empero, no todo el panorama es oscuro. Aun con las dificultades tanto de orden técnico, legislativo y político, muchos países y regiones ya están llevando a cabo esfuerzos de ciberseguridad. No existe un consenso dominante sobre cómo tratar el fenómeno, ya que todos tienen sus propios dilemas, dependiendo las condiciones propias de cada país. Pero es posible reconocer tendencias globales, las cuales México ha consultado para establecer su propia estrategia; de estas se hicieron algunas referencias, como la GCA, de la UIT.

En este capítulo se aseveró que la ciberseguridad es un tema transversal que debe ser abordado en México, para diseñar y construir los cimientos en torno al uso

y apropiación de las TIC, que permitan coadyuvar, desde el ciberespacio, en la seguridad multidimensional del país. Se determinó que la ciberseguridad no es un fin en sí misma, sino que todas las actividades relacionadas tienen el objetivo de construir confianza en el ciberespacio y la meta de asegurar que no se dañen los intereses de los internautas, la infraestructura y los canales de comunicación.

Se concluyó que la ciberseguridad no es un concepto cerrado, ni limitado en su margen de acción, sino que es todo un conjunto de estrategias, planeaciones, estructuras, acciones y evaluaciones. Comprender esta importancia y alcances, permitieron definirla como un fenómeno que tiene que ser examinado desde sus perspectivas no solo tecnológicas sino también sociales, políticas, económicas, jurídicas y culturales, a niveles locales, nacionales, regionales y globales.

En el capítulo 3 se presenta la evaluación de la Estrategia Nacional de Ciberseguridad desde los estudios CTS partiendo de que los fenómenos tecnológicos van más allá de la lógica del mercado y la satisfacción de una necesidad, y que penden de procesos contingentes y conflictivos, relacionado con grupos públicos de interés, y no con etapas autocontenidas que pueden ser organizadas y administradas desde y hacia un punto u objetivos centrales específicos. Para operacionalizar lo anterior se recurrió a dos esquemas explicativos de los trabajos CTS: la Construcción Social de la Tecnología (COST) y la Teoría de Red Actores (TAR).

De la COST se retomó la deconstrucción de la versión lineal y de sus herramientas metodológicas principales, las más relevantes para la presente tesis fueron: la inclusión de los grupos sociales relevantes asociados con el desarrollo de las medidas de ciberseguridad; la existencia de una flexibilidad interpretativa, a partir de la cual la ciberseguridad puede tener diversos significados y utilidades para los individuos y los sectores sociales, dependiendo los riesgos a los que se expongan; y el marco tecnológico, distinto también por las condiciones de cada país, los niveles de conexión y los usos de la infraestructura, entre otros factores.

Siguiendo los presupuestos de la TAR, se consideró al ciberespacio como un actor-red y sus enlaces son las relaciones entre éstos en un entorno virtual. Los actores-mundo son los estados, las empresas, las organizaciones civiles, los grupos

criminales, cuya conjunción se da a partir del proceso de traducción, que son las estrategias de ciberseguridad. El conjunto de los actores-mundo y las estrategias de ciberseguridad, como procesos de traducción, constituyen una parte importante de la constante construcción del ciberespacio como actor-red; convirtiéndolo en una entidad que no obedece reglas definitivas, compuesto por múltiples entidades cuyas asociaciones están en permanente y creciente interacción y construcción.

A partir de la revisión de las propuestas analíticas de los estudios CTS, y más puntualmente de la COST y la TAR, se dilucidó que el ciberespacio no es sólo un fenómeno técnico, sino que está compuesto por toda una serie de elementos interactivos que permiten, o no, su desarrollo y consolidación en el imaginario social y que dentro de éste se reproducen todo tipo de relaciones dadas en el contexto social, como la delincuencia, con sus características concretas.

En la segunda parte del capítulo, se presentó, desde la institucionalidad, cómo conciben los creadores de la Estrategia al fenómeno de la ciberseguridad y cuáles son las medidas con las que se pretende dar confianza al ciberespacio. Se plasmó gran parte del documento que ostenta la Estrategia Nacional de Ciberseguridad (ENCS), que establece la visión del Estado mexicano en la materia.

Presentada el 13 de noviembre de 2017, la Estrategia es un documento de 30 páginas, compuesto de 9 apartados que, al examinarlos, se pueden dividir en 3 partes. La primera parte, que consta de cinco subtítulos, muestra el contexto y los fundamentos sobre los que se asienta la visión del Estado mexicano respecto al tema de la ciberseguridad y la necesidad de haber creado dicho instrumento institucional; los siguientes dos apartados entran en materia de la estrategia, despliegan los principios, ejes y objetivos, asimismo, explican el marco institucional para la ejecución de dichas medidas; la última parte es complementaria, y en ella se brinda un glosario para entender a cabalidad la terminología utilizada y se anexa la información con las reuniones a través de las cuales se llevó a cabo el proceso colaborativo entre los distintos actores sociales para desarrollar la ENCS.

Enseguida, con el propósito de conocer en forma y fondo lo que dice la Estrategia, se exploraron las dos partes relevantes de la ENCS. Primero las bases, justificación y contextos tomados en cuenta para que se generara dicha estrategia,

después se revisó su margen de acción, al conocer sus principios, ejes, estructura, objetivos y marco institucional. Esto se logró reproduciendo las partes más significativas del documento de la ENCS, a modo de síntesis, y haciendo observaciones pertinentes para explicar la visión plasmada por sus creadores.

Luego de examinarla a nivel documental, fue notable que la ENCS se inserta en la visión instrumental que ha imperado sobre la tecnología en los programas y políticas gubernamentales, donde se le atribuye al desarrollo científico y tecnológico una capacidad por encima de otros factores, la inexpugnable facultad de impactar al entorno social, como si surgiera cual elemento externo a la sociedad. En el caso de la ENCS, se señalan en reiteradas ocasiones los supuestos e inherentes beneficios de la inserción de las TIC al desarrollo de la sociedad.

También se pudo concluir que no es una guía práctica, sino un instrumento marco, donde no están especificadas cada una de las acciones. Se despliegan una serie de principios, objetivos y encomiendas y se identificó la conciencia de que la ciberseguridad debe ser abordada de manera integral e incluyente. El propósito era ver en forma y fondo lo qué dice la Estrategia y, una vez conocidos estos elementos, se podría realizar tanto un diagnóstico como una evaluación de la ciberseguridad, más enfocados en lo que –en el supuesto institucional- debería derivar la ENCS, comparado con la realidad de los datos, es decir, el ser *versus* el deber ser.

Establecidas estas consideraciones, en el último capítulo se desplegó un análisis sobre la situación actual de la ciberseguridad y una evaluación de la Estrategia. Se dividió en dos apartados. El primero para conocer las condiciones generales de la ciberseguridad a lo largo del sexenio (2012-2018), donde se conocieron las principales incidencias en la materia, las acciones y esfuerzos de los distintos actores y sectores sociales durante el periodo. En la segunda parte se realizó la evaluación de la ENCS, observada a partir de dos estándares.

Con los datos presentados en el diagnóstico se pudo determinar que, en la cotidianeidad del mexicano promedio, cada vez son menos las restricciones para internarse al ciberespacio, por más tiempo y sin distinción de lugar, lo que implicaba riesgos ante el descuido o la poca conciencia que pudiera tener la sociedad mexicana en temas de protección cibernética.

Asimismo, se observó que, a pesar de los esfuerzos realizados para lograr mantener la seguridad y la confianza en el ciberespacio, antes de la generación y publicación de la ENCS, las instituciones mexicanas actuaron, generalmente, de forma reactiva. No respondían a una estrategia previamente diseñada, a planes definidos de fortalecimiento institucional o medidas preventivas; las acciones eran desarticuladas, las actividades que se organizaban no se guiaban por un procedimiento conjunto con otras instituciones; no seguía un objetivo general de alcance nacional; tampoco se concretaba algún plan, una serie de líneas de acción u objetivos particulares, así como metas medibles.

