UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES

ARAGÓN

“LA CIBERSEGURIDAD EN MÉXICO ANTE DESAFÍOS Y AMENAZAS DEL SIGLO XXI”

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN RELACIONES INTERNACIONALES

P R E S E N T A:

ANDRÉS ZURITA HIGUERA

ASESOR:

MTRO. VÍCTOR FRANCISCO OLGUÍN MONROY

Ciudad Nezahualcóyotl, Estado de México, 2018

Dedicatoria

Este trabajo se lo dedico a toda mi familia por ser quienes me han alentado a llegar más lejos, principalmente a mi mamá por su amor incondicional y todo el esfuerzo que ha hecho para que pudiera llegar hasta aquí.

Gracias a mi hermano por ser mi fuente de inspiración, y mi motivo de superarme para que algún día llegue a ser su ejemplo a seguir.

Gracias a Dios, por estar siempre a lado mío y ser quien me ha estado guiando y motivando en los momentos más difíciles.

Gracias a Catherine (Cui), por compartir tantos momentos importantes en mi vida, los cuales he recorrido junto a ella.

Gracias a mis maestros por dejar una huella en mí a lo largo de la carrera y a mi universidad que me ha dado una oportunidad muy valiosa, que es la educación.

ÍNDICE

INTRODUCCIÓN

La ciberseguridad como tal nace aproximadamente a principios del Siglo XXI cuando el Internet empieza su expansión a consecuencia del crecimiento exponencial de aparatos conectados a ella, el crecimiento de usuarios y de las amenazas que empiezan a cruzar las barreras nacionales e incluso las barreras físicas (un ataque cibernético tiene las capacidades de afectar al mundo físico); es por eso que la ciberseguridad se volvió un pilar importante en la Seguridad Nacional de los países.

Es posible que nadie se imaginara que Internet llegaría a ser una parte fundamental en el desarrollo de la actividad humana, una tecnología nacida en el seno militar en pleno contexto de la Guerra Fría y con apenas unos 100,000 usuarios a finales del Siglo XX, llegara al día de hoy a abarcar el 51.8% de la actual población mundial,[1] con miles de dispositivos conectados a ella, desde una computadora hasta un teléfono, desde aparatos industriales hasta estructuras militares, desde edificios hasta automóviles y este número crecerá gracias al Internet de las Cosas (IoT, por sus siglas en inglés)[2].

Actualmente existe un desafío para delimitar el concepto de ciberseguridad dado a la complejidad y el punto de vista de quién lo defina, conduciendo a una plétora de conceptualizaciones para lograr explicar y comprender qué es ciberseguridad, pues éste es un término relativamente nuevo, a pesar que cada vez se vuelve más común que varios países agregan dicho término dentro de sus políticas nacionales de seguridad. Aún falta mucho por avanzar en su concepto,

[1] Internet World Stats. (30 de junio de 2017). Estadísticas mundiales de uso y de la población en internet. Recuperado de: http://www.internetworldstats.com/stats.htm Fecha de consulta: 10/11/2017.

[2] *Internet Of Things (IoT)*: "Se refiere a un sistema de dispositivos de computación interrelacionados, máquinas mecánicas y digitales, objetos, animales o personas que tienen identificadores únicos y la capacidad de transferir datos a través de una red, sin requerir interacciones humano a humano o humano a computadora." Rouse Margaret & Wigmore Ivy. (enero de 2017). Internet de las cosas (IoT). *TechTargetES*. Recuperado de: http://searchdatacenter.techtarget.com/es/definicion/Internet-de-las-cosas-IoT Fecha de consulta: 09/11/2017.

enfrentándose que al paso de tiempo se va agregando más áreas de competencia y por lo tanto su definición como sus capacidades va evolucionando.

Los Estados, a través de sus agencias de Seguridad Nacional en cooperación con Organismos Internacionales, se han esforzado en crear leyes para regular el ciberespacio,[3] agregándola como una área más en cuestiones militares (aérea, marítima, terrestre, ultraterrestre y ahora ciberespacio) y creando bases normativas para el actuar de las instancias policiales, esto a consecuencia de que los ataques cibernéticos actuales a dispositivos, terminales, instituciones o al mismo Estado, no dejan por lo general, un rastro de quiénes podrían ser los perpetradores, sumando que los daños y consecuencias de dichos ataques han repercutido a la seguridad de los países; es por eso que a nivel internacional los Estados se han ido regulando, preparando y creando cibercomandos, para poder hacer frente a estas amenazas a la Seguridad Nacional, mientras el sector policial, empieza su rápido desarrollo de capacidades cibernéticas, ante el alto índice de delitos cometidos en el ciberespacio.

La problemática de México es que se encuentra en pleno desarrollo de su ciberseguridad, con una tardía implementación de políticas comparadas con otros países, que ya se han desarrollado cibernéticamente; teniendo como desafío que México no cuenta con una infraestructura e instituciones adecuadas para contener, castigar o repeler un ciberataque, tan solo las instancias que se encargan de perseguir delitos cibernéticos, no han podido hacer frente a ellas, esto se vio en el ataque cibernético que aconteció en el año 2017 con el *ransomeware* llamado WannaCry que afectó a más de 180 países alrededor del mundo, y México fue uno de los más afectados,[4] el cual no fue difundido por las instancias gubernamentales.

[3] Definido en el documentado de la Estrategia Nacional de Ciberseguridad de México como: 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. Gobierno Federal. (2017). *Estrategia Nacional de Ciberseguridad*. [Archivo PDF]. Recuperado de: https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad Fecha de consulta: 29/06/2017.

[4] Gabriela Chávez. (15 de mayo de 2017). Este es el país de Latinoamérica más afecto por el ciberataque WannaCry. *CNN en Español*. Recuperado de: http://cnnespanol.cnn.com/2017/05/15/este-es-el-pais-de-latinoamerica-mas-afectado-por-el-ciberataque-wannacry/ Fecha de consulta: 29/06/2017.

Para el marco jurídico, la ciberseguridad se vuelve obsoleta por la ausencia de leyes adecuadas, así como la falta de instituciones que protejan a la población y al Estado de los riesgos que enfrentan en el ciberespacio. La poca preparación de México en este ámbito lo hace uno de los países más vulnerables en sufrir ataques cibernéticos, coadyuvando la falta de cultura que tiene la población en el manejo de aparatos tecnológicos conectados a internet; como también, el desconocimiento de las amenazas y leyes que los protejan dentro del ciberespacio.

El sector militar es considerado el más importante para el desarrollo de la ciberseguridad, dado a la existencia de potenciales amenazas provenientes del ciberespacio[5] que hacen vulnerable la Seguridad Nacional de México. Es por eso que en el actual sexenio (2012-2018) empezó a crecer dentro de este sector la ciberseguridad exponencialmente. La Secretaría de Marina (SEMAR) junto con la Secretaria de Defensa Nacional (SEDENA) han creado instancias especiales que resguarden la integridad nacional, homologación de términos; como también, el mejoramiento de sus capacidades cibernéticas, los cuales serán mencionados más adelante en los Informes de Gobierno como en los Planes Sectoriales.

La hipótesis de la presente tesis es que "México no está preparado aún y se encuentra en el umbral del desarrollo de su ciberseguridad, debido a diversos factores como: la deficiencia del campo de estudio que enfrenta el país en el ámbito cibernético, la tardía implementación de la ciberseguridad dentro de las Fuerzas Armadas, un marco jurídico rebasado por los delitos cibernéticos, y una policía con capacidad de acción limitada. Ante la necesidad de contar con un marco referencial que coadyuve al sector militar, policial e institucional a hacer frente a los desafíos y amenazas que acontecen en el presente Siglo XXI -como ya lo han hecho diversos países y organismos regionales al crear leyes ya sea nacional y regional para hacer frente a los retos de un mundo cada vez más conectado y digitalizado- la Organización de Estados Americanos (OEA) ha brindado ayuda a México para

[5] La mención de "ciberespacio" data en 1984 en la novela *Neuromante* del estadounidense William Ford Gibson en 1984, después se populariza con el trabajo: *Declaración de Independencia del Ciberespacio* por John Perry Barlow en 1990. Secretaría de Marina & Centro de Estudios Superiores Navales, (2015), *Seguridad y Defensa en el Ciberespacio*, (pág. 89), México: Secretaría de Marina & Centro de Estudios Superiores Navales.

elaborar la Estrategia Nacional de Ciberseguridad en el actual sexenio, aunque esta Estrategia tarde todavía años en implementarse satisfactoriamente y su actualización sea tardada, es un gran paso para México; pero no suficiente, dado a la complejidad y la mejora tecnológica que transcurre en poco tiempo y que en dicha Estrategia existan algunas carencias."

El objetivo general es analizar el avance de México en materia de ciberseguridad; así como, sus principales desafíos actuales con los que se enfrenta y las potenciales amenazas provenientes desde el exterior como al interior de México, implementando una metodología explorativa, ante un tema muy actual dentro del país, y usando una metodología comparativa con otros países y organizaciones internacionales para entender el nivel de desarrollo que tienen y a las dificultades que se enfrentan.

En el primer capítulo, el objetivo particular abordará una breve historia del internet, dado que es el área de trabajo de la ciberseguridad, este capítulo introductorio es para entender cómo surge, evoluciona y su actualidad a nivel nacional; después, se analizará el concepto de ciberseguridad y sus diferencias dependiendo el área que lo defina (Estado o sector privado), también, cómo la ciberseguridad, desde el punto de vista del Estado entra a la Teoría de Complejos de Seguridad Regional de Barry Buzan y Ole Waever, ambos de la corriente de la Escuela de Copenhague, en donde dicha teoría dará la visión de la importancia de la regionalización para la seguridad y la securitización (ciberseguridad en este caso), para enfrentar las amenazas de seguridad que hoy en día existen regionalmente; así como, de la interacción de los Estados dentro de una región.

Como objetivo particular en el segundo capítulo se analizará el panorama general de la ciberseguridad a nivel internacional, abordando los principales sucesos que marcaron a la ciberseguridad y una breve mención de ataques cibernéticos a modo de ejemplificar la importancia de la ciberseguridad para algunos países; también se analizará a los organismos regionales que más han desarrollado sus políticas cibernéticas para sus Estados miembros.

En el tercer y último capítulo, el objetivo particular es el analizar el desarrollo cibernético de México para dar una idea de cuáles son los principales desafíos y amenazas que enfrenta el país. Se mencionará brevemente la evolución de la ciberseguridad dentro de los Planes Nacionales de Desarrollo (PND) e Informes de Gobierno de los tres últimos sexenios: Vicente Fox (2000-2006), Felipe Calderón (2006-2012) y Enrique Peña Nieto (20012-2018); el marco jurídico actual a nivel federal y los retos que tiene; también se abordará, la importancia de la ciberseguridad para la Seguridad Nacional de México ante los riesgos que existen dentro del ciberespacio y la creación de la Estrategia Nacional de Ciberseguridad.

Al final del trabajo en forma de listado estarán las conclusiones generales sobre el panorama actual de México en materia de ciberseguridad ante las amenazas y desafíos que existen en la actualidad, junto con algunas recomendaciones para mejorar la ciberseguridad de México ante los nuevos retos del presente Siglo XXI.

CAPÍTULO I INDUCCIÓN A LA CIBERSEGURIDAD

1.1 HISTORIA DEL INTERNET Y SU ACTUALIDAD EN MÉXICO

Para hablar de ciberseguridad, se tiene que conocer su entorno de trabajo y éste es el Internet, muchos de los grandes avances tecnológicos de la humanidad se han desarrollado por motivaciones bélicas, y este no es la excepción, pues se ha impuesto de sobremanera a las sociedades contemporáneas.

Su inicio se remonta en la década de los 50´s en el pleno contexto de la Guerra Fría, donde se creó la Agencia de Proyectos de Investigación de Avanzada (ARPA, por sus siglas en inglés) derivada del Departamento de Defensa de Estados Unidos el cual financió un proyecto denominado ARPANET, que dio el resultado de lo que hoy se conoce como Internet.

El Internet es todo un fenómeno a estudiar, diversas disciplinas como la Sociología, Economía, Política e Historia así lo hacen. Su importancia radica en el cómo ha transformado al mundo y las consecuencias que trae a su entorno. También es considerada una de las mejores inversiones, pues en sus inicios se calcula que costó entre los 100 millones y 200 millones de dólares,[6] el cual actualmente la cifra del valor de Internet se calcula en miles de millones de dólares.

En el presente trabajo se tocará brevemente la creación y desarrollo del Internet, donde se aborda lo que era conocido como ARPANET, su evolución, de dónde sale y por qué de este proyecto en pleno contexto de la Guerra Fría; posteriormente la creación del *World Wide Web* (WWW), cómo revolucionó el Internet y su actualidad en México, dado que es considerada una herramienta

[6] García Mexía, Pablo, (2012), *Historias de Internet Casos y Cosas de la Red de Redes*, (pág. 12), Valencia, España: TIRANT HUMANIDADES.

demasiado valiosa en este siglo, proporcionando acceso a una vasta cantidad de información que se puede encontrar dentro de ella. [7]

1.1.1 GÉNESIS Y DESARROLLO DEL INTERNET

El Internet que hoy se conoce no siempre se llamó así. A finales de la década de los 50´s en pleno contexto de la Guerra Fría, que además de ser un conflicto ideológico, se tradujo en tensiones y escaladas militares entre las dos potencias que eran Estados Unidos de América (EUA) y la Unión de Repúblicas Socialistas Soviéticas (URSS), en esta época existía una carrera espacial, donde en 1957 la URSS se convirtió en el primer país en lanzar un satélite llamado Sputnik 1, posteriormente seguiría los EUA al lanzar el Explorer 1.[8]

Un año más tarde, dicho suceso haría que el presidente 34° Dwight David Eisenhower creara la Agencia de Proyectos de Investigación Avanzada (ARPA, *Advanced Research Projects Agency*)[9] que dependería del Departamento de Defensa de Estados Unidos; esta agencia se le concedería un gran presupuesto con el objetivo de la creación de nuevas tecnologías para uso militar y así hacer un contraste al avance tecnológico de la URSS; hasta la fecha esta agencia sigue operando.

Durante este periodo se encontraba la amenaza latente de una guerra nuclear entre ambos países, y es por eso que ARPA se interesó en un proyecto que

[7] En la actualidad existen varias capas de accesibilidad en la red donde no se ve más allá de lo que los motores de búsqueda convencionales pueden mostrar, para entrar en esas capas es necesario contar con programas especiales para poder acceder a dicho lugar denominado *DeepWeb*. Tan solo la información que se encuentra en la *DeepWeb* es 600 veces más grande de la que se encuentra en la web convencional. Secretaría de Marina & Centro de Estudios Superiores Navales. Op. Cit., (págs. 24-25).

[8] DARPA. Where the Future Becomes Now. *DARPA.* Recuperado de: https://www.darpa.mil/about-us/darpa-history-and-timeline Fecha de consulta: 29/06/2017.

[9] Su nombre cambió en 1972 como *Defense Advanced Research Projects Agency* (DARPA), pero en el año de 1993 vuelve a denominarse ARPA; esto vuelve a cambiar en 1996 agregando de nuevo la "D".
DARPA. ARPA Changes Names. *DARPA.* Recuperado de: https://www.darpa.mil/about-us/timeline/arpa-name-change Fecha de Consulta: 29/06/2017.

consistía en comunicar ordenadores desde puntos geográficamente diferentes,[10] con el objetivo de descentralizar la información, ya que en ese entonces con un ataque hipotético a uno de sus puntos, tendría un error en las transmisión de flujo de datos y podría descomponer el resto de la información, principalmente se buscaba que el flujo de información no fuera interrumpido, para poder contar con una posible respuesta a la agresión por parte de Estados Unidos.[11]

Así se creó el ARPANET, un proyecto colaborativo entre el Departamento de Defensa de los Estados Unidos, ARPA y las principales universidades estadounidenses.[12] Tuvo sus inicios con Joseph Carl Robnett Licklider, un ingeniero informático del Instituto Tecnológico de Massachusetts (MIT, *Massachusetts Institute of Technology*) que había propuesto la idea de una "Red Galáctica" donde existiría un conjunto de ordenadores conectados a nivel global que ayudaría a las personas a acceder a información como programas o datos desde cualquier punto.[13] Sus sucesores Iván Sutherland, Robert W. Taylor y Lawrence G. Roberts continuarían con esta visión concretando el proyecto de ARPANET en 1969, el cual se mandó el primer mensaje a través de ella, desde la Universidad de UCLA a la Universidad de Stanford.[14]

Existía un problema en las comunicaciones, pues se operaba mediante la técnica telefónica denominada "conmutación de circuitos", el cual solo dos puntos podían conectarse en un solo circuito para comunicarse, por el cual se propuso la diversificación de dichos circuitos, asemejando una red neuronal para que existiera ese flujo de información; sumando la propuesta de que la información fuera mandada desde "Paquetes de Red"[15] y no como se hacía tradicionalmente con el

[10] DARPA. ARPANET and the Origins of the Internet. *DARPA.* Recuperado de: https://www.darpa.mil/about-us/timeline/arpanet Fecha de consulta: 29/06/2017.
[11] García Mexía. Op. Cit., (pág. 44).
[12] Ibíd., (pág.43).
[13] Barry M. Leiner, Vinton G. Cerf, David D. Clarck, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts & Stephen Wolff. (1997). Breve Historia de Internet. *Internet Society*. Recuperado de: https://www.internetsociety.org/es/breve-historia-de-internet#Origins Fecha de consulta: 29/06/2017.
[14] García Mexía. Op. Cit., (pág. 43).
[15] El mensaje se descompone en paquetes reducidos, previo a su etiquetado (el cual se hace para que posteriormente se identifique el mensaje completo y no hubiera algún paquete perdido) una vez hecho esto

flujo continuo de datos, concluyendo que al mandar una mayor cantidad de información no se congestionara el circuito, logrando que ARPANET tuviera éxito.[16]

En 1971 Raymond Tomlinson crea el primer programa de correo electrónico y con ello la arroba. Todavía ARPANET seguía para uso académico y científico, sin contar que existían muy pocos usuarios en ella. Años más tarde, en 1973 se hace la primera conexión internacional a la *University Collage of London*[17] y surge el protocolo denominado TCP/IP por Vinton Cerf y Robert E. Kahn,[18] este protocolo homologaba las comunicaciones de los ordenadores y de las empresas de telecomunicaciones para que todas las computadoras conectadas a la red tuvieran un lenguaje común y así fuera más fácil su comunicación.

El 12 de noviembre de 1988 se registra el primer ataque cibernético, un gusano informático denominado Morris (se le da el nombre por el creador Robert Tappan Morris)[19] que infectó por correo electrónico a un aproximado de 6,000 usuarios, entre ellos equipos de la NASA y otras dependencias del gobierno estadounidense, un par de días después se logra controlar y por este motivo en 1984 se crea el primer Equipo de Respuesta ante Emergencias Informáticas (CERT, *Computer Emergency Response Team*), también conocidos como Equipo de Respuesta ante Incidencias de Seguridad (CSIRT, *Computer Security Incident Response Team*), los cuales se convierten en un centro de respuesta, de coordinación y prevención ante incidentes cibernéticos, de ahí en adelante fueron aumentando en todo el mundo. El primer CERT que se creó fue el de la Universidad

---

el mensaje viaje a través de la red y una vez llegada al destinatario se recompone, y en caso que faltará alguna parte de información, esta se reenvía y así se recuperaba el mensaje completo.

[16] García Mexía. Op. Cit., (págs. 49-51).

[17] Raúl Rivero. (2002). Evolución de ARPANET/Internet. *EL MUNDO*. Recuperado de: http://www.elmundo.es/imasd/docs/cursos/masterperiodismo/2002/rivero-master01-usa.html Fecha de consulta: 30/06/2017.

[18] Segura Serrano, A., Gordo García, F., (Coords.), (2013), *Ciberseguridad Global Oportunidades y Compromisos en el Uso del Ciberespacio*, (pág. 79), España: Editorial Universidad de Granada & Campus Universitario de Cartuja. Granada.

[19] Un estudiante de 23 años del Instituto Tecnológico de Massachusetts (MIT, por sus siglas en inglés), el cual aclaró que lo esparció por error y no pensaba que tuviera tal magnitud, el cual ocasionó pérdidas de 96 millones de dólares aproximadamente. Álef. (2 de noviembre de 2014). ¿Una broma cibernética? El primer gusano de internet salió el 2 de noviembre de 1988. *Álef.* Recuperado de: http://alef.mx/wp/una-broma-cibernetica-el-primer-gusano-de-internet-salio-el-2-de-noviembre-de-1988-2/ Fecha de consulta: 23/11/2017.

Carnegie Mellon, en el Instituto de Ingeniería de Software,[20] el cual cuenta con la financiación de Fondos Federales por parte del Departamento de Defensa de Estados Unidos, y en la actualidad es el país con más CERT´s al nivel mundial, tan solo existen más de 75 CERT´s alrededor de todo el país, los cuales pertenecen a instituciones gubernamentales, privadas y académicas. A finales de la década de los 80´s ARPANET deja de existir y se convierte en Internet, su nombre actual se deriva de la palabra *Internetworking* (Interconexión de redes).

El Internet con el que hoy se está familiarizado, inició en la década de los 90´s, y es una etapa crucial porque fue aquí donde se le dio forma. Todo comenzó con Tim Berners-Lee, un científico perteneciente a la Organización Europea para la Investigación Nuclear (CERN, *Conseil Européen pour la Recherche Nucléaire*)[21] que junto con su equipo lograron crear la *World Wide Web* (WWW); la cual fue lanzada al público en 1991.

Esta aportación fue transcendental, con ello se logra organizar toda la información que se encontraba dentro de la red y así se volviera más fácil para el usuario navegar dentro de ella. Esto consiste principalmente en el "Hipertexto", que es un sistema que organiza la información y datos permitiendo al usuario el evitar la necesidad de leerlo todo en corrido, logrando mediante links, enlaces o vínculos el saltar partes de la página, de documentos u a otros archivos; pero no solo fue el Hipertexto, también fueron direcciones, lenguaje, etcétera.

En este periodo fue cuando Internet empezó a crecer notoriamente, gracias a Marc Andreesen que en 1993 creó el primer navegador de la historia llamado Mosaic, el cual permitió acceder a la WWW con más facilidad. A partir de ésta década Internet se fue desarrollando hasta llegar a los 360 millones de usuarios en el año 2000.[22]

---

[20] Carnegie Mellon University. About Us. *Instituto de Ingeniería de Software*. Recuperado de: https://www.cert.org/about/ Fecha de consulta: 13/08/2017.

[21] Es una organización internacional creada en 1954 con el propósito de la investigación científica dentro del campo de la física; en la actualidad cuenta con 22 Estados miembros. CERN. About CERN. *CERN*. Recuperado de: http://home.cern/about Fecha de consulta: 02/07/2017.

[22] Bartlett Jamie, (2017), *La Red Oculta*, (Franco Mundo Velázquez, Trans.), (pág. 41), Ciudad de México, México: PAIDÓS. (Trabajo original publicado en 2014).

1.1.2 EL INTERNET EN MÉXICO

Internet ha llegado a ser un pilar para el desarrollo de las comunicaciones a nivel mundial, logrando conectar a personas que se encuentran a miles de kilómetros de distancia, y no solo eso, también mejoró los procesos industriales, los económicos, los tecnológicos, expandió el alcance de los medios informativos, entre otras cosas.[23] Su importancia es tal, que es considerado como un recurso importante para el desarrollo de las actividades diarias, acaparando todos los aspectos importantes de la vida de un individuo como lo social, económico, laboral y ocio.[24]

Generalmente se tiende a pensar que las telecomunicaciones dependen de los satélites que se encuentran orbitando el planeta; pero la realidad es que no, ya que más del 80% de las telecomunicaciones a nivel mundial se realizan mediante cables submarinos para mandar datos alrededor del mundo. Estimaciones de *TeleGeography* en su último conteo realizado a principios del 2017 hace mención de la existencia de 428 cables, una red de 1.1 millones de kilómetros de cables submarinos que dan sustento a la red mundial de telecomunicaciones.[25]

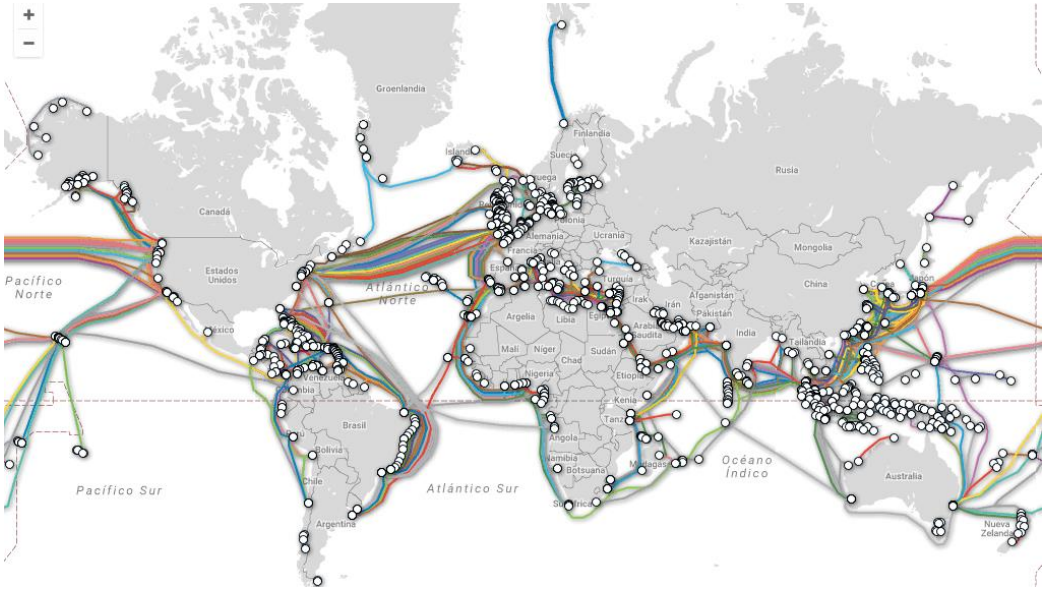
[23] Una de las características que tiene Internet, es que ha logrado reducir drásticamente el número de idiomas hablados dentro de su red (los 5 principales idiomas que se hablan: inglés, chino, español, árabe y portugués), esto tiene una gran importancia dado que la internet empieza a sesgar los demás idiomas que existen en el mundo, de hecho se prevé que la mitad de los 6,000 idiomas hablados actualmente desaparezcan a finales del siglo XXI. UNESCO. (27 de febrero de 2017). Los idiomas importan. *UNESCO.* Recuperado de: http://www.unesco.org/new/es/communication-and-information/wsis-10-review-event-25-27-february-2013/feature-stories/languages-matter/ Fecha de consulta: 10/11/2017.

[24] García Mexía. Op. Cit., (pág. 17).

[25] TeleGeography. Submarine Cable Frequently Asked Questions. *TeleGeography*. Recuperado de: http://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions Fecha de consulta: 11/07/2017.

Mapa 1:

Red Mundial de Cables Submarinos



Nota: Los propietarios de estos cables son diversos, la mayoría son de empresas internacionales del ramo tecnológico como Google, Facebook, Microsoft, entre otras. Fuente: TeleGeography. (2017). Recuperado de: https://www.submarinecablemap.com/#/ Fecha de consulta: 11/07/2017.

Gracias a esta red de cables submarinos, se puede visualizar páginas en Internet que se encuentran ubicadas dentro de servidores de otros países o continentes, incluso también funciona con las llamadas telefónicas. Dado que la actualidad, el panorama del internet es muy diferente del cómo inicio.

Cifras presentadas por *Internet World Stats* hablan que tan solo a finales del año 2017, el número de usuarios registrados en internet a nivel mundial fue de 4,050,247,583[26] lo que equivale al aproximado de 51.8% de la población mundial, duplicándose tal vez para mediados del presente siglo o antes; dicho crecimiento del Internet y usuarios responde a un desafío para los países, incrementando los riesgos y por ende, los delitos cibernéticos cometidos dentro de ella; es por eso de la importancia de la regularización internacional del Internet y el avance de la ciberseguridad que le dé cada país.

[26] Internet World Stats. (15 de febrero de 2018). Usuarios de Internet al nivel mundial. *Internet World* Stats. Recuperado de: http://www.internetworldstats.com/stats.htm Fecha de consulta: 02/07/2017.

En el caso de México, es importante avanzar rápidamente en el desarrollo de la ciberseguridad ante las cifras y la situación actual del Internet en el país. La definición de Internet proviene de la Ley Federal de Telecomunicaciones y Radiodifusión, Artículo 3, fracción XXXII:

> "Internet: Conjunto descentralizado de redes de telecomunicaciones en todo el mundo, interconectadas entre sí, que proporciona diversos servicios de comunicación y que utiliza protocolos y direccionamiento coordinados internacionalmente para el enrutamiento y procesamiento de los paquetes de datos de cada uno de los servicios. Estos protocolos y direccionamiento garantizan que las redes físicas que en conjunto componen Internet funcionen como una red lógica única"[27]

Dentro de la red de cableado submarina, México cuenta con cuatro cables que pasan a lo largo del territorio y brindan conexión nacional, estos son:

Mapa 2:

Cable Submarino: Pan-American Crossing (PAC)

Nota: Inició su operación en Marzo del 2000; tiene una longitud de 10,000 km; y su propietario es Level3. Fuente: TeleGeography. (Junio de 2017). Recuperado de: https://www.submarinecablemap.com/#/submarine-cable/pan-american-crossing-pac Fecha de consulta: 11/07/2017.

[27] Diario Oficial de la Federación. (14 de julio de 2017). Ley Federal de Telecomunicaciones y Radiodifusión. *SEGOB*. Recuperado de: http://www.dof.gob.mx/nota_detalle.php?codigo=5352323&fecha=14/07/2014 Fecha de Consulta: 06/07/2017.

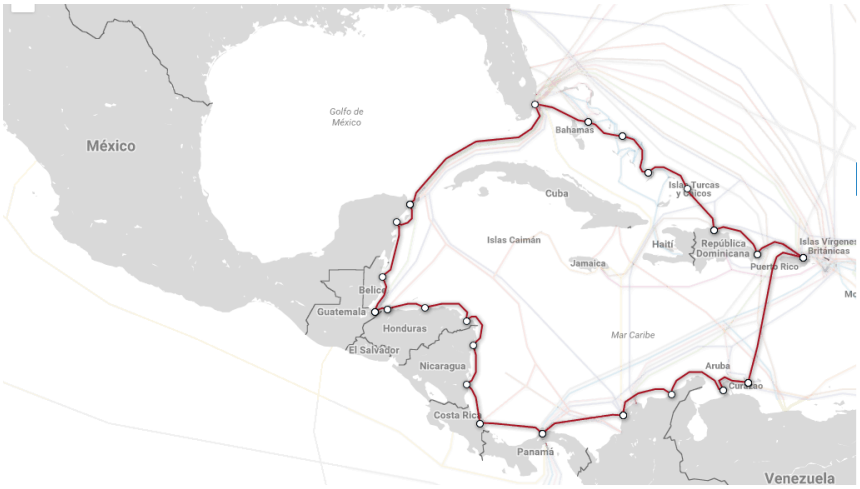
Mapa 3:

Cable Submarino: America Movil Submarine Cable System-1 (AMX-1)

Nota: Inició sus operaciones en el 2014; tiene una longitud de 17,800 km; y su propietario es: América Móvil. Fuente: TeleGeography. (Junio de 2017). Recuperado de: https://www.submarinecablemap.com/#/submarine-cable/america-movil-submarine-cable-system-1-amx-1 Fecha de consulta: 11/07/2017.

Mapa 4:

Cable Submarino: Arcos



Nota: Inició su operación en Diciembre del 2001; tiene una longitud de 8,600 km; y sus propietarios son: C&W Networks, CANTV, Codetel, Hondutel, Belize Telemedia, Enitel, AT&T, Alestra, Verizon, RACSA, United Telecommunication Servics (UTS), Telecarrier, Tricom USA, Telecomunicaciones Ultramarinas de Puerto Rico, Internexa, Orbinet Overseas,Telepuerto San Isidro, Bahamas Telecommunications Company, Instituto Costarricense de Electricidad, y Orbitel. Fuente: TeleGeography. (Junio de 2017). Recuperado de: https://www.submarinecablemap.com/#/submarine-cable/arcos Fecha de consulta: 11/07/2017.

Mapa 5:

Cable Submarino: Maya-1

Nota: Inició su operación en Octubre 2000; tiene una longitud de 4,400 km; y su propietario es: Verizon, AT&T, Sprint, Hondutel, Telefónica, Orbitel, Telecom Italia Sparckle, C&W Networks, Entel Chile, Embratel, ETB, Axtel, Instituto Costarricense de Electricidad, Belgacom, Prepa Networks, Orange, Tricom, RSL Telecom, América Móvil. Fuente: TeleGeography. (Junio de 2017). Cable submarino Maya-1. Recuperado de: https://www.submarinecablemap.com/#/submarine-cable/maya-1 Fecha de consulta: 11/07/2017.

En el último estudio realizado por la Asociación de Internet en México; [28] se estima que existen unos 70 millones de usuarios de internet[29] el cual alcanza el 63% de penetración en la población, a comparación de hace una década que solo existían 20.2 millones; tan solo en 10 años el crecimiento de usuarios de internet fue de 350%. Con base a dicha encuesta, que se realizó a 1,626 entrevistados, lo más destacado fue: [30]

- El 51% de usuarios son mujeres y 49% hombres.

[28] Es una asociación civil sin fines de lucro que desde 1999 junta empresas y entidades del gobierno más relevantes dentro de la industria del internet. Su principal propósito es realizar estudios y eventos anuales que permitan conocer más sobre las últimas tendencias en línea y la percepción de los usuarios alrededor de internet. Asociación de Internet.mx. ¿Qué es la asociación de internet.mx?. *Asociación de Internet.mx.* Recuperado de: https://www.asociaciondeinternet.mx/es/que-es/descripcion Fecha de consulta: 05/07/2017.

[29] Su información se basa en usuarios a partir de los 6 años de edad, el cual son 111 millones de mexicanos.

[30] Estadística Digital. (18 de mayo de 2017). 13° Estudio sobre los Hábitos de los Usuarios de Internet en México 2017. *Asociación de internet.mx & INFOTEC*. [Archivo PDF]. Recuperado de: https://www.asociaciondeinternet.mx/es/estudios Fecha de consulta: 23/11/2017.

- La edad que tienen los usuarios de Internet se concentra entre los 12 a 34 años (57% del total de internautas en nuestro país).
- Las tres principales barreras de acceso a Internet son: conexión muy lenta en su zona (33%), costos elevados (22%) y el no saberlo utilizar (21%).
- El tiempo promedio que están conectados en Internet en un día es de 8 horas 1 minuto, el cual 2 horas 58 minutos se destina a las redes sociales.
- Dentro de sus hábitos de conexión: el 82% lo hace desde su casa, y el 61% por su plan de datos contratados.
- Los dispositivos que más se usan para el acceso al Internet es: el teléfono celular (90%) y desde la PC/Laptop (73%).
- El mayor uso que se le da al Internet es: Acceder a las redes sociales (83%), enviar y recibir emails (78%), enviar o recibir mensajes instantáneos (77%) y búsqueda de información (74%).
- Las 5 principales redes sociales más usadas son:[31] Facebook (95%), WhatsApp (93%), YouTube (72%), Twitter (66%) e Instagram (59%).

Facebook es la red social predominante en México,[32] donde más de la mitad se conecta a diario para revisar sus redes sociales y la mayoría de las conexiones a Internet se registran desde su teléfono celular. Es gracias al celular, que incrementa la cantidad de usuarios de Internet en el país.

En la Estadística a Propósito del Día Mundial del Internet[33] elaborada por el Instituto Nacional de Estadística y Geografía (INEGI)[34] con base a la encuesta

[31] Como dato interesante: Cada usuario en México posee 5 redes sociales en promedio y solo el 1% no se encuentra inscrito en ninguna; y de estas 5 redes sociales, 3 son la misma compañía: Facebook es propietario de WhatsApp e Instagram.

[32] Esto también se puede observar en el reporte realizado por We are social: *Digital 2017. Global Overview*. donde muestra a México en el top #5 de países con mayor usuarios registrados en Facebook (76 millones) y a la Ciudad de México como la segunda ciudad después de Bangkok, con más usuarios en dicha red (19 millones). We are Social. (2017). *Digital 2017. Global Overview*. *We are Social.* Recuperado de: https://wearesocial.com/uk/special-reports/digital-in-2017-global-overview Fecha de consulta: 06/12/2017.

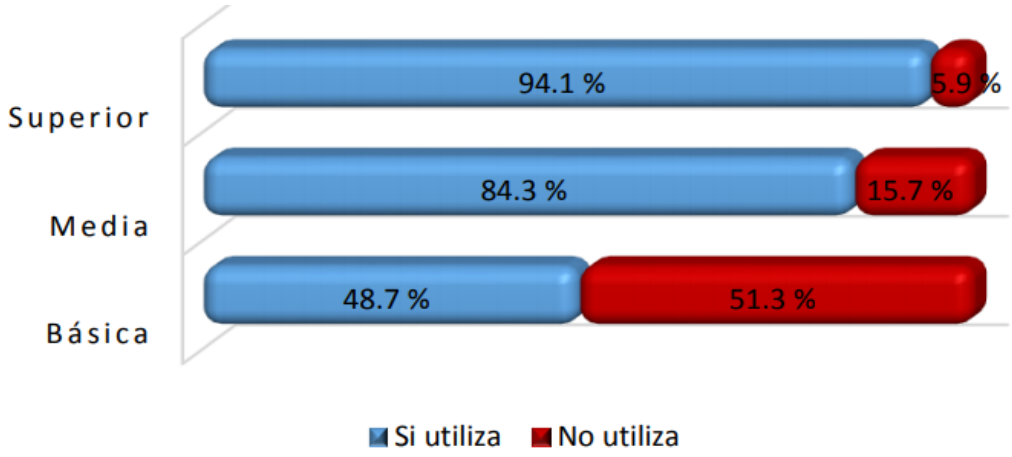
[33] BETA de INEGI. Sala de Prensa. *INEGI*. Recuperado de: http://www.beta.inegi.org.mx/app/saladeprensa/ Fecha de consulta: 06/07/2017.

[34] Es un organismo público autónomo creado en 1983, es responsable de normar y coordinar el Sistema Nacional de Información Estadística y Geográfica, así como de captar y difundir información de México en cuanto territorio, los recursos, la población y economía, que permite dar las características de nuestro país y

nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2016[35] menciona que el 47% de los hogares del país tienen conexión a Internet y su uso está asociado al nivel de estudios; entre mayor sea el grado de estudios, es más el uso de Internet.

Gráfica 1:

Usuarios de Internet por Nivel de Escolaridad 2016



Nota: Excluye a la población sin escolaridad o que omitió indicar su nivel de escolaridad. Dicha gráfica se encuentra dentro del documento. Fuente: INEGI. (15 Mayo 2017). Estadística a propósito del Día Mundial de Internet (17 Mayo) Datos Nacionales. (pág. 3). Recuperado de: http://www.inegi.org.mx/saladepr Fecha de consulta: 23/11/2017.

Lo que llama la atención es la comparación entre los usuarios de Internet en México[36] y las cifras de pobreza en el país; en el informe estadístico de pobreza en México 2014[37] elaborado por el Consejo Nacional de Evaluación de la Política de

ayuda a la toma de decisiones. BETA de INEGI. Quiénes somos. *INEGI*. Recuperado de: http://www.beta.inegi.org.mx/inegi/quienes_somos.html Fecha de consulta: 06/07/2017.

[35] BETA de INEGI. (2016) Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2016. *INEGI.* Recuperado de: http://www.beta.inegi.org.mx/proyectos/enchogares/regulares/dutih/2016/ Fecha de consulta: 06/07/2017.

[36] En México 65.6 millones de personas de seis años o más utilizan Internet. INEGI. (14 de marzo de 2017). Aumentan uso de internet, teléfonos inteligentes y TV digital: Encuesta Nacional sobre Disponibilidad y uso de Tecnologías de la Información en los Hogares, 2016. [Archivo PDF]. Recuperado de: http://www.inegi.org.mx/saladeprensa/boletines/2017/especiales/especiales2017_03_02.pdf Fecha de consulta: 10/11/2017.

[37] CONEVAL. (2014). Medición de la Pobreza. *CONEVAL.* Recuperado de: http://www.coneval.org.mx/Medicion/MP/Paginas/AE_pobreza_2014.aspx Fecha de consulta: 06/07/2017.

Desarrollo Social (CONEVAL),[38] 55.3 millones de mexicanos se encuentran en esta situación. Estas cifras sorprendentes y parejas se debe al incremento del uso de teléfonos inteligentes que creció en 2016 a 60.6 millones de usuarios[39] y el incremento de hogares con acceso a Internet; a pesar que tal vez no tengan computadora ya sea de escritorio o portátil, si tienen un teléfono celular con el cual puedan acceder a Internet.

El incremento de usuarios de Internet durante la década de 2006-2016 tiene un factor importante en la reforma de telecomunicaciones elaborada por el sexenio (2012-2018). En el Análisis Especial Estadístico: "Las telecomunicaciones a 3.5 años de la reforma constitucional en México"[40] , elaborado por el Instituto Federal de Telecomunicaciones (IFT)[41], señala el incremento de hogares con suscripción a banda ancha, donde creció de 39 a 48 hogares por cada 100 en un periodo de 3 años (2013-2016), esto gracias a los bajos costos y el aumento de actores en el mercado de telecomunicaciones; en cuestión de suscripción de banda ancha para móviles esta creció al grado de casi triplicarse, de 23 a 61 por cada 100 teléfonos contaban con suscripción a Internet, es aquí donde incrementó exponencialmente los usuarios de Internet en México; dando como resultado una disminución de acaparamiento en el mercado que tenía América Móvil (Telmex/Telcel)[42], y el crecimiento de otras empresas de telecomunicaciones en el país.

---

[38] Es el Consejo Nacional de Evaluación de la Política de Desarrollo Social, un organismo público descentralizado, con autonomía para generar informes sobre la situación política social y la medición de la pobreza en México. CONEVAL. ¿Quiénes somos?. *CONEVAL.* Recuperado de: http://www.coneval.org.mx/quienessomos/Conocenos/Paginas/Quienes-Somos.aspx Fecha de consulta: 06/07/2017.

[39] Expansión. (14 de marzo de 2017). 10 puntos que debes conocer sobre el internet en México. *EXPANSIÓN*. Recuperado de: http://expansion.mx/tecnologia/2017/03/14/10-puntos-que-debes-conocer-sobre-el-internet-en-mexico Fecha de consulta: 06/07/2017.

[40] IFT. Las telecomunicaciones a 3 ½ años de la Reforma Constitucional en México. *IFT*. [Archivo PDF]. Recuperado de: http://www.ift.org.mx/sites/default/files/contenidogeneral/estadisticas/a3anosreforma-vf6.pdf Fecha de consulta: 06/07/2017.

[41] El Instituto Federal de Telecomunicaciones creado a partir de la reforma de telecomunicaciones en 2013; es un organismo autónomo encargado de supervisar el uso y la prestación de servicios adecuados, asociados a la radiodifusión y a las telecomunicaciones en México. IFT. ¿Qué es el IFT?. [Archivo PDF]. Recuperado de: http://www.ift.org.mx/sites/default/files/que-es-ift.pdf Fecha de consulta: 06/07/2017.

[42] A pesar que aún sigue teniendo más del 50% del mercado en el país.

Dentro de los principales beneficios destacados de la reforma de telecomunicaciones mencionados por el IFT están:[43]

- Neutralidad de las Red (Artículo 145): Para los usuarios de Internet, la Ley contempla las principales características de la neutralidad de la red a las que se deben de sujetar las empresas que ofrecen el servicio de conexión a Internet como son: libre elección, no discriminación, privacidad, transparencia e información, calidad, entre otros.
- Prestación de servicios de telecomunicaciones a poblaciones no servidas por medio de la red pública compartida (Artículo 140): De acuerdo con la Ley, con la red compartida se podrán prestar servicios e infraestructura de telecomunicaciones, cuando en una determinada población ningún otro operador preste servicios, con lo cual se fomenta el servicio universal.
- Prohibición de intervención de llamadas telefónicas (Artículo 190): La Ley señala que las comunicaciones privadas son inviolables. Exclusivamente un juez, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de las comunicaciones privadas.
- Bloqueo de teléfonos reportados como robados o extraviados (Artículo 190, fracción VII): De acuerdo con la Ley, los operadores tienen la obligación de realizar el bloqueo inmediato de líneas de comunicación móvil que funcionen bajo cualquier modalidad reportadas por los clientes como robadas o extraviadas.
- Confidencialidad de información de usuarios en redes públicas (Artículo 122): La Ley establece expresamente que la información que se transmita a través de las redes y servicios de telecomunicaciones será confidencial, salvo que exista orden de autoridad judicial competente.

El Internet dentro de México ha tenido un gran auge y su crecimiento va a ritmos acelerados, abarcando a más del 50% de población; pero eso aún no es

[43] IFT. Principales beneficios para los usuarios y las audiencias. *IFT.* [Archivo PDF]. Recuperado de: http://www.ift.org.mx/que-es-el-ift/principales-beneficios-para-los-usuarios-y-las-audiencias Fecha de consulta: 06/07/2017.

suficiente, estimaciones de *Internet World Stats* lo clasifica en tercer lugar de 8 posiciones dentro de América Central, con una penetración del (65.3%).[44]

Con estos datos sobre la situación del Internet en el país, se ve la importancia del desarrollo de la ciberseguridad por parte del Estado, el Internet ya ha penetrado más de la mitad de la población mexicana y las leyes actuales no son suficientes para hacer frente a las amenazas provenientes de ella, incluso la información sobre ciberseguridad aún es escasa y reservada en el país; esto se agravia más con el desinterés por parte de la sociedad mexicana relacionado a la cultura de seguridad dentro del ciberespacio.[45]

Dentro de Internet todos pueden llegar a ser víctimas tales como instituciones de gobierno, empresas privadas, hasta la misma población y es aquí la importancia de conocer bien el entorno donde se desarrolla la ciberseguridad, que es el Internet; pues todo dispositivo conectado a la red puede ser vulnerable.

1.2 CIBERSEGURIDAD: TEORÍA Y CONCEPTUALIZACIÓN

Conceptualizar la ciberseguridad es un actual desafío dado a su complejidad e implicaciones, a pesar que se han hecho algunas definiciones de lo que es la ciberseguridad, estas son definiciones generales o son definiciones que le quitan competencias al concepto mismo. El conocer bien el concepto de ciberseguridad y entenderlo puede ayudar mucho en las legislaciones nacionales de cada país y también, comprender el grado de competencias que tiene la ciberseguridad.

Existiendo dicha problemática, algunos Estados están avanzando en esta área, visualizando que en el futuro las guerras ya no solo serán en la tierra, mar,

[44] Con base al porcentaje de penetración que tiene el Internet dentro de la población en Centro América: Costa Rica ocupa el primer lugar con 86.4% de población, seguido de Panamá con 69.1%. Esto se debe a la cantidad de población, México está en tercer lugar porque la población es mucho mayor que en los países de dicha región. Internet World Stats. (30 de junio de 2017). Usuarios de Internet de Centro Américas y Población. *Internet World Stats.* Recuperado de: http://www.internetworldstats.com/stats12.htm#central Fecha de Consulta: 17/11/2017.

[45] Secretaría de Marina & Centro de Estudios Superiores Navales. Op. Cit., (pág. 150).

aíre o espacio exterior; sino también, dentro de esta red; esto se puede ver con la creación de cibercomandos por los países más desarrollados o en los últimos ataques cibernéticos globales hacia instalaciones estratégicas vitales de algunos países.

La ciberseguridad es un área nueva en México y "nueva" relativamente hablando, porque apenas en los últimos 10 años se empezó a entender como tal la noción de la ciberseguridad dentro de las instituciones, centros académicos y legislaciones. En caso de sufrir un ataque que paralizara las comunicaciones, red eléctrica o sistema bancario como ha sucedió en otros países, no se cuenta con instituciones sólidas para hacer frente a dichos sucesos.

Esta es un área nueva que le compete principalmente al Estado, seguido por las empresas privadas y por último a la población, aunque se ha visto un gran avance de la ciberseguridad dentro del país, esto es gracias a la iniciativa empresarial del sector de la seguridad privada, dado a su naturaleza en cuestión al control de datos confidenciales, donde el sector privado es más recelosos. Algo que no debería de estar pasando, pues si el sector privado es el único que se está desarrollando en esta área y el Estado se está rezagando, entonces se puede esperar un alto grado de vulnerabilidad para los tres niveles, Estado-sector privado-población, a pesar de que solo uno lo esté trabajando.

1.2.1 TEORÍA DE COMPLEJOS DE SEGURIDAD REGIONAL

La Teoría de Complejos de Seguridad Regional (CSR) es propuesta principalmente por Barry Buzan en su libro *People, States and Fear* en el año 1991[46] y posteriormente Buzan junto con Ole Weaver la complementan en su libro *Regions and Power. The Structure of International Security* del año 2003. Esta teoría sale de

[46] La Primera Edición del libro: *People, States and Fear: The National Security Problem in International Relation*s del año 1983 ya hablaba sobre esta teoría, pero en la Segunda Edición de su libro llamado: *People, States and Fear: An Agenda for International Security Studies in the Post Cold War Era* de 1991, mejoró muchos aspectos de la primera edición.

la corriente de la Escuela de Copenhague, surgiendo ante la necesidad de ampliar la agenda de seguridad; debido a que la seguridad ya no se puede abordar desde la perspectiva tradicional y estatocéntrica por el significante cambio que tuvo el fin de la Guerra Fría en el escenario internacional, pues las amenazas ya no provienen solamente de los Estados, sino que se ha diversificado en actores (grupos subversivos, terrorismo y se podría agregar el crimen organizado); como también en sectores, donde no solo se estudie los aspectos de seguridad militar, sino también el político, social, económico, medioambiental, y en este caso se podría agregar el cibernético.

Por otro lado, explica el fenómeno de la interdependencia de la seguridad dentro de las regiones;[47] las categorías de los Estados y su influencia en las políticas de seguridad de una o varias regiones, dado que contempla a tres tipos de Estados: superpotencia, una gran potencia y potencia regional; y sus interacciones dentro de los tres niveles: local, regional y global.

La teoría de CSR asimila lo más importante de la perspectiva neorrealista y la perspectiva globalista[48], y a su vez la crítica debido a que su visión es muy reducida y que no toman en cuenta aspectos importantes como el local o regional. En el caso de la perspectiva neorrealista, concuerda que el Estado es un factor importante en el ámbito internacional y de la importancia de la seguridad territorial, dado a que ambas perspectivas (neorrealista y regionalista) tienen en cuenta eso, pero a su vez la crítica dado que no cuestiona la primacía del nivel global y solo se limita en los cambios unipolares y multipolares, no ve un factor importante del desarrollo de la seguridad internacional, en el ámbito regional, y no amplia el estudio de la seguridad, el cual solo se enfoca en el sector militar, cuando existen otros tipos de sectores a estudiar (seguridad ampliada).

[47] Una región es entendida como la proximidad geográfica de los Estados; los lazos culturales, políticos-económicos que comparten y la interacción que exista entre ellos. Un ejemplo sería la región de América Latina, que comparte una proximidad geográfica, lazos culturales y la estrecha relación dentro de ella.

[48] Se aclara que el globalismo no es una teoría, sino un paradigma dentro de las Relaciones Internacionales, el cual se sigue desarrollando, por lo cual aquí no lo maneja como "Teoría" sino como una "perspectiva"; mientras el Neorrealismo sí es una teoría dentro del campo de las Relaciones Internacionales.

Mientras para la perspectiva globalista y considerada la antítesis del neorrealismo, concuerda con la importancia de diversos factores y actores dentro del escenario internacional, pero critica que no aborda a fondo el estudio de la seguridad en ninguna de sus dos corrientes: Marxista o Liberal, cuando el globalismo fue el responsable de complicar la agenda de seguridad; y solo se enfoca en el estudio del centro-periferia, dejando un lado el ámbito regional; como también, no concuerda que el globalismo desvanezca las fronteras nacionales.[49] La primera definición original de CSR fue hecha en 1983 por Buzan como:

> "Un grupo de Estados cuyas principales cuestiones de seguridad, los vinculan estrechamente entre sí, que sus seguridades nacionales no pueden ser consideradas separadas de unas sobre otras".[50]

Está definición fue reformulada por Buzan y Waever en 1998, donde el aspecto estatocéntrico y político-militar ya no es el factor principal a estudiar; y agregan nuevos conceptos, reconociendo a diversos actores y sectores de seguridad, y la definen como:

> "Conjunto de unidades cuyo procesos de securitización, desecuritización, o ambos están tan relacionados que sus problemas de seguridades no pueden ser analizadas o resueltas de forma separadas de unas sobre otras".[51]

Se reconoce que en la seguridad existen diferentes sectores para su estudio, y eso lo hace tan complejo que vuelve a los Estados completamente interdependientes entre ellos, creando la regionalización de la seguridad. Si bien, lo importante a destacar es la palabra "securitización",[52] ya que se admite que el estudio de la seguridad se puede enfocar desde múltiples sectores, el cual permite

[49] Buzan, Barry. & Waever, Ole., (2003), *Regions and Powers The Stucture of International Security*, (págs. 6-14), New York, United States of America: Cambridge University Press.

[50] Versión original en inglés, traducción propia de: Buzan, Barry, (1991), People, States and Fear (2nd ed.): An Agenda for International Security in the Post-Cold War Era, (pág. 190), Colorado, United States of America: LYNNE RIENNER PUBLISHERS.

[51] Versión original en inglés, traducción propia de: Buzan, Barry. & Waever, Ole. Op. Cit., (pág. 44).

[52] La palabra "securitización" se refiere a dar prioridad a una situación en particular dentro de la agenda de seguridad de una región, un ejemplo sería la securitización de la ciberseguridad dentro de la región de América Latina por la Organización de Estados Americanos (OEA), al notar la deficiencia que existe y cómo el ciberespacio contiene una amenaza para las Seguridades Nacionales de los Estados que la conforman.

ampliar la agenda tradicional de seguridad, agregando nuevos temas al estudio de la seguridad, sin quitarle la importancia al Estado, adaptándose a los cambios del sistema internacional.

A pesar de la existencia de diversas discrepancias entre los Estados dentro de una región, siempre habrá un Estado con gran poder y participación que pueda liderar e influenciar a toda la región en temas de seguridad, dado a que ninguno de sus problemas se resuelve de manera separa debido a la estrecha relación que hay dentro de la región. Es por eso que la teoría habla sobre la existencia de tres tipos de poderes a nivel regional, estos son superpotencia *(Superpowers)*, una gran potencia *(Great powers)* y potencia regional *(Regional powers)*; y las define como:[53]

- Superpotencias: El criterio para definir a una superpotencia, es que tengan un amplio espectro de capacidades de ejercicio a través de todo el sistema internacional. Ellos poseen un gran poder político-militar de primera clase, y un poder económico que sustentan dichas capacidades; como también son un factor importante en los procesos de securitización y desecuritización de uno o varias regiones, actualmente el único Estado que entraría en esta definición es Estados Unidos.
- Gran potencia: Los Estados considerados dentro de este término, son actores activos e importantes en los procesos de toma de decisiones en cada región, pero no cuentan con un grado suficiente de influencia a nivel global, a pesar que tienen el poder económico, militar y político para ser una superpotencia. Los Estados que entrarían en esta clasificación serían: Rusia, China, Japón, entre otros.
- Potencia regional: Se refiere a los Estados que solo su poder le permite tomar decisiones dentro de su región, ya que están limitados. A su vez esto le ocasiona confrontaciones con Estados denominados Gran potencia o

[53] También existe dos términos que menciona: Estados aisladores *(insulator states)* los cuales procesos de securitización alrededor de ellos son tan amplias que no pueden pertenecer exclusivamente a un solo CSR, sino que llegan a pertenecer dos o incluso más, como sería el caso de Turquía; mientras los Estados amortiguadores *(buffer states),* cumplen el objetivo de separar a las potencias rivales dentro de un complejo de seguridad. Versión original en inglés, traducción propia de: Buzan. & Waever. Op. Cit., (págs. 34-37,314-316,394 y 483-487).

Superpotencia ante la polaridad de la región y la prioridad de la securitización que cada país tenga.

La teoría también divide el nivel de estudio de la seguridad en tres: nacional, regional y global, el cual generalmente solo se estudia el nivel nacional y global, dejando a lado el regional, y es aquí donde está teoría entra al abordar el estudio regional de seguridad y unificándolo con el estudio global y nacional de la seguridad.[54]

La teoría menciona la existencia de cuatro niveles que se interrelacionan y que estudia la teoría de CSR, lo cual conforman la llamada "constelación de seguridad", y podría considerarse como las etapas de un CSR, estas son:[55]

1.- Nacionalmente en los Estados de la región, particularmente sus vulnerabilidades generadas en el ámbito interno (¿es la fortaleza o debilidad, debida a la estabilidad del orden interno y corresponde entre el Estado y la nación? La vulnerabilidades específicas de un Estado define el tipo de temores de seguridad que tiene y a veces hace a otro Estado o grupo de Estados una amenaza estructural, incluso si ellos no tienen intenciones hostiles).

2.- Relación entre Estado-Estado (donde le da forma a la región como tal).

3.- Interacción entre la región con otras regiones vecinas (este supuesto está relativamente limitado, dado que la interacciones internas en la región son más importantes que las externas. Pero en los cambios sustanciales en los patrones de interdependencia de la seguridad que define los complejos están en marcha, este

[54] Ibíd., (pág.43).

[55] Versión original: 1.- *domestically in the states of the region, particularly their domertically generated vulnerabilities (is the state strong or weak due to stability of the domestic order and correspondence between state and nation? The specific vulnerability of a state defines the kind of security fears it has and sometimes makes another state or group of states a srtuctural threat even if it or they have no hostile intentions).* 2.- *state-to-state relations (which generate the region as such).* 3.- *the region´s interaction with neighbouring regions (this is suposed to be relatively limited given that the complex is defined by interaction internally being more important. But if major changes in the patterns of security interdependence that define complexes are underway, this level can become significant, and in situations of gross asymmetries a complex without global powers that neigbours one with a global power can have strong interregional links in one direction).* 4.- *the role of global powers in the region (the interplay between the global and regional security structures).* Ibíd., (pág.51).

nivel puede convertirse significante y en situaciones de groso asimétricas un complejo sin poderes globales que sus vecinos uno con poder global puede tener la fuerza interregional vinculada en una dirección).

4.- El rol de los poderes globales en la región (la interacción entre las estructuras globales y regionales de seguridad).

Esta teoría fue elegida al aceptar que la seguridad tradicional quedó rebasada ante el nuevo panorama internacional, admitiendo que el Estado ya no es el único actor y de la existencia de múltiples actores; como también, de diversos sectores para el estudio de la seguridad, a pesar que esta teoría no reconozca el sector cibernético para el estudio de la seguridad, en la realidad internacional este ya es mencionado en dos de los tres niveles e incluso ya está securitizado: Local (Seguridad Nacional de los países donde se admite los riesgos del ciberespacio), Regional (donde existe un desarrolló regional de la ciberseguridad como el caso de la OTAN, Unión Europea y de la Organización de Estados Americanos), mientras en el caso Global, no existe todavía una coordinación entre los Estados para el desarrollo cibernético dentro del Derecho Internacional, pero se empieza a buscar.

En el caso de México, su evolución en materia de ciberseguridad se debe mucho la Organización de Estados Americanos (OEA), el cual en el año 2017 ayudó a desarrollar su Estrategia Nacional de Ciberseguridad, aquí se ve como la securitización de la ciberseguridad dentro de la región principalmente latinoamericana se ha ido consolidando, al ser la OEA un punto referente para la evolución de la ciberseguridad dentro de la región, por eso la Teoría de los Complejos de Seguridad Regional explica muy bien el desarrollo de los sectores de seguridad dentro de las regiones y sus interacciones tanto interna como externamente.

1.2.2 PROBLEMÁTICA DE CONCEPTOS PARA LA CIBERSEGURIDAD

Antes de iniciar con el concepto de ciberseguridad, se debe de tener claro lo que significa “ciber” y “seguridad”, la Real Academia Española (RAE) define “seguridad” como: Cualidad de seguro[56]; o entendido mejor como ausencia de peligro o riesgo. Esto a modo general, porque hay diferentes variantes de seguridad dependiendo el contexto. Mientras “ciber”: elemento- compositivo: Indica relación con redes informáticas[57]. Como tal el concepto de ciberseguridad no existe en la RAE.

Se entiende que la ciberseguridad se enfoca en la prevención y el uso seguro dentro de su entorno de trabajo que es la red. La ciberseguridad en la actualidad no es la misma que la de principios de siglo, ya que el concepto va evolucionando conforme la tecnología va avanzando; también se le suma una problemática que es la ambigüedad y diversidad en las definiciones para la ciberseguridad hechas por organismos internacionales, instituciones gubernamentales, sector privado o académicas, donde persiguen objetivos diversos, es por eso que se decidió citar algunas definiciones para demostrar las diferentes variantes del concepto de ciberseguridad:

La Unión Internacional de Telecomunicaciones (UIT)[58] en su resolución 181, donde se encuentra la recomendación UIT-T X.1205[59] (se realizó en la Ciudad de

[56] RAE. Definición de “Seguridad”. *RAE.* Recuperado de: http://dle.rae.es/?id=XTrIaQd Fecha de consulta: 12/10/2017.
[57] RAE. Definición de “Ciber”. *RAE.* Recuperado de: http://dle.rae.es/?id=98ULSyc Fecha de consulta: 12/10/2017.
[58] Es un organismo internacional autónomo y especializado para las Naciones Unidas en materia de Telecomunicaciones, es una de las pocas organizaciones internacionales más longevas, su fundación data desde 1865 y en la actualidad cuenta con 193 Estados miembros y con la participación de más de 700 organizaciones del sector gubernamental y privado, como académicas, empresariales (líderes en comunicaciones), organismos regionales, entre otros. Su objetivo principal es el apoyar el desarrollo de las tecnologías de comunicación, hacer recomendaciones y dar asesoramientos. UIT. Acerca de la UIT. *UIT.* Recuperado de: http://www.itu.int/es/about/Pages/default.aspx Fecha de consulta: 10/07/2017.
[59] UIT. (2010). Ciberseguridad. *UIT.* [Archivo PDF]. Recuperado de: https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf Fecha de consulta: 13/07/2017.

Guadalajara, Jalisco, México), define a la ciberseguridad y llama a trabajarla con base a esta definición:

> "Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: Disponibilidad; Integridad, que pueda incluir la autenticidad y el no repudio; Confidencialidad"

Otra definición, es hecha por la Conferencia de Profesionales de Seguridad de la Asociación de Auditoría y Controles de Sistema de Información (ISACA, por sus siglas en inglés)[60], capítulo Monterrey en que la ciberseguridad lo define como[61]:

> "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados."

Estas dos definiciones de ciberseguridad se basan dentro del área empresarial y de usuarios, no desde el punto de vista del Estado, no es de extrañar que exista una norma por parte de la Organización Internacional de Estandarización (ISO, por sus siglas en inglés)[62] el cual emite el "ISO 27001- Sistema de Gestión de Seguridad de la Información". Esta norma consiste en describir el cómo gestionar

[60] Es una asociación internacional independiente fundada en 1967, que se dedica al desarrollo, adopción y uso de conocimientos y prácticas globales aceptados por la industria para sistemas de la información. ISACA. Sobre ISACA. *ISACA.* Recuperado de: http://www.isaca.org/about-isaca/Pages/default.aspx Fecha de consulta: 13/07/2017.