Por eso fue necesario generar y publicar la Estrategia Nacional de Ciberseguridad, como política pública que pretende funcionar de marco general, para guiar y articular las acciones aplicables ante cada incidencia y actividad relacionada a la ciberseguridad sucedida en México. Consecuentemente, resultaba imperioso evaluar si la Estrategia estaba consiguiendo sus fines.

La investigación finalizaba con una evaluación puntual de la Estrategia, tanto de su concepción como de la efectividad de su aplicación. Además de ir desplegando un análisis cualitativo, se fue otorgando un valor cuantitativo. El análisis generaría una calificación que pudiera representar, en forma numérica, la evaluación general y, con base en los resultados, se presentarían algunas consideraciones. La ENCS se evaluó con base en dos pautas:

a) A partir de la comparación de la ENCS con la Agenda de Ciberseguridad Global (GCA) de la UIT, al ser el marco de referencia que expresa el estándar más aceptado, a nivel global, para construir y evaluar estrategias de ciberseguridad.
b) Se cotejaron los ocho ejes que menciona la propia ENCS, con las acciones que se han realizado sobre ciberseguridad de noviembre de 2017 hasta octubre de 2018, correspondientes a cada uno de dichos ejes.

La GCA se justificó como el marco de referencia internacional más sólido y aceptado, tanto en su concepción como en su alcance. Ya que la UIT es la instancia internacional pionera en estrategias de ciberseguridad y cuenta con la participación de expertos en la materia y de múltiples actores. Enseguida, se aplicó el

comparativo, mostrando de qué manera los principios, objetivos y ejes transversales de la ENCS se relacionan y hasta qué punto son aplicables a las recomendaciones de la GCA. Se concluía una evaluación sobre el planteamiento de cada fundamento de la ENCS, la cual coincidía con la otorgada para México en el GCI.

La primera parte de la evaluación de la ENCS contrastaba claramente con la GCA. Sin embargo, la ENCS no está basada en la GCA, por lo que era necesario hacer una extracción de conceptos para examinarlos con base en un marco de referencia internacional. Eso permitió comprender a cabalidad la razón de la calificación de México en el GCI de 0.66, misma que coincidía con las observaciones realizadas en la investigación, una valoración estimada apenas por encima de la media de lo que serían las mejores prácticas en ciberseguridad a nivel internacional.

De manera general, en la primera parte de la evaluación fue posible resaltar la finalidad de llevar el tema a todos los actores y sectores, así como la intención de fortalecer al Estado mexicano en diversos rubros para lograr una sociedad que madure en su cultura de ciberseguridad, instituciones sólidas que puedan prevenir y responder a los riesgos, así como el fortalecimiento de la ciberresiliencia. Pero no se presentan líneas de acción más concretas, no se propone específicamente la creación de una estructura organizacional, no se nombra responsable a ninguna instancia o persona de ejecutarla y evaluarla, no hay una propuesta seria de una ley de ciberseguridad de alcance general y no se establecen indicadores u objetivos medibles como lo recomienda la UIT.

Como última instancia, se aplicó un segundo elemento de análisis para evaluar la implementación de las acciones indicadas en la Estrategia. Se cotejaron los ocho ejes transversales, con las actividades, gestiones, operaciones y labores correspondientes a cada uno de dichos ejes. Así se podría establecer, en los hechos, que tan efectiva había sido la aplicación de la ENCS, desde que se publicó en noviembre de 2017, hasta el cierre de la investigación, en octubre de 2018.

Al final del análisis de cada eje transversal, se le asignaba una calificación, que permitía establecer un valor cuantitativo a la evaluación, basado en las diferencias identificadas entre las propuestas de la ENCS y la ejecución de las actividades relativas a dicho eje. La calificación dependía de qué tan empatadas

eran las actividades con respecto al documento, mientras más alejadas estaban entre sí, el balance era negativo, mientras más cercanas la evaluación era positiva. El numero para calificar, al igual que en la GCA, estaba en una escala de 0 a 1, hasta decimal y centesimal. Entonces, se fue evaluando la ejecución de los ocho ejes.

Después de repasar las acciones relacionadas con cada eje transversal, se aplicó la fórmula de la media aritmética, para obtener la calificación sobre la implementación de la ENCS en el periodo mencionado. Se sumaron los valores asignados a cada eje y ese resultado se dividió entre el total de datos:

0.20 + 0.75 + 0.80 + 0.10 + 0.70 + 0.70 + 0.30 + 0.50 = **4.05**

4.05 / 8 = **0.50625**

Por lo tanto, la calificación asignada, en la presente investigación, para la implementación de la ENCS resultó ser de **0.50**, en una escala de 0 a 1.

Ahora se tenían dos calificaciones de cada una de las pautas para evaluar:

- ✓ Calificación con respecto a la GCA **0.66**
- ✓ Calificación sobre la implementación de la ENCS **0.500625**

Como se explicó, el análisis generaría una calificación que representaría, de forma cuantitativa, la evaluación general de la ENCS. Para llegar a este valor numérico se volvió a aplicar la fórmula de la media aritmética:

0.50625 + 0.66 = **1.16625**

1.16625 / 2 = **0.583125**

De este resultado, se tomaron el decimal y el centesimal. Por tanto, la calificación general que se le asignaba a la Estrategia Nacional de Ciberseguridad en México era de **0.58**, en una escala de 0 a 1. Ese es el valor numérico que representaba la evaluación realizada en la presente investigación.

Así finalizaba la evaluación aplicada en el último capítulo. La calificación final revelaba que la ENCS tiene una ejecución medianamente satisfactoria, su nivel de desempeño resulta insuficiente para lograr el objetivo que la misma Estrategia se plantea, de fortalecer 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.

Era notable el contraste que hay entre la concepción de la propia ENCS, comparada con la GCA, y de las indicaciones propuestas en los ejes transversales, cotejadas con las acciones implementadas. Había puntos donde la ENCS era más acertada y otros donde hay una distancia considerable entre el ser y deber ser. De esta manera se distinguía entre el discurso y los hechos concretos enmarcados en la ENCS, con base en un modelo de análisis comparativo y una visión alejada del reduccionismo y el determinismo tecnológico.

Lograr generar un valor numérico permite concluir que un 58% de efectividad en su implementación resulta ser un porcentaje de éxito sucinto y poco loable para un tema que ha incrementado en magnitud e importancia en lo últimos años en México, en la región y a nivel global, como la ciberseguridad.

Al examinar cada punto, se generó, en primera instancia, una evaluación individual, esto reveló qué tan cercana está la concepción y ejecución de cada eje y ayudó a identificar los rubros donde se ha podido trabajar con certidumbre, aquellos donde se tienen que redoblar esfuerzos y unos más donde, incluso, se deberían replantear los objetivos y las acciones. Un examen bajo este procedimiento coadyuva en la afinación de las recomendaciones y parámetros de medición que permitan una ejecución más adecuada de una política pública con la importancia que pretende tener la ENCS. En tres ejes el contraste es significativo, la evaluación es sumamente negativa, mientras que sólo en dos puntos se supera el 75% de efectividad en su implementación. Del promedio y la evaluación general se pudo determinar que está por encima de la media, pero no se alcanza una calificación satisfactoria; al no tener más del 60% de valoración positiva, se puede considerar que la ENCS está reprobada.

No obstante, tener una revisión en lo global y en lo específico de la ENCS, podría coadyuvar en su mejoramiento, puesto que, en los rubros donde se ha trabajado de manera fluida y eficaz, se pueden afinar o continuar las acciones para consolidar esfuerzos, pero donde se tiene un desempeño negativo, buscar redoblar o incluso replantear metas y procedimientos (el eje 4 es muestra de esto último).

Con base en el objeto de estudio trazado, la investigación se propuso responder la siguiente pregunta: ¿cuál ha sido el nivel de desempeño del Estado mexicano en materia de ciberseguridad durante el presente sexenio y de qué manera el enfoque de los estudios CTS permite realizar una evaluación integral sobre el desarrollo de la Estrategia Nacional de Ciberseguridad?