[61] Miguel Ángel Mendoza. (16 de junio 2015) ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia. *Welivesecurity*. Recuperado de: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/ Fecha de consulta: 13/07/2017.

[62] Es una organización internacional no gubernamental, creada en 1947, que en la actualidad cuenta con 163 organismos nacionales de normalización. Es la responsable de emitir los "ISOS" el cual ofrecen especificaciones de clase mundial para productos, servicios y sistemas, para garantizar la calidad, seguridad y la eficiencia. ISO. Sobre ISO. *ISO.* Recuperado de: https://www.iso.org/about-us.html Fecha de consulta: 14/07/2017.

la seguridad de la información dentro de una empresa, de hecho puede ser aplicada en cualquier tipo de organización ya sea gubernamental o privada, permitiendo la certificación de organizaciones dentro de esta norma.[63]

En el caso de definiciones en diccionarios, existe una ausencia de concepto dentro de la Real Academia Españolan (RAE), esto se debe porque la palabra ciberseguridad es tomada de *cybersecurity*, una palabra anglosajona que aún no se encuentra registrada en la RAE; sin embargo, en el caso de diccionarios anglosajones, estos ya la definen. En el Diccionario de Inglés de Oxford lo define como: "El estado de protección contra el uso criminal o el acceso no autorizado de datos electrónicos, o las medidas adoptadas para lograrlo"[64]; mientras el Diccionario de Cambridge, define a la ciberseguridad como: "Maneras de proteger sistemas informáticos contra amenazas tales como virus".[65] Dichas definiciones son muy ambiguas, limitando a la ciberseguridad y por ende sus competencias.

Hablando desde el punto de vista del Estado y la que más importa en el presente trabajo; se notará que los objetivos que persigue la ciberseguridad son diferentes al del sector privado, y esto se ve con la definición de ciberseguridad por parte de España, el cual se encuentra en el Boletín Oficial del Ministerio de Defensa, mediante la Orden Ministerial 10/2013, del 19 de febrero de 2013, donde se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas:

> "Artículo 2.3 Ciberseguridad: Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan."[66]

---

[63] 27001 Academy. ¿Qué es norma ISO 27001? *ADVISER.* Recuperado de: https://advisera.com/27001academy/es/que-es-iso-27001/ Fecha de consulta: 14/07/2017.

[64] Versión original en inglés, traducción propia de: Oxford. Definición de "Ciberseguridad". *OXFORD.* Recuperado de: https://en.oxforddictionaries.com/definition/cybersecurity Fecha de consulta: 13/08/2017.

[65] Versión original en inglés, traducción propia de: Diccionario de Cambridge. Definición de "Ciberseguridad". *Cambridge.* Recuperado de: http://dictionary.cambridge.org/es/diccionario/ingles/cybersecurity#translations Fecha de consulta: 13/08/2017.

[66] Ministerio de Defensa de España. (26 de febrero de 2013). Boletín Oficial del Ministerio de Defensa Núm. 40. [Archivo PDF]. Recuperado de: http://www.emad.mde.es/Galerias/MOPS/novoperaciones/multimedia/documentos/20130226_CIBERDEFENSA.pdf Fecha de consulta: 14/07/2017.

Para enriquecer más a la definición, se puede agregar de la Ley de Seguridad Nacional de España:

> "Artículo 10. Ámbitos de Especial Interés en la Seguridad Nacional: Se considerarán ámbitos de especial interés de la Seguridad Nacional aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales. A los efectos de esta ley, serán, entre otros, la ciberseguridad (…).[67]"

Colombia es uno de los países latinoamericanos que más ha avanzado en materia de ciberseguridad, desde el 2011 se aprobó los "Lineamientos de Política para Ciberseguridad y Ciberdefensa" Conpes 3701[68], el cual fue el antecedente de la "Política Nacional de Seguridad Digital" aprobada en el 2016. En el Conpes 3701 define a la ciberseguridad como:

> "Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética"

Para Estados Unidos la definición de ciberseguridad se encuentra en el Glosario del 2015 del Comité del Sistema Nacional de Seguridad (CNSS, *Committee on National Security Systems*) el cual cuenta con una gran cantidad de definiciones relacionadas al aparato estatal de Seguridad Nacional de los Estados Unidos.

> "Prevención de daños, protección y restauración de ordenadores, sistema de comunicación, servicios de comunicación electrónicos, servicio por cable, y comunicaciones electrónicas, incluyendo información contenida en ellas, para asegurar su disponibilidad, integridad, autenticación, confidencialidad y el no ser negadas*".*[69]

---

[67] Ministerio de la Presidencia y para las Administraciones Territoriales de España. (28 de septiembre de 2015). Ley de Seguridad Nacional. Recuperado de: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10389 Fecha de consulta: 24/11/2017.

[68] Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (14 de julio de 2011). Lineamientos de Política para Ciberseguridad y Ciberdefensa. *CONPES.* [Archivo PDF]. Recuperado de: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf Fecha de consulta: 13/08/2017.

[69] Versión original en inglés, traducción propia de: Comité del Sistema Nacional de Seguridad. (6 de abril de 2015). *Committee on National Security Systems (CNSS) Glossary*. [Archivo PDF]. Recuperado de: https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf Fecha de consulta: 13/08/2017.

Para extender más esta definición, de lo que le compete a la ciberseguridad y los riesgos que se encuentran en el ciberespacio, el Departamento de Seguridad Nacional (*Homeland Security*) de Estados Unidos, en su página oficial[70] cuenta con una visión amplia de la ciberseguridad, donde acepta que el ciberespacio y su infraestructura subyacente, son vulnerables a sufrir ataques cibernéticos provenientes de sofisticados actores cibernéticos y de Estados, estos actores explotan las vulnerabilidad encontradas para el robo de información y dinero, y desarrollan capacidades para interrumpir, dañar y sabotear servicios esenciales. En el caso de los delitos tradicionales, el ciberespacio hace factible los delitos relacionados con la pornografía infantil, fraude bancario y financiero, violaciones a la propiedad intelectual, entre otras. Ellos consideran al ciberespacio difícil de asegurar debido a la capacidad de diversos actores para operar desde cualquier parte del mundo para cometer ataques cibernéticos y encontrar alguna vulnerabilidad.[71]

Por parte de la Unión Europea (UE), en un comunicado por el Secretario General de la Comisión Europea el 8 de febrero del 2013, relacionado a la "Estrategia de Ciberseguridad de la Unión Europea: Un Ciberespacio Abierto, Protegido y Seguro"; define a la ciberseguridad como:

> "La ciberseguridad abarca por lo general las salvaguardias y medidas que pueden utilizarse para proteger el ciberespacio, en los ámbitos tanto civil como militar, de las amenazas inherentes a sus redes interdependientes e infraestructuras de información, o que pueden dañarlas. La ciberseguridad tiene como objetivo mantener la disponibilidad e integridad de las redes e infraestructuras y la confidencialidad de la información que contienen.[72]"

---

[70] Homeland Security. Cybersecurity Overview. *Homeland Security.* Recuperado de: https://www.dhs.gov/cybersecurity-overview Fecha de consulta: 14/07/2017.

[71] Con esa visión se puede ver el grado de importancia que le da Estados Unidos ya que cuenta con su propio cibercomando conocido como USACYBERCOM creado en el 2009 y formaba parte del Comando Estratégico (uno de los 9 Comandos del Departamento de Defensa de los Estados Unidos) pero en agosto de 2017 el actual presidente Donald Trump elevó al USACYBERCOM como un Comando Combatiente Unificado centrado en las operaciones militares cibernéticas con el que se finaliza con 10 comandos del Departamento de Defensa. Comando Estratégico de los Estados Unidos. *U.S. Cyber Command (USCYBERCOM).* Recuperado de: http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/ Fecha de consulta: 13/08/2017.

[72] Secretario General de la Comisión Europea. (8 de febrero de 2013). Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro. *Consejo de la Unión Europea*. Recuperado de: http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=es Fecha de consulta: 16/07/2017.

En el caso de México existen ya dos definiciones para la ciberseguridad, pero se abordarán en el último capítulo, que está relacionado a la Estrategia Nacional de Ciberseguridad.

Dentro de las definiciones anteriores mencionadas, existe una diferencia de prioridades para el concepto de ciberseguridad, para algunos (sector privado) la ciberseguridad tiene que ver con la protección de activos de información, protección de usuarios y organizaciones, integridad de servicios y aplicaciones, información almacenada, entre otros; mientras para los Estados, las competencias de la ciberseguridad abarcan la protección de infraestructura crítica, correcto funcionamiento de servicios e información, bienestar de ciudadanos e integridad de los servicios básicos para el funcionamiento del país, protección de información confidencial tanto civil como militar.

Es ahí que el concepto de la ciberseguridad es diferente entre el sector privado y el Estado, la discrepancia se da por los objetivos que persiguen, incluyendo que no puede existir una definición exacta y única para la ciberseguridad, pues conforme avance la tecnología, las características y competencia van aumentando, por ende el concepto va evolucionando; sumando que existe diferentes visiones para definir dicho concepto.

En el caso de México el sector privado es el que más desarrollado está en cuestiones de ciberseguridad, pero tienen una debilidad, pues la inversión de la ciberseguridad es para la protección de las infraestructuras de las TIC´s, excluyendo la capacitación y concientización para el personal de la empresa, a pesar que estudios han demostrado que el éxito de los ciberataques dentro del sector privado se debe gracias al personal que labora interna y externamente.[73]

[73] Secretaría de Marina & Centro de Estudios Superiores Navales. Op. Cit., (pág. 151).

1.2.3 CUANDO LA CIBERSEGURIDAD SE TERGIVERSA

Anteriormente se mencionó cuáles eran los muchos de los objetivos que perseguía la ciberseguridad dentro de las diversas definiciones y cómo se relacionaban con la Seguridad Nacional, teniendo en cuenta que algunas veces la ciberseguridad se moldea para cumplir intereses particulares. Este es el caso que se ha suscitado a nivel nacional e internacional, respeto al espionaje, robo de información y violación de la privacidad.

En Estados Unidos salió un caso con mucho eco internacional en el 2013; sobre Edward Snowden, un contratista que trabajó para la Agencia Central de Inteligencia (CIA, *Central Intelligence Agency)* y era consultor en la Agencia de Seguridad Nacional (NSA, *National Security* Agency), el cual filtró documentos sobre lo que se considera el mayor caso de ciberespionaje en el mundo. Las repercusiones diplomáticas para los Estados Unidos fueron graves principalmente con los países como Rusia y China, mientras con sus socios europeos como España, Alemania y Reino Unido, estos no le dieron tanta importancia ya que más adelante se destaparía que las agencias de inteligencia de dichos países trabajaban en coalición con Estados Unidos en cuestiones de espionaje. Conforme pasaba el tiempo salieron documentos sobre la colaboración y el uso de programas de espionaje por parte de Estados Unidos hacia su población, mandatarios y países, todo esto justificado por sus políticas de Seguridad Nacional para la prevención del terrorismo. De las revelaciones más importantes que hizo Snowden se encuentra:

- Programa PRISM: que era un sistema lanzado en 2007 por la NSA que permite interceptar miles de comunicaciones privada de gigantes tecnológicos como Google, Yahoo, Facebook, Apple, Microsoft, entre otras, (con o sin su consentimiento) por parte de cualquier agencia estadounidense de vigilancia e inteligencia. Esta información recopilada era analizada por diversos sistemas.[74]

[74] Jenaro Villamil. (2016, Agosto). Las redes sociales vértigo y pasión. *Proceso. (Edición Especial 53).* pág. 33.

- El servicio de inteligencia del Reino Unido: Cuartel General de Comunicaciones del Gobierno (GCHQ, *Government Communications Headquarters*)[75] junto con la NSA de Estados Unidos, intervenían los cables submarinos de internet, instalando accesos a través de puertas traseras a los servidores de compañías privadas y trabajaban para romper (y debilitar) los estándares de encriptación.[76]

- Espionaje a embajadas, instituciones y diversos mandatarios, entre ellos al ex presidente de México, Felipe Calderón.[77]

- Geolocalización por parte de la NSA, que guarda datos de geolocalización de varios millones de dispositivos móviles. Con dicha información se puede indagar si hubo contacto entre ciertas personas y sus conexiones, con el comparar la ubicación, fecha y hora de los celulares. [78]

Existe mucho más información relacionada a los documentos desclasificados, pero solo se mencionaron cuatro en el presente trabajo. ¿Hasta dónde puede ser permisible el escudarse en la Seguridad Nacional (ciberseguridad) para la invasión a la privacidad y el espionaje masivo a la propia población y países aliados? La justificación viene supuestamente del terrorismo y la prevención de amenazas provenientes de otros países, pero como se ha visto con los documentos filtrados, la visión del espionaje, recopilación de información e intrusión cibernética va más allá del terrorismo y la prevención, casi se podría decir, que es al grado de un autoritarismo y control gubernamental que se empieza a desarrollar en esta época; incluso Estados Unidos no es el único Estado que ha desarrollado y aplicado estas

[75] Agencia de Inteligencia de señales y comunicaciones del Reino Unido, con una historia que la ubica desde 1914; su propósito es Defender los sistemas gubernamentales, protección de amenazas cibernéticas, terrorismo, espionaje y apoyo a las operaciones de la Fuerzas Armadas. Depende del Ministerio de Asuntos Exteriores, y su sede principal está en Cheltenham, Gloucestershire. GCHQ. *Who we are*. Recuperado de: https://www.gchq.gov.uk/ Fecha de consulta: 24/07/2017.

[76] Bartlett. Op. Cit., (págs. 103 y 104).

[77] Proceso. (21 de octubre de 2013). Calderón se indigna por espionaje en su contra: es un agravio a instituciones, dice. *Proceso.* Recuperado de: http://www.proceso.com.mx/356019/calderon-se-indigna-por-espionaje-en-su-contra-es-un-agravio-a-instituciones-dice Fecha de consulta: 20/07/2017.

[78] MILENIO. (31 de julio de 2014). Las Principales Revelaciones de Snowden. Recuperado de: http://www.milenio.com/internacional/principales-revelaciones-Snowden_0_345565796.html; Fecha de consulta: 24/07/2017.

herramientas, sino que varios países considerados potencias lo han hecho; como también, algunos países que se les ubica en vías de desarrollo, han aplicado acciones similares o de otro tipo, pero que tienen el mismo fin.

México no se queda atrás, la ciberseguridad se centra principalmente al campo del espionaje a partidos políticos, contra Organizaciones No Gubernamentales, personajes públicos y la manipulación de información dentro de las redes sociales, logrando influir en la opinión pública, algo que se convirtió en una rutina dentro del sexenio actual. El ciberespionaje está considerado como una herramienta dentro de la ciberseguridad y está sustentado en diversas leyes, como en la Ley de Seguridad Nacional de México, siempre y cuando sea para salvaguardar precisamente la integridad del Estado o perseguir delitos.

En el presente año salió a la luz información sobre un *spyware*[79] israelí llamado "Pegasus" adquirido por el gobierno de Enrique Peña Nieto, con el propósito de espiar a otros sectores políticos, a medios de comunicación y a dirigentes de organizaciones civiles; el uso de este software está relacionado con el actual gobierno, porque solo puede ser adquirido por Estados, con el objetivo principal de combatir el terrorismo y crimen organizado; algo que México no considera tan prioritario, o en aras de la libertad de expresión y otros derechos fundamentales.

En el informe documentado[80] por Red en Defensa de los Derechos Digitales (R3D)[81] en colaboración con *Citizen Lab*[82] y otras organizaciones, menciona a las

[79] Es un tipo de software que se instala automáticamente sin el consentimiento del usuario y se ocupa de recopilar información y rastrear la actividad dentro del dispositivo infectado. Puede conocer las páginas web que se visita, compras en línea, correo electrónico, cuentas bancarias, entre otros. Sandra Fernández Moreno. (12 de octubre de 2015). ¿Qué es spyware? Definición y tipos. *ValorTOP.* Recuperado de: http://www.valortop.com/blog/que-es-un-spyware Fecha de consulta: 13/10/2017.

[80] R3D: Red en Defensa de los Derechos Digitales. (19 de junio de 2017). Informe: Gobierno Espía: Vigilancia Sistemática a Periodistas y Defensores de Derechos Humanos en México. *R3D*. Recuperado de: https://r3d.mx/2017/06/19/gobierno-espia/ Fecha de consulta: 19/07/2017.

[81] Es una organización mexicana que se dedica a la defensa de los derechos humanos en el entorno digital. R3D. Quiénes somos / Qué hacemos. Recuperado de: https://r3d.mx/nosotros/ Fecha de consulta: 19/07/2017.

[82] Es un laboratorio ciudadano de la Universidad de Toronto, que se encarga de la investigación y desarrollo en la intersección de las tecnologías de la información y la comunicación, los derechos humanos y la seguridad global. Sus investigaciones incluyen: espionaje digital contra la sociedad civil, documentación filtrada en internet, análisis de privacidad, entre otras. THE CITIZEN LAB. About the citizen lab. *THE CITIZEN LAB* Recuperado de: https://citizenlab.ca/about/ Fecha de consulta: 19/07/2017.

instituciones que adquirieron Pegasus: la Secretaría de la Defensa Nacional (SEDENA), Procuraduría General de la República (PGR) y el Centro de Investigación y Seguridad Nacional (CISEN), éste último de acuerdo a fuentes consultadas del sector de seguridad, el CISEN tiene el "Switch Access" para operar los equipos y sistemas, mientras las otras dependencias tienen el acceso restringido.[83]

El software fue vendido por NSO Group[84], una empresa israelita que se dedica a proporcionar tecnologías de invasión y espionaje a gobiernos. El contagio se produce mediante un mensaje de texto (SMS) o por enlaces maliciosos en correos electrónicos[85], una vez infectado el dispositivo, se obtiene acceso a todo el teléfono: archivos, datos del calendario, listas de contactos, contraseñas, fotos, aplicaciones instaladas; así como, acceso a escuchar llamadas realizadas por teléfono, a través de WhastApp o Viper y permiso para grabar activa o pasivamente utilizando micrófono y cámara. Todo esto desde manera remota y teniendo como características que se puede autodestruir una vez que se haya descubierto o lleve tiempo sin comunicarse a los servidores. De los principales afectados se encuentran:

- Promotores del impuesto a bebidas azucaradas y otras regularizaciones para combatir a la obesidad[86]: Alejandro Calvillo, director de El Poder del

[83] Jorge Carrasco & Mathieu Tourliere. (24 de junio de 2017). Pegasus, el arma peñista para espiar. *Proceso.* Recuperado de: http://www.proceso.com.mx/492358/pegasus-arma-penista-espiar Fecha de consulta: 19/07/2017.

[84] En un artículo publicado en *Forbes* hablando sobre esta empresa israelita, menciona el autor que la ha estado siguiendo por 2 años, pero no cuentan con sitio web y ha estado erradicando; desde su fundación, casi toda su presencia en línea. También ha estado buscando entrevistar a su fundador, pero éste lo evade; el autor habla de la creencia que el cofundador y fundador son egresados del brazo de inteligencia israelí "Unit 8200". Thomas Fox-Brewster. (18 de abril de 2017). NSO Group: Los espías israelíes que hackean iphone con un solo SMS. *Forbes México.* Recuperado de: https://www.forbes.com.mx/nso-group-los-espias-israelies-que-hackean-iphones-con-un-solo-sms/ Fecha de consulta: 19/07/2017.

[85] R3D: Red en Defensa de los Derechos Digitales. (11 de febrero de 2017). Destapa la vigilancia: promotores del impuesto al refresco, espiados con malware gubernamental. *R3D.* Recuperado de: https://r3d.mx/2017/02/11/destapa-la-vigilancia-promotores-del-impuesto-al-refresco-espiados-con-malware-gubernamental/ Fecha de consulta: 19/07/2017.

[86] El Poder del Consumidor. (13 de febrero de 2016). El espionaje del gobierno de México contra defensores del derecho a la salud no debe quedar impune: OSC. [Archivo PDF]. Recuperado de: http://elpoderdelconsumidor.org/wp-content/uploads/2017/02/b-el-espionaje-del-gobierno-de-mexico-a-activistas-no-debe-quedar-impune.pdf Fecha de consulta: 19/07/207.

Consumidor; Doctor Simón Barquera, investigador del Instituto Nacional de Salud Pública y Luis Encarnación, director de la coalición ContraPESO.

- Aristegui Noticas
- Centro de Derechos Humanos Miguel Agustín Pro Juárez, A.C. (Centro Prodh)
- Carlos Loret de Mola
- Instituto Mexicano para la Competitividad A.C. (IMCO)
- Mexicanos contra la Corrupción y la Impunidad (MCCI)

En el 2016, organizaciones defensoras de derechos digitales querían ampararse contra los artículos 189 y 190 de la Ley Federal de Telecomunicaciones, en donde las compañías proveedoras de telecomunicaciones se les ordenaban guardar los "metadatos"[87] por 2 años de sus usuarios, en caso que instituciones competentes las requirieran. Dichas organizaciones estaban en contra de ambos artículos, ante la violación de privacidad y la revelación de cuestiones sensibles de los individuos como sus preferencias políticas, religiosas o sociales.[88]

Este uso indebido que le da el gobierno a este tipo de tecnologías viene de la mano con los casos de corrupción e impunidad que han salido durante el sexenio del presidente Enrique Peña Nieto, la baja aprobación en su gobierno ha ocasionado que instituciones del gobierno federal lleven a cabo estas tipo de acciones y que van en contra de las leyes que marcan diversos estatutos dentro del país.

En el caso de solicitudes de información por parte del gobierno, a las principales redes sociales como Facebook, Google o Twitter[89]; se menciona que:

[87] Es toda la información producida por un individuo que abarca, llamadas y mensajes con fecha, hora y duración, contactos y geolocalización.
[88] Jenaro Villamil. (2016, Agosto). Las redes sociales vértigo y pasión. *Proceso. (Edición Especial 53).* pág. 34-36.
[89] Ernesto Aroche Aguilar. (3 de julio de 2017). Gobierno duplica en 4 años sus solicitudes de datos sobre usuarios de Facebook, Twitter y Google. *Animal Político.* Recuperado de: http://www.animalpolitico.com/2017/07/datos-solicitudes-redes-gobierno/ Fecha de consulta: 19/07/2017.

- Google: en el año 2013 el gobierno mexicano solicitó 164 peticiones de información que involucraba a 286 usuarios; para el 2016 estas ascendieron a 352, involucrando a 475 usuarios.
- Facebook: En el primer año del gobierno de Enrique Peña Nieto solicitó 573 peticiones de información que involucraba a 986 usuarios; para el cuarto año creció a 1,162 peticiones que involucraban a 1,922 usuarios, pero Facebook solo respondió para el 2016, 74.3% de solicitudes.
- Twitter: En al año 2013 se hicieron 12 solicitudes de información que involucraba 23 cuentas; para el año 2016 subió a 25 peticiones, involucrando a 62 cuentas.

Otro estudio que evidencia estas prácticas por parte de los Estados, fue en el año 2017, donde salió en los medios informativos un estudio realizado por la Universidad de Oxford llamado: *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*[90], el cual evidenció a 28 países usando "soldados cibernéticos" para manipular la opinión pública o censurar información dentro de las principales redes sociales,[91] figurando México en dicha lista; lo sorprendente fue que no solo los gobiernos autoritarios sino también países democráticos llevan a cabo dichas prácticas.[92]

En el estudio se destaca la capacidad operativa de algunos países para controlar la opinión pública, desviarla o incluso censurarla, dentro de sus capacidades, aplicando diversas herramientas, también se hace mención del uso de Bots, Cyborgs y Capital Humano, esto con el propósito de crear diversas

[90] Universidad de Oxford. (2017). Troops, Trolls and Troublemakers: A Gblobal Inventory of Organized Social Media Manipulation.Oxford Internet Institute. Oxford. *Oxford.* [Archivo PDF]. Recuperado de: http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf Fecha de consulta: 18/07/2017.

[91] Adam Satariano. (17 de julio de 2017). Gobierno mexicano, entre los que "meten mano" a redes para influir en opinión pública: estudio. *El Financiero.* Recuperado de: http://www.elfinanciero.com.mx/tech/mexico-entre-gobiernos-que-manipulan-facebook-y-redes-sociales-estudio.html Fecha de consulta: 18/07/2017.

[92] Los países mencionados son: Argentina, Azerbaiyán, Australia, Brasil, República Popular de China, República Checa, Ecuador, Alemania, India, Irán, Israel, México, Corea del Norte, Filipinas, Polonia, Rusia, Arabia Saudita, Serbia, Corea del Sur, Siria, Taiwán, Turquía, Ucrania, Estados Unidos, Reino Unido, Venezuela y Vietnam.

expectativas mediante “Likes”, influenciar a los usuarios o desviar acontecimientos importantes que ocurran dentro de los países.

En el caso de México se ha creado mediante estas técnicas, comentarios a favor del gobierno; como también, interacciones negativas o agresivas hacia usuarios que critiquen al gobierno a través de cuentas falsas, de las cuales son operadas por Bots, Cyborgs[93] e incluso agentes de gobierno. Dentro de las principales categorías de actores que ocupan está estrategia se encuentran[94]:

- Gobiernos, para influenciar la opinión social positivamente;
- Políticos y Partidos, para crear expectativas sobre ellos y así obtener más votos;
- Contratistas Privados, generalmente son individuos o empresas contratadas por políticos o el gobierno;
- Grupos Voluntarios, para favorecer la opinión a favor de una ideología o programa político;
- Ciudadanos, conocidos como *Hackers*[95] para trabajar individualmente a favor del gobierno, estos no están afiliados al gobierno, pero comparten ideas con él.

En México, el estudio menciona a 3 tipo de actores: Dentro de la categoría de Políticos y Partidos: El Partido Revolucionario Institucional (PRI), de la categoría de Ciudadanos: Tiene evidencia encontrada (pero no se menciona): y por último dentro de la categoría de Contratistas Privados se encuentra el caso de Andrés

[93] Es la combinación de la automatización e interacción humana, para ayudar a evitar la detección y hacer las interacciones más naturales.

[94] Estados Unidos es el único que hace uso de estas 5 categorías, seguido de Filipinas, Rusia y Arabia Saudita usan solo 4 categorías.

[95] Existe una problemática para definir el concepto de la palabra *Hacker* esto debido a tres factores: el primero es que esta contiene diversas definiciones, algunos le dan atribuciones relacionadas a personas que se dedican al cibercrimen o ciberataques (cibercriminales), mientras otros lo definen como personas eruditas del tema y que se dedican a señalar los fallos de redes o programas; el segundo factor es que la palabra *Hacker* es un extranjerismo el cual se traduciría como “pirata informático”, pero este término es opacado por su traducción, pues “pirata informático” le da un lado negativo y no comprende su lado positivo; y el tercer factor es la existencia de diversas categorías de la palabra *Hacker.* En este trabajo tendrá las connotaciones negativas. Bartlett. Op. Cit., (pág. 28).

Sepúlveda[96]. El estudio también hace referencia a que México ha gastado un aproximado de 600,000 dólares para el uso de estas herramientas y su aplicación.

Todo esto demuestra un fenómeno que se empieza a normalizar a nivel internacional y nacional, donde el Estado tergiversa a la ciberseguridad para perseguir sus propios intereses particulares y no de seguridad, justificando el espionaje masivo y la recopilación de información como acciones para prevenir el terrorismo o amenazas militares de países que se consideren una amenaza a la Seguridad Nacional, pero estas acciones no va en contra de los objetivos antes mencionados sino en contra de la sociedad civil o medios sociales e informativos Un panorama donde para el Estado, el fin sí justifica los medios.

[96] Es el hacker colombiano que logró ayudar a ganar al presidente Enrique Peña Nieto, en las elecciones presidenciales del 2012, aplicando métodos como el robo de estrategias de campaña, manipulación de redes sociales para crear falsos sentimientos de entusiasmo e instalaciones de spyware en sedes de campaña de la oposición; también se le atribuye el haber intervenido en las elecciones de diversos países latinoamericanos como Nicaragua, Panamá, Honduras, El Salvador, Colombia, Costa Rica, Guatemala y Venezuela. Jordan Robertson, Michael Riley & Andrew Willis. (31 de marzo de 2016). Cómo Hackear una Elección. *Bloomberg Businessweek.* Recuperado de: https://www.bloomberg.com/features/2016-como-manipular-una-eleccion/ Fecha de consulta: 19/07/2017.

CAPÍTULO II PANORAMA DE LA CIBERSEGURIDAD A NIVEL INTERNACIONAL

2.1 PRINCIPALES SUCESOS QUE MARCARON A LA CIBERSEGURIDAD

Se han suscitado a lo largo de este siglo diversos ataques cibernéticos a nivel mundial, muchos de ellos tuvieron objetivos y rangos de daños diferentes, pero solo ha habido tres sucesos que marcaron la ciberseguridad a nivel mundial, el primero, marcó la importancia de la ciberseguridad para un país; el segundo, de la importancia militar y el grado de desarrollo de armas cibernéticas de diversos países; y el tercero, demostró lo que les espera a los Estados con ataques cibernéticos cada vez más sofisticados y con un rango de alcance global.

El primer suceso fue en el 2007 a un país del Báltico llamado Estonia, este país fue el objetivo de una serie de ataques que tumbaron todas las páginas de gobierno, sistema financiero, medios informativos, entre otras páginas web, sembrando el caos dentro de la población. Este ciberataque marcó un hito que demostró a nivel internacional la importancia de trabajar en la concepción de la ciberseguridad, y de cómo un simple ataque dentro de Internet pudo tener afectaciones en el mundo físico y a la Seguridad Nacional de un país, sin mencionar que gracias a esto, la Organización del Tratado del Atlántico Norte (OTAN) desarrolló la ciberseguridad al grado de contarla como una campo operacional militar y un área a evolucionar dentro de la defensa colectiva de la organización.

El segundo ataque fue a las instalaciones nucleares de la República Islámica de Irán, con un tipo de virus llamado Stuxnet, el cual tenía como objetivo sabotear su programa nuclear con el fin de evitar su desarrollo, este virus a diferencia de otros podía actuar autónomamente, a pesar de las sospechas de quienes lo perpetraron, no se pudieron recabar las pruebas necesarias para culparlos. El virus se logró ubicar y controlar, teniendo como resultado la creación del cibercomando de Irán y el inicio de programas cibernéticos militares.

El tercero y último ocurrió en el 2017, y demostró el grado de alcance que tendrán los ataques cibernéticos. El ciberataque fue hecho con un gusano informático llamado *Wannacry*, que se expandió en cuestión de horas a nivel mundial teniendo afectaciones en más de 150 países. Es la primera vez que se tiene registro de un ataque de esta magnitud, el cual muchos especialistas en temas de ciberseguridad creen que en un futuro serán más agresivos y complejos, y hacen un llamado a la comunidad internacional para empezar a trabajar en sus políticas cibernéticas tanto nacional e internacionalmente.

2.1.1 ESTONIA

Estonia nace en 1991 al independizarse por segunda vez de la Federación Rusa (la primera fue del Imperio Ruso y la segunda de la extinta URSS). Se ubica en la zona báltica que se encuentra en Europa del Este y es miembro desde el 2004 de la Unión Europea (UE) y la Organización del Tratado del Atlántico Norte (OTAN).

Estonia se convirtió en el centro cibernético de la OTAN y Europa, ya que es considerado el *Silicon Valley* europeo; es el principal país con políticas cibernéticas avanzadas a nivel mundial, que desde el 2002 ya ofrecía a su población la capacidad de votar en elecciones desde Internet; más del 90% de las operaciones bancarias se hacen por internet[97]; casi todo el territorio tiene conexión wifi pública; y el Internet lo consideran un derecho fundamental.[98] Como también, en él se encuentra el Centro de Excelencia de Cooperación de Ciberdefensa (CCDCOE por

[97] Actualmente el gobierno de Estonia busca lanzar una moneda virtual "Estcoin", la cual sería controlada por el gobierno, pero el Banco Central Europeo se opuso a ésta iniciativa dado que solo el Euro es la única moneda que puede utilizar un país miembro. Reuters Staff. (7 de septiembre de 2017). *ECB´s Draghi rejects Estonias´s virtual currency idea. Reuters.* Recuperado de: http://www.reuters.com/article/us-ecb-bitcoin-estonia/ecbs-draghi-rejects-estonias-virtual-currency-idea-idUSKCN1BI2BI?feedType=RSS&feedName=technologyNews Fecha de consulta: 12/09/2017.

[98] De hecho se ha introducido el acceso a Internet como un derecho básico por diversos países, entre ellos se encuentran: Estonia (2000), Grecia (2001, lo elevó como un derecho constitucional), la Unión Europea (2002), España y Finlandia (2003), Alemania (2004), Turquía (2010), y la Organización para la Seguridad y la Cooperación en Europa OSCE (2011). García Mexía. Op. Cit., (pág. 104).

sus siglas en inglés), la base cibernética de la OTAN, todo esto gracias al efecto que tuvo un ataque cibernético sufrido en el 2007.

Este ataque inició por cuestiones históricas, en la II Guerra Mundial Estonia había sido ocupada por la Alemania Nazi, hasta que los soldados de la URSS los expulsaron y terminaron ocupándola, en ese momento miles de rusos fueron enviados a vivir a Estonia y erigieron un monumento en la capital para los soldados soviéticos caídos. Cuando Estonia se separó de la ya extinta URSS en 1991, aún existía una proporción significante de comunidad rusa. En el 2007 el gobierno estonio aprobó un plan para trasladar el monumento del centro de la capital a un cementerio militar,[99] esto inició una serie de protestas por parte de población étnica rusa, el cual obligó al gobierno a trasladar el monumento en la madrugada, y en la mañana inicio el primer ataque cibernético a gran escala hacia el país.

El ataque fue hecho en base a la denegación de servicio (DDoS)[100], a través de Botnets[101] los cuales se les ordenó conectarse e incrementar el tráfico de información en los servicios de bancos, instituciones, medios de comunicación, páginas de gobierno, página web de la policía y el servicio nacional de emergencias,[102] logrando que se cayeran todos estos servicios dentro del Internet, ocasionando una parálisis completa dentro del país, para contrarrestar esto, el gobierno de Estonia bloqueó todo el tráfico internacional de Internet y acusó al

[99] Ricardo Martínez de Rituerto. (18 de mayo de 2017). Los "ciberataques" a Estonia desde Rusia desatan la alarma en la OTAN y la UE. *El País.* Recuperado de: https://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html Fecha de Consulta: 31/08/2017.

[100] El diccionario del CERT-UNAM lo define como: Un tipo de ataque de Negación de Servicio en el cual un intruso utiliza código malicioso instalado en varias computadoras para atacar un solo objetivo. Un intruso podría utilizar éste método para tener un efecto mayor en el objetivo que el que se obtendría con un ataque desde una sola computadora. CERT-UNAM. Diccionario. *CERT-UNAM.* Recuperado de: https://www.seguridad.unam.mx/taxonomy/term/1030 Fecha de consulta: 13/10/2017.

[101] Los Botnets son una red de dispositivos infectados que están compuestas por máquinas de todo el mundo. Estos dispositivos son controlados por Bots el cual es un programa malicioso que permite tomar el control de la máquina infectada convirtiéndolos en "zombies". Norton. Bots y botnets: Una amenaza creciente. *Norton.* Recuperado de: https://mx.norton.com/botnet Fecha de consulta: 13/10/2017.

[102] García Mexía. Op. Cit., (pág. 99).

gobierno ruso de Vladimir Putin de llevar acabo dichos ataques, al encontrar direcciones IP ubicadas en Rusia, el cual el Kremlin negó rotundamente.[103]

Estos sucesos marcaron la pauta del desarrollo cibernético de la OTAN, al ver que no pudieron hacer nada para contrarrestar el ataque. De ahí en adelante se ha desarrollado políticas colectivas cibernéticas, principalmente en el área militar creándose en Estonia el Centro de Excelencia de Cooperación de Ciberdefensa (CCDCOE, por sus siglas en inglés), el cual es un *Think-Tank* para las estrategias de ciberseguridad de la OTAN.

2.1.2 STUXNET

El segundo ataque fue realizado en el 2010 con el objetivo de sabotear el programa nuclear iraní. Este ataque fue hecho por un gusano tan sofisticado que sorprendió a los analistas de ciberseguridad a nivel mundial, al descubrir que su programación lo hacía único al darle autonomía e inteligencia. Este gusano llamado Stuxnet fue el primer ataque que logró dañar infraestructura del mundo real.[104] Los primeros indicios de Stuxnet se encontraron en una compañía de seguridad informática en Bielorrusia, el cual era el encargado de proteger el equipo informático de la central nuclear de Irán.

El objetivo de Stuxnet consistía en localizar y atacar el programa que controlaba a las centrifugadoras para el enriquecimiento de uranio en una planta nuclear, haciéndose del control de más de 1,000 máquinas las cuales autodestruía. Los científicos tardaron meses para lograr descubrirlo, y automáticamente culparon a Israel, pues a pesar que no se tenía pruebas sabían que ellos lo habían hecho.

---

[103] Álvaro Fernández. (12 de agosto de 2015). Estonia, baluarte de la ciberseguridad europea. *El Orden Mundial en el S.XXI.* Recuperado de: http://elordenmundial.com/2015/08/12/estonia-ciberseguridad-europea/ Fecha de consulta: 31/08/2017.

[104] BBC Mundo. (11 de octubre de 2015). El virus que tomó control de mil máquinas y les ordenó autodestruirse. *BBC Mundo.* Recuperado de: http://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet Fecha de consulta: 31/08/2017.

Años más tarde el periodista David E. Sanger en un adelanto del libro *Confront and Conceal: Obam´s Secret Wars and Suprising Use of America Power*, a través de varias entrevistas a funcionarios militares retirados, se confirmaría que el virus fue lanzado a las instalaciones nucleares de Irán para impedir la fabricación de armas nucleares y disuadir a Israel de atacar militarmente a Irán.[105]

Pero la pregunta fue el cómo logró entrar este virus a la planta nuclear, donde la red era aislada del Internet. En el documental *ZeroDays*[106] se menciona que robaron certificados originales para acceder al sistema operativo de Windows de dos empresas en Taiwán que resguardan certificados, una vez teniendo los certificados para esconder el virus dentro de los programas oficiales de Windows, dicho gusano se introdujo mediante la infección de dispositivos portátiles de los contratistas sin que ellos se dieran cuenta, logrando entrar a la terminal nuclear.

También el documental entrevista a una mujer con voz y cara desdibujada que pertenece a los servicios de inteligencia de Estados Unidos, el cual menciona que los creadores del gusano fueron principalmente la NSA, la CIA y el comando cibernético, en colaboración con la agencia de inteligencia israelí, Unidad 8200. También aborda las características que le dieron, el cual a diferencia otros virus convencionales que se conectan con su creador o atacante para recibir órdenes, este no lo hacía, ya que se le dio la habilidad de multiplicarse y entender qué objetivos atacar.

La entrevistada comenta que Stuxnet no tuvo el objetivo previsto, dado que fue lanzado por los israelís sin el consentimiento de la NSA sin antes mejorarlo, eliminando el factor sorpresa al ser descubierto por Irán y con las filtraciones de

[105] Lucía Luna. (5 de julio de 2013). Stuxnet: La filtración de un ciberataque. *Proceso.* Recuperado de: http://www.proceso.com.mx/346707/stuxnet-la-filtracion-de-un-ciberataque Fecha de consulta: 31/08/2017.

[106] El nombre del virus es escogido dentro de una serie de palabras que están dentro del código binario del virus: Stub+xnet: Stuxnet, pero su nombre oficial por el que lo conocían las agencias de inteligencia era Juegos Olímpicos. Recuperado de: Documental *Zero Days.* (2016). Directo Alex Gibney. Se puede visualizar en la plataforma de YouTube: https://www.youtube.com/watch?v=J50bUcf8gfc Fecha de consulta: 25/11/2017.

Snowden se supo que para utilizar un arma cibernética se necesita el consentimiento del presidente de los Estados Unidos.

Como consecuencia Irán creó su propio comando cibernético y lanzó ataques a Saudi Aramco, la petrolera más grande del mundo; y después una serie de ataques a bancos estadounidenses. Al terminar el documental la entrevistada mencionó que en caso de entrar en guerra con Irán en algún momento, Estados Unidos cuenta con un arma cibernética llamada *Nitro Zeus*, el cual es un arma a gran escala que se infiltraría en toda la red iraní tumbando toda telecomunicación del país.

2.1.3 WANNACRY

El tercer ataque ocurrió en mayo del 2017 y es el primer ataque a gran escala que se ha tenido registrado. El *ransomware*[107] WannaCry consistió en un tipo de virus informático que secuestraba y cifraba archivos y datos de una máquina, pidiendo al dueño un rescate entre $300-$600 dólares en *Bitcoins*[108] lo cual dificultaba el rastreo del dinero; como también, se llegó a convertir en la principal dificultad para cobrarlo, debido a que los usuarios infectados no sabían cómo conseguir *Bitcoins*. Su expansión consistió en que la víctima recibía un correo electrónico con un archivo relacionado a ella, tan pronto abría el archivo, WannaCry accedía al sistema de la máquina, haciéndose con todos los datos y bloqueaba cualquier acceso a esa información. WannaCry se expandió en cuestión de horas alrededor del mundo, afectando a más de 150 países; gracias a una vulnerabilidad

[107] Es un software malicioso que infecta a una máquina y le da al ciberdelincuente la capacidad de bloquear el dispositivo desde una ubicación remota, logrando encriptar todo archivo que se encuentre en ella y así le quita el control de toda la información y datos almacenados. Panda. (15 de noviembre de 2013). ¿Qué es un Ransomware?. *Panda.* Recuperado de: https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/ Fecha de consulta: 13/10/2017.

[108] Un bitcoin es una moneda virtual que no tiene un valor independiente, no está ligada a ninguna divisa del mundo real y no hay autoridad central que la controle. Las transacciones son seguras, rápidas y confiables ya que está basada en una cadena de bloques que no permite gastarse dos veces, está cadena de bloques llamada *Blockchain* permite que el Bitcoin sea una moneda segura contra los ciberdelincuentes (solo pueden existir 21 millones de Bitcoins). Bartlett. Op. Cit., (págs. 80, 81 y 98).

en el sistema operativo Windows[109] que Microsoft había arreglado dos meses atrás[110]. Este virus logró infectar a más de 300,000 computadoras alrededor del mundo.

Entre sus principales características, es que no necesitaba ser controlado por el atacante ya que se ejecutaba autónomamente igual que el virus Stuxnet. Dicho *ransomware* contenía los códigos de un arma cibernética desarrollada por un grupo de hackers llamados Equation Group para la Agencia de Seguridad Nacional (NSA); que salieron gracias al robo de herramientas de hackeo de la NSA a finales del 2016 por la organización de hackers llamados Shadow Brokers, dando códigos en subasta. Snowden había señalado a Rusia como responsable, [111] pero a finales de diciembre de 2017, el gobierno de Estados Unidos, culpó de forma oficial y pública a Corea del Norte como el responsable de dicho ataque cibernético, afirmando tener evidencia sólida y respaldada por diversos Estados y empresas.[112]

Microsoft culpó a las agencias de inteligencia de guardar en secreto las vulnerabilidades y usarlas como armas, ya que fue explotado un fallo por una herramienta llamada EternalBlue que le dio la característica de poder expandirse rápidamente en los sistemas operativos de Windows.[113] En cuestión de horas se

[109] El virus afectó a los sistemas: Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows XP, Windows 7, Windows 8.1, Windows RT 8.1, Windows Server 2012 and R2, Windows 10 y Windows Server 2016. Boletín de Seguridad UNAM-CERT-2017-001. (12 de mayo de 2017). Alerta por ransomware WannaCry. *CERT-UNAM.* Recuperado de: https://www.seguridad.unam.mx/node/355 Fecha de consulta: 02/09/2017.

[110] WannaCry se expandió porque las empresas no habían actualizado el sistema operativo, lo que ocasionó que no tuvieran el parche para bloquear el *ransomware* teniendo como consecuencia la rápida propagación. Microsoft al percatarse del virus también lanzó parches a los anteriores sistemas operativos que ya no ofrecía soporte.

[111] El País. (17 de agosto de 2016). Un grupo de hackers filtra programas de espionaje robados a la NSA. *El País.* Recuperado de: https://elpais.com/internacional/2016/08/17/actualidad/1471436554_088389.html Fecha de consulta: 03/09/2017.

[112] Estos son: Reino Unido, Australia, Canadá, Nueva Zelanda, Japón, Microsoft, Google, Symantec, FireEye, entre otras. Secuelist. (22 de diciembre de 2017). Estados Unidos acusa de forma frontal y sin tapujos a Corea del Norte por los ataques de WannaCry. *Securelist.* Recuperado de: https://securelist.lat/estados-unidos-acusa-de-forma-frontal-y-sin-tapujos-a-corea-del-norte-por-los-ataques-de-wannacry/85880/ Fecha de consulta: 28/12/2017.

[113] Forbes Staff. (15 de mayo de 2017). Microsoft acusa de negligencia a la NSA por hackeo masivo. *Forbes México.* Recuperado de: https://www.forbes.com.mx/microsoft-acusa-negligencia-la-nsa-hackeo-masivo/ Fecha de consulta: 02/09/2017.

logró controlar gracias a la vulnerabilidad[114] que descubrió un joven británico llamado Marcus Hutchins, el cual unos meses después fue arrestado por el Buró Federal de Investigaciones (FBI, *Federal Bureau of Investigation*) cuando iba rumbo a una conferencia de ciberseguridad en las Vegas, acusándolo de haber ofrecido tiempo atrás un software malicioso que robaba claves y contraseñas de páginas web de bancos en ordenadores infectados, si llegara a considerarse culpable por los delitos, se le pondría una condena de 40 años de cárcel en Estados Unidos.[115]

Después de dicho ataque surgió otro *ransomware* llamado Petya, el cual contaba con características similares a WannaCry, pero este gusano informático tuvo un menor rango de propagación, debido a las actualizaciones de Windows que impidió expandirse rápidamente; dicho *ransomware* infectó alrededor de 2 mil computadoras en países como Alemania, Estados Unidos, Francia y Reino Unido, pero el más afectado fue Ucrania; donde para liberar los equipos informáticos, se pedía un rescate de $300 dólares en Bitcoins.[116]

El sector más afectado en estos tipos de ataques es el empresarial, que aceptan pagar el monto solicitado para recuperar sus equipos, ya que cuentan con seguros que cubren los gastos realizados; sabiendo que no es recomendable pagar el rescate, debido a que en muy pocos casos los equipos son desbloqueados y fomentan este tipo de delitos cibernéticos.[117] Si bien, el ransomware se ha vuelto el más usado por los cibercriminales, gracias al auge de las criptomonedas como el Bitcoin, se espera que en un futuro estos ataques ya se empiecen a trasladar hacia

---

[114] Encontró que el *rasomeware WannaCry* se estaba esparciendo usando una dirección en internet, el cual no llevaba a ningún sitio dado que nadie había registrado ese dominio. (El dominio es la página base por el cual se estaba expandiendo. Un ejemplo de dominio es cuando se ingresa el URL de una dirección web esta termina en .com, .mx, entre otros.) El joven compró el dominio con $10,96 dólares, y al momento de ser propietario del dominio, se detuvo la expansión de *WannaCry.* BBC Mundo. (13 de mayo de 2017). MalwareTech, el joven que detuvo el ciberataque que secuestró computadoras en caso 100 países. *Animal Político*. Recuperado de: http://www.animalpolitico.com/2017/05/malwaretech-ciberataque-100-paises/ Fecha de consulta: 25/11/2017.

[115] Rosa Jiménez Cano. (6 de agosto de 2017). La caída del héroe que paró el virus WannaCry. *El País.* Recuperado de: https://elpais.com/internacional/2017/08/06/actualidad/1502011078_699717.html Fecha de consulta: 02/09/2017.

[116] Humberto Guerrero García & Staff Seguridad en América. (2017, Septiembre-Octubre). Seguridad en tiendas minoristas. *Seguridad en América.* (N° 104). págs. 46 y 47.

[117] Pablo Corona Fraga. (2017, Primer Cuatrimestre). Infraestructuras críticas. *SEGURILATAM.* (N°4). págs. 56 y 57.

los aparatos conectados a internet (IoT), como lavadoras, estufas, refrigeradores o autos; ocasionando ganancias y daños significativos.[118]

2.2 EL AVANCE DE LA CIBERSEGURIDAD A NIVEL INTERNACIONAL

La ciberseguridad ha empezado a afianzarse en políticas nacionales y regionales, creando marcos jurídicos para hacer frente a las amenazas provenientes del espacio cibernético. Existen leyes que rigen otros aspectos del ciberespacio como por ejemplo el tratado sobre la Propiedad Intelectual de la Organización Mundial de la Propiedad Intelectual (OMPI)[119] o la Convención de Budapest sobre el cibercrimen de la Unión Europea (UE)[120]; pero no existe ninguna relacionada a la ciberseguridad que abarque los aspectos militares o tenga alcances globales como es el caso de la Convención sobre las Armas Químicas o la Convención de Armas Biológicas.

En la actualidad la ciberseguridad dentro del Derecho Internacional, se encuentra en pleno auge, buscando nuevas alternativas para crear ramas como el derecho del Internet; la Organización de las Naciones Unidas (ONU) ha intentado

[118] Francisco Javier García Lorente. (2017, Segundo Cuatrimestre). Seguridad Aeroportuaria. *SEGURILATAM.* (N° 5). págs. 50 y 51.

[119] Es un organismo de las Naciones Unidas creado en 1967, que tiene como objetivo el desarrollar políticas, servicios, cooperación e información en materia de Propiedad Intelectual, la cual abarca el Sistema Internacional de Patentes, Sistema Internacional de Marcas y Sistema Internacional de Registro de Diseños. La OMPI cuenta con 189 Estados miembros. OMPI. ¿Qué es la OMPI?. Recuperado de: http://www.wipo.int/about-wipo/es/ Fecha de consulta: 10/08/2017.

[120] Hablando sobre el cibercrimen y la Unión Europea, a mediados del 2017 se llevó a cabo un gran golpe coordinado entre el Buró Federal de Investigaciones (FBI, por sus siglas en inglés), la Administración para el Control de Drogas (DEA, por sus siglas en inglés), la Policía Nacional de Países Bajos y la Europol contra dos sitios dentro de la Deepweb: Alphabay y Hansa, estos sitios eran considerados importantes en la venta ilícita de armas, drogas, malware, y donde se hicieron transacciones por más de 1.000 millones de dólares. Para más información véase en: Chema Flores. (20 de julio de 2017). Estados Unidos y Europa tumban los mercados ilegales más grandes de la dark web. *El Economista America.com* Recuperado de: http://www.economiahoy.mx/telecomunicacion-tecnologia-mx/noticias/8510839/07/17/Operacion-policial-sin-precedentes-EEUU-y-Europa-tumban-los-mercados-ilegales-mas-grandes-de-la-dark-web.html & Chris Baraniuk. (20 de julio de 2017). Duro golpe contra los traficantes de armas y drogas en la internet oscura: FBI y Europol cierran los mercados AlphaBay y Hansa. *BBC Mundo.* Recuperado de: http://www.bbc.com/mundo/noticias-internacional-40674538 Fecha de consulta: 06/12/2017.

desarrollar políticas similares, las cuales han sido entorpecidas o bloqueadas, incluso hay una laguna para considerar si un ciberataque puede ser considerado una “agresión” y en caso de eso, usar la “legítima defensa”.[121]

El problema de crear un convenio sobre ciberseguridad es la implicación que tiene al regular el dominio cibernético, algo muy difícil de hacer; dado que cada país tiene sus leyes nacionales que regulan el ciberespacio, difiriendo de otras; también existen intereses particulares de países potencia para no hacerlo, como es el caso de la República Popular de China donde se habla de una muralla digital, reafirmando así su cibersoberanía[122], o en el caso de Estados Unidos donde utiliza y desarrolla armas cibernéticas y de espionaje para sus objetivos de “Seguridad Nacional”; contando que el ciberespacio es considerada una competencia más de la soberanía nacional; todo esto se suma con las opiniones divididas para regularlo, debido a que algunos abogan que el ciberespacio debe ser libre, fuera de la jurisdicción de cualquier Estado, pero otros llaman a regularlo debido a la existencia de una “ciber-anarquía” dentro de Internet.[123]

Es muy complejo el regular un ámbito que está en constante evolución y es perfecto para fines militares, ya que un ataque proveniente de este entorno es muy difícil de ser rastreado; como también, el copilar pruebas para determinar de dónde provino, convirtiéndolo en un medio atractivo para el anonimato. Todo esto ha ocasionado que varias naciones empiecen a trabajar en ello, creando cibercomandos como el caso de España con el Mando Conjunto de Ciberdefensa o el de Estados Unidos con el USCYBERCOM.

---

[121] Segura Serrano, A., Gordo García, F., (Coords.). Op. Cit., (págs. 96-98).

[122] Definida por Zuo Xiaodong, director de la Universidad de China de Investigación de Seguridad de la Información: “La Cibersoberanía es la manifestación y extensión de la soberanía del Estado en el ciberespacio”. KATEHON. (20 de junio de 2017). La Ciber Política de China. *KATEHON.* Recuperado de: http://katehon.com/es/article/la-ciber-politica-de-china Fecha de consulta: 25/11/2017.

[123] Segura Serrano, A., Gordo García, F., (Coords.). Op. Cit., (pág. 42).

Cuando se suscitó el ataque a nivel mundial de WannaCry, el presidente y director jurídico de Microsoft, Brad Smith, señaló en la *RSA Conference*[124] la necesidad de crear un "Convenio Digital de Ginebra"[125] el cual comprometa a los Estados a proteger a su población de ataques cibernéticos en tiempos de paz y con la participación de empresas tecnológicas; también se señaló que el cibercrimen ocasionará para el 2020, pérdidas económicas de 3 billones de dólares. Por otro lado, Tomáš Minárik y LTC Kris van der Meij investigadores del Centro de Excelencia de Cooperación de Ciberdefensa (CCDCOE, por sus siglas en inglés) perteneciente a la Organización del Tratado del Atlántico Norte (OTAN), afirmaron que no es necesario un "Convenio Digital de Ginebra" porque ya la OTAN aplica los Convenios de Ginebra en el ciberespacio, considerándola un área de competencia dentro de sus políticas de seguridad.[126]

> "Los Convenios de Ginebra originales y sus protocolos adicionales forman parte del derecho internacional humanitario o del derecho de la guerra. Están diseñados principalmente para un conflicto armado, tal como la guerra en curso entre Rusia y Ucrania. Se aplican a operaciones cibernéticas que tienen un vínculo con un conflicto armado; sin embargo, tienen una aplicabilidad limitada fuera del alcance de un conflicto" dijo Tomáš Minárik
>
> "Sin embargo, otras normas de derecho internacional desempeñan un papel importante con respecto a las actividades cibernéticas en tiempo de paz, tales como las que figuran en la Convención del Consejo de Europa sobre ciberdelincuencia o las normas de derecho consuetudinario relativas a la responsabilidad de los Estados por actividades ilícitas que se han establecido en el proyecto de artículos de la Comisión de Derecho Internacional sobre "La responsabilidad de los Estados por actos ilícitos internacionalmente" dijo LTC Kris van der Meij

Quienes han avanzado notoriamente en las políticas de ciberseguridad son los organismos regionales como el caso de la Organización del Tratado del Atlántico

---

[124] Es una serie de conferencias que reúne a profesionales y líderes de la industria de seguridad informática, inaugurada en 1991. RSA Conference. Recuperado de: https://www.rsaconference.com/ Fecha de consulta: 10/08/2017.

[125] Microsoft. (14 de febrero de 2017). The need for a Digital Geneva Convention. *Microsoft.* Recuperado de: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/ Fecha de consulta: 10/08/2017.

[126] Versión original en inglés, traducción propia de: Centro de Excelencia de Cooperación de Ciberdefensa. (18 de julio de 2017). Geneva Conventions Apply to Cyberspace: No Need for a "Digital Geneva Convention". *CCDCOE.* Recuperado de: https://ccdcoe.org/geneva-conventions-apply-cyberspace-no-need-digital-geneva-convention.html Fecha de consulta: 10/08/2017.

Norte (OTAN), el de la Unión Europea (UE) y la Organización de Estados Americanos (OEA), el cual se consideran los principales organismos regionales que más han desarrollado su ciberseguridad.

A lo largo de la segunda década del Siglo XXI se han suscitado ataques cibernéticos cada vez más avanzados y hacia objetivos específicos; el desarrollo de la ciberseguridad a nivel global, es un factor importante para garantizar la estabilidad de los países como también su completo desarrollo. A continuación se mostrarán algunos casos de ataques cibernéticos dirigidos a Estados:

Hackers obtienen acceso a las redes eléctricas estadounidenses y europeas: Un informe elaborado por investigadores de Symantec, sobre un grupo al que le llaman "DragonFly". Afirman de contar con evidencia de que en más de 20 casos los hackers accedieron a las redes de compañías eléctricas, en algunos casos en Estados Unidos y de países europeos; lograron acceder a las interfaces que se usan para controlar el equipo de la red eléctrica, pero aún no han demostrado la capacidad de manipular los sistemas que están buscando. Se cree que este grupo está siendo financiado por otro gobierno para obtener información secreta de las infraestructuras críticas eléctricas de varios países.[127]

Dinamarca y Suecia impulsan lazos de defensa para luchar contra ataques cibernéticos rusos: Los ministros de defensa de ambos países mencionan la importancia de la cooperación contra la creciente amenaza rusa de campañas peligrosas de desinformación, noticias falsas y ciberataques. Un estudio realizado por el Instituto Internacional de Estocolmo, acusa a Rusia de querer

[127] Securelist. (07 de septiembre de 2017). Hackers adquieren conocimientos y habilidades para controlar las operaciones de plantas de energía en Europa y Estados Unidos. *Securelist.* Recuperado de: https://securelist.lat/hackers-adquieren-conocimientos-y-habilidades-para-controlar-las-operaciones-de-plantas-de-energia-en-europa-y-estados-unidos/85503/ & Rhett Jones. (9 de junio de 2017). *Hackers Have Reportedly Gained "Operational Access" to US Power Grids, But Dont´Freak Yet. GIZMODO.* Recuperado de: http://gizmodo.com/hackers-have-reportedly-gained-operational-access-to-us-1800755045 Fecha de consulta: 07/09/2017.

persuadir mediante noticias falsas y documentos apócrifos a la población para que Suecia no se una a la OTAN.[128]

Se investigan posibles ataques cibernéticos que probablemente han ocasionado las coaliciones de barcos de la armada de Estados Unidos: En menos de un año, cinco buques militares se han estrellado en el océano pacífico, por tal motivo la Marina estadounidense ha iniciado una investigación para esclarecer los motivos. De los diversos motivos que se cree, uno de ellos es que existe una falsificación de señales GPS de los buques.[129]

Virus informático capaz de paralizar centrales eléctricas: Un reporte publicado por *WashingtonPost*[130]; arrojó que Rusia ha logrado desarrollar ciberarmas capaces de paralizar centrales eléctricas que han tenido efectos positivos como fue el caso en el 2015 de Kiev, Ucrania[131]; el cual lograron cerrar una quinta parte del suministro total generada en la capital ucraniana. La firma de ciberseguridad Dragos, investiga el posible uso de esta arma para dañar y extenderse en las plantes de producción de energía de Estados Unidos.

Ataques con el fin de derribar el Internet a nivel global: En el blog personal de Bruce Schneier mencionan sondeos a compañías claves de internet (éstas se encargan de sustentar las principales páginas web en el mundo y sus dominios) estos sondeos es para medir las capacidades y el nivel de defensa de

---

[128] Jon Henly. (31 de agosto de 2017). *Denmark and Sweden boost defence ties to fight Russian cyber-attacks. The Guardian.* Recuperado de: https://www.theguardian.com/world/2017/aug/31/denmark-and-sweden-boost-defence-ties-to-fight-russian-cyber-attacks Fecha de consulta: 14/09/2017.

[129] Keith Griffith. (22 de agosto de 2017). Were they hacked? US Navy to investigate wether BOTH warships that crashed into much larger merchant vessels with deadly results were the victims of a cyber attack. *Daily Mail.* Recuperado de: http://www.dailymail.co.uk/news/article-4811516/amp/US-Navy-consider-crashed-warships-hacked.html Fecha de consulta: 14/09/2017.

[130] Ellen Nakashima. (12 de junio de 2017). Russia has developed a cyberweapon that can disrupt power grids, according to new research. *The Washington Post.* Recuperado de: https://www.washingtonpost.com/world/national-security/russia-has-developed-a-cyber-weapon-that-can-disrupt-power-grids-according-to-new-research/2017/06/11/b91b773e-4eed-11e7-91eb-9611861a988f_story.html?hpid=hp_hp-top-table-main_russiascyber-810a%3Ahomepage%2Fstory&utm_term=.a942776d6e98 Fecha de consulta: 15/09/2017.

[131] Ucrania ha sido uno de los principales países donde se vive una guerra cibernética, en agosto del presente año un ataque DDoS paralizó por 48 horas el servicio postal nacional. BBC News. (10 de agosto de 2017). Ukrainian postal service hit by 48-hour cyber-attack. *BBC News.* Recuperado de: http://www.bbc.com/news/technology-40886418 Fecha de consulta: 15/09/2017.

estas compañías y sus consecuencias al atacarlas. El autor comenta del incremento de ataques DDoS y cree que los que están detrás de ello son grandes Estados como Rusia o China.[132]

Existe una gran cantidad de noticias relacionada a ataques cibernéticos, a lo largo del presente siglo, pero su aumento se ha visto en estos últimos años conforme la tecnología va mejorando, teniendo como consecuencia la proliferación de unidades militares cibernéticas, creación de leyes nacionales actualizadas, y el fortalecimiento policial dentro del ciberespacio; principalmente con la ayuda de Organizaciones Internacionales Regionales, por eso se hablará brevemente del desarrollo cibernético de la OTAN, Unión Europea (UE) y la Organización de Estados Americanos (OEA), donde la Teoría de Complejos de Seguridad Regional nos dará la visión de la securitización de la ciberseguridad, y como dichas organizaciones regionales han homologado las políticas cibernéticas dentro de ellas.

2.2.1 LA CIBERSEGURIDAD DE LA OTAN

La Organización del Tratado del Atlántico Norte (OTAN) es una organización política-militar creada en 1949, en el contexto de la Guerra Fría, con el propósito de garantizar la libertad y seguridad de sus miembros a través de medios políticos y militares[133]; en la actualidad cuenta con 29 miembros[134], la mayoría de ellos también son miembros de la Unión Europea.

---

[132] Schneier. (2016). Someone is learning how to take down the internet. *Blog Personal.* Recuperado de: https://www.schneier.com/blog/archives/2016/09/someone_is_lear.html Fecha de consulta: 15/09/2017.

[133] OTAN. What is NATO. *OTAN*. Recuperado de: http://www.nato.int/nato-welcome/index.html Fecha de consulta: 23/07/2017.

[134] A continuación los países miembros y la fecha de su adhesión: Albania (2009), Bélgica(1949), Bulgaria (2004), Canadá (1949), Croacia (2009), República Checa (1999), Dinamarca (1949), Estonia (2004), Francia (1949), Alemania (1955), Grecia (1952), Hungría (1999), Islandia (1949), Italia (1949), Letonia (2004), Lituania (2004), Luxemburgo (1949), Montenegro (2017), Países Bajos (1949), Noruega (1949), Polonia (1999), Portugal (1949), Rumania (2004), Eslovaquia (2004), Eslovenia (2004), España (1982), Turquía (1952), Reino Unido (1949) y Estados Unidos (1949). OTAN. Member countries. *OTAN.* Recuperado de: http://www.nato.int/cps/en/natolive/topics_52044.htm Fecha de consulta: 23/07/2017.