Para dar respuesta, la hipótesis que se planteó formulaba que, a través del enfoque de los estudios CTS, se puede establecer que la Estrategia Nacional de Ciberseguridad en México está basada en una visión determinista de los fenómenos tecnológicos, por lo que es necesario realizar un viraje analítico para ejecutar un diagnóstico y evaluación sobre las condiciones actuales de la ciberseguridad, es por eso que no se han podido desplegar ni desarrollar, hasta el momento, de manera óptima las líneas de acción planteadas en la Estrategia.

Después de revisar los postulados de los estudios CTS, de conocer a fondo lo que significa el ciberespacio para la sociedad internacional y de las implicaciones globales de la ciberseguridad, se pudo diagnosticar y evaluar a la ENCS y, al obtener los resultados de dicha evaluación, se sometió a consideración la hipótesis planteada, demostrando la pertinencia de dicha idea, previamente planteada.

La comprobación de la hipótesis permite concluir, de manera general, que para brindar confianza al ciberespacio que requiere en un país en desarrollo como México, es necesario dar un viraje a la concepción de la Estrategia, para dejar de lado los determinismos y la idea lineal de la consecución del progreso y desarrollo de una sociedad a través de la inserción de realizaciones técnicas o de políticas que no surgen de la sociedad misma.

Se recomienda constituir una visión integral de ciberseguridad, que incluya a todos los actores y factores nacionales e internacionales que interactúan y se ven afectados de las relaciones en el quinto entorno, de esa manera se podrán generar las perspectivas y condiciones adecuadas para integrar una agenda de ciberseguridad que permita el desempeño óptimo de una estrategia nacional en la materia durante el próximo sexenio.

Es importante reiterar que la ciberseguridad no es un fin en sí misma, sino un medio, con el objetivo de construir la confianza en el ciberespacio; con la meta de

asegurar que la infraestructura de la información funcionará de forma fiable incluso cuando esté bajo amenaza. Por lo que la evaluación permite observar que el bajo desempeño en la ejecución de la ENCS se aleja del fin último, que es brindar protección y confianza al mexicano que interactúa socialmente en el ciberespacio.

Mantener un ciberespacio protegido, gestionando los riesgos, salvaguardado de amenazas y reforzando la resistencia y resiliencia ante ataques, implica que la promoción de la ciberseguridad debe estar en altos niveles de prioridad para los gobiernos, el sector privado, el ámbito académico, las asociaciones civiles y las familias mexicanas en general, sobre todo cuando casi 80 millones de mexicanos pasan más de una tercera parte de sus días internados en el ciberespacio.

Asimismo, debe señalarse que, si bien la ENCS en México no tiene un porcentaje de desempeño satisfactorio, desde su publicación a la fecha (12 meses), se han realizado acciones más enfocadas, se han incluido a más actores y se le ha destinado mayores recursos, lo cual demuestra una ruta que puede lograr avances significativos en un par de años.

El hecho de que se hayan organizado cuatro ediciones de la Semana Nacional de Ciberseguridad; la suscripción de distintos convenios con asociaciones civiles, instancias gubernamentales y empresas del ramo de la seguridad informática y las telecomunicaciones; los pasos para homologar estándares y criterios de medición; la implementación de acciones enfocadas en la creación de capacidades; entre otras actividades significativas; demuestran que la conciencia sobre la promoción de la ciberseguridad es creciente y ha tomado una relevancia a los más altos niveles de los tomadores de decisiones. Se considera que es cuestión de tiempo para que muchos de estos esfuerzos se consoliden, que sin duda suman para lograr el objetivo de la generación de confianza en el ciberespacio.

Respecto al documento de la ENCS, se puede concluir que ésta es un marco general, no un manual de acciones y estándares, por lo que resulta ser flexible en su aplicación, pero también permite muchas generalidades, incluso ambigüedades, que podrían poner en riesgo su ejecución pensando en un largo plazo, como política de Estado, de alcance transexenal.

Relativo a lo anterior, hay un último e importante factor que mencionar, la presente investigación se da en un periodo de transición política en México. La evaluación realizada a la ENCS cobra importancia porque revela cómo se ha manejado el tema en todo un sexenio y puede ser referente para el periodo del presidente Andrés Manuel López Obrador (2018-2024), de quien no se ha conocido –hasta el momento- una propuesta concreta en materia de ciberseguridad; por lo que el documento de la ENCS puede tener continuidad, ser descartado o ser tomado como referencia para la construcción de una agenda de ciberseguridad o una nueva estrategia, que incluya mayor apoyo de los diferentes sectores sociales.

En este trabajo se considera que un análisis integral de la ciberseguridad debe estar influenciado por elementos sociales y que los diversos intereses de los grupos humanos desempeñan un papel importante en el momento de tomar una decisión sobre ella. Por lo tanto, una estrategia efectiva para brindar confianza en el ciberespacio debe estar influenciada en su diseño, desarrollo, apropiación e implementación, por los distintos sectores sociales y por los elementos no humanos suficientes para su ejecución eficaz.

El objetivo general de la presente investigación era realizar un diagnóstico y una evaluación integral sobre la Estrategia Nacional de Ciberseguridad en México durante el periodo 2017-2018, a través del enfoque de estudios en Ciencia, Tecnología y Sociedad. Este propósito se cumplió al utilizar dos pautas referenciales para evaluarla, así como hacer observaciones puntuales en cada pilar y en cada eje transversal, sobre cómo un enfoque integral –basado en la visión de los estudios CTS- podría dar un viraje sustancial a la ENCS, tanto en su concepción como en su implementación, que se traduciría en una asimilación de la propia Estrategia en la sociedad mexicana. Dadas estas consideraciones, se concluye la investigación señalando que se ha cumplido el objetivo general que se proyectó.

Fuentes de consulta.

- Bijker Wiebe, *Of Bicycles, Bakelite and Bulbs. Toward a Theory of Sociotechnical Change*. Cambridge, The MIT Press, 1997, 380 pp.
- Cadena Gustavo et al, *Administración de proyectos de innovación tecnológica*, Gernika, 1986, México, 149 pp.
- Candau Romero Javier, *Estrategias nacionales de ciberseguridad. Ciberterrorismo*, en "Ciberseguridad. Retos y amenazas a la seguridad en el ciberespacio", Instituto Español de Estudios Estratégicos, Madrid,cfebrero 2011, pp. 257-322.
- Casas Rosalba, *Los estudios sociales de la ciencia y la tecnología: enfoques, problemas y temas para una agenda de investigación*, en Santos Corral, María Josefa (Coord), "Perspectivas y desafíos de la educación, la ciencia y la tecnología", UNAM, México, 2003, pp. 139-196.
- Clarke Richard A. y Knake Robert, *Cyber War: The Next Threat to National Security and What to Do About It Paperback*, Harper Collins, Estados Unidos, 2010, 320 pp.
- Cutcliffe Stephen, *Ideas máquinas y valores: los estudios de ciencia tecnología y sociedad,* Anthropos-UAM, España, 2003, 228 pp.
- Davara Miguel Ángel, *Fact Book del Comercio Electrónico*, Ediciones Arazandi, Segunda Edición, Pamplona, 2002, 1065 pp.
- Díaz Rodrigo y Lee Marta, *La innovación tecnológica: dos aproximaciones teóricas en competencia*, Roberto Varela (ed.), Prospectiva social y revolución científico-tecnológica, UAM, México, pp. 55-73.
- Freeman Christopher, John Clark y Luc Soete, U*nemployment and technical innovation: a study of long waves and economic development,* Editorial Burns & Oates, Estados Unidos, 1982, 214 pp.
- Ganuza Néstor, *La situación de la ciberseguridad en el ámbito internacional y en la OTAN*, Instituto Español de Estudios Estratégicos, Madrid, febrero 2011, pp. 165-214.
- Gibson William, *Neuromante*, Editorial Minotauro, España, 1984, 271 pp.