La OTAN se considera como la principal organización internacional que ha avanzado en materia de ciberseguridad para el beneficio de sus Estados miembros, y es de esperarse, pues es una asociación política-militar, la cual la obliga al estar al día en las últimas tecnologías de uso militar y hacer frente a sucesos al nivel mundial -con la visión de considerar al ciberespacio un campo más de batalla- como el que influenció al desarrollo de la política cibernética de la OTAN: el ataque cibernético que sufrió Estonia en el 2007, el cual afecto al sector público y privado.

Después del desarrollo tecnológico de la última década, la OTAN considera a la ciberseguridad un pilar muy importante para sus políticas de seguridad colectiva tras los ataques cibernéticos sufridos a diversos Estados, miembros y no miembros. Tan solo en una década, ha desarrollado exitosamente su ciberseguridad,[135] remontándose desde la Cumbre de Praga de 2002 y la Cumbre de Riga del 2006, donde se colocó en la agenda política a la ciberseguridad.

En el 2007 con los ataques cibernéticos que sufrió Estonia, la OTAN anunció un paquete de políticas de defensa cibernética como respuesta, aprobándose la *NATO Cyber Defense Policy* y posteriormente la *NATO Cyber Defense Concept* (ambos documentos con acceso restringido). Un año después del ataque cibernético a Estonia, siete países de la OTAN y el Comando Aliado de Transformación (ACT, *Allied Command Transformation)* crearon en Tallin, Estonia, el Centro de Excelencia de Cooperación de Ciberdefensa (CCDCOE, *Cooperative Cyber Defence Centre of Excellence*), [136] que es el primer Centro con el estatus de organización militar internacional acreditada por la OTAN; entre sus objetivos se encuentra el mejorar la cooperación e intercambio de información entre la OTAN, Estados miembros y asociados para el mejoramiento de la defensa cibernética

[135] Para más información, véase la Cumbre de Praga (2002); Cumbre de Riga (2006); Cumbre de Bucarest (2008); Cumbre de Lisboa (2010); Cumbre de Chicago (2012); Cumbre de Gales (2014) y Cumbre de Varsovia (2016).

[136] Se recomienda visitar su página oficial, en la cual existe una gran cantidad de información sobre la ciberseguridad de la OTAN, de Estados no miembros y organismos regionales, documentos oficiales, ciber conceptos, artículos, Estrategias de ciberseguridad de diversas naciones, como también, noticias sobre acontecimientos a nivel internacional de ciberseguridad. Centro de Excelencia de Cooperación de Ciberdefensa. Recuperado de: https://ccdcoe.org/index.html Fecha de consulta: 31/07/2017.

colectiva; y actualmente cuenta con la participación activa y el financiamiento de países miembros de la OTAN y de países no miembros.[137]

En la Cumbre de Lisboa del 2010 la OTAN adoptó un nuevo concepto de estrategia, el cual lo desarrolló el Consejo del Atlántico Norte (NAC, *North Atlantic Council*) que consistía en diseñar la política cibernética sólida, al preparar un plan de acción para su aplicación, mejorando sus capacidades de defensa cibernética de manera colaborativa y rentable. [138]

A mediados del 2011, los Ministros de Defensa de la OTAN aprobaron la segunda Política de Ciberdefensa[139], que estableció la prevención de ataques cibernéticos y la construcción de la resistencia contra estos ataques, y a su vez, un plan de acción para su rápida implementación.

En 2012, la ciberdefensa empieza a integrarse al Proceso de Planificación de Defensa (*NATO Defence Planning Process)* el cual identifica y lo prioriza en las políticas de defensa de la OTAN. Con la Cumbre de Chicago, los dirigentes de los países miembros pusieron todas las redes de la OTAN bajo protección centralizada de (NCIRC, *NATO Computer Incident Response Capability*), el cual en mayo del 2014 logra la plena capacidad operativa, fungiendo como el principal encargado de la defensa cibernética de la OTAN; en ese mismo año, se establece la *NATO Communications and Information Agency* (NCIA)[140] como parte de las agencias de la OTAN.

[137] Estos países son: República Checa, Estonia, Francia, Alemania, Hungría, Italia, Letonia, Lituania, Grecia, Países Bajos, Polonia, Eslovaquia, España, Turquía, Reino Unido, Estados Unidos; y también de países no miembros como Finlandia y Austria.

[138] OTAN. NATO Nations to boost cyber defence cooperation. *OTAN.* Recuperado de: http://www.nato.int/cps/en/natolive/news_70519.htm Fecha de consulta: 28/07/2017.

[139] OTAN. NATO Defence Ministers adopt new cyber defence policy. *OTAN.* Recuperado de: http://www.nato.int/cps/en/SID-4DC51D3F-30C063BB/natolive/news_75195.htm Fecha de consulta: 28/07/2017.

[140] Es la encargada de conectar a la OTAN, defender sus redes, proporcionar apoyo rápido a las operaciones de la OTAN, apoyar a las naciones en la certificación de sus elementos de la Fuerza de Respuesta, entre otras. La agencia se encarga de brindar apoyo a las operaciones y conectar a los miembros en una sola red.

En 2013 Canadá, Dinamarca, Países Bajos, Rumania y Noruega se unieron al proyecto del Desarrollo de Capacidades Multinacionales de Ciberdefensa[141], en dicho año se publica el Manual de Tallin sobre el Derecho Internacional Aplicable a la Guerra Cibernética.[142]

En 2014 los ministros de defensa aliados encargan a la OTAN el desarrollo de una nueva y mejorada política de defensa cibernética en materia de defensa colectiva, asistencia a aliados, racionalización de la gobernanza, consideraciones jurídicas y relaciones con la industria; en dicho año el *North Atlantic Council* (NAC) cambió el nombre del Comité de Políticas y Planificación de Defensa/Ciberdefensa al de Comité de Defensa Cibernética; para la Cumbre de Gales, la OTAN lanza una iniciativa de cooperación con el sector privado en relación a la ciberseguridad para mejorar los objetivos de la Política Cibernética, creando así la Asociación Cibernética de la Industria con la OTAN (NICP, *NATO Industry Cyber Partnership*).[143]

A inicios del 2016, la OTAN y la Unión Europea concluyen el Acuerdo Técnico de Ciberdefensa entre el *NATO Computer Incident Response Capability* (NCIRC) y el *Computer Emergency Response Team* (CERT-EU)[144], proporcionando el intercambio de información y de mejores prácticas entre los equipos de respuesta. En ese mismo año con la Cumbre de Varsovia, la OTAN empieza a considerar al ciberespacio un dominio operacional en el que se deben de defender, actualizando

[141] Es una organización que tiene la finalidad de facilitar el desarrollo de las capacidades de defensa cibernética entre los países y la OTAN a través de esfuerzos de colaboración, proporcionando la facilidad de que las naciones concentren sus esfuerzos en las áreas de su elección sin ninguna restricción monetaria. MN CD2. About the MN CD Project. *MN CD2.* Recuperado de: https://mncd2.ncia.nato.int/pages/about.aspx Fecha de consulta: 28/07/2017.

[142] En Febrero del 2017, salió la segunda edición del manual con el título de *Tallin Manual 2.0 on the International Law Applicable To Cyber Operations;* impreso por la universidad de Cambridge.

[143] Es el órgano de la OTAN que se encarga de la cooperación de defensa cibernética entre la industria privada y los miembros de la OTAN, sus principales objetivos son: mejorar la defensa cibernética; facilitar la participación del sector privado en proyectos de defensa; contribuir a los esfuerzos de la Alianza en la educación, capacitación y ejercicios de defensa cibernética; mejorar el intercambio de mejores prácticas, como también el intercambio de conocimiento especializados; y facilitar el acceso a sus Estados miembros a una red de empresas de confianza. NATO Industry Cyber Partnership. Recuperado de: http://www.nicp.nato.int/objectives-and-principles/index.html Fecha de consulta: 31/07/2017.

[144] OTAN. NATO and European Union enhance cyber defence cooperation. *OTAN.* Recuperado de: http://www.nato.int/cps/en/natohq/news_127836.htm Fecha de consulta; 28/07/2017.

el Plan de Defensa Cibernética, para implementar al ciberespacio como un dominio operacional, el cual en caso de un ataque cibernético a algún miembro se activaría el Artículo 5.[145]

Dentro de su estructura de gobernanza se encuentra:

- Consejo del Atlántico Norte: Es el principal órgano que toma las decisiones políticas de la OTAN, está compuesto de un representante de cada país miembro.
- Comité de Defensa Cibernética: Subordinado al Consejo del Atlántico Norte y que se encarga de proporcionar supervisión y asesoramiento a los países Aliados sobre los esfuerzos de la defensa cibernética de la OTAN al nivel de expertos.
- Comité Administrativo de la Ciberdefensa de la OTAN:[146] El cual es responsable de coordina la defensa cibernética a través de los cuerpos militares y civiles de la OTAN, aquí se comprende a los líderes de política, militares, cuerpos operacionales y técnicos de la OTAN.[147]

La OTAN es una organización por excelencia en el avance de la ciberseguridad, es por eso que se considera como la principal organización más avanzada en esta materia a comparación de otras organizaciones. Su avance ha permitido el desarrollo de la ciberseguridad en Europa, esto a consecuencia que la mayoría de sus miembros pertenecen a la Unión Europea, creando una securitización de la ciberseguridad en toda la región.

[145] Artículo referido a la Defensa Colectiva, el cual una agresión en contra de un país miembros se consideraría un ataque contra todos los demás países miembros. OTAN. Collective defence-Article 5. *OTAN.* Recuperado de: http://www.nato.int/cps/cn/natohq/topics_110496.htm Fecha de consulta: 29/07/2017.

[146] Es también el órgano que se encarga de procesar las solicitudes de países miembros que sufran un ataque cibernético significativo en caso de solicitar apoyo a la OTAN. Mientras el Consejo del Atlántico Norte se encarga de las solicitudes de países que no son parte de la organización. OTAN. (13 de marzo de 2012). NATO Rapid Reaction Team to fight cyber attack. *OTAN.* Recuperado de: http://www.nato.int/cps/en/SID-CF294941-345E723F/natolive/news_85161.htm Fecha de consulta: 28/07/2017.

[147] OTAN. (10 de noviembre de 2017). Cyber defence. *OTAN.* Recuperado de: http://www.nato.int/cps/en/natohq/topics_78170.htm Fecha de consulta: 12/10/2017.

2.2.2 LA CIBERSEGURIDAD DE LA UNIÓN EUROPEA

La Unión Europea era conocida como la Comunidad Económica Europea (CEE), fundada en 1958 después de la Segunda Guerra Mundial, tenía el fin de evitar una guerra más en el continente y lograr así unificar a las naciones europeas. Es única en su clase, pues ha pasado procesos complejos que han originado lo que hoy se conoce como la Unión Europea (UE), una organización económica y política que cuenta con 28 Estados miembros[148] y es la segunda organización internacional después de la OTAN que ha desarrollado sus políticas de ciberseguridad, esto se debe mucho a la colaboración en materia cibernética con la OTAN, al incremento de delitos cibernéticos dentro de sus Estados miembros y la importancia de estar cada vez más preparados; como también, a que más de la mitad de sus miembros forman parte de la OTAN.

Como antecedente de la política de ciberseguridad de la UE, se encuentra el Convenio sobre la Ciberdelicuencia o Convención de Budapest que entró en vigor en el 2004, [149] considerado el primer tratado internacional relacionado a crímenes cometidos en el ciberespacio, y cuenta con 47 ratificaciones hasta la fecha de Estados miembros y no miembros de la UE, donde a México se le ha invitado a unirse.[150]

Hoy en día, la UE cuenta su propia agencia encargada de desarrollar sus políticas de ciberseguridad, conocida como la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA), que es un centro de especialización y la principal agencia que desarrolla la ciberseguridad de la UE.

---

[148] Ordenado por fecha de adhesión: Alemania, Bélgica, Francia, Italia, Luxemburgo y Países Bajos (1958); Dinamarca, Irlanda y Reino Unido (1973); Grecia (1981); España, Portugal (1986); Finlandia, Austria, Suecia (1995); Chipre, Eslovaquia, Eslovenia, Estonia, Hungría, Letonia, Lituania, Malta, Polonia, República Checa (2004), Bulgaria, Rumania (2007), Croacia (2013). En la actualidad el Reino Unido se encuentra en trámites para abandonar la UE, los cuales aún no finalizan, por lo tanto todavía es considerado parte de la UE. Unión Europea. Todos los países de la UE. *Unión Europea.* Recuperado de: https://europa.eu/european-union/about-eu/countries/member-countries_es Fecha de consulta: 01/08/2017.

[149] Secretaría de Marina & Centro de Estudios Superiores Navales. Op. Cit., (pág. 76).

[150] Ibíd., (pág. 165).

Cuenta con la colaboración tanto del sector privado como de los Estados miembros de la UE. Fundada en el 2004[151] por el Reglamento (CE) N° 460/2004 del Parlamento Europeo y el Consejo[152], el cual fue derogado y actualizado en el 2013 por el Reglamento (UE) N° 526/2013[153], con una vigencia de 7 años (2013-2020). En el Artículo 2° del Reglamento (UE), ENISA tiene como objetivo:

- Desarrollar y mantener un alto nivel de conocimientos especializados.
- Ayudar a las instituciones, órganos y organismos de la Unión Europea a desarrollar las políticas necesarias en materia de seguridad de las redes y de la información.
- Ayudar a las instituciones, órganos y organismos de la Unión Europea y a los Estados miembros a aplicar las políticas necesarias para cumplir los requisitos legales y reglamentarios relativos a la seguridad de las redes y de la información que figuran en actos jurídicos actuales y futuros de la Unión, contribuyendo así al correcto funcionamiento del mercado interior.
- La Agencia ayudará a la Unión y a los Estados miembros a potenciar y reforzar su capacidad y preparación para prevenir, detectar y dar respuesta a los problemas e incidentes relacionados con la seguridad de las redes y de la información.
- Utilizar sus conocimientos especializados para fomentar una amplia cooperación entre los agentes de los sectores público y privado.

ENISA es la homóloga de CCDCOE, y cuenta con competencias como: la elaboración de ejercicios cibernéticos entre los países miembros; publicación de

[151] Unión Europea. Agencia de Seguridad de las Redes y de la Información de la Unión Europea. *Unión Europea.* Recuperado de: https://europa.eu/european-union/about-eu/agencies/enisa_es Fecha de consulta: 01/08/2017.

[152] Unión Europea. (13 de marzo de 2004). Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. Recuperado de: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML Fecha de consulta: 01/08/2017.

[153] Para mayor información se recomienda ver el documento oficial para saber más de las competencias, organización y objetivos de ENISA. Unión Europea. (18 de junio de 2013). Reglamento (UE) N° 526/2013 del Parlamento Europeo y del Consejo, relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA). [Archivo PDF]. Recuperado de: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32013R0526&from=EN Fecha de consulta: 01/08/2017.

informes y estudios relacionados a la ciberseguridad; elaboración de políticas y legislaciones de la UE, para el sector privado y los países miembros; y con una estrategia para el periodo 2016-2020.[154]

También ENISA[155] colabora y ayuda a varias agencias europeas como:

- Europol: Es la agencia de la UE en materia policial, para la lucha de la delincuencia internacional, terrorismo, tráfico de drogas, lavado de dinero, fraude, falsificación de euros y contrabando de personas, entre otros.[156]
- Centro Europeo de Ciberdelincuencia (EC3): Fundada por la Europol en el 2013, este centro se encarga de reforzar la respuesta policial contra el cibercrimen en la UE y ayudar a proteger a los ciudadanos, empresas y gobiernos de Europa de la delincuencia en línea.[157]
- Agencia de la Unión Europea para la Formación Policial (CEPOL): Fundada en el 2005, la Agencia desarrolla, ejecuta y organiza cursos de formación para la policía y otros funcionarios de las fuerzas y cuerpos de seguridad del Estado.[158]
- Oficina del Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE): Fundado en el 2010, la Agencia proporciona apoyo profesional y administrativo al Organismo de Reguladores Europeos de Comunicaciones Electrónicas (ORECE), la ORECE aspira a que la legislación de la UE pertinente se aplique de manera uniforme, de forma que

[154] ENISA. (2016). ENISA Strategy 2016-2020. *ENISA.* [Archivo PDF]. Recuperado de: https://www.enisa.europa.eu/publications/corporate/enisa-strategy Fecha de consulta: 01/08/2017.

[155] Actualmente la Comisión Europea quiere que ENISA cree un sistema de certificación de ciberseguridad en toda UE para homologarlo en todos los países miembros y ayudar a la UE a mejorar su área cibernética. Zeljka Zorz. (14 de septiembre de 2017). European Commission wants ENISA to introduce EU-wide cybersecurity certification scheme. *HELPNETSECURITY.* Recuperado de: https://www.helpnetsecurity.com/2017/09/14/eu-wide-cybersecurity-certification-scheme/?ct=t() Fecha de consulta: 16/09/2017.

[156] EUROPOL. Acerca de EUROPOL. *EUROPOL.* Recuperado de: https://www.europol.europa.eu/es/about-europol Fecha de consulta: 01/08/2017.

[157] EUROPOL. European Cybercrime Centre-EC3. *EUROPOL.* Recuperado de: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 Fecha de consulta: 01/07/2017.

[158] Unión Europea. Agencia de la Unión Europea para la Formación Policial (CEPOL). *Unión Europea.* Recuperado de: https://europa.eu/european-union/about-eu/agencies/cepol_es Fecha de consulta: 01/08/2017.

la UE disponga de un mercado único de comunicaciones electrónicas que funcione. La ORECE está compuesta del denominado Consejo de Reguladores.[159]

- Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu- LISA): Fundada en el 2011 y entrando en funcionamiento en el 2012, la agencia se encarga de contribuir a la aplicación de las políticas de justicia y asuntos de interior de la UE mediante la gestión de sistemas informáticos de gran magnitud.[160]
- Agencia Europea de Seguridad Aérea (AESA): Fundada en el 2002, esta agencia garantiza la seguridad y la protección del medio ambiente en el sector de la aviación civil en Europa; cuenta con todos los miembros de la UE, Islandia y Liechtenstein, Noruega y Suiza. [161]

Por último, en julio del 2016 con la Directiva (EU) 2016/1148[162] del Parlamento Europeo y el Consejo, se adopta una Directiva sobre la Seguridad de las Redes y de la Información (NIS), esta Directiva tiene como objetivo elevar el nivel de seguridad de las redes y sistemas de información dentro de la UE para el mejoramiento de su mercado interno. Entre lo más destacable tenemos:

- Obliga a los Estados miembros a adoptar una Estrategia Nacional de Seguridad de las Redes y Sistemas de Información a fin de alcanzar los objetivos de la Directiva.

---

[159] Unión Europea. Oficina del Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE). Unión *Europea.* Recuperado de: https://europa.eu/european-union/about-eu/agencies/berec_es Fecha de consulta: 01/08/2017.

[160] Unión Europea. Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu- LISA). *Unión Europea.* Recuperado de: https://europa.eu/european-union/about-eu/agencies/eu-lisa_es Fecha de consulta: 01/08/2017.

[161] Unión Europea. Agencia Europea de Seguridad Aérea (AESA). *Unión Europea.* Recuperado de: https://europa.eu/european-union/about-eu/agencies/easa_es Fecha de consulta: 01/08/2017.

[162] Presidencia y para las Administraciones Territoriales de España. (19 de julio de 2016). Directiva (EU) 2016/1148 del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión. [Archivo PDF]. Recuperado de: https://www.boe.es/doue/2016/194/L00001-00030.pdf Fecha de Consulta: 01/08/2017.

- Cada Estado miembro tendrá una o varias redes de equipos de respuesta a incidentes de seguridad informática CSIRT (*Computer Security Incident Response Teams*) cual dotaran de recursos adecuados para el completo funcionamiento. (Estos CSIRT son los homólogos de los CERT de la OTAN), esto creará una red de cooperación cibernética entre el sector privado y los Estados miembros de la Unión Europea.
- El 9 de noviembre del 2018, los Estados miembros deben de haber identificado a los operadores de servicios esenciales dentro de su territorio.[163] (Esto se refiere a las empresas privadas prestadoras de servicios importantes para el Estado, que sin ellas afectaría la vida cotidiana dentro de un país, estas son como las empresas financieras, eléctricas, transporte, de servicios, entre otras).

2.2.3 LA CIBERSEGURIDAD DE LA OEA

La Organización de Estados Americanos (OEA) es una organización internacional gubernamental de carácter regional, creada en 1948 con el objetivo de "lograr un orden de paz y justicia, fomentar su solidaridad, robustecer su colaboración y defender su soberanía, su integridad territorial y su independencia"[164] de los Estados Americanos; cuenta con 35 Estados miembros[165] y es la tercera organización internacional que se considera avanzada es las políticas

[163] Los criterios de identificación son los siguientes: Debe ser una entidad que preste servicio esencial de mantenimiento de actividades sociales o económicas cruciales, la prestación de dicho servicio depende de las redes y sistemas de información y, un incidente tendría efecto perturbador significativo en la prestación de dicho servicio.

[164] OEA. Artículo 1 De la Carta de la Organización de Estados Americanos. [Archivo PDF]. Recuperado de: http://www.oas.org/es/sla/ddi/docs/tratados_multilaterales_interamericanos_A-41_carta_OEA.pdf Fecha de consulta: 02/08/2017.

[165] Antigua y Barbuda, Argentina, Bahamas, Barbados, Belize, Bolivia, Brasil, Canadá, Chile, Colombia, Costa Rica, Cuba, Dominica, Ecuador, El Salvador, Estados Unidos de América, Granada, Guatemala, Guyana, Haití, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Saint Kitts y Nevis, San Vicente y las Granadinas, Santa Lucía, Suriname, Trinidad y Tobago, Uruguay y Venezuela. OEA. Estados Miembros. Recuperado de: http://www.oas.org/es/estados_miembros/default.asp Fecha de consulta; 02/08/2017.

cibernéticas, esto a consecuencia de uno de sus miembros: Estados Unidos, quien es un país activo en cuestiones de ciberseguridad y principal miembro de la OTAN y líder en la materia. Aquí se puede observar como la Teoría de Complejos de Seguridad Regional, le da el estatus de superpotencia, dado a la intervención de Estados Unidos en la securitización de la ciberseguridad dentro de diversos bloques regionales.

El desarrollo cibernético de los países de América Latina se le debe mucho a la OEA, quien desde el 2004 cuenta con su propia Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética que se encuentra en la resolución AG/RES. 2004 (XXXIV-O/04)[166] la cual le dio las facultades a la Secretaría del Comité Interamericano contra el Terrorismo (CICTE) de trabajar en asuntos de Seguridad Cibernética[167]. A continuación su organigrama:

- Secretaría General: La Secretaría General es el órgano central y permanente de la Organización de los Estados Americanos.
    - Secretaría de Seguridad Multidimensional: Coordina la cooperación entre los Estados miembros para combatir las amenazas a la Seguridad Nacional y a los ciudadanos.
        - Secretaría del Comité Interamericano contra el Terrorismo (con rango de Departamento): Promueve y desarrolla la cooperación de Estados Americanos para prevenir, combatir y eliminar el terrorismo.

Este programa de Seguridad Cibernética[168] es la base del desarrollo cibernético de la OEA y de sus países miembros ante los retos de ciberseguridad que se

[166] OEA. (8 de junio de 2004). Adopción de una estrategia interamericana integral de seguridad cibernética: un enfoque multidimensional y multidisciplinar para la creación de una cultura de seguridad cibernética. *OEA.* [Archivo PDF]. Recuperado de: http://www.oas.org/es/sms/cicte/documents/asambleas/AG-RES.%202004%20(XXXIV-O-04)_SP.pdf Fecha de consulta: 02/08/2017.

[167] Se recomienda visitar la página oficial en la cual se encuentra información sobre la ciberseguridad de cada país miembros de la OEA, artículos, informes; como también los CERT´S de cada país miembro. OEA. Seguridad Cibernética. Recuperado de: https://www.sites.oas.org/cyber/ES/Paginas/default.aspx Fecha de consulta: 02/08/2017.

[168] También la OEA cuenta con otros órganos que apoyan al programa de Seguridad Cibernética como: Comisión Interamericana de Telecomunicaciones (CITEL) y el Grupo de Expertos Gubernamentales en Materia de Delito Cibernético de la Reunión de Ministros de Justicia de las Américas (REMJA).

enfrenta la región, dentro de su resolución AG/RES. 2004 (XXXIV-O/04) los puntos más destacados son:

- Insta a los Estados miembro de implementar la Estrategia Interamericana Integral de Seguridad Cibernética.
- Establecer o identificar en cada país, grupos nacionales de Equipos de Respuesta a Incidentes (CSIRT, por sus siglas en inglés) para hacer frente a las amenazas cibernéticas.
- Instar a la cooperación entre los Estados miembros, órganos, organismos y al Grupo de Expertos Gubernamentales en Materia de Delito Cibernético (REMJA), para incrementar la seguridad cibernética.
- Implementar las recomendaciones del Grupo de Expertos Gubernamentales en Materia de Delito Cibernético (REMJA), como la creación de centros especializados en materia de delitos cibernéticos.

En su último informe anual del 2016[169], la OEA menciona los resultados alcanzados como el apoyo al desarrollo de la Estrategia Nacional de Ciberseguridad de Chile, Costa Rica, Guatemala, Paraguay y Republica Dominicana; la capacitación de más de 3,000 oficiales de gobierno, sector privado y sociedad civil en la investigación forense digital, protección de infraestructura crítica y gestión de crisis; y por último y el más importante es el lanzamiento del Observatorio de Ciberseguridad[170] de la OEA, el cual cuenta con su página de internet que permite conocer mediante un mapa interactivo el desarrollo de la ciberseguridad en América Latina y el Caribe, en cuestiones como: Política y Estrategia, Cultura y Sociedad, Educación, Marcos Legales y Tecnologías; también permite comparar a los países para ver las diferencias que tiene cada uno y su desarrollo. En el caso de México, el observatorio menciona que:

[169] OEA. Informe Anual del Secretario General 2016. *OEA*. [Archivo PDF]. Recuperado de: http://www.oas.org/es/centro_informacion/informe_anual.asp Fecha de consulta: 30/11/2017.

[170] La información que se presenta sobre México no se encuentra actualizada, como también en el mapa interactivo no se cuenta con la información de América del Norte (Canadá y Estados Unidos), ni tampoco de Cuba. Observatorio de la Ciberseguridad en América Latina y el Caribe. Recuperado de: http://observatoriociberseguridad.com/country/mx Fecha de consulta: 02/08/2017.

- El Gobierno de México trabaja en una Estrategia Nacional de Ciberseguridad donde la Defensa Cibernética estará a cargo de las Fuerzas Armadas.[171]
- Existen 4 CERT´s[172] que son miembros del Foro Mundial de Respuesta a Incidentes y Equipos de Seguridad (FIRST)[173].
- En todas las agencias gubernamentales se realizan copias de seguridad y se actualiza las tecnologías adhiriéndose al Manual Administrativo de Aplicación General de Tecnologías de Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI, donde más adelante se explicará) el cual se desarrolló con base al ISO 27001, como otras normas.
- El Instituto Nacional de Transparencia, Acceso a la información y Protección de Datos Personales (INAI)[174] publica informes, propone leyes estrictas en la protección de datos y hace campañas de sensibilización para los ciudadanos con base a los derechos de usuarios de las tecnologías de la información y la comunicación

Este panorama da una idea del avance en ciberseguridad que aún le falta por hacer a América Latina, de la discrepancia que hay dentro de la región y la insuficiencia que tiene aún México en hacer frente a las amenazas de ciberseguridad; es por eso que en junio del 2017 la OEA en el evento realizado en el marco de la Asamblea General, en Cancún, entregó a al gobierno mexicano una serie de recomendaciones para el desarrollo de la Estrategia Nacional de

[171] La Estrategia Nacional de Ciberseguridad ya fue presentada el 13 de noviembre del 2017, aunque todavía no se ve reflejado en la información del sitio. Esta Estrategia no solo estuvo a cargo de las Fuerzas Armadas sino que contó con la participación de varios expertos de diferentes sectores tanto empresarial, como académico.

[172] México cuenta con 4 CERT´s estos son: CERT-MX, UNAM-CERT, Mnemo-CERT y Scitum-CSIRT. Los cuales pertenecen a FIRTS y más adelante se abordarán.

[173] Es una organización creada en 1990 a respuesta de los primeros ataques cibernéticos en Internet (Morris 1988 y Wank worm 1989), aglutina a más de 300 miembros (CERT/ CSIRT) del sector militar, estatal, privado, académico, comercial y financiero, con el objetivo de fomentar la prevención, cooperación, coordinación y reacción inmediata ante incidentes informáticos, también promueve el intercambio de información entre los miembros y la comunidad en general. FIRST. Recuperado de: https://www.first.org/ Fecha de consulta: 02/08/2017.

[174] Es un organismo descentralizado encargado de garantizar en el país los derechos de las personas a la información pública y la protección de datos personales, promueve la cultura de la transparencia, y la rendición de cuentas. Página Oficial del INAI. Misión, Visión y Objetivos. Recuperado de: http://inicio.ifai.org.mx/SitePages/misionViosionObjetivos.aspx Fecha de consulta: 03/08/2017.

Ciberseguridad[175], el cual debe contar con: Un marco estratégico que contenga claramente el apoyo más alto en el nivel de gobierno y explicar el por qué es importante para nuestro país; la Estrategia debe abarcar la aplicación de la legislación federal y estatal en materia de ciberdelincuencia; y por último establecer un marco constitucional que garantice las responsabilidades, la autoridad y los recursos para actuar de las instituciones.

Dicha Estrategia ya se presentó en noviembre del 2017, el cual se considera la base de lo que sería el desarrollo cibernético de México. La Teoría de Complejos de Seguridad Regional nos da la visión del porqué de la securitización de la ciberseguridad dentro de la región latinoamericana. La regionalización de la ciberseguridad es una consecuencia tanto de Estados Unidos (superpotencia) para blindar al continente y homologar las directrices dentro de diversos Estados; como también, a que los Estados que conforman la región se han dado cuenta de la importancia de la ciberseguridad ante el incremento de delitos y amenazas dentro del ciberespacio, no es de sorprenderse que en un futuro la OEA tenga su primer tratado vinculante entre todos sus Estados para regular el ciberespacio y castigar los delitos cibernéticos.

[175] OEA. (20 de junio de 2017). Comunicado de Prensa. *OEA.* Recuperado de: http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-049/17 Fecha de consulta: 05/08/2017.

CAPÍTULO III LA CIBERSEGURIDAD EN MÉXICO

3.1 EL DESARROLLO DE LA CIBERSEGURIDAD EN MÉXICO

A finales del 2017, México terminó la elaboración de su Estrategia Nacional de Ciberseguridad, esto a consecuencia de la necesidad y al factor geopolítico que tiene el país -gracias a la cercanía con Estados Unidos, las constantes amenazas de ciberseguridad en el país, y el incremento de delitos cibernéticos- donde el 13 de noviembre del 2017 se presentó lo que sería la Estrategia Nacional de Ciberseguridad, esta Estrategia permitirá darle a México un marco referencial para sus políticas cibernéticas nacionales, algo con lo que no se contaba en los dos pasados sexenios (2000-2006 y 2006-2012), ya que no hubo un avance significativo como el que se está teniendo en el sexenio actual (2012-2018).