- Hope Alejandro y López Aranda Jaime, *La mentada estrategia. Dos ensayos y treinta y nueve preguntas sobre seguridad, justicia, violencia y delito*, primera edición, Senado de la República, México, julio 2015, 110 pp.
- Horton Dave, Rosen Paul y Cox Peter, *Cycling and society*, Reino Unido, Ashgate Publishing Company, 2007, 222 pp.
- Joyanes Aguilar Luis, *El estado del arte de la ciberseguridad*, Instituto Español de Estudios Estratégicos, Madrid, febrero 2011, pp. 11-46.
- Latour Bruno, *La ciencia en acción. Cómo seguir a los científicos e ingenieros a través de la sociedad*, traducción de Eduardo Aibar, Roberto Méndez, Estela Ponisio, editorial Labor, España, 1992, 278 pp.
- Latour Bruno, *La esperanza de Pandora. La realidad de los Estudios de la Ciencia*, traducción de Tomás Fernández Aúz, editorial Gedisa, España, 2001, 384 pp.
- Levy Pierre, *Cibercultura, sociedad de la información y conocimiento*, en "Cibercultura. La cultura de la sociedad digital", Barcelona, Anthropos-UAM, 2007, 230 pp.
- Marquina Lourdes, *Gobernanza global del comercio en Internet*, Primera edición, INAP, México, 2012, 393 pp.
- Medellín Enrique, *Construir la innovación: Gestión de tecnología en la empresa*, Siglo XXI editores, México, 2013, 258 pp.
- Merle Marcel, *Sociología de las Relaciones Internacionales*, versión española de Roberto Mesa, Alianza editorial, 1991, 592 pp.
- Moss Rosabeth, *The change master: Innovations for productivity in the American Corporation*, Editorial Simon & Schuster, Estados Unidos, 1983, 432 pp.
- Newton-Small, Jay, *Why The Deep Web Has Washington Worried*, en Revista "Time", Vol. 182, No. 20, Time Inc., Nueva York, 11 de noviembre de 2013, pp. 26-30.

- Pérez Salazar Gabriel, *Hacia una tecnología socialmente significativa,* en Santos, M. J. y De Gortari, R. (coords.), Computadoras e Internet en la biblioteca pública mexicana, México, UNAM – IIS – Pearson, 2009, pp. 3-28.
- Pinch Trevor J., Bijker Wiebe E. y Hughes Thomas P., *The Social Construction of Technological Systems. New Directions in the Sociology and History of Technology*, MIT Press, Estados Unidos, 198, 470 pp.
- Quintana Solórzano Fausto, *El reto de la incorporación de nuevos temas en el estudio de Relaciones Internacionales*, en Revista de Relaciones Internacionales, UNAM, No. 109, enero-abril de 2011, pp. 145-153.
- Quintanilla Miguel Ángel, *Tecnología: Un enfoque filosófico y otros ensayos de filosofía de la tecnología*, Fondo de Cultura Económica, México, 2005, 295 pp.
- Roberts Edward, *Gestión de la Innovación Tecnológica,* Clásicos COTEC 1, Madrid, 1996, 426 pp.
- Santos Corral María Josefa (Coord), *Perspectivas y desafíos de la educación, la ciencia y la tecnología*, México, UNAM, 2003, 405 pp.
- Santos Josefa y Díaz Rodrigo, *El análisis del poder en la relación tecnología y cultura: una Perspectiva Antropológica*, en Santos Corral, M. J. (coord.), "Perspectivas y desafíos de la educación, la ciencia y la tecnología", México, IIS-UNAM, 2003, pp. 335-402.
- Santos María Josefa y Lopátegui Marco Antonio, *La Construcción Global de la Ciencia y la Tecnología Bajo la Lupa de los Enfoques CTS*, en Castañeda, Dávila y Morales (Coord), "El futuro de las ciencias sociales en un entorno social globalizado", UNAM, México, 2017, pp 251-260.
- Schmookler Jacob, *Invention and economic growth*, Harvard University Press, Estados Unidos, 1990, 332 pp.
- Schumpeter Joseph, *Capitalismo, socialismo y democracia*, edición en español, Ediciones Folio, Barcelona, 1996, 308 pp.
- Schumpeter Joseph, *Teoría del desenvolvimiento económico*, Edición en español, Quinta Reimpresión, Fondo de Cultura Económica, México, 1978, 256 pp.

- Severance Charles, *Alan Turing and Bletchley Park*, Revista Computer, vol. 45, junio de 2012, pp. 6-8.
- Téllez Julio*, Derecho Informático*, 2ª. Ed, Mc Graw Hill, México, 1996, 744 pp.
- UIT, *ITU Global Cybersecurity Agenda* (GCA), High-Level Experts Group (HLEG), Suiza, 2007.
- Unión Europea*, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Comunicado conjunto al Parlamento Europeo, el Consejo, el Comité Económico y Social Europeo y la Comunidad de Regiones, Bruselas, 2013.
- Vaccarezza Leonardo, *El campo CTS en América Latina y el uso social de su producción*, CTS: Revista iberoamericana de ciencia, tecnología y sociedad, Vol. 1, Nº. 2, 2004, pp. 211-218.
- Valderrama Andrés, *Teoría y crítica de la construcción social de la tecnología*, en Revista Colombiana de Sociología, No. 23, Bogotá, 2004, 217-233 pp.
- Wiener Norbert, *Cybernetics or control and communication in the animal and the machine*, The MIT press, second edition, Cambridge, Massachusetts, 1948, 212 pp.

CIBEROGRAFÍA

- Al Momento MX (Redacción), *México en busca de la Secretaría TIC y Ley de ciberseguridad*, 30 de enero de 2018, consultado en: almomento.mx/mexico-en-busca-de-la-secretaria-tic-y-la-ley-de-ciberseguridad/ [agosto 2018]
- Asociación de Internet Mx, *Banca electrónica 2013*, México, 2013, consultado en: https://www.amipci.org.mx/estudios/banca_por_internet/Banca_Electronica_2013_VP.pdf[septiembre 2018]
- Asociación de Internet Mx, *Estudio Comercio Electrónico en México 2015*, en asociaciondeinternet.mx, México, 2015, consultado en: https://amipci.org.mx/estudios/comercio_electronico/Estudio_de_Comercio_Electronico_AMIPCI_2015_version_publica.pdf [septiembre 2018]

- Asociación de Internet MX, *14° Estudio sobre los Hábitos de los Usuarios de Internet en México 2018*, Ciudad de México, mayo de 2018, consultada en: https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/14-Estudio-sobre-los-Habitos-de-los-usuarios-de-Internet-en-Mexico-2018/lang,es-es/?Itemid= [octubre 2018]
- Banco Mundial, *Datos México*, en World Bank Group, consultado en: https://datos.bancomundial.org/pais/mexico [septiembre 2018]
- Bárcena Alicia, *Innovación para el Desarrollo: Reflexiones desde América Latina y el Caribe*, en Sitio Oficial de CEPAL, 2011, consultado en: http://www.cepal.org/noticias/paginas/8/33638/innovacionparaeldesarrollo.pdf [abril 2018]
- BBC [Redacción*], El virus que tomó control de mil máquinas y les ordenó autodestruirse*, BBC, sección IWonder, 11 de octubre 2015, consultado en: http://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet [agosto 2017]
- Bucio Rafael y Laguna Jocsan,*La Ciberseguridad Industrial en México*, Centro de Ciberseguridad Industrial, México, consultado en: https://www.cci-es.org/detalle-congreso?p_p_id=101&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_101_struts_action=%2Fasset_publisher%2Fview_content&_101_assetEntryId=349146&_101_type=content&_101_urlTitle=mexico [agosto 2018]
- Bumgarner John, *US Cyber Consequences Unit*, Jane's Defence Weekly, Chief Technology Officer, 29 de septiembre de 2010, consultado en: www.jdw.janes.com, [junio 2015]
- Bunster Álvaro, *El crimen organizado frente al derecho*, en "Boletín Mexicano de Derecho Comparado", IJJ-UNAM, año XXIX, num. 87, México, 1998, 769 pp., consultado en: http://biblio.juridicas.unam.mx/revista/pdf/DerechoComparado/87/art/art1.pdf, [agosto 2015]
- CANIETI, *Evaluación de la Ciberseguridad en México: brechas y recomendaciones en un mundo híper-conectado*, Reporte final de

Ciberseguridad (iniciativa privada y asociación civil), Ciudad de México, 6 de septiembre de 2017, 167 pp., consultado en: https://docplayer.es/65552142-Evaluacion-de-la-ciberseguridad-en-mexico-brechas-y-recomendaciones-en-un-mundo-hiper-conectado.html [enero 2018]

- Cárdenas Guzmán Guillermo, *Ciberacoso*, en revista "Cómo ves" en línea, UNAM, México, 2012, consultado en: http://www.comoves.unam.mx/numeros/articulo/197/ciberacoso [septiembre 2015]
- Cassou Ruiz Jorge, Delitos informáticos en México, consultado en: https://www.ijf.cjf.gob.mx/publicaciones/revista/28/Delitos_inform%C3%A1ticos.pdf
- CCM Benchmark Group, *Introducción a los ataques por denegación de servicio*, en ccm.net, consultado en: http://es.ccm.net/contents/22-ataque-por-denegacion-de-servicio [septiembre 2015]
- Ciberacoso.net, *Qué es el ciberacoso*, en ciberacoso.net, consultado en: http://www.ciberacoso.net/definicion.html [septiembre 2015]
- Cisco Systems, *2014 Midyear Security Report*, sitio web Cisco Systems Company, San Francisco, 2014, consultado en: http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html [marzo 2015]
- CISCO SystemsInc, *Spam Overview*, CISCO, Estados Unidos, 2016, consultado en: https://www.senderbase.org/static/spam/#tab=4 [junio 2018]
- Cisneros Inés, et. al; *¿Sociedad de la información o sociedad del conocimiento?*, consultado en: http://tecnologiaedu.us.es/edutec/paginas/43.htm [abril 2017]
- CNC, *PF y TELMEX-SCITUM fortalecen la cooperación entre instituciones públicas y privadas en torno a la seguridad informática*, prensa CNS, México,boletín 707/17, 17 de noviembre de 2017, consultado en: https://www.gob.mx/cns/prensa/pf-y-telmex-scitum-fortalecen-la-cooperacion-entre-instituciones-publicas-y-privadas-en-torno-a-la-seguridad-informatica-164392?idiom=es[julio 2018]

- CNS, *Académicos y Policía Federal debaten sobre el estudio e investigación policial en materia de ciberseguridad*, en cns.gob.mx, Comisión Nacional de Seguridad, Comunicado de Prensa No. 705, México, 28 de Octubre de 2015, consultado en: http://www.cns.gob.mx/portalWebApp/appmanager/portal/desk;jsessionid=13GWWxdKGR1n095M0Rfj1x1GVhQ1V1qW0nzvYzPVG0cpXR8y9MTX!-1153552922?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1398180 [julio 2018]
- CNS, *Fortalece CNS estrategias para la protección del ciberespacio mexicano,* en cns.gob.mx, Comisión Nacional de Seguridad, comunicado de prensa no.32, México, 25 de febrero de 2015, consultado en: http://www.cns.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1368028 [agosto 2018]
- CNS, I*mpulsan Policía Federal y Microsoft México seguridad informática y prevención de delitos cibernéticos*, en cns.gob.mx, Comisión Nacional de Seguridad,Boletín de prensa No. 119, México, 5 de agosto de 2014, consultado en: http://cns.gob.mx/portalWebApp/portal/movil.portal?_nfpb=true&_pageLabel=portal_movil_portal_contenido&content_id=1344173#wlp_portal_movil_portal_contenido [julio 2018]
- CNS, *La Comisión Nacional de Seguridad inaugura campaña de concientización en "Ciberseguridad México 2018"*, prensa de la CNS, boletín 103/18, México, publicada 28 de febrero de 2018, consultado en: https://www.gob.mx/cns/prensa/la-comision-nacional-de-seguridad-inaugura-campana-de-concientizacion-ciberseguridad-mexico-2018-164033?idiom=es [julio 2018]
- CNS, *Policías de América estrechan lazos de cooperación contra el crimen durante la VII Cumbre AMERIPOL*, en cns.gob.mx, Comisión Nacional de Seguridad, Comunicado de Prensa No.168, México, 9 de agosto de 2014, consultado en:

http://www.cns.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=true&_pageLabel=portals_portal_page_m3p2_boletin&id=1348081 [julio 2018]

- CNS, *Policía Federal detecta intentos de extorsión cibernética*, en cns.gob.mx, Comisión Nacional de Seguridad, Comunicado de prensa No. 31, México, 23 de febrero de 2015, consultado en: http://www.cns.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1368028 [septiembre 2018]
- CNS, *Policía federal suma sus capacidades tecnológicas a los esfuerzos internacionales liderados por la ONU para proteger los derechos y el patrimonio de los ciudadanos*, en cns.gob.mx, Comisión Nacional de Seguridad, Comunicado de prensa No. 169, México, 10 de agosto de 2014, consultado en: http://www.cns.gob.mx/portalWebApp/appmanager/portal/desk;jsessionid=qxLTTzpNmsQGD0nBMtCvbgGJwHpnBGT1SnLGknpbYL4vzZ6JQpWG!432963533?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1348094[julio 2018]
- Comisión Europea, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace Brussels*, Unión Europea, Bruselas, 7 de febreo de 2013, consultado en: https://ec.europa.eu/digital-single-market/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security [diciembre 2017]
- Comisión Europea*, Glosario y Acrónimos en sociedad de la información*, Sitio oficial European Comission, consultado en: http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c. [agosto 2017]
- Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, en Agencia Española de Protección de Datos, Budapest, 23 de noviembre de 2001, consultado en: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF [julio 2015]

- Contreras Santos Georgina, *Ciberespacio y Educación*, Organización de Estados Iberoamericanos, IBERCIENCIA, Comunidad de Educadores para la Cultura Científica, 31 de marzo de 2015, consultado en: https://www.oei.es/historico/divulgacioncientifica/?Ciberespacio-y-Educacion [abril 2017]
- Control Risks, *CyberThreatstotheMexicanFinancial Sector*, 21 de diciembre de 2016, consultado en: https://www.controlrisks.com/en/services/security-risk/cyber-threats-to-the-mexican-financial-sector [junio 2018]
- Cram Bestor y Majoros Mike, *Weapons of mass disruption (Amenaza cibernética*), Documental en línea, producido por Nothern Light Productions, trasmitido por Odisea Channel, Washington D. C., 2011, consultado en: https://www.youtube.com/watch?v=nWXQacWRn5I [enero 2015]
- Cyberseguridad.net, *Ataques de denegación de servicio (DoS) (Ataques Informáticos III)*, en Cyberseguridad.net, España, 29 de junio de 2012, consultado en: http://cyberseguridad.net/index.php/197-ataques-de-denegacion-de-servicio-dos-ataques-informaticos-iii [septiembre 2015]
- Cyberseguridad.net, *Las estafas más habituales en la red*, en Cyberseguridad.net, 26 de enero de 2015, consultado en: http://cyberseguridad.net/index.php/408-las-estafas-mas-habituales-en-la-red [septiembre de 2015]
- De Solla Derek J., *Price, Little Science, Big Science… and Beyond*, Columbia University Press, Nueva York, 1986, consultado en: http://www.andreasaltelli.eu/file/repository/Little_science_big_science_and_beyon .pdf [11 de enero de 2016].
- ECPAT International, *Monitoreo global de las acciones en contra de la explotación sexual comercial de niños, niñas y adolescentes*, Saladaeng Printing Co.Ltd, México, 2006, 27 pp., consultado en: http://www.derechosinfancia.org.mx/Global%20Monitoring%20Report-MEXICO.pdf [septiembre 2015]
- El Financiero (Redacción), *10 puntos para entender la nueva Ley Fintech*, en sitio oficial El Financiero, 1 de marzo de 2018, Ciudad de México, consultado

en: http://www.elfinanciero.com.mx/empresas/diez-puntos-para-entender-la-nueva-ley-fintech [septiembre 2018]