A lo largo del 2017 se ha notado un incremento en ataques cibernéticos a nivel nacional e internacional que ocupan los titulares en los principales medios informativos, estos ataques van dirigidos a individuos, empresas y Estados; ataques que incluso han afectado a México como el caso del *ransomware* WannaCry, el cual según la Policía Federal (PF), la primer instancia en defensa cibernética del país, había mencionado que WannaCry afectó mínimamente al país[176], pero este fue desmentido cuando Kaspersky Lab América Latina[177] dio a conocer que México ocupó el primer lugar en América Latina como el país más afectado[178] y entre los

[176] Julio Sánchez Onofre. (15 de mayo de 2017). Policía Federal ha identificado sólo 4 infecciones de WannaCry en México. *El Economista.* Recuperado de: http://eleconomista.com.mx/tecnociencia/2017/05/15/policia-federal-ha-identificado-solo-4-infecciones-wannacry-mexico Fecha de consulta: 05/08/2017.

[177] Actualmente la empresa de seguridad informática Kaspersky está siendo señalado por el gobierno de EUA de ocultar puertas traseras dentro de su software para ayudar a Moscú a espiar usuarios y dependencia de alto nivel en los Estados Unidos, esto a consecuencia que la mayoría de instituciones gubernamentales en Estados Unidos tienen instalado el antivirus de dicha compañía. Joan Faus. (14 de septiembre de 2017). EEUU veta el uso del software Kaspersky a las agencias gubernamentales por miedo al espionaje ruso. *El País.* Recuperado de: https://elpais.com/tecnologia/2017/09/13/actualidad/1505330916_156194.html Fecha de consulta: 30/11/2017.

[178] Mauricio Hernández Armenta. (15 de mayo de 2017). México es el país más afectado por el virus WannaCry en AL. *Forbes México.* Recuperado de: https://www.forbes.com.mx/mexico-es-el-pais-mas-afectado-por-el-virus-wannacry-en-al/ Fecha de consulta: 05/08/2017.

primeros 5 a nivel mundial. Estas discrepancias entre las instituciones gubernamentales y las entidades del sector privado es uno de los tantos problemas de México en materia de ciberseguridad, sumando que la información de ataques cibernéticos es muy reservada en el país.

Forbes[179] sacó una notica sobre la vulnerabilidad de México ante estos ataques, y el cómo el país es considerado un mercado fértil para llevar a cabo ataques cibernéticos. Esto se debe a la falta de un marco jurídico actualizado de ciberseguridad en México, que permite que los delitos relacionados al ciberespacio queden impune o se tengan que relacionar con otros delitos para poder castigar a los culpables, pues no existe como tal el concepto de delitos cibernéticos dentro de las leyes[180]. Esto también va de la mano con el crimen organizado, quien obliga al estado mexicano a actualizar sus políticas cibernéticas para el uso policial y militar; ya que se ha visto que empiezan a usar técnicas cibernéticas para el lavado de dinero, fraude y usurpación de identidad, entre otras.

El sector financiero junto con otras industrias también son las más afectadas en México, según Cisco[181], en el reporte de ciberseguridad del primer semestre del 2017 menciona que la industria manufacturera, sector financiero, de salud y servicio han recibido ataques cibernéticos importantes, su incremento se debe al surgimiento de las Fintech[182] que son el principal blanco de ataques cibernéticos.

---

[179] Mauricio Hernández Armenta. (12 de junio de 2017). México, vulnerable ante más ataques cibernéticos. *Forbes México.* Recuperado de: https://www.forbes.com.mx/mexico-vulnerable-ante-mas-ataques-ciberneticos/ Fecha de consulta: 05/08/2017.

[180] Jair López. (1 de junio de 2017). Especialistas ven impunidad en ciberseguridad en México. *Expansión*. Recuperado de: http://expansion.mx/tecnologia/2017/06/01/especialistas-ven-impunidad-en-ciberseguridad-en-mexico Fecha de consulta: 05/08/2017.

[181] Itzel Castañares. (20 de julio de 2017). Ciberataques en México afectan a sector financiero: Cisco. *El Financiero.* Recuperado de: http://www.elfinanciero.com.mx/tech/ciberataques-en-mexico-afectan-a-sector-financiero-cisco.html Fecha de consulta: 05/08/2017.

[182] "El término "Fintech" deriva de las palabras "*finance technology*" y se utiliza para denominar a las empresas que ofrecen productos y servicios financieros, haciendo uso de tecnologías de la información y comunicación, como páginas de internet, redes sociales y aplicaciones para celulares. De esta manera prometen que sus servicios sean menos costosos y más eficientes que los que ofrecen la banca tradicional. Actualmente operan alrededor de 158 Fintech en el país". Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF). ¿Qué son las fintech?. Recuperado de: http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/educacion-financiera/763-que-son-las-fintech Fecha de consulta: 05/08/2017.

México hasta ahora cuenta con 4 Equipos de Respuesta ante Emergencias Informáticas (CERT), el principal CERT es el que se encuentra en la Comisión Nacional de Seguridad-Policía Federal; el segundo depende de la Universidad Nacional Autónoma México; y los últimos dos del sector privado. Los CERT son los encargados de monitorear los incidentes de ciberseguridad dentro del país:

1.- Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX)[183]

Sede: Comisión Nacional de Seguridad - Policía Federal

Tipo: Sector Gubernamental

El CERT-MX depende de la Policía Federal y se encuentra dentro de la División Científica[184], -A su vez, dicha División cuenta con el área de Coordinación para la Prevención de Delitos Electrónicos, conocida como la Policía Federal Cibernética-. El CERT-MX es miembro del Foro Mundial de Respuesta a Incidentes y Equipos de Seguridad (FIRST, *Forum for International Incident Response*), y tiene como objetivo vigilar la integridad de las infraestructuras tecnológicas estratégicas del país; como también, ataques a la ciudadanía en general. El CERT-MX es la única acreditada a nivel federal que tiene la autorización del intercambio de información con policías cibernéticas a nivel nacional e internacional.

[183] Secretaría de Marina & Centro de Estudios Superiores Navales. Op. Cit., (págs. 120-122).

[184] Es una de las 7 divisiones de la Policía Federal (División Antidrogas; División Científica; División de Fuerzas Federales; División de Gendarmería; División de Inteligencia; División de Investigación y División de Seguridad Regional). La División Científica tiene como objetivo: "Encargarse de generar metodología científica y tecnológica para la prevención e investigación del delito, a través del desarrollo de herramientas técnico-científicas, con la participación de personal experto en criminalística, investigación cibernética y seguridad de sistemas de información y servicios científico tecnológicos, que contribuyen a los objetivos de la Policía Federal." Cabe señalar que la Policía Federal elaboró su propia *Estrategia de Ciberseguridad de la Policía Federal*. Policía Federal. Directorio. Recuperado de: https://www.gob.mx/policiafederal & Para ver las competencias de la División Científica, revisar el Reglamento de la Ley de la Policía Federal (Art. 15, Art. 27). Página Oficial del Diario Oficial de la Federación. (17 de mayo de 2010). Reglamento de la Ley de la Policía Federal. *SEGOB*. Recuperado de: http://www.dof.gob.mx/nota_detalle.php?codigo=5143004&fecha=17/05/2010 Fecha de consulta: 06/08/2017.

2.- Coordinación de Seguridad de la Información (CSI) / UNAM-CERT[185]

Sede: Universidad Nacional Autónoma de México

Tipo: Sector Académico

Se encuentra en la Dirección General de Cómputo y Tecnologías de Información y Comunicación de la UNAM, en su página oficial el CERT tiene como misión el prestar servicios especializados, formación de capital humano y el fomentar la cultura de seguridad de la información dentro del país, es miembro de FIRST desde el 2001.

3.- Mnemo-CERT[186]

Sede: Mnemo

Tipo: Sector Privado

Es una consultora española de tecnologías y ciberseguridad con presencia en México y Colombia, creada desde el 2001 y forma parte de FIRST. Trabaja con las entidades bancarias más importantes del país contra el fraude digital.

4.- Scitum- CSIRT[187]

Sede: Scitum

Tipo: Sector Privado

Es una empresa consultora y de servicios administrativos de seguridad de la información con presencia en México y diversos países de Latinoamérica, creada en 1998, forma parte de Telmex y Grupo Carso; como también, es miembro activo de FIRST.

La creación de los CERT´s del sector privado, es el resultado de la necesidad de abarcar un mercado fértil en México enfocado al sector empresarial que busca cada vez más estos tipos de servicios ante el número creciente de ataques

[185] Se recomienda visitar la página oficial del CERT de la UNAM el cual contiene información importante, documentos, boletines, infografía, eventos, entre otros. UNAM-CERT. Acerca de la Coordinación de Seguridad de la Información (CSI). *DGTIC.* Recuperado de: https://www.seguridad.unam.mx/ Fecha de consulta: 12/08/2017.

[186] Mnemo. Nosotros. *Mnemo.* Recuperado de: https://www.mnemo.com/nosotros/ Fecha de consulta: 12/08/2017.

[187] Scitum. ¿Quiénes somos?. *Scitum.* Recuperado de: https://www.scitum.com.mx/ScitumCSIRT Fecha de consulta: 30/11/2017.

cibernéticos, sumando que en México no hay muchos competidores para ofrecer dichos servicios; por otro lado, el país cuenta con CERT´s del sector académico, privado e institucional/policial, pero no se existe ninguno por parte de las Fuerzas Armadas, algo que no debería pasar por alto, ya que demuestra que aún le falta recorrer camino al sector militar.

Cabe señalar que hay una colaboración cada vez más estrecha entre el sector privado e instituciones de Estado; donde a inicios del 2017, Microsoft en colaboración con la Policía Federal abrió en la Ciudad de México el Centro de Ciberseguridad, con el que se busca ofrecer una mejor respuesta ante el incremento de incidentes cibernéticos, como también, en ayudar al desmantelamiento del crimen organizado que opera ya mediante delitos cibernéticos en México y en la región de América Latina. El propósito del Centro es:[188]

- Aprovechar el papel proactivo de Microsoft en materia de combate al cibercrimen, en particular en el desmantelamiento de las organizaciones criminales que operan a través de esquemas de Botnet.
- Permitir a expertos en seguridad cibernética de México y América Latina trabajar con especialistas de Microsoft para combatir en conjunto el cibercrimen.
- Fungir como sede para desarrollar actividades de capacitación, dirigidas a autoridades y sector público en general, para apoyar la generación y fortalecimiento de capacidades técnicas.

El marco jurídico nacional y el desarrollo de la ciberseguridad en México ya no es un lujo, ya es una necesidad, ante los eminentes ataques que seguirán aumentando con un rango de alcance y daño cada vez mayor.

[188] También se firmó un Programa de Seguridad Gubernamental entre Microsoft y el gobierno a través de la Policía Federal, el cual agrupa iniciativas de las compañías Cyber Threat Intelligence Program (CTIP), el Security Cooperation Program (SCP), y Microsoft Malware Protection Center; este programa le permitirá al gobierno mexicano acceder a información importante relacionado a la seguridad cibernética. XTREM SECURE. (2017, Marzo-Abril). Novedades Tecnológicas en Seguridad. *XTREM SECURE*. pág. 52.

3.1.1 EL AVANCE DE LA CIBERSEGURIDAD DENTRO DEL PERIODO 2000-2017

Se revisó los avances en materia de ciberseguridad de los Informes de Gobierno y los Planes Nacional de Desarrollo de los tres sexenios: Vicente Fox (2000-2006), Felipe Calderón (2006-2012) y Peña Nieto (2012- 2018), existiendo una gran diferencia en el desarrollo de políticas de ciberseguridad entre el actual sexenio y los otros últimos dos.

En el transcurso del sexenio de Vicente Fox, no se contaba con ningún avance en políticas cibernéticas en México y a nivel internacional todavía no tenía mucho eco, por eso no se encuentra nada relacionado a ello en sus Informes de Gobierno y Plan Nacional de Desarrollo, esto debido a que al principio del siglo no existía una amenaza cibernética como tal a la Seguridad Nacional, aunque ya se contaba en algunas regiones o países un avance en políticas cibernéticas como por ejemplo el Convenio de Budapest de la Unión Europea, mientras en México la Ley de Seguridad Nacional nacía a finales de sus sexenio (dicha ley en la actualidad aún sigue sin incorporar a la ciberseguridad como un área de competencia de la Seguridad Nacional). Por lo tanto, a principios del siglo la ciberseguridad aún no era tan conocida, y todavía no estaba priorizada dentro de la Seguridad Nacional de diversos países.

3.1.1.1 SEXENIO DE FELIPE CALDERÓN (2006-2012)

En el caso de Felipe Calderón, en su Plan Nacional de Desarrollo[189] como también en su Primer Informe de Gobierno[190] no hay ninguna mención sobre

[189] Su PND lo divide en 5 ejes: 1.- Estado de Derecho y seguridad, 2.- Economía competitiva y generadora de empleos, 3.- Igualdad de oportunidades, Sustentabilidad ambiental y 5.- Democracia efectiva y política exterior responsable. Plan Nacional de Desarrollo 2007-2012. [Archivo PDF]. Recuperado de: http://pnd.calderon.presidencia.gob.mx/index.php?page=documentos-pdf Fecha de consulta: 30/11/2017.

[190] Primer Informe de Gobierno de Felipe Calderón. [Archivo PDF]. Recuperado de: http://calderon.presidencia.gob.mx/informe/primer/descargas/index.html Fecha de consulta: 30/11/2017.

ciberseguridad ni nada relacionado, sino hasta el Segundo Informe de Gobierno, donde ya empieza el despegue de la ciberseguridad en el país. Se enfatiza que solo se abordará y mencionará los más importante o lo que ha marcado un hito de ciberseguridad en el país, para evitar extenderse.

- Segundo Informe de Gobierno[191]

En este Segundo Informe inicia lo que sería la base de la ciberseguridad, pues es donde se encuentra el primer registro de las políticas cibernéticas del país, lo más interesante es que inició en una institución policial y no en una militar, a pesar que este Segundo Informe salió en el mismo año que ocurrió el ataque cibernético a Estonia. Dentro del informe, la ya extinta Secretaría de Seguridad Pública (SSP), inició con una participación en una reunión de Delitos Cibernéticos en Estados Unidos, en el caso de la difusión, las misma Secretaría coordinó e implementó programas públicos sobre delitos cibernéticos donde se abordaron temas sobre los riesgos de ser víctima de algún hecho delictivo a través de internet, por otro lado la Procuraduría General de la República (PGR) a través del Centro Nacional de Atención Ciudadana (CENAC) atendió y dio seguimiento a 57 denuncias relacionadas a delitos cibernéticos. Aquí se recalca que la baja tasa de delitos cibernéticos en este periodo se debía a que el Internet empezaba a crecer y su porcentaje de penetración dentro de la población apenas llegaba a 20 millones de usuarios, como se había mencionado anteriormente.

- Tercer Informe de Gobierno[192]

En este informe se destaca solo la participación de la Secretaría de Seguridad Pública (SSP) en diversas reuniones internacionales para el intercambio de información, experiencias y mejores prácticas en temas como los delitos cibernéticos, también a través de programas, se inicia la difusión de la prevención de delitos cibernéticos. Este informe solo se dedica a hacer difusión, todavía no hay

[191] Segundo Informe de Gobierno de Felipe Calderón. [Archivo PDF]. Recuperado de: http://calderon.presidencia.gob.mx/informe/segundo/descargas/index.html Fecha de consulta: 30/11/2017.
[192] Tercer Informe de Gobierno de Felipe Calderón. [Archivo PDF]. Recuperado de: http://calderon.presidencia.gob.mx/informe/tercer/descargas/index.html Fecha de consulta: 30/11/2017.

una mayor participación de otras instancias gubernamentales; como también, no hay ningún avance notorio.

- Cuarto Informe de Gobierno[193]

En este Cuarto Informe las Secretaría de Seguridad Pública, ya se coordina con los tres niveles de gobierno a través de la Policía Federal, para apoyar a las entidades estatales en programas de Delitos Cibernéticos para su implementación. Aquí ya se menciona un registro de la participación del sector académico, donde Comisión Intersecretarial para Prevenir y Sancionar la Trata de Personas (CIPSTP) junto con la Universidad Iberoamericana, organizaron el foro académico "Prevención del Delito de Trata de Personas en el Siglo XXI: los Riesgos, Trampas Cibernéticas y Trata en línea".

En el escenario internacional México participó en el Comité Interamericano Contra el Terrorismo (CICTE), para el fortalecimiento de lazos de cooperación a partir del desarrollo de programas de capacitación y personal dentro de los ámbitos de seguridad cibernética, entre otros; esto es importante dado que desde el 2004 la CICTE ya contaba con un programa de Seguridad Cibernética para sus Estados miembros, pero México empieza su participación activa 5 años después.

- Quinto Informe de Gobierno[194]

Este Informe es muy importante, debido a la creación de la División Científica (actualmente se encuentra ahí la Policía Cibernética) dentro de la Policía Federal. Este periodo habla de una captación de 4,991 denuncias sobre delitos cibernéticos, con un resultado destacado en febrero del 2011, ya que se hace la primera sentencia federal por el delito de pornografía infantil, en la cual se condenó a un ciudadano canadiense que desde Tijuana, Baja California, operaba 36 sitios web. Aquí ya la Policía Federal empieza a difundir más lo que sería los delitos

[193] Cuarto Informe de Gobierno de Felipe Calderón. [Archivo PDF]. Recuperado de: http://calderon.presidencia.gob.mx/informe/cuarto/informe-de-gobierno/ Fecha de consulta: 30/11/2017.
[194] Quinto Informe de Gobierno de Felipe Calderón. [Archivo PDF]. Recuperado de: http://calderon.presidencia.gob.mx/informe/quinto/descargas/ Fecha de consulta: 30/11/2017.

cibernéticos, dando capacitaciones a jóvenes y niños; como también, a personal gubernamental.

En el escenario internacional, lo más destacado fue que se aprobó en Guadalajara, Jalisco la resolución de la Unión Internacional de Telecomunicaciones (UIT) para le definición de Ciberseguridad.

- Sexto Informe de Gobierno[195]

En este último Informe, lo más destacado es el incremento exponencial de la captación por parte de la División Científica de la Policía Federal de denuncias ciudadanas en materia de delitos cibernéticos (11,264 denuncias en el periodo de septiembre del 2011 a junio de 2012)

Algo también destacable y que solo se mencionó hasta este Informe de Gobierno, fue la creación del Manual Administrativo de Aplicación General en materias de TIC y de Seguridad de la Información (MAAGTICSI) [196] el cual nace en el 2010 con el objetivo de definir los procesos de las instituciones gubernamentales para observar, implementar y operar los criterios relacionados a la seguridad de la información.

El MAAGTICSI se ha ido modificando principalmente en el sexenio de Enrique Peña Nieto hasta llegar a ser aproximado a la Ley de Seguridad Nacional, ya que la seguridad de la información se considera una competencia de la Seguridad Nacional tal en el Artículo 28 del Manual, como también se señala el tipo de grado de importancia que tienen una institución o instalación a través de la medidas “AAA”, “AA” y “A”[197].

---

[195] Sexto Informe de Gobierno de Felipe Calderón. [Archivo PDF]. Recuperado de: http://calderon.presidencia.gob.mx/informe/sexto/sexto_informe.html Fecha de consulta: 30/11/2017.

[196] Nace por del Programa Especial de Mejora de la Gestión en la Administración Pública Federal 2008-2012, el cual es coordinado por la Secretaría de la Función Pública. Diario Oficial de la Federación. (13 Julio 2010). Acuerdo por el que se expide el Manual Administrativo de Aplicación General en materias de TIC y de Seguridad de la Información. *SEGOB.* Recuperado de: http://dof.gob.mx/nota_detalle.php?codigo=5151475&fecha=13/07/2010 Fecha de consulta: 14/08/2017.

[197] Secretaría de la Función Pública. (4 de febrero de 2016). Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad dela información, así como el Manual Administrativo de Aplicación

En el sexenio de Felipe Calderón se empezó lo que sería las bases de las políticas de ciberseguridad de México. Durante su periodo, lo más importante fue la creación de la División Científica de la Policía Federal, que en la actualidad cuenta con uno de los 4 CERT´s en México: CERT-MX, gracias a esto se empieza a dar seguimiento de delitos cibernéticos de alto impacto en el país. También empezó a difundir a través de talleres, conferencias y actividades, el conocimiento ciudadano en materia de delitos cibernéticos, todas ellas llevadas a cabo por la SSP a través de la Policía Federal (en este sexenio se eliminó la Secretaría de Seguridad Pública, pero la Policía Federal sigue llevando a cabo estas actividades). También se nota un ligero incremento en la participación de México en diversos foros y reuniones en temas relacionados con los delitos cibernéticos.

3.1.1.2 SEXENIO DE ENRIQUE PEÑA NIETO (2012-2018)

El sexenio de Calderón se considera el inicio de la ciberseguridad en el país, pero quien lo está desarrollando es el presidente Enrique Peña Nieto, el cual en su sexenio actual se implementó la Estrategia Nacional de Ciberseguridad, esto a consecuencia del Plan Nacional de Desarrollo[198] que en dicho documento solo se menciona el fortalecimiento de la ciberseguridad, donde el sector militar empieza su desarrollo cibernético; esto se encuentra en el eje de México en Paz, estrategia 1.2.3: "Fortalecer la inteligencia del Estado Mexicano para identificar, prevenir y contrarrestar riesgos y amenazas a la Seguridad Nacional", el cual menciona:

> "Impulsar, mediante la realización de estudios e investigaciones, iniciativas de ley que den sustento a las actividades de inteligencia civil, militar y naval, para

General en dichas materias. *Secretaría de la Función Pública.* [Archivo PDF]. Recuperado de: https://www.gob.mx/cms/uploads/attachment/file/79205/MANUAL_ADMINISTRATIVO_DE_APLICACION_GENERAL_EN_MATERIA_DE_TECNOLOGIAS_DE_LA_INFORMACION_Y_COMUNICACIONES.pdf Fecha de consulta: 30/11/2017.

[198] Se encuentra dividido en 5 ejes: 1.- México en paz; 2.- México Incluyente; 3.- México con Educación de Calidad; 4.- México Prospero y 5.- México con Responsabilidad Global. Plan Nacional de Desarrollo 2013-2018 de Enrique Peña Nieto. [Archivo PDF]. Recuperado de: http://pnd.gob.mx/ Fecha de consulta: 01/12/2017.

fortalecer la cuarta dimensión de operaciones de seguridad[199]: ciberespacio y ciberseguridad"

Del Plan Nacional de Desarrollo nacen diversos programas y estrategias, el cual solo se abordarán las cuatro más importantes, que es el Programa para la Seguridad Nacional 2014-2018, Programa Nacional de Seguridad Pública 2014-2018, Programa Sectorial de Defensa Nacional 2013-2018 y Programa Sectorial de Marina 2013-2018; los cuales por primera vez abarcan temas relacionados al fortalecimiento de México en materia de ciberseguridad para los cuerpos policiales y cuerpos militares. Se quiere dejar claro, que solo se mencionará lo más importante y destacado de cada Programa e Informe de Gobierno.

- Programa para la Seguridad Nacional 2014-2018[200]

Este programa reconoce por fin a la ciberseguridad como un área de competencia de la Seguridad Nacional, al aceptar a la ciberseguridad como la cuarta dimensión operacional de seguridad del país, abordando la necesidad que tiene el país en el fortalecimiento de las instituciones, creación de leyes y la cooperación con América del Norte para combatir las amenazas a la Seguridad Nacional y delitos cibernéticos. También se habla del ciberespacio como un entorno peligroso debido al notorio incremento de ataques cibernéticos al nivel internacional, debido a esto la ciberseguridad se ve como una prioridad a desarrollar en México, creando políticas y estrategias de Estado, para evitar en un futuro afectaciones a las comunicaciones e integridad de sistemas de información estratégicos del país. Considerando lo anterior mencionado, el programa trabajará en:

- Impulsar proyectos normativos para la regularización de seguridad de la información, homologándose en todos los sectores del país.

[199] México solo considera tres dimensiones: aire, tierra y mar, agregando al ciberespacio como la cuarta dimensión operacional; mientras en países más avanzados consideran el espacio ultraterrestre la cuarta dimensión, y el ciberespacio como la quinta dimensión. Secretaría de Marina & Centro de Estudios Superiores Navales. Op. Cit., (pág. 38).

[200] Programa para la Seguridad Nacional 2014-2018. *Enrique Peña Nieto* [Archivo PDF]. Recuperado de: https://www.gob.mx/presidencia/articulos/programa-para-la-seguridad-nacional-2014-2018 Fecha de consulta: 01/12/2017.

- Asignar una unidad administrativa para encargarse del cumplimiento de la política de seguridad Cibernética y Ciberdefensa para el Ejecutivo Federal.
- Fortalecimiento de mecanismos de coordinación para atender los incidentes de Ciberseguridad y Ciberdefensa para el Ejecutivo Federal.
- Impulsar el cumplimiento y desarrollo de procedimientos para la evaluación y fortalecimiento de equipos de respuesta a incidentes de ciberseguridad en el ámbito Ejecutivo Federal.
- Fortalecimiento de capacidades tecnológica, humana e infraestructura para atender a los incidentes de ciberseguridad.
- Cooperación internacional en materia de ciberseguridad y ciberdefensa para prevenir y enfrentar ataques cibernéticos en el país.
- Desarrollar la capacitación y el adiestramiento del personal militar y naval en materia de inteligencia, contrainteligencia, ciberseguridad y ciberdefensa.

Como se ve, las Fuerzas Armadas tienen un objetivo más elaborado y apegado a los temas coyunturales de un desarrollo cibernético del país para la Seguridad Nacional, de hecho a continuación vienen los Programas Sectoriales de la Marina y Ejército, el cual se resalta que la institución que más desarrollada está en ciberseguridad es la Secretaría de Marina (SEMAR), quedando atrás la Secretaría de Defensa Nacional (SEDENA).

- Programa Sectorial de Defensa Nacional 2013-2018[201]

La Secretaría de Defensa Nacional menciona al ciberespacio como un ámbito a desarrollar, considerando que se ha visto descuidado desde el punto de vista militar, ya que solamente se ha abordado en el ámbito de seguridad Institucional y persecución de delitos. Esto se refleja en la Agenda Nacional de Riesgos 2012, donde plantea la vulnerabilidad cibernética un factor al impacto de la defensa de México. También se habla de la necesidad de crear un organismo centralizado que prevea seguridad y defensa a la institución dentro del ciberespacio. Con base a esto la SEDENA creará doctrinas de temas relacionados al ciberespacio, impulsando

[201] Programa Sectorial de Defensa Nacional 2013-2018. *Enrique Peña Nieto* [Archivo PDF]. Recuperado de: http://www.sedena.gob.mx/archivos/psdn_2013_2018.pdf Fecha de consulta: 01/12/2017.

acciones y promoviendo una política pública a las actividades relacionadas al ámbito. Dentro de sus Objetivos, Estrategias y Líneas de Acción a desarrollar se habla de:

- Fortalecimiento del marco jurídico de las Fuerzas Armadas al impulsar un marco legal para el desarrollo de la cuarta dimensión de operaciones: Ciberespacio.
- Fortalecimiento del Sistema de Inteligencia Militar al desarrollar al cuarto campo de operación: "Ciberespacio" con recursos humanos, materiales y tecnológicos, teniendo como interés, el contribuir a la protección de activos informáticos y comunicaciones de ataques que pretendan vulnerar los centros de control estratégicos; también fortalecer la Escuela Militar de Inteligencia, la capacitación y adiestramiento del personal militar en las materias de inteligencia, contrainteligencia y ciberespacio.
- Crear el Centro de Operaciones del Ciberespacio (COC)[202], el cual se creará por primera vez en este sexenio, dentro de un periodo de 2013 al 2018, con el fin de desarrollar la capacidad operacional de la cuarta dimensión: Ciberespacio.

La SEDENA considera a la ciberseguridad importante y acepta que no se había abordado desde el enfoque militar; por eso crea el Centro de Operaciones del Ciberespacio, el cual la SEDENA contará con un área especializada en temas relacionados al ciberespacio, algo que se considera que debió de haberlo hecho el sexenio anterior; si bien la SEDENA ya cuenta con estrategias y líneas de acción para la ciberseguridad y ciberdefensa, todavía tiene mucho que avanzar dado que se ha quedado rezagada a comparación de la Secretaría de Marina, como se verá a continuación.

[202] Definido como: Organismo encargado de planear, coordinar y dirigir los esfuerzos del Ejército y Fuerza Aérea, para identificar, prevenir y contrarrestar toda amenaza o incidente proveniente en el ciberespacio, que atente contra la información e infraestructura crítica de la SEDENA, soportada en TIC y aquella que se asigne bajo su responsabilidad.

- Programa Sectorial de Marina 2013-2018[203]

El avance cibernético es más profundo en la Secretaría de Marina, aquí la SEMAR se propone elaborar el Diagnóstico Institucional de Seguridad de la Información, Ciberdefensa y Ciberseguridad (DISICC); elaborar e implementar la Estrategia Institucional de Seguridad de la Información, Ciberdefensa y Ciberseguridad (EISICC); modernizar con equipamiento, capacitación y tecnologías el Sistema Integral de Seguridad de la Información Institucional acorde a la Estrategia Nacional; constituir un Centro de Control de Ciberdefensa y Ciberseguridad (CCCC) para fortalecer la cuarta dimensión de Operaciones de Seguridad; adquirir infraestructura tecnológica y capacitación para llevar a cabo acciones de Seguridad en el Ciberespacio y fortalecer la coordinación interinstitucional para impulsar la Estrategia Nacional de Seguridad de la Información, todo esto en un periodo de 5 años.

La SEMAR y SEDENA se basan en el Plan Nacional de Desarrollo 2012-2018, pero el avance cibernético es más notorio y le da más prioridad la SEMAR; esto se ve en su Programa Sectorial, mientras la SEDENA creará un Centro de Control, la SEMAR aparta de crear el Centro de Control, elaborará estrategias, diagnósticos y modernización de sus equipo para hacer frente a los retos de ciberdefensa y ciberseguridad. Si bien cada una creará su propio Centro de Control de Ciberseguridad y Ciberdefensa institucional, no se menciona nada relacionado a crear un Cibercomando unificado, el cual dotaría al país de un avance cibernético militar; y en caso que se llegara a crear uno, existiría una problemática sobre a qué institución pertenecería o si sería independiente.

[203] Programa Sectorial de Marina 2013-2018. *Enrique Peña Nieto* [Archivo PDF]. Recuperado de: http://www.semar.gob.mx/informes/programa_sectorial_13.pdf Fecha de consulta: 01/12/2017.

- Programa Nacional de Seguridad Pública 2013-2018[204]

El programa reconoce la capacidad del crimen organizado a nivel internacional y nacional al adoptar a las Tecnologías de la Información y la Comunicación (TIC), para coordinar y cometer delitos con un alto impacto relacionado a la pornografía infantil, secuestro, extorsión y trata de personas; como también, delitos cibernéticos como fraudes, usurpación de identidad (phishing), acceder ilegalmente a sistemas y equipos de informática y delitos relacionados a derechos de autor. Dentro de las estrategias y líneas de acción menciona:[205]

- Fortalecimiento de las capacidades, la infraestructura tecnológica de las instituciones policiales y el desarrollo de la investigación científica para prevenir e investigar delitos cibernéticos.
- Implementar acciones contra delitos de alto impacto como la pornografía infantil, fraude, extorsión, phishing y derechos de autor.
- Diseñar protocolos operacionales para evitar delitos cibernéticos en las instancias que contengan información reservada o confidencial.
- Creación y fortalecimiento de unidades especializadas en la prevención e investigación de delitos dentro de Internet.
- Desarrollar un modelo de policía cibernética para las Entidades Federativas.
- Generar indicadores y estadísticas de delitos cibernéticos para el diseño de estrategias de prevención.
- Impulsar acciones para consolidar los esquemas de ciberseguridad que ayuden al desarrollo de la economía digital e impulsar la cultura de seguridad cibernética para niños y jóvenes ya que son las principales víctimas de delitos cibernéticos.

[204] Diario Oficial de la Federación. (30 de abril de 2014). Programa Nacional de Seguridad Pública 2013-2018. *SEGOB.* Recuperado de: http://dof.gob.mx/nota_detalle.php?codigo=5343081&fecha=30/04/2014 Fecha de consulta: 01/12/2017.