- Estados Unidos Mexicanos, *Código Penal Federal*, en info4.juridicas.unam, vigente desde 1931, consultado en: http://info4.juridicas.unam.mx/ijure/tcfed/8.htm?s [septiembre 2018]
- Fayad Omar, *Iniciativa con proyecto de decreto por el que se expide la Ley federal para prevenir y sancionar los delitos informáticos*, en sil.gobernacion.gob.mx, Senado de la República, México, 27 de octubre de 2015, consultado en: sil.gobernacion.gob.mx/Archivos/Documentos/2015/10/asun_3291220_20151027_1445523938.pdf [agosto 2018]
- Fernández Laura, "*Me quedé corto cuando definí el ciberespacio. Nunca pensé que serviría para cotillear",* entrevista a William Gibson para Vanity Fair, 27 de abril de 2012, consultado en: https://www.revistavanityfair.es/poder/articulos/el-futurismo-de-william-gibson/16450 [diciembre 2017]
- Forsyth James, *Structural Causes and Cyber Effects. Why International Order is Inevitable in Cyberspace?*, Strategic Studies Quaterly-The Air University, Alabama, 2014, consultado en: http://www.au.af.mil/au/ssq/digital/pdf/winter_14/forsyth.pdf [junio 2015]
- Garavilla Miguel Estrada, *Delitos Informáticos*, en Universidad Abierta Université de Freibourg, 2013, consultado en: https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf [agosto 2015]
- Gobierno de la República, *Estrategia Nacional de Ciberseguridad*, en www.gob.mx, México, noviembre de 2017, 30 pp., consultado en: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf [diciembre 2017]
- Gobierno de la República, *Programa para la Seguridad Nacional 2014 - 2018 del Estado mexicano*, en dof.gob.mx, Gobierno de la República, México, 30 de abril de 2014, consultado en:

http://www.dof.gob.mx/nota_detalle.php?codigo=5342824&fecha=30/04/2014&print=true [mayo 2018]

- Gobierno de la República*, Plan Nacional de Desarrollo 2013-2018,* Gobierno de la República, México, 2013, consultado en: http://pnd.gob.mx/ [mayo 2018].
- Gobierno de la República, *Reforma en materia de Telecomunicaciones*, Presidencia de la República 2012-2018, consultado en: http://reformas.gob.mx/reforma-en-materia-de-telecomunicaciones/que-es[julio 2018]
- Gobierno de México, *Estrategia Digital Nacional*, Gobierno de la Republica, México, 2013, consultado en: http://www.presidencia.gob.mx/edn/#descargas [diciembre 2017]
- Google, *En qué creemos*, en línea, Sitio oficial de Google Google (acerca de), consultado en: https://www.google.com.mx/intl/es/about/company/philosophy/ [marzo 2018]
- IBM, *The Net Result: Social Inclusion in the Information Society,* Special Report IBM, Reino Unido, 1997, 71 pp., consultado en: http://www.local-level.org.uk/uploads/8/2/1/0/8210988/netresult.pdf [marzo 2018]
- ITU, *Global Cybersecurity Index 2017*, en uit.org, Unión Internacional de Telecomunicaciones-ABI research, 2017, consultado en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
- ITU, *ITU National Cybersecurity Strategy Guide*, 2012, Ginebra, Suiza, 119 pp., consultado en: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf [agosto 2015]
- Jiménez Andrés, *La delincuencia organizada en el ciberespacio, en el marco de la sociedad de la información y el conocimiento: la estrategia de ciberseguridad en México (2013-2015),* FCPyS-UNAM, México, 2016, 210 pp., consultada en: http://132.248.9.195/ptd2016/octubre/0751124/Index.html [diciembre 2017]

- Jiménez Becerra Javier, *Origen, desarrollo de los estudios CTS y su perspectiva en América Latina*, FLACSO, Publicado en "Ciencia, política y poder. Debates contemporáneos desde Ecuador", Edición electrónica, noviembre 2010, Ecuador, consultado en: https://www.researchgate.net/publication/259043117_Origen_desarrollo_de_los_estudios_CTS_y_su_perspectiva_en_America_Latina [abril 2018]
- Lessig Lawrence, *El Código 2.0*, Cambridge, Basic Books, Reino Unido, 2006, 563 pp., consultado en: http://www.articaonline.com/wp-content/uploads/2011/07/El-c%C3%B3digo-2.0-Lawrence-Lessig.pdf [diciembre 2017]
- Levy Pierre, *Cibercultura. Informe Al Consejo De Europa*, Anthropos Editorial, Universidad Autónoma Metropolitana, México, 2007, consultado en: https://Antroporecursos.Files.Wordpress.Com/2009/03/Levy-P-1997-Cibercultura.Pdf [diciembre 2017]
- Lira Arteaga Oscar, *Cibercriminalidad*, Instituto Nacional de Ciencias Penales, primera edición, México, 2010, 178 pp., consultado en: http://biblio.juridicas.unam.mx/libros/7/3169/15.pdf [septiembre 2015].
- Lynn III Wiliam, *Defending a New Domain. The Pentagon's Cyberstrategy*, en Revista *Foreign Affairs*, publicada por el Council on Foreign Relations, septiembre-octubre 2010, Estados Unidos, consultado en: https://www.foreignaffairs.com/articles/sunited-states/2010-09-01/defending-new-domain [abril 2015]
- Mahajan Romi, Administración de TI: La singularidad en la innovación, en Sitio oficial de Microsoft, consultado en: https://technet.microsoft.com/es-es/library/hh641413.aspx [marzo 2018]
- Molina Mateos José María, *Globalización, ciberespacio y estrategia especial. Consideración a la estrategia de la información,* boletín electrónico del Instituto Español de Estudios Estratégicos, Ministerio de Defensa [España], 12 septiembre de 2014, España, consultado en: http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO100-

2014_Globalizacion-CIberseguridad-Estrategia_JMMolinaMateos.pdf [enero 2018]

- Montoya Suárez Omar, *Schumpeter, Innovación y Determinismo Tecnológico*, Revista Scientia et Technica Año X, No. 25, agosto 2004, consultado en: https://dialnet.unirioja.es/descarga/articulo/4842897.pdf [junio 2018]
- Morales Eduardo y Rajsbaum Sergio, *Norbert Wiener y el origen de la cibernética*, en revista Ciencia, edición de enero-marzo de 2016, Academia Mexicana de Ciencias, México, consultado en: https://www.revistaciencia.amc.edu.mx/images/revista/67_1/PDF/Presentacion.pdf [marzo 2018]
- Naciones Unidas, *12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal*, Oficina contra la Droga y el Delito de Naciones Unidas, Salvador (Brasil), 12 a 19 de abril de 2010, 18 pp., consultado en: https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050385s.pdf [agosto 2015]
- Naciones Unidas, *13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal*, Oficina de Naciones Unidas contra la Droga y el Delito, Doha, 12 a 19 de abril de 2015, consultado en: https://www.unodc.org/documents/congress//Documentation/A-CONF.222-12_Workshop3/ACONF222_12_s_V1500666.pdf [octubre 2015]
- Naciones Unidas, *Estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno*, por el Grupo de expertos encargado de realizar un estudio exhaustivo del delito cibernético, Oficina contra la Droga y el Delito de Naciones Unidas, Viena, 23 de enero de 2013, 18 pp., consultado en https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_S.pdf [agosto 2015]
- Naciones Unidas, *Pornografía infantil: Relatora especial urge a adoptar legislación y proteger a víctimas*, en Centro de Noticias ONU, 16 de

septiembre de 2009, consultado en: http://www.un.org/spanish/News/story.asp?NewsID=16500#.Vp1iKCrhDIU [septiembre 2015]

- Naciones Unidas, *Science, technology and innovation and intellectual property rights: The vision for development*, En Sitio Oficial de Naciones Unidas, mayo 2012, 14 pp., consultado en: http://www.un.org/millenniumgoals/pdf/Think%20Pieces/11_ips_science_innovation_technology.pdf [abril 2018]
- Naider, *El tigre de la innovación ¿Por qué es Samsung una compañía tan innovadora?*, en Sitio Oficial de Naider, mayo 2017, consultado en: http://naider.com/por-que-es-samsung-una-compania-tan-innovadora/ [mayo 2018]
- Nájera Alejandro, *Inversión en ciberseguridad fundamental en la transformación digital*, en Info Security México, 7 de abril 2018, consultado en: https://infosecuritymexicoblog.com/2017/11/21/inversion-en-ciberseguridad-fundamental-en-la-transformacion-digital/
- National Security Presidential Directive, *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure*, Sitio Oficial de la Presidencia de Estados Unidos, consultado en: https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf [julio 2017]
- OCDE, *Declaración Ministerial sobre la Economía Digital: Innovación, Crecimiento y Prosperidad Social, s*itio oficial, centro de información de la OCDE, 23 de junio de 2016, consultado en: http://www.oecd.org/centrodemexico/medios/declaracion-ministerial-sbore-la-economia-digital.htm [abril 2018]
- OCDE*, La Estrategia de Innovación de la OCDE, Empezar Hoy el Mañana*, 2010, 240 pp., consultado en: http://www.foroconsultivo.org.mx/libros_editados/estrategia_innovacion_ocde.pdf [junio 2018]

- OEA, *Cybersecurity: Are We Ready in Latin America and the Caribbean?*, 2016, consultado en: http://caribbean.cepal.org/content/cybersecurity-are-we-ready-latin-america-and-caribbean [septiembre 2018]
- OEA, *Innovación y competitividad*, En Sitio Oficial de la OEA, 2008, consultado en: http://portal.oas.org/Portal/Topic/CienciaTecnolog%C3%ADaeInnovaci%C3%B3n/Programas/Innovaci%C3%B3nyCompetitividad/tabid/1535/Default.aspx [abril 2018]
- OEA, *México presentó Estrategia Nacional de Ciberseguridad desarrollada con apoyo de la OEA*, Organización de Estados Americanos, comunicado de prensa, 13 de noviembre de 2017, consultado en: http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-082/17 [marzo 2018]
- OECD, Understanding the digital divide, OECD Publications, 2001, consultado en: https://www.oecd.org/sti/1888451.pdf [consultado el 14 de noviembre de 2017]
- Parraguez Luisa, *TheStateofCybersecurity in Mexico: AnOverview*, Wilson Center, enero de 2017, consultado en: https://www.wilsoncenter.org/publication/the-state-cybersecurity-mexico-overview [junio 2018]
- Perry Barlow John*, A Declaration of the Independence of Cyberspace*, 8 de febrero de 1996, Davos, Suiza, consultado en: https://homes.eff.org/~barlow/Declaration-Final.html [agosto 2015]
- Pinch Trevor, *La construcción social de la tecnología: una revisión*, en Santos,M. J. Y Díaz Cruz, R. (compiladores), "Innovación tecnológica y procesos culturales. Nuevas Perspectivas Teóricas", Fondo de Cultura Económica, México, 1997, consultado en: https://es.scribd.com/document/140890763/Pinch-T-1997-La-construccion-social-de-la-tecnologia-una-revision [agosto 2016]
- Policía Federal, *Arranca la Tercera Edición de la Semana Nacional de Ciberseguridad de la Policía Federal, Fecha de publicación*, 12 de noviembre

de 2017, consultado en: https://www.gob.mx/policiafederal/prensa/arranca-la-tercera-edicion-de-la-semana-nacional-de-ciberseguridad-de-la-policia-federal [agosto 2018]

- Policía Federal, *Centro Nacional de Respuesta a Incidentes Cibernéticos de la Policía Federal*, sitio oficial PF, México, 17 de mayo de 2018, consultado en: https://www.gob.mx/policiafederal/articulos/centro-nacional-de-respuesta-a-incidentes-ciberneticos-de-la-policia-federal?idiom=es [agosto 2018]
- Policía Federal, *CNS, a través de la División Científica de la PF, instrumenta acciones ante ataque cibernético internacional*, prensa PF, boletín 320, México, 15 de mayo de 2017, consultado en: https://www.gob.mx/policiafederal/prensa/cns-a-traves-de-la-division-cientifica-de-la-pf-instrumenta-acciones-ante-ataque-cibernetico-internacional [agosto 2018]
- Policía Federal, *CNS-Policía Federal suma capacidades con Cisco Systems para prevenir y atender delitos cibernéticos en el país,* comunicado de la PF, México, 20 de marzo de 2017, consultado en: https://www.gob.mx/policiafederal/prensa/cns-policia-federal-suma-capacidades-con-cisco-systems-para-prevenir-y-atender-delitos-ciberneticos-en-el-pais [agosto 2018]
- Policía Federal,*CNS realiza Primer Coloquio de Ciberseguridad para Medios de Comunicación*, comunicado PF, México, 19 de julio de 2017, consultado en: https://www.gob.mx/policiafederal/prensa/cns-realiza-primer-coloquio-de-ciberseguridad-para-medios-de-comunicacion [agosto 2018]
- Policía Federal, *División Científica de la Policía Federal*, sitio oficial PF, México, 11 de julio 2018, consultado en: www.gob.mx/policiafederal/articulos/division-cientifica-de-la-policia-federal?idiom=es [septiembre 2018]
- Policía Federal, *Impulsa Policía Federal la creación del primer Comité de Ciberseguridad a nivel nacional*, prensa PF, 16 de noviembre de 2017, consultado en: https://www.gob.mx/policiafederal/prensa/impulsa-policia-

federal-la-creacion-del-primer-comite-de-ciberseguridad-a-nivel-nacional [septiembre 2018]

- Policía Federal, *PF clausura la 4ta. Semana Nacional de Ciberseguridad y suma esfuerzos con la Condusef para generar acciones de prevención*, prensa de la PF, boletín 548, 28 de octubre de 2018, consultado en: https://www.gob.mx/policiafederal/prensa/pf-clausura-la-4ta-semana-nacional-de-ciberseguridad-y-suma-esfuerzos-con-la-condusef-para-generar-acciones-de-prevencion?idiom=es [octubre 2018]
- Policía Federal, *PF se capacita para adquirir habilidades que permitan planear, desarrollar y ejecutar acciones que garanticen resultados exitosos*, prensa PF, 30 de julio de 2018, consultado en: https://www.gob.mx/policiafederal/prensa/policia-federal-se-capacita-para-adquirir-habilidades-que-permitan-planear-desarrollar-y-ejecutar-acciones-que-garanticen-resultados-exitosos?idiom=es [agosto 2018]
- Policía Federal, *Policía Federal pide a empresas de telefonía e Internet coordinar esfuerzos en beneficio de la Ciberseguridad*, comunicado PF, México, 16 de noviembre de 2017, consultado en: https://www.gob.mx/policiafederal/prensa/policia-federal-pide-a-empresas-de-telefonia-e-internet-coordinar-esfuerzos-en-beneficio-de-la-ciberseguridad [agosto 2018]
- Policía Federal, *Policía Federal realiza la cuarta edición de la Semana Nacional de Ciberseguridad*, prensa PF, boletín 540, México, 23 de octubre de 2018, consultado en: https://www.gob.mx/policiafederal/prensa/policia-federal-realiza-la-cuarta-edicion-de-la-semana-nacional-de-ciberseguridad [octubre 2018]
- Policía Federal, *Policía Federal y Condusef inauguran ciclo de conferencias en materia de Ciberseguridad*, prensa PF, México, 4 de mayo de 2018, consultado en: https://www.gob.mx/policiafederal/prensa/policia-federal-y-condusef-inauguran-ciclo-de-conferencias-en-materia-de-ciberseguridad?idiom=es [agosto 2018]