[205] Menciona a la Secretaría de Gobernación (SEGOB), SEMAR, SEDENA y la Procuraduría General de la República (PGR) como instituciones participantes de la Estrategia 2.7 Detectar y atender oportunamente los delitos cibernéticos.

- Fortalecer la seguridad de la infraestructura digital de México.

A diferencia del sector militar, se busca que la policía a nivel nacional pueda hacer frente al incremento de delitos cibernéticos por parte del crimen organizado, de hecho esta sería la primera instancia en tomar medidas contra las amenazas de ciberseguridad a ciudadanos y sector privado, cuando la amenaza rebase las competencias policiales es cuando el sector militar entraría en operación, como el caso de un ataque cibernético a una instalación estratégica en el país.

Existe un problema de centralismo en el área cibernética policial, esto debido que la Policía Federal es la que atiende y abarca los delitos nacionales en casi todas las entidades estatales; por el cual se busca ayudar a las policías estatales a formar su propia Policía Cibernética para poder quitar la carga de trabajo a las Policía Federal y preparar a las policías de los estados en hacer frente a delitos cibernéticos cada vez más presentes. Otra problemática, es que la Policía Cibernética está subordinada y forma parte de la División Científica, esto le quita más dinamismo y entorpece su funcionamiento, el cual sería bueno crear una División más en la Policía Federal para la Policía Cibernética, dándole un mayor presupuesto, peso, personal y capacidad de acción para que se dedique completamente y con una mayor autoridad y competencia a perseguir los delitos cibernéticos que cada vez son más comunes en México.

- Primer Informe de Gobierno[206]

En los Informes de Gobierno del sexenio actual, existe una mayor participación de México a nivel internacional y un mejor fortalecimiento interinstitucional a nivel federal y estatal en materia de ciberseguridad. Se recuerda que para evitar extenderse solamente se mencionará lo más destacado en cada informe de gobierno. En este Primer Informe se crea un Protocolo entre el CERT-MX y las instancias que forman el Consejo de Seguridad Nacional[207] para el

[206] Primer Informe de Gobierno de Enrique Peña Nieto. [Archivo PDF]. Recuperado de: http://www.presidencia.gob.mx/primerinforme/ Fecha de consulta: 30/11/2017.

[207] Se encuentra en el Artículo 12 de la Ley de Seguridad Nacional, y está conformado por El Titular del Ejecutivo Federal; el Secretario de Gobernación, quien fungirá como Secretario Ejecutivo; El Secretario de la Defensa Nacional; El Secretario de Marina; El Secretario de Seguridad Pública (no existe ya la Secretaría, por

fortalecimiento de tareas de coordinación, gestión y respuesta a incidentes que atenten contra la infraestructura cibernética de México.

Se genera un documento para la creación del Centro Coordinador de Respuesta a Incidentes de Seguridad para el sector de Seguridad Nacional, y proyectos de reformas a diversas leyes como el Código Penal Federal, Código Federal de Procedimientos Penales, Ley de la Policía Federal y Ley Federal de Telecomunicaciones, para impulsar el marco jurídico nacional en materia de ciberdelitos.

Se fortalece los lazos entre la SEMAR y SEDENA para homologar la visión acerca del ciberespacio; con el fin de desarrollar las capacidades de ciberdefensa y garantizar la seguridad interior en el ámbito del ciberespacio; dicha cooperación se debió al ataque cibernético de DDoS que sufrió en enero del 2013 la página web de la Secretaría de Marina, mientras la página web de la Secretaría de Defensa Nacional fue hackeada por Anonymous, el cual colocó un video y un extracto de un mensaje del Ejército Zapatista de Liberación Nacional (EZLN).[208]

México estrechó la colaboración con el CICTE de la OEA para promover una mayor alianza con el sector privado y el sector académico en cuestiones de ciberseguridad; como también, la participación en ejercicios de simulación de ataques cibernéticos a fin de sumar esfuerzo para mantener la ciberseguridad en sectores importantes del país.

- Segundo Informe de Gobierno[209]

En este Segundo Informe se incrementó la participación de la SEDENA a nivel internacional en diversas reuniones de trabajo, entre las que se destaca la primera edición del Entrenamiento Internacional de Ciberespacio, el cual tuvo como

---

lo tanto toma lugar el titular de la CNS); El Secretario de Hacienda y Crédito Público; El Secretario de la Función Pública; El Secretario de Relaciones Exteriores; El Secretario de Comunicaciones y Transportes; El Procurador General de la República y El Director General del Centro de Investigación y Seguridad Nacional.

[208] CCO Noticias. (17 de enero de 2013). Sedena y Marina niegan robo de datos; reestablecen sitios. *CCO Noticias.* Recuperado de: https://cconoticias.com/2013/01/17/sedena-y-marina-niegan-robo-de-datos-reestablecen-sitios/ Fecha de consulta: 27/12/2017.

[209] Segundo Informe de Gobierno de Enrique Peña Nieto. [Archivo PDF]. Recuperado de: http://www.presidencia.gob.mx/segundoinforme/ Fecha de consulta: 30/11/2017.

objetivo compartir experiencias y conocimientos generales en ciberespacio; como también designó a un representante ante la misión de México en la OEA para desempeñarse como gerente del Programa en Seguridad Cibernética en el CICTE del 1 de octubre de 2013 al 30 de septiembre de 2015.

En el caso de la SEMAR, lo más destacado es que se reestructuró y modernizó el "Centro de Monitoreo y Respuesta a Incidentes de Seguridad en el Ciberespacio"[210]; y con la SEDENA celebró el "Protocolo de Colaboración para el Intercambio de Información Relacionada con la Ciberdefensa, Ciberseguridad y Seguridad de la Información en el Ciberespacio". Y se inició la coordinación con el área de Ciberdefensa de las Fuerzas Armadas de Francia y España, para establecer protocolos de colaboración e intercambio de información. A su vez el gobierno generó inteligencia táctica y operativa especializada en temas considerados en la Agenda Nacional de Riesgos (ANR)[211], abordando diversos temas, el cual se encuentra la ciberseguridad.

- Tercer Informe de Gobierno[212]

En este informe existe una estrecha relación entra la SEMAR y el Comando Norte de Estados Unidos, para realizar diversos ejercicios; a su vez se fortaleció la colaboración con el Estado Mayor Conjunto de Francia para el intercambio de información relacionada a la seguridad cibernética (ciberseguridad y ciberdefensa). La Secretaría de Gobernación como miembro del Comité Especializado en Seguridad de la Información[213] del Consejo de Seguridad Nacional, participó en la

[210] Controlada por la Subsección de Protección de Infraestructuras de Información perteneciente a la Sección Segunda del Estado Mayor General de la Armada.
[211] La ANR es un instrumento que identifica los riesgos a la Seguridad Nacional del país y en ella se encuentran mecanismos de coordinación y políticas para hacer frente a las amenazas y dar continuidad al proyecto de Nación. Este ANR es aprobada anualmente por el presidente en el seno del Consejo de Seguridad Nacional a propuesta del secretario técnico.
[212] Tercer Informe de Gobierno de Enrique Peña Nieto. [Archivo PDF]. Recuperado de: http://www.presidencia.gob.mx/tercerinforme/ Fecha de consulta: 30/11/2017.
[213] La conforman: Presidencia de la República, Secretaría de Gobernación, Secretaría de la Defensa Nacional, Secretaría de Marina, Secretaría de Hacienda y Crédito Público, Secretaría de la Función Pública, Secretaría de Relaciones Exteriores, Secretaría de Comunicaciones y Transportes, Secretaría de Energía, así como la Procuraduría General de la República, Comisión Nacional de Seguridad, Servicio de Administración Tributaria y Centro de Investigación y Seguridad Nacional; como invitados el Banco de México, Petróleos Mexicanos y Comisión Federal de Electricidad.

actualización de la Estrategia Nacional de Seguridad de la Información y del protocolo de colaboración entre el CERT-MX y las instancias de seguridad nacional, así mismo, participó en el proyecto de creación de un Área Especializada en Seguridad de la Información y la elaboración de un Catálogo de Infraestructuras Críticas de Información en el Gobierno Federal; como también, participó en la elaboración y aplicación del "Procedimiento de Análisis Remoto de Vulnerabilidades" a portales Web de las dependencias que integran el Consejo de Seguridad Nacional, con objeto de identificar las principales vulnerabilidades y emitir recomendaciones en prevención de ataques cibernéticos.

La SEDENA participó en la Primera Ronda de Conversaciones en Temas de Ciberdefensa con el Comando Conjunto de Fuerzas Armadas de Perú; y a su vez, en el 4o. Seminario de Seguridad Interior, Conferencia en materia de Defensa, Inteligencia, Ciberseguridad y Sistemas de Prisiones, organizado por el Ministerio de Defensa de Israel. Se integró al subgrupo de "Seguridad Cibernética" dentro del Grupo Bilateral de Cooperación en Seguridad México-Estados Unidos.

- Cuarto Informe de Gobierno[214]

México asistió a la 14° Sesión del Comité del Convenio sobre la Ciberdelincuencia, en Francia (depende del Consejo de Europa), el cual se presentaron actualizaciones, tendencias y mejores prácticas sobre ciberseguridad, el cual se evaluó para una posible implementación en el país; a su vez participó en el Entrenamiento Internacional de Ciberseguridad organizado por el Grupo de Delitos Electrónicos del Servicio Secreto de Estados Unidos y la OEA, el cual fue dirigido a personal con conocimientos en investigaciones de crímenes cibernéticos y pertenecientes a una unidad de investigación de ciberdelincuencia; y la visita de intercambio de experiencias y buenas prácticas en ciberseguridad a España y Estonia, con el apoyo de la OEA.

La SEDENA participó en la "I Reunión del Subgrupo sobre Políticas Cibernéticas México-Estados Unidos", realizado en Ciudad de México y en

[214] Cuarto Informe de Gobierno de Enrique Peña Nieto. [Archivo PDF]. Recuperado de: http://www.presidencia.gob.mx/cuartoinforme/ Fecha de consulta: 30/11/2017.

reuniones de coordinación realizadas por el subgrupo de Seguridad Cibernética del Grupo Bilateral de Cooperación en Seguridad México-Estados Unidos. Fue sede y anfitrión del ejercicio de gabinete "CYBERLIBERTAD II 2016", con la participación de la Secretaría de Marina, Policía Federal, Centro de Investigación y Seguridad Nacional, Secretaría de Comunicaciones y Transportes, Secretaría de Relaciones Exteriores, Servicios a la Navegación en el Espacio Aéreo Mexicano, Instituto Politécnico Nacional, Universidad Nacional Autónoma de México y una delegación de las Fuerzas Armadas de Estados Unidos, para desarrollar una compresión mutua sobre la ciberseguridad, funciones y responsabilidades. En este informe se menciona ya la creación de Centro de Operaciones del Ciberespacio de la Secretaría de Defensa Nacional.

La Secretaría de Gobernación participó en la Cumbre de Líderes de América del Norte (México, Estados Unidos y Canadá), se integró al Subgrupo de Temas Cibernéticos, el cual pondrá los esfuerzos para apoyar iniciativas de colaboración internacional sobre temas ciberseguridad.

- Quinto Informe de Gobierno[215]

En la plataforma digital de participación ciudadana dentro de la página web oficial, se llevó acabo dos encuestas dentro del marco del proceso de la Estrategia Nacional de Ciberseguridad; se sometió a consulta pública el primer documento de trabajo de la Estrategia Nacional de Ciberseguridad; como también se impartieron talleres para su elaboración contando con la participación de la Secretaría de Defensa Nacional y la Secretaría de Marina.

México fue sede de la Conferencia Internacional Meridian 2016 dedicada a la protección de infraestructuras críticas de información el cual desarrolló con el apoyo del Foro Global de la Experiencia Cibernética (GFCE, por sus siglas en inglés), de la OEA y otros organismos nacionales e internacionales, logrando la participación de 11 países latinoamericanos.

[215] Quinto Informe de Gobierno de Enrique Peña Nieto. [Archivo PDF]. Recuperado de: http://www.presidencia.gob.mx/quintoinforme/ Fecha de consulta: 30/11/2017.

En el caso de la PGR, [216] participó en Viena, Austria, a la Tercera Reunión del Grupo Intergubernamental de Expertos de Composición Abierta, encargado de realizar un estudio exhaustivo sobre delito cibernético, en la cual se examinaron opciones para fortalecer las actuales respuestas jurídicas ante dicho ilícito en los planos, nacional e internacional.

La SEMAR creó la Unidad de Ciberseguridad (UNICIBER), dependiendo del Estado Mayor General de la Armada, con la misión de planear, conducir y ejecutar actividades de seguridad de la información, ciberseguridad y ciberdefensa, para la protección de la infraestructura crítica de la Institución; a su vez, fortaleció su Sistema de Mando y Control, con la implementación de una sala de inteligencia marítima y portuaria para la coordinación de acciones, y también una sala de ciberseguridad para incorporar la dimensión operacional del ciberespacio.

Durante este sexenio la ciberseguridad alcanza un punto de desarrollo en México, a pesar que aún le falta mucho por recorrer comparándola con otros países. En todos los informes de gobierno fue destacado la colaboración con tres Estados: Francia, Estados Unidos e Israel; por otro lado, con quien se tiene una mayor participación en el área de Organismos Internacionales, es con la Organización de Estados Americanos (OEA), quien ha ayudado a México en la elaboración de su Estrategia Nacional de Ciberseguridad, un documento que marcará un hito en las políticas cibernéticas del país; como también, en la capacitación de funcionarios, cuerpos policiales y militares. Cabe destacar que existe información omitida en estos informes de gobierno, como por ejemplo la obtención de software espías por parte de las agencias de inteligencia de México.

[216] En este mismo año la PGR crea la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas, la cual se crea como la instancia de inteligencia encargada de la ejecución y supervisión de las acciones policiales para apoyar las investigaciones relacionadas con medios tecnológicos y electrónicos bajo el liderazgo del Ministerio Público Federal. Notimex. (05 Septiembre 2017). PGR crea la Unidad de Investigaciones Cibernéticas. *El Economista.* Recuperado de: http://eleconomista.com.mx/tecnociencia/2017/09/05/pgr-crea-unidad-investigaciones-ciberneticas Fecha de consulta: 08/09/2017.

3.2 MARCO JURÍDICO DE LA CIBERSEGURIDAD A NIVEL FEDERAL

En México existe ya un avance de leyes que castiguen los delitos cibernéticos, aunque todavía existen lagunas dentro de esta, dado que los conceptos sean obsoletos o inexistentes; tan solo en el informe de Ciberseguridad de Cisco[217] de mitad de año, señala que existe un incremento exponencial de delitos cometidos en el ciberespacio, el más vulnerable será el sector privado dado a la magnitud de ataques parecidos al de WannaCry, el cual tienen como característica la rápida propagación, con consecuencias que podrían llevar a la destrucción de información y de las copias de seguridad de las empresas; por otro lado, el cibercrimen se posiciona como una industria lucrativa, donde empresas legalmente constituidas compran y venden códigos maliciosos (malware) o incluso ofrecen cursos orientados a personas para cometer delitos cibernéticos[218], esto demuestra la importancia por avanzar jurídicamente en estos temas relacionado a la ciberseguridad y definir mejor los nuevos delitos cibernéticos que están surgiendo.

Dentro del marco jurídico actual de ciberseguridad existen leyes que abordan pobremente los delitos cibernéticos[219], pero en este apartado y dado que se considera más importante y con más competencia, solo se abordará el Código Penal

[217] Mauricio Hernández Armenta. (08 de agosto de 2017). Cisco prevé destrucción de servicios y más ciberataques. *Forbes México.* Recuperado de: https://www.forbes.com.mx/cisco-preve-destruccion-de-servicios-y-mas-ataques-ciberneticos/ Fecha de consulta: 23/08/2017.

[218] Rodrigo Riquelme. (18 de noviembre de 2017). Cibercrimen como servicio, la industria de los ataques digitales. *El Economista.* Recuperado de: https://www.eleconomista.com.mx/tecnologia/Cibercrimen-como-servicio-la-industria-de-los-ataques-digitales-20171118-0010.html Fecha de consulta: 06/12/2017.

[219] Para no extender este tema demasiado, aparte del Código Penal Federal se recomienda ver: la Ley Federal del Derecho de Autor (Art. 101, 102, 106, 108, 109, 110- 114); Ley Federal de Telecomunicaciones y Radiodifusión (Art 3); Ley de Instituciones de Crédito (Art. 112 Bis, Art. 112 Ter, Art. 112 Quáter, Art. 112 Quintus); Ley de Vías Generales de Comunicación (Art. 533); Ley de la Propiedad Industrial (Art. 223, Art. 223 Bis); el nuevo Código Nacional de Procedimientos Penales (Art. 291, Art. 303) y Ley de Seguridad Nacional (Art. 5, Art. 31, Art. 33-36).

Federal.[220] Relacionado a los delitos de vías de comunicación y correspondencia se tiene tres artículos:[221]

> **Artículo 167.-** Se impondrá de uno a cinco años de prisión y de cien a diez mil días multa:
>
> Fracción VI.- Al que dolosamente o con fines de lucro, interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas o de fibra óptica, sean telegráfica, telefónica o satelitales, por medio de las cuales se transfieran señales de audio, de video o de datos;
>
> **Artículo 168 bis.-** Se impondrán de seis meses a dos años de prisión y de trescientos a tres mil días multa, a quien sin derecho:
>
> I. Descifre o decodifique señales de telecomunicaciones distintas a las de satélite portadoras de programas, o
>
> II. Transmita la propiedad, uso o goce de aparatos, instrumentos o información que permitan descifrar o decodificar señales de telecomunicaciones distintas a las de satélite portadoras de programas.
>
> **Artículo 177.-** A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

El artículo 167 y 168 bis se habla sobre la irrupción, interferencia y decodificación de las comunicaciones, pero en caso de un ataque cibernético de Denegación Distribuida de Servicios (DDoS, por sus siglas en inglés), -aquí se podría poner de ejemplo los servidores y páginas de gobierno- este delito se podría relacionar al artículo 167, pero aquí no se tiene el concepto de ataques DDoS dentro del artículo por lo tanto no se puede castigar de igual manera un ataque que tumbe páginas de gobierno importantes a uno que tumbe la página de una empresa, pues ambos ataques irrumpen pero no son de igual magnitud, por lo tanto debe de haber una separación en la forma de castigarlo; ahora si el ataque proviene fuera del país no hay forma de perseguir y castigar, dado al factor del anonimato dentro del ciberespacio.

---

[220] Código Penal Federal. [Archivo PDF]. Recuperado de: https://docs.mexico.justia.com/federales/codigo_penal_federal.pdf Fecha de consulta: 05/12/2017.

[221] Se encuentra en: Titulo Quinto en Materia de Vías de Comunicación y Correspondencia; Capítulo I: Ataques a las vías de comunicación y violación de correspondencia (Artículos 167- Fracción VI y Artículo 168 bis); Capítulo II: Violación de Correspondencia (Artículo 177).

En el sexenio de Calderón se emitió la primera sentencia relacionada a la pornografía infantil a un canadiense por lucrar y ser propietario de contenido pederasta en páginas web. Desgraciadamente las víctimas más vulnerables son los niños y jóvenes quienes son los que más utilizan las redes sociales; pues el Internet constituye la principal fuente de propagación de pornografía infantil.[222] En el Código Penal Federal existe un mayor desarrollo en esta área pero no lo suficiente[223]:

> **Artículo 200.-** Al que comercie, distribuya, exponga, haga circular u oferte, a menores de dieciocho años de edad, libros, escritos, grabaciones, filmes, fotografías, anuncios impresos, imágenes u objetos, de carácter pornográfico, reales o simulados, sea de manera física, o a través de cualquier medio, se le impondrá de seis meses a cinco años de prisión y de trescientos a quinientos días multa.
>
> **Artículo 201.-** Comete el delito de corrupción de menores, quien obligue, induzca, facilite o procure a una o varias personas menores de 18 años de edad o una o varias personas que no tienen capacidad para comprender el significado del hecho o una o varias personas que no tienen capacidad para resistirlo a realizar cualquiera de los siguientes actos:
>
> f) Realizar actos de exhibicionismo corporal o sexuales simulados o no, con fin lascivo o sexual. A quién cometa este delito se le impondrá pena de prisión de siete a doce años y multa de ochocientos a dos mil quinientos días
>
> **Artículo 202.-** Comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientos a dos mil días multa.
>
> A quien fije, imprima, video grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participen una o varias personas menores de dieciocho años de edad o una o varias personas que no tienen capacidad para comprender el significado del hecho o una o varias personas que no tienen capacidad para resistirlo, se le

[222] García Mexía. Op. Cit., (pág. 92).

[223] Relacionado a la Pornografía Infantil, esta se encuentra en: Título Octavo: Delito contra el libre desarrollo de la personalidad: Capítulo I: Corrupción de personas menores de Dieciocho Años de Edad o de Personas que no tienen Capacidad para comprender el Significado del Hecho o de Personas que no tienen Capacidad para Resistirlo (Artículo 200, 201) y Capitulo II Pornografía de Personas Menores de Dieciocho Años de Edad o de Personas que no tienen Capacidad para comprender el Significado del Hecho o de Personas que no tienen Capacidad para Resistirlo (Artículo 202 y 202 Bis).

impondrá la pena de siete a doce años de prisión y de ochocientos a dos mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito.

La misma pena se impondrá a quien reproduzca, almacene, distribuya, venda, compre, arriende, exponga, publicite, transmita, importe o exporte el material a que se refieren los párrafos anteriores.

Artículo 202 BIS.- Quien almacene, compre, arriende, el material a que se refieren los párrafos anteriores, sin fines de comercialización o distribución se le impondrán de uno a cinco años de prisión y de cien a quinientos días multa. Asimismo, estará sujeto a tratamiento psiquiátrico especializado.

Actualmente no existe a nivel federal leyes actualizadas que los protejan de los diversos peligros que hay dentro del Internet, como por ejemplo el grooming[224] (también se puede relacionar al phishing, pues existe una usurpación o robo de identidad por parte del victimario para poder engañar a su víctima) usado principalmente por pedófilos dentro de la red; o los famosos retos que atentan con la integridad del menor como es el caso del reto de la "Ballena Azul", el cual se originó en Rusia y consiste en cumplir una serie de retos (50 retos) los cuales cada vez van subiendo de intensidad hasta llegar al último que consiste en quitarse la vida[225]; o al incremento de ciberacoso o ciberbullying (ambas relacionadas a la porno-venganza)[226] gracias a las tendencia del sexting[227] entre adolescentes y jóvenes adultos. En México a nivel federal no existe como tal estos conceptos dentro de las leyes, porque apenas se empiezan a desarrollar, pero si hay otras que

[224] El Grooming es cuando un adulto se hace pasar por un niño o adolescente para envolver a un menor con el propósito de obtener una satisfacción sexual.

[225] Proceso. (30 de marzo de 2017). Policía Cibernética de la CDMX alerta sobre el reto suicida "Ballena azul". *Proceso.* Recuperado de: http://www.proceso.com.mx/480180/policia-cibernetica-la-cdmx-alerta-reto-suicida-ballena-azul & Proceso. (11 de mayo de 2017). Ubican en Iztapalapa el primer caso del reto suicida de la "Ballena azul". *Proceso.* Recuperado de: http://www.proceso.com.mx/486162/ubican-en-iztapalapa-primer-caso-del-reto-suicida-la-ballena-azul Fecha de consulta: 23/08/2017.

[226] En diciembre del 2017, el Senado de la República aprobó la propuesta de un senador panista, para tipificar dentro del Código Penal Federal el delito de hostigamiento sexual en internet (porno-venganza), con una pena de 6 meses a 3 años y de 800 a dos mil días de multa a quien divulgue, sin consentimiento o autorización, alguna fotografía, imagen, audio o video de contenido sexual de una persona, con la que haya mantenido una relación de confianza, afectiva o sentimental, afectando su intimidad. La pena incrementará hasta la mitad si la víctima es menor a 18 años. Senadores del PAN LXIII Legislatura. (15 de diciembre de 2017). Aprueba Senado propuesta del senador Victor Hermosillo para sancionar la "porno-venganza". *Senadores del PAN LXIII Legislatura.* Recuperado de: http://www.pan.senado.gob.mx/2017/12/aprueba-senado-propuesta-del-senador-victor-hermosillo-para-sancionar-la-porno-venganza/ Fecha de consulta: 27/12/2017.

[227] El *Sexting* consiste en el envío de contenidos de tipo sexual (principalmente fotografías y/o vídeos) producidos generalmente por el propio remitente, a otras personas por medio de teléfonos móviles.

castigan estás acciones después de haberlas cometido y no antes de hacerlas, como se ve en el Artículo 200, 201 y 202 del Código Penal Federal; en el caso del nivel estatal, el Congreso de Jalisco aprobó en septiembre del 2017 la tipificación del sexting, grooming y retos suicidas dentro de su Código Penal[228], el cual se castigarán considerando lo siguiente:

- Relacionado al sexting: Se sancionará de 4 a 8 años de prisión cuando se transmitan imágenes íntimas de una persona por medios electrónicos, en caso que se trate de un menor de edad, el delito se equiparía a Pornografía Infantil y se castigará de 7 a 12 años de prisión y una multa desde 60 mil 392 pesos hasta 150 mil 980 pesos.
- Relacionado al grooming: Seis años de prisión si el corruptor incita al menor a practicar actividad sexual, a enviar imágenes o sonidos de índole sexual o aceptar encuentros íntimos, así como una multa de 18 mil 872 pesos. Si la víctima es menor de 12 años, se incrementa a 15 años de cárcel y una multa de 51 mil 899 pesos.
- Relacionado a retos suicidas: Quien difunda retos suicidas entre menores de 12 años será de 16 días hasta 50 años de cárcel. En caso que la persona quien difunda sea menor de edad el Estado no tendría competencia en eso, pues se vería en la Ley Nacional del Sistema Integral de Justicia para Adolescentes.

Es un gran avance para el estado de Jalisco, al agregar estos delitos a su Código Penal, algo que a nivel federal se empieza a desarrollar dicha visión, al intentar tipificar los delitos cibernéticos en el Código Penal Federal, esto a propuesta de un diputado llamado, Roberto Cañedo Jiménez, el cual reconoce que hay una deficiencia en defensa jurídica en estos temas e intenta tipificarlos como delitos específicos y autónomos dentro del Código Penal Federal.[229] En el caso relacionado

[228] Gloria Reza M. (07 de septiembre de 2017). Penalizan en Jalisco el sexting, grooming y los retos suicidas. *Proceso.* Recuperado de: http://www.proceso.com.mx/502292/penalizan-en-jalisco-sexting-grooming-los-retos-suicidas Fecha de consulta: 23/08/2017.

[229] Notimex. (12 de diciembre de 2017). Tipificar delitos informáticos en Código Penal Federal, plantea diputado. *20 MINUTOS*. Recuperado de: http://www.20minutos.com.mx/noticia/296447/0/tipificar-delitos-informaticos-en-codigo-penal-federal-plantea-diputado/ Fecha de consulta: 06/12/2017.

a la Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática se tiene:[230]

> **Artículo 210.-** Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.
>
> **Artículo 211.-** La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial.
>
> **Artículo 211 Bis.-** A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.
>
> **Artículo 211 Bis 1.-** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.
>
> **Artículo 211 Bis 2.-** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.
>
> **Artículo 211 Bis 3.-** Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa. Al que estando

[230] Se puede consultar en el: Titulo Noveno: Revelación de secretos y acceso ilícito a sistemas y equipos de informática: Capítulo I: Revelación de secretos (Artículo 210, 211 y 211 Bis) y Capítulo II: Acceso ilícito a sistemas y equipos de informática (Artículo 211 Bis 1, Artículo 211 Bis 2 y Artículo 211 Bis 3).

> autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa. A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Si bien, esta es el área que más avanzada se considera, tiene una vulnerabilidad como todas: el descubrir quién comete el delito y en el caso que fuera hecho en otro país, cómo perseguir estos delitos fuera de las fronteras territoriales (es por la necesidad de crear un tratado internacional relacionado a dichos delitos cibernéticos).

En el caso del Sistema Financiero de México, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) alertó a los usuarios sobre casos de phishing dentro de las instituciones bancarias como: *The Hong Kong and Shanghai Banking Corporation* (HSBC), Banamex, Banco Bilbao Vizcaya Argentaria (BBVA) Bancomer, entre otras, donde a la víctima se le manda un correo relacionado a su cuenta bancaría y le pide que ingrese a un sitio web para pedirle sus datos personales.[231]

> **Artículo 211 Bis 4.-** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.
>
> **Artículo 211 Bis 5.-** Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero,

[231] El Economista. (20 de julio de 2017). Condusef alerta de nuevo caso de phishing de HSBC. *El Economista.* Recuperado de: http://eleconomista.com.mx/finanzas-personales/2017/07/20/condusef-alerta-nuevo-caso-phishing-hsbc Fecha de consulta: 07/09/2017

> indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Uno de los problemas del Código Penal es que no especifica al phishing como delito castigable, y es uno de los delitos cibernéticos más usados para el robo de información bancaria; aunque el phishing también puede ser usada para otros fines como: la utilización de claves electrónicas de identificaciones bancarias para acceder a cuentas, apertura de cuentas bancarias y obtención de crédito, contratación de líneas de teléfono celular u obtención de documentos oficiales (credenciales de votar, acta de nacimientos, pasaportes, licencia de conducir, entre otras).[232]

Para el sector financiero nacional, la ciberseguridad es muy importante, dado que un ataque cibernético que paralizara al sector financiero, traería graves daños a la economía de México, por eso en el año 2017 se firmó una Declaración de Principios para el Fortalecimiento de la Ciberseguridad para la Estabilidad del Sistema Financiero Mexicano,[233] el cual abarca a todas las instituciones financieras privadas del país[234] (una vez más el sector privado es el que más adelantado se

[232] El robo de datos personales, mediante el phishing, no siempre se usa para cuestiones económicas, ya que también se relaciona con tráfico y robo de personas, delincuencia organizada e intervención indebida en los procesos electorales. Newsweek. (2017, Marzo, 10). Conciencia y compromiso: el destino de la seguridad. *Newsweek.* (Edición Especial).págs. 42-45.

[233] Edgar Juárez & Fernando Gutiérrez. (24 de octubre de 2017). Crean frente nacional sobre Ciberseguridad. *El Economista.* Recuperado de: https://www.eleconomista.com.mx/sectorfinanciero/Crean-frente-nacional-sobre-ciberseguridad-20171024-0002.html Fecha de consulta: 05/12/2017.

[234] Este acuerdo fue firmado por la : Asociación de Bancos de México, de Intermediarios Bursátiles, de Sociedades Financieras Populares, Consejo Mexicano de Uniones de Crédito, Confederación de Cooperativas de Ahorro y Préstamos, la Asociación Fintech de México, Secretaría de Hacienda y Crédito Público y la Comisión Nacional Bancaria y de Valores.

encuentra sobre temas de ciberseguridad). En dicho documento se tiene como principios el:[235]

- Adoptar y mantener actualizadas las políticas, métodos y controles para identificar, evaluar y mitigar los riesgos de ciberseguridad que se autoricen por los órganos de gobierno de mayor decisión y permeen a todos los niveles de la organización.
- Establecer mecanismos seguros para el intercambio de información entre las entidades del sistema financiero y las autoridades, (…) protegiendo la confidencialidad de la información.
- Impulsar iniciativas para actualizar los marcos regulatorios y legales que den soporte, y hagan converger las acciones y esfuerzos de las partes, considerando las mejores prácticas y acuerdos internacionales.
- Colaborar en proyectos para fortalecer los controles de seguridad de los distintos componentes de las infraestructuras y plataformas operativas que soportan los servicios financieros del país, promoviendo el aprovechamiento de las tecnologías de información para prevenir, identificar, reaccionar, comunicar, tipificar y hacer un frente común ante las amenazas presentes y futuras.
- Fomentar la educación y cultura de ciberseguridad entre los usuarios finales, y el personal de las propias instituciones que, a través de una capacitación continua, redunde en una participación activa para mitigar los riesgos actuales de ciberataques.

Con este pasó se reconoce al sector financiero como un actor vulnerable y quien debe de darle prioridad a la ciberseguridad. De los artículos antes mencionados, se puede resaltar que existen leyes que castiguen la intromisión, sabotaje y robo de secretos industriales, de redes informáticas del Estado y del Sistema Financiero, considerando esto dentro de la competencia policial y en casos

[235] Comisión Nacional Bancaria y de Valores. (23 de octubre de 2017). Foro de Ciberseguridad. *CNBV*. Recuperado de: https://www.gob.mx/cnbv/articulos/foro-de-ciberseguridad Fecha de consulta: 05/12/2017.

extremos, en la competencia militar, siempre y cuando sea una amenaza a la Seguridad Nacional. Si bien hay una inexistencia de conceptos de delitos cibernéticos actuales, algunos de ellos pueden relacionarse con otros delitos para poder castigarlos.

Aquí lo más recomendable sería crear un Código Penal Cibernético a nivel federal y que contenga todo lo relacionado a delitos de dicha índole y conglomere artículos que aparezcan en diversas leyes (juntando todos en una sola ley). Dicho Código deberá de tener una constante actualización de términos, para poder contar con una mejor base jurídica para castigar los delitos que cada vez van en aumento.

3.3 LA IMPORTANCIA DE LA CIBERSEGURIDAD PARA LA SEGURIDAD NACIONAL

El completo progreso de la ciberseguridad en México ayudará a mantener la integridad, estabilidad y permanencia del país, tal como lo dice el Artículo 3 de la Ley de Seguridad Nacional, y esto se ve con otros países, los cuales ya han integrado el concepto de ciberseguridad en sus marcos jurídicos de Seguridad Nacional, como el caso de España, en donde también crea a su cibercomando.

Hay que recordar que el Estado se compone de cuatro factores: territorio, población, soberanía y gobierno, sin uno de estos cuatro, el Estado no podría existir; la Seguridad Nacional cuida de estos aspectos para el completo funcionamiento del aparato estatal, incluso dentro de la definición de Política Exterior se encuentra el concepto de Seguridad Nacional.

Para México las características y amenazas de la Seguridad Nacional se encuentran en su Ley de Seguridad Nacional publicada en el Diario Oficial de la Federación el 31 de enero de 2005:[236]

[236] Ley de Seguridad Nacional. [Archivo PDF]. Recuperado de: http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac.pdf Fecha de consulta: 17/07/2017.

Artículo 3.- Para efectos de esta Ley, por Seguridad Nacional se entienden las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, que conlleven a:

I. La protección de la nación mexicana frente a las amenazas y riesgos que enfrente nuestro país;

II. La preservación de la soberanía e independencia nacionales y la defensa del territorio;

III. El mantenimiento del orden constitucional y el fortalecimiento de las instituciones democráticas de gobierno;

IV. El mantenimiento de la unidad de las partes integrantes de la Federación señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos;

V. La defensa legítima del Estado Mexicano respecto de otros Estados o sujetos de derecho internacional, y

VI. La preservación de la democracia, fundada en el desarrollo económico social y político del país y sus habitantes

Artículo 5.- Para los efectos de la presente Ley, son amenazas a la Seguridad Nacional:

I. Actos tendentes a consumar espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional;

II. Actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado Mexicano;

III. Actos que impidan a las autoridades actuar contra la delincuencia organizada;

IV. Actos tendentes a quebrantar la unidad de las partes integrantes de la Federación, señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos;

V. Actos tendentes a obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada;

VI. Actos en contra de la seguridad de la aviación;

VII. Actos que atenten en contra del personal diplomático;

VIII. Todo acto tendente a consumar el tráfico ilegal de materiales nucleares, de armas químicas, biológicas y convencionales de destrucción masiva;

IX. Actos ilícitos en contra de la navegación marítima;

X. Todo acto de financiamiento de acciones y organizaciones terroristas;

XI. Actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia, y

XII. Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.

En ambos artículos se entiende las áreas de competencia que tiene la Seguridad Nacional en México; a pesar que la ciberseguridad también comparte los mismos objetivos y se considera a la ciberseguridad como un área a desarrollar dentro de la Seguridad Nacional de México, esta no se encuentra plasmada en la ley, ni se reconoce al ciberespacio como una amenaza para el país dentro del Artículo 5.

En caso de un ataque cibernético hacia las instalaciones energéticas como Pemex o la Comisión Federal de Electricidad (CFE) o un ataque hacia el sistema financiero, páginas institucionales, red de telecomunicaciones, instituciones militares, el daño sería imaginable, considerando ya estar en estado de guerra, pues en la actualidad un ataque de esa magnitud solo se podría llevar a cabo por una Estado.

En México existen instalaciones estratégicas que brindan un completo desarrollo y funcionamiento del país, y se encuentran definidas dentro de la Ley General del Sistema Nacional de Seguridad Pública[237]:

> "Artículo 146: Para efectos de esta Ley, se consideran instalaciones estratégicas, a los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, así como de aquellas que tiendan a mantener la integridad, estabilidad y permanencia del Estado Mexicano, en términos de la Ley de Seguridad Nacional."

Es por eso que en el sexenio de Calderón como ya se había mencionado, se creó el Manual Administrativo de Aplicación General en materias de TIC y de Seguridad de la Información (MAAGTICSI), el cual se ha ido reformando con el objetivo de definir los procesos y regular las operaciones de las Tecnologías de la Información y la Comunicación (TIC) y de la seguridad de la información dentro de las instituciones gubernamentales y empresas paraestatales. Este manual va ligado

[237] Diario Oficial de la Federación. (02 de enero de 2009). Ley General del Sistema Nacional de Seguridad Pública. *SEGOB.* Recuperado de: http://www.dof.gob.mx/nota_detalle.php?codigo=5076728&fecha=02/01/2009 Fecha de consulta: 18/07/2017.

con las instancias y leyes referidas a la Seguridad Nacional, es por eso que en el Artículo 2, del presente manual define a las Infraestructuras Críticas de Información como:

> “Las infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la Ley de la materia”

Esta definición se relaciona con la anterior, que tiene que ver con las Instalaciones Estratégicas, de hecho a las Infraestructuras Críticas de Información se les asigna un nivel de importancia o prioridad, este nivel se clasifica en “A”, “AA” O “AAA” tal como está en el Artículo 28 del MAAGTICSI:

> a) "AAA": se asignará este nivel cuando se trate de información requerida para el proceso de decisiones políticas fundamentales, esto es, para la adopción de decisiones sobre riesgos y amenazas a la seguridad nacional, por parte del Presidente de la República, previa consideración del Consejo de Seguridad Nacional, cuya revelación no autorizada pueda dañar la integridad, estabilidad o permanencia del Estado mexicano;
>
> b) “AA”: este nivel se asignará a la información resultante del ejercicio de atribuciones sustantivas, cuya revelación no autorizada pueda actualizar o potenciar un riesgo o amenaza a la seguridad nacional en términos de la Ley de la materia, o bien, comprometer su operación, las condiciones de seguridad de las instalaciones estratégicas o la integridad física de su personal, y
>
> c) "A": se asignará este nivel a aquella información que derive del cumplimiento de las disposiciones jurídicas en materia de ejercicio del gasto, transparencia y rendición de cuentas, cuya revelación no autorizada pueda comprometer su operación, las condiciones de seguridad de las instalaciones estratégicas o la integridad física de su personal.

Existe un reconocimiento y clasificación de Instalaciones Estratégicas y de las Infraestructuras Críticas de Información por parte de México, ambas relacionadas con la Ley de Seguridad Nacional, pero la ciberseguridad sigue sin ser reconocida en dicha ley, sabiendo que ya es un pilar fundamental en la Seguridad Nacional de los países a nivel internacional, donde existe un mundo cada vez más interconectado, y por ende amenazas compartidas. En el caso nacional se mencionará algunos ejemplos de ataques cibernéticos que han afectado al país,

esto para concientizar de la importancia de la gestación de la ciberseguridad en México:

- **Saguaro, el virus especialmente para México:** La empresa de seguridad informática Kaspersky Lab afirmó en la Cumbre Internacional de Analistas de Ciberseguridad 2016 de la existencia de un virus troyano llamado Saguaro (nombre de un cactus típico del Desierto de Sonora), el cual se tiene registros desde el 2009 con un total de más de 120,000 personas afectadas; este virus opera principalmente en América Latina y el país más afectado es México (los hallazgos de sus investigaciones concluyen que los atacantes hablan español y tienen raíces en México), el cual ha afectado también a otros países como es el caso de Colombia, Brasil, Estados Unidos, Venezuela, República Dominicana, entre otros; afirma Dimitry Bestuzhev, Director para América Latina del Equipo Global de Investigación y Análisis para Kaspersky Lab.[238]
- **Falta de especialistas en México para cubrir la demanda de empleos en Ciberseguridad:** Para el 2019 faltará 1.5 millones de personas para cubrir la demanda de puestos de ciberseguridad en el mundo, tan solo en México 40% de las empresas fueron atacadas cibernéticamente (2015). Esto se debe que en el país no existe talento humano ni calificado para hacer frente a los ataques cibernéticos, sumando que las empresas no invierten en tecnología, capacitaciones y certificados para su personal. Esto ocasionará una pérdida de clientes para la empresa y una cada vez, más incrementada falta de expertos en ciberseguridad dentro de México.[239]

[238] Este virus solo opera en máquinas que tengan el sistema operativo de Windows, y el modo de contagio es a través de correos electrónicos, donde se engaña a la víctima haciéndose pasar por una institución financiera o institución de gobierno, para abrir el documento que adjuntan y así infectar al usuario; al momento de la infección, el troyano recolecta toda la información personal entre ellos los correos electrónicos de contactos para seguir su expansión. Kaspersky. (31 de agosto de 2017). Oculto a simple vista: el grupo "Saguaro" ataca América Latina utilizando técnicas sencillas, pero eficaces. *Kaspersky.* Recuperado de: https://latam.kaspersky.com/blog/oculto-a-simple-vista-el-grupo-saguaro-ataca-america-latina-utilizando-tecnicas-sencillas-pero-eficaces/7589/ Fecha de consulta: 07/09/2017.

[239] Gabriela Chávez. (16 de agosto de 2016). A México le faltan expertos para cubrir la demanda de empleos en ciberseguridad. *Expansión.* Recuperado de: http://expansion.mx/tecnologia/2016/08/16/a-mexico-le-faltan-expertos-para-cubrir-la-demanda-de-empleos-en-ciberseguridad Fecha de consulta: 30/09/2017.

- **Página oficial de gobierno mexicano es blanco de ataques cibernéticos:** La estrategia del actual sexenio consistió en unificar las páginas web de diversas instituciones de gobierno en una: www.gob.mx, el cual facilitaría la búsqueda de información, trámites, noticias, etc., pero también ocasionaría que los cibercriminales se concentrarán en un solo objetivo, tan solo la Policía Cibernética de la División Científica de la Policía Federal, detecto 170 mil ataques cibernéticos dentro del periodo 2012-2016.[240]
- **La débil ciberseguridad de México pone en riesgo a los Estados Unidos:** El director de producto de protección de infraestructura crítica de Kaspersky, Matvey Voytov, mencionó que el incremento de las conexiones de máquina y complejos industriales de red aumentarían los ataques cibernéticos a las infraestructuras vitales nacionales, poniendo en riesgo a la Seguridad Nacional. También menciona que por la cercanía de México con Estados Unidos dejaría al país en una situación estratégica y atractiva para que los cibercriminales lo utilicen como puente para hacer ataques cibernéticos en Estados Unidos, esto se debe porque en México los empleados no tienen los conocimiento en materia de ciberdefensa y hay una ineficiencia de leyes y falta de protocolos. Voytov recomienda una homologación de estándares de ciberseguridad entre ambos países. [241]
- **México como el quinto país con más ataques en el mundo y el segundo en América Latina con más ataques en celulares:** La empresa FORTINET considera a México entre los 5 países del mundo que más ataques cibernéticos recibe, llama a las empresas a considerar a la ciberseguridad una prioridad debido al alto costo de dichos ataques. [242] Mientras Kaspersky considera a México como el segundo país con más usuarios afectados por

[240] Tania Campos. (07 de septiembre de 2017). La página gob.mx es blanco frecuente de ataques cibernéticos. *XATAKA México.* Recuperado de: https://www.xataka.com.mx/otros-1/la-pagina-gob-mx-es-blanco-frecuente-de-ataques-ciberneticos Fecha de consulta: 30/09/2017.

[241] Gabriela Chávez. (13 de mayo de 2016). La débil ciberseguridad en México pone en riesgo a Estados Unidos. *Expansión.* Recuperado de: http://expansion.mx/tecnologia/2016/05/13/la-debil-ciberseguridad-en-mexico-pone-en-riesgo-a-estados-unidos Fecha de consulta: 30/09/2017.

[242] Publicado durante la Séptima Cumbre Latinoamericana de Analistas de Seguridad, realizada en Argentina. El primer lugar lo ocupa Brasil con el 31%, en segundo México con el 29% y en tercero Colombia con el 7%.

ataques a teléfonos. El analista de seguridad de Kaspersky, Thiago Marques menciona que el número de ataques a teléfonos crece cada año debido al comercio en línea y la fácil propagación. [243]

- **Infraestructuras críticas de México ya están bajo ataques cibernéticos:** El consultor Mikel Santos de PA Consulting en la entrevista realizada para *El Economista*, menciona que a nivel mundial ya existen ataques cibernéticos a las infraestructuras nacionales de energía, como el caso divulgado en 2014 por parte de *Bloomberg*, donde una investigación hecha por la empresa de ciberseguridad Cylance, PEMEX fue uno de los blancos de una campaña de ciberataques ligadas a Irán. Si bien, en México no se ha llegado a tal grado de daños, se menciona que existen ataques pero de bajo perfil, estos ataques no han ocasionado daños significativos gracias a la falta de conectividad a la Red de Sistemas Industriales (SCADA)[244], por parte de Petróleos Mexicanos (PEMEX), Comisión Federal de Electricidad (CFE) o la Comisión Nacional del Agua (CONAGUA), exentándolas de ataques cibernéticos de mayor magnitud. PA Consulting menciona que PEMEX en el 2012 gastó en ciberseguridad 175 millones de dólares, esta cifra comparada con otras empresas grandes de petróleo como Exxon Mobil, representa una octava parte. Al final el experto recomienda la creación de mecanismos y colaboración en tiempo real sobre las infraestructuras críticas, mencionando que en la Estrategia Nacional de Ciberseguridad, el sector privado propuso la creación de una agencia a cargo de la Secretaría de Gobernación (SEGOB) para cumplir funciones relacionadas a la protección de Infraestructuras Críticas como en otros países.[245]

[243] Life and Style. (08 de septiembre de 2017). México es el quinto país con más ciberataques en el mundo. *Life and Style.* Recuperado de: https://lifeandstyle.mx/tech/2017/09/08/mexico-es-el-quinto-pais-con-mas-ciberataques-del-mundo Fecha de consulta: 30/09/2017.

[244] Supervisión, Control y Adquisición de Datos (Supervisory Control And Data Acquisition), es un tipo de software que controla y supervisa todos los procesos industriales a distancia.

[245] Julio Sánchez Onofre. (28 de septiembre de 2017). Las infraestructuras críticas de México ya están bajo ciberataques. *El Economista.* Recuperado de: http://eleconomista.com.mx/tecnociencia/2017/09/28/las-infraestructuras-criticas-mexico-ya-estan-bajo-ciberataques Fecha de consulta: 01/10/2017.

Como se ve, la importancia de México a fortalecerse en materia de ciberseguridad y el completo funcionamiento de la Estrategia Nacional de Ciberseguridad es fundamental, para hacer frente a las amenazas, como es el caso de los ejemplos anteriormente señalados. Aquí no se mencionó ataques cibernéticos por parte de otros Estados, dado que en México son casi inexistentes, o se tiene muy poca información sobre ello, pero esta opción no se descarta.

3.4 LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

Como ya se ha mencionado, el 13 de noviembre del 2017 salió el documento que contiene la Estrategia Nacional de Ciberseguridad de México, dicha Estrategia contó con la ayuda técnica y recomendaciones de la Organización de Estados Americanos (OEA) a través del Programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo (CICTE)[246], el apoyo financiero del gobierno de Canadá, las recomendaciones hechas por expertos en los talleres impartidos y la participación de diversos actores: académicos, sociedad civil, sector privado y comunidad técnica; está Estrategia es un plan impulsado por el actual sexenio de Enrique Peña Nieto, ante incremento de delitos cibernéticos y cuestiones relacionadas a la Seguridad Nacional.[247]

En México existen dos definiciones para ciberseguridad, la primera es hecha por la Secretaría de Marina (SEMAR) en su Programa Sectorial de Marina 2013-2018, el cual define al concepto mucho antes de la Estrategia Nacional de Ciberseguridad:

[246] México es uno de los países como Paraguay, Chile y Costa Rica que han elaborado sus Estrategias Nacionales de Ciberseguridad en el 2017. Secretaría de Relaciones Exteriores. (2017). México Presentó Estrategia Nacional de Ciberseguridad desarrollada con el apoyo de la OEA. *SER.* Recuperado de: https://mision.sre.gob.mx/oea/index.php/actividades/25-avisos-2017/420-mexico-mexico-presento-estrategia-nacional-de-ciberseguridad Fecha de consulta: 07/12/2017.

[247] El primer taller se llevó acabo el día 19 y 29 de abril 2017, y el segundo el 12 y 13 de julio del mismo año, también contó con encuestas hechas desde la página oficial del gobierno para recopilar comentarios de expertos, académicos y población en general.

> "Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno"

Antes de la Estrategia Nacional de Ciberseguridad, la Secretaría de Marina era la única instituciones que intentó darle una definición a la ciberseguridad, ahora con la nueva Estrategia, se homologa la definición a nivel nacional, principalmente para las instituciones de gobierno, la cual en dicho documento se define como:

> "Conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicación"[248]

Dicha Estrategia Nacional de Ciberseguridad tiene como objetivo principal el fortalecimiento del país en materia de ciberseguridad ante los riesgos y amenazas que se encuentran en el ciberespacio y afectan al sector económico, social y político; la Estrategia consideró tres principios rectores para su desarrollo que fueron: perspectiva de derechos humanos, enfoque basado en gestión de riesgos y colaboración multidisciplinaria y de múltiples actores; y como visión se prevé el completo avance cibernético de México para el 2030, algo que no se está visualizando que para el 2030 los ataques cibernéticos y el desarrollo de ciberarmas por parte de Estados ya habrá avanzado notoriamente.[249]

[248] Cabe resaltar que para las Fuerzas Armadas el concepto de "ciberseguridad" es una competencia para el sector policial, mientras el concepto de "ciberdefensa" es de uso militar y relacionado a la Seguridad Nacional. Aún existe una problemática para definir diversos conceptos, como los dos anterior mencionado, pero conforme México vaya desarrollando su ciberseguridad, los conceptos se irán aclarando. Secretaría de Marina & Centro de Estudios Superiores Navales. Op. Cit., (pág. 288).

[249] Documentos. (13 de noviembre de 2017). Estrategia Nacional de Ciberseguridad. *Gob.mx.* [Archivo PDF]. Recuperado de: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf Fecha de consulta: 07/12/2017.

La Estrategia plantea cinco objetivos estratégicos, el cual requiere 8 ejes transversales para su fructífero desarrollo, todos estos se encuentran interrelacionados. Los cinco objetivos estratégicos van encaminados a la:

- Sociedad y Derechos: Generar las condiciones para que la población realice sus actividades de manera responsable, libre y confiable en el ciberespacio dentro de un marco de respeto de derechos humanos como la libertad de expresión, vida privada, protección de datos personas, entre otros.

- Economía e Innovación: Fortalecimiento de la ciberseguridad para proteger la economía de los diversos sectores productivos del país para el fructífero desarrollo e innovación tecnológica y el impulso de la industria de ciberseguridad dentro del país.

- Instituciones Públicas: Proteger la información y sistemas informáticos de las instituciones de gobierno al nivel nacional para el óptimo desarrollo de éstas.

- Seguridad Pública: Incrementar las capacidades de prevención e investigación de conductas delictivas en el ciberespacio que afecten a las personas y su patrimonio, con la finalidad de mantener el orden y la paz pública.

- 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. (la más importante a desarrollar).

Estos cinco objetivos estratégicos, comparten los mismos ocho ejes transversales para su completo desarrollo, y estos son:

1.- Cultura de ciberseguridad: Aquí se desarrollará e implementará estrategias para campañas de concientización, educación y formación para la: sociedad, sector académico, sector privado e instituciones públicas, para incidir cómo interactuar dentro del ciberespacio.

2.- Desarrollo de capacidades: Se busca fortalecimiento y generación de las capacidades organizacionales, dividiendo lo que le compete al sector público y

privado; fomentar el capital humano, con el desarrollo de especialistas, investigadores y profesionales de ciberseguridad; y recursos tecnológicos, mediante la generación de infraestructura tecnológica; así para incrementar la resiliencia nacional.

3.-Coordinación y colaboración: Creación de acciones orientadas a coordinar y establecer canales de cooperación a nivel internacional y nacional con las instituciones públicas, académicas, sociedad civil y organizaciones privadas para consolidar el ecosistema de ciberseguridad en México.

4.- Investigación, desarrollo e innovación en TIC: Se busca establecer los mecanismos de políticas, programas y acciones para la fomentación de la investigación; desarrollo e innovación para el favorecimiento del capital humano; e innovación tecnológica, a fin de impulsar el mercado nacional de ciberseguridad.

5.- Estándares y criterios técnicos: Conjunto de acciones enfocadas al desarrollo, adopción y fortalecimiento de los estándares, criterios técnicos y de la normalización en materia de ciberseguridad para la homologación y aplicación de las mejores prácticas y procesos en el uso, y adopción de las TIC.

6.- Infraestructura crítica: Conjunto de acciones y mecanismos dentro del marco de la Ley de Seguridad Nacional, necesarios para minimizar la probabilidad de riesgos y vulnerabilidades del uso de las TIC para la gestión de infraestructuras críticas; así como, la capacidad del fortalecimiento para mantener la estabilidad y continuidad de los servicios en caso de un ataque cibernético.

7.- Marco jurídico y autorregulación: Establecer acciones y mecanismos para un adecuado marco jurídico que brinde certeza a los usuarios dentro del ciberespacio; así como, homologar y armonizar los códigos penales y leyes complementarias en relación a ciberdelitos, y brindar herramientas jurídicas con las que cuenten las instancias de procuración de justicia para la persecución de dichos delitos.

8.- Medición y seguimiento: Conjunto de acciones y procedimientos que fomenten los mecanismos homologados de medición al desarrollo e implementación

de la Estrategia Nacional de Ciberseguridad, y su impacto en el desarrollo social y económico en el país, para identificar las áreas de oportunidad para su constante mejora.

Si bien la Estrategia menciona sus objetivos a nivel general, aún falta mucho para adecuarse y consolidar las políticas cibernéticas en México. En dicho documento menciona la creación de una Subcomisión de Ciberseguridad,[250] el cual estará subordinada a la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE),[251] que a su vez es competencia de la Secretaria de la Función Pública. Esta Subcomisión tendrá la tarea de: Aprobar y dar a conocer la Estrategia; dar seguimiento y coordinar la implementación de la Estrategia Nacional de Ciberseguridad en colaboración con las diferentes dependencias y entidades de la Administración Pública Federal; impulsar los esquemas de colaboración y cooperación interinstitucional en materia de ciberseguridad; y por último, fomentar la colaboración y cooperación con los diferentes actores involucrados: sociedad civil, sector privado, comunidades técnicas y académicas.

Por otro lado, dentro de la renegociación del Tratado de Libre Comercio de América del Norte (TLCAN), se busca crear un marco de cooperación y colaboración

[250] La Subcomisión está conformada por: La División Científica de la Policía Federal quien la preside; Jefe de la Unidad de Innovación y Estrategia Tecnológica de la Oficina de la Presidencia de la República; Unidad de Gobierno Digital de la Secretaría de la Función Pública; Titulares de las Unidades de Tecnologías de la Información y Comunicaciones de la Secretaria de Gobernación, de Economía, de Educación Pública, de Hacienda y Crédito Público; así como, el titular de la Unidad de Tecnologías de la Información y Comunicaciones de la Procuraduría General de la República. **Mientras las instancias como invitados permanentes son:** Secretaría de Marina, Secretaría de la Defensa Nacional, Servicio Administración Tributaria, Comisión Nacional Bancaria y de Valores, Procuraduría General del Consumidor, Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, Instituto Politécnico Nacional, Consejo Nacional de Ciencia y Tecnología, Centro Nacional de Control de Energía, Secretaría de Relaciones Exteriores, Secretaría de Salud, Secretaría Técnica del Consejo Nacional de Seguridad, Secretaría de Economía-Sistema Nacional de Protección Integral de Niñas, Niños y Adolescentes (SE-SIPINNA) y el Secretariado Técnico-Consejo Nacional de Salud (STCNS-OPR). Cabe señalar que en esta Subcomisión las Fuerzas Armadas quedan excluidas, y los ponen como invitados permanentes, a pesar que se abordan temas relacionados a la Seguridad Nacional.

[251] Es un órgano colegiado que se estableció mediante el Acuerdo Presidencial que tiene por objetivo crear de forma permanente la CIDGE, publicada en el Diario Oficial de la Federación el 9 de diciembre del 2005 y queda excluido del presente Acuerdo, las materias concernientes a la Seguridad Nacional. Diario Oficial de la Federación (09 de diciembre de 2005). Acuerdo que tiene como objeto crear en forma permanente la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico. *SEGOB.* Recuperado de: http://www.dof.gob.mx/nota_detalle.php?codigo=2101617&fecha=09/12/2005 Fecha de consulta: 07/12/2017.

entre los tres países (México-Canadá-Estados Unidos) en cuestiones de ciberseguridad, esto con la ayuda de la CANIETI,[252] este acuerdo impulsaría la cooperación y coordinación de la ciberseguridad con países que cuentan ya con experiencia en el tema.

Para finalizar, existe una problemática de definir concretamente la dependencia que se encargará de dicha Estrategia junto con sus bases jurídicas claras, el cual le permita tener un mayor rango de acción y aplicación. Si bien, la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI), había propuesto la creación de una Agencia Nacional de Ciberseguridad (como lo había recomendado la OEA), a cargo de la Secretaría de Gobernación, [253] el problema aquí es que dicha Secretaría centralizaría más las competencias de seguridad y esto abriría paso a que la agencia de usará para intereses políticos y no de seguridad, por lo tanto es importante que la agencia sea autónoma de cualquier secretaría de Estado; por otro lado no se concuerda completamente con la propuesta de la CANIETI, pues el desarrollo de la ciberseguridad no debería de estar a cargo de una solo agencia (aquí se vuelve al mismo problema que tiene México al centralizar todo), sino que se debe de diversificar en todos los sectores, tanto académicos, militares, institucionales, policiales, y empresariales, como es el caso de Estados Unidos que dichos sectores están desarrollados óptimamente.

El camino es largo para México, su digitalización ha ocasionado la rápida aceleración de leyes e instituciones que protejan a la población y a la integridad del Estado de amenazas provenientes del ciberespacio, como se hace en diversos países que entendieron que en el ciberespacio existe una variedad amplia de amenazas, obligándolos a desarrollar su ciberseguridad oportunamente.

---

[252] Claudia Juárez Escalona. (06 de septiembre de 2017). Canieti busca que la ciberseguridad sea discuta en el TLCAN. *El Economista.* Recuperado de: http://eleconomista.com.mx/industrias/2017/09/06/canieti-busca-que-ciberseguridad-sea-discuta-tlcan Fecha de consulta: 03/10/2017.

[253] Carla Martínez. (07 de septiembre de 2017). Piden a Segob coordinar ciberseguridad. *El Universal.* Recuperado de: http://www.eluniversal.com.mx/cartera/economia/piden-segob-coordinar-ciberseguridad Fecha de consulta: 03/10/2017.

CONCLUSIONES

La hipótesis se corrobora, al concluir que México aún le falta por desarrollarse en materia de ciberseguridad para hacer frente a las amenazas y desafíos que han surgido en este Siglo XXI. El país se encuentra en una etapa tardía en la implementación de la ciberseguridad a nivel nacional, donde apenas se logró crear una Estrategia Nacional de Ciberseguridad, que definirá y enmarcará las líneas de acción a seguir para crear un marco jurídico adecuado, un fortalecimiento institucional, y unas Fuerzas Armadas como cuerpos policiales que empiezan a inmiscuirse dentro de la ciberseguridad, para estar a la altura de estos nuevos retos; a pesar que existe deficiencias dentro de dicha Estrategia; como también diversos problemas internos, tales como: la falta de información y el ocultamiento de ataques cibernéticos por parte del gobierno, la deficiencia en el estudio académico de la ciberseguridad, el desinterés y la falta de cultura de la población de los riesgos y amenazas que hay en el ciberespacio, entre otros. A pesar de todo lo anterior mencionado dicha Estrategia ha sido un gran paso para el país, dado a que demuestra que México empieza a preocuparse y darle interés a la ciberseguridad, reconociendo que el ciberespacio existen potenciales amenazas, que vulneran a la Seguridad Nacional. A continuación se mencionará conclusiones más específicas:

- El crecimiento de usuarios de Internet a nivel internacional está abriendo pauta a un nuevo campo para actos delictivos, amenazas a la Seguridad Nacional de países cada vez más digitalizados y un grado de alcance mayor para ataques cibernéticos, ya que actualmente el 51.8% de la población a nivel mundial es usuaria de Internet.
- México cuenta con más de la mitad de la población conectada al Internet (70 millones de usuarios) y más de la mitad de población que vive en situación de pobreza (55.3 millones de personas), este similitud es gracias al crecimiento de los teléfonos inteligentes dentro del país, dado que es más accesible un celular que una computadora, pues 61 por cada 100 teléfonos contaban con suscripción al Internet.

- Aunque haya en México una población más inmiscuida dentro de Internet, existe un desinterés por parte de los usuarios relacionada a la cultura de seguridad dentro del ciberespacio.
- La digitalización del país se logró en menos de una década, por lo tanto ha rebasado al marco jurídico actual. La importancia de crear leyes acorde a la evolución del Internet ayudará a proteger a usuarios de ciberdelitos; como también a las Infraestructuras Críticas e Instituciones de Seguridad Nacional de ataques cibernéticos. Existe una correlación, entre mayor sea la digitalización de un país, mayor será la cantidad de ataques cibernéticos dentro de él, y por ende mayor daño y alcance pueden tener.
- La Teoría de Complejos de Seguridad Regional, brinda la visión de la importancia del estudio de la Seguridad a nivel regional, dado que la seguridad tradicional quedo rebasada ante el nuevo panorama internacional; esta teoría acepta la existencia de múltiples actores (no solo Estados) como de diversos sectores para el estudio de la seguridad, que en un futuro se podría agregar el sector cibernético. También explica la convivencia de diversos países dentro de una región y cómo algunos influyen en la securitización de un tema, en este caso sería la securitización regional de la ciberseguridad, influenciada por Estados Unidos al que la teoría clasifica como “superpotencia”, dicha securitización es un fenómeno que empieza a desarrollarse en diversas regiones, por la necesidad de salvaguardar la integridad principalmente del Estado, como de otros actores. Gracias a esto, la Organización de Estados Americanos (OEA), ayudó en la elaboración de las políticas cibernéticas de México con la Estrategia Nacional de Ciberseguridad, algo con el que se benefició el país.
- Existe una problemática para definir el concepto de ciberseguridad dado que es un término relativamente nuevo, y esto se enfrenta a que: en primer lugar dicha palabra viene del inglés *cybersecurity* (incluso

existe en el idioma inglés problemas para definirla), por lo tanto no existe su concepto en el diccionario de la Real Academia Española (RAE); en segundo