- Policía Federal, *Policía Federal y FBI suman capacidades, conforman grupo de fuerza para atender delitos de alto impacto*, comunicado PF, México, 8 de noviembre de 2017, consultado en: https://www.gob.mx/policiafederal/prensa/policia-federal-y-fbi-suman-capacidades-conforman-grupo-de-fuerza-para-atender-delitos-de-alto-impacto [agosto 2018]
- Policía Federal*, Policía Federal y la Secretaría de la Función Pública firman convenio en materia de ciberseguridad*, 25 de noviembre de 2017, consultado en: https://www.gob.mx/policiafederal/prensa/policia-federal-y-la-secretaria-de-la-funcion-publica-firman-convenio-en-materia-de-ciberseguridad [agosto 2018]
- Policía Federal*, Reúne CNS a las Unidades de Policía Cibernética del país y realiza la primera Sesión del Comité de Ciberseguridad*, México, 21 de abril de 2018, consultado en: https://www.gob.mx/policiafederal/prensa/reune-cns-a-las-unidades-de-policia-cibernetica-del-pais-y-realiza-la-primera-sesion-del-comite-de-ciberseguridad?idiom=es [agosto 2018]
- Policía Federal, *¡Cibernauta con Estrella!,* en sitio oficial de la PF, México, 16 de mayo de 2018, consultado en: https://www.gob.mx/policiafederal/articulos/cibernauta-con-estrella [julio 2018]
- PwC Mexico, *Cybersecurity in Mexico*, PwC, Mexico, 2015, consultado en: https://www.pwc.com/mx/es/knowledge-center/archivo/20150917-kc-cybersecurity.pdf [junio 2018]
- Real Academia Española, *Ciberespacio,* Diccionario en línea, consultado en: http://dle.rae.es/?id=98Wdd57&o=h [agosto 2017].
- Real Academia Española, *Cibernético, ca (definición),* diccionario en línea, consultado en: http://dle.rae.es/srv/fetch?id=98YYoXW [agosto 2017].
- Real Academia Española, *Internet*, consultado en: http://dle.rae.es/srv/fetch?id=LvskgUG [agosto 2017]
- Riley Michael y Robertson Jordan, *Ciberataque ruso en elecciones de EU es más grande de lo que se creía*, en Bloomberg, 13 de junio de 2017,

consultado en: http://www.elfinanciero.com.mx/mundo/ciberataque-ruso-en-elecciones-de-eu-es-mas-amplio-de-lo-que-se-creia [abril 2018]

- Ríos Juan José, *Derecho e Informática en México*, Instituto de Investigaciones Jurídicas UNAM, México, 1997, 44 pp., consultado en: https://archivos.juridicas.unam.mx/www/bjv/libros/1/147/5.pdf [agosto 2017]
- Spanish Oxford Dictionaries, *Cibernética (definición),* diccionario en línea, consultado en: https://es.oxforddictionaries.com/definicion/cibernetica [agosto 2017].
- Samsung, *Samsung: Innovando para el futuro*, en Sitio Oficial de Samsung, 26 de julio de 2017, consultado en: htts://news.samsung.com/ar/articulo-sobre-innovacion-parte-1-samsung-innovando-para-el-futuro [marzo 2018]
- Sánchez Gonzalo, *Temas candentes de la Ciberseguridad. Un nuevo espacio lleno de incógnitas*, por el CEO de PWC España, publicado por PWC España, 2015, consultado en: https://www.pwc.es/es/publicaciones/gestion-empresarial/assets/temas-candentes-ciberseguridad.pdf [abril 2016]
- Sánchez-Criado Tomás y Blanco Florentino, *Constructivismos ante el Reto de los Estudios de la Ciencia y la Tecnología*, publicado en AIBR, Revista de Antropología Iberoamericana, edición electrónica, No. Especial, noviembre-diciembre 2005, Madrid, Madrid, 43 pp., consultado en: http://www.aibr.org/antropologia/44nov/articulos/nov0519.pdf [mayo 2018]
- Spanish Oxford Dictionaries, *Espacio (definición),* diccionario en línea, consultado en: https://es.oxforddictionaries.com/definicion/espacio [agosto 2017].
- SSP, *Centro Nacional de Respuesta a Incidentes Cibernéticos CERT-MX*, Secretaría de Seguridad Pública, Coordinación para la Prevención de Delitos Electrónicos,México, 23 de marzo de 2012, consultado en: http://seguridad2012.politicadigital.com.mx/pdf/03.pdf[julio 2018]
- Symantec, *Bots y botnets: Una amenaza creciente*, en Norton.com, consultado en: http://mx.norton.com/botnet [septiembre 2015]

- Symantec, *Stuxnet*, en Symantec.com, *Symantec* Inc., Estados Unidos, 2015, consultado en: http://www.symantec.com/es/mx/page.jsp?id=stuxnet [septiembre 2015]
- Symantec, *Tipos de piratería*, en Symantec.com, consultado en: https://www.symantec.com/es/mx/about/profile/antipiracy/types.jsp [septiembre 2015]
- Symantec, *¿Qué es el crimen cibernético?*, en Norton.com, Symantec Inc., Estados Unidos, 2015, consultado en: http://mx.norton.com/cybercrime-definition/promo [agosto 2015]
- The Economist (redacción*), Cyberwar. War in the fifth domain*, en linea, The Economist, Reino Unido, 1 de junio de 2010, consultado en: http://www.economist.com/node/16478792 [febrero 2015]
- The Economist [redacción], *Defending the digital frontier, Special report on cyber-security*, 10 de julio de 2014, consultado en: https://www.economist.com/special-report/2014/07/10/defending-the-digital-frontier [enero 2018]
- The Economist [redacción], *How John Perry Barlow views his internet manifesto on its 20th anniversary*, entrevista a John Pery Barlow para The Economist, 8 de febrero de 2016, consultado en: https://www.economist.com/international/2016/02/08/how-john-perry-barlow-views-his-internet-manifesto-on-its-20th-anniversary [diciembre 2017]
- Tula Molina, Fernando; Giuliano, Héctor Gustavo, "La teoría crítica de la tecnología: revisión de conceptos", *Redes*, vol. 21, núm. 41, diciembre, 2015, 214 pp., Universidad Nacional de Quilmes, Buenos Aires, Argentina, consultado en: https://www.redalyc.org/pdf/907/90748415006.pdf.
- UIT, *El ciberdelito: guía para los países en desarrollo*, en División de Aplicaciones TIC y Ciberseguridad, Departamento de Políticas y Estrategias Sector de Desarrollo de las Telecomunicaciones de la UIT, abril de 2009, consultado en: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf [noviembre 2015]

- UIT, *Expertos de alto nivel determinan una hoja de ruta para la ciberseguridad*, en uit.int, Sala de prensa de la UIT, consultado en: http://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=06&ipage=05&ext=html [octubre 2015]
- UIT*, Global Cybersecurity Index 2017*, en uit.org, Unión Internacional de Telecomunicaciones-ABI research, 2017, 65 pp., consultado en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
- UIT, *Trabajar juntos para proteger la Sociedad mundial de la información: Agenda de la UIT sobre ciberseguridad global*, en itu.int, Sala de prensa de la UIT, consultado en: http://www.itu.int/net/pressoffice/backgrounders/itu/5-es.aspx#.VqUrXyrhDIU [octubre 2015]
- UIT, *Global Cybersecurity Index & Cyberwellness Profiles*, en itu.org, UIT-ABI research, Suiza, abril 2015, 515 pp., consultado en: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf [octubre 2018]
- UNESCO, *Observatorio Mundial de Lucha Contra la Piratería*, en unesco.org, consultado en: http://portal.unesco.org/culture/es/ev.php-URL_ID=39412&URL_DO=DO_TOPIC&URL_SECTION=201.html [septiembre 2015]
- UNICEF, *Explotación sexual comercial,* en UNICEF.org, Adaptado de la Declaración del Congreso Mundial contra la Explotación Sexual Comercial de los Niños (Suecia, 1996), Nueva York, 2006, consultado en: http://www.unicef.org/spanish/protection/files/Explotacion_sexual_comercial.pdf [septiembre 2015]
- Wamala Frederick, *The ITU National Cybersecurity Strategy Guide*, Unión Internacional de Telecomunicaciones, Ginebra, septiembre 2011, 119 pp., consultado en: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf [abril 2015]
- Wegener Henning, *Un concepto de ciberespacio*, en “La búsqueda de la Paz en el Ciberespacio”, UIT, Ginebra, 2011, 127 pp., consultado en:

https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-S.pdf [marzo 2015].

- Wojcicki Susan, Los ocho pilares de la innovación, en Sitio Oficial de Google (acerca de), diciembre de 2012, consultado en: https://www.thinkwithgoogle.com/intl/es-es/insights/los-ocho-pilares-de-la-innovacion/ [marzo 2018]
- World Economic Forum, *Global Agenda Council on Cybersecurity*, White Paper, abril 2016, consultado en: http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf [abril 2016]
- World Economic Forum, *The Global Risks Report 2017*, 12th Edition, enero 2017, consultado en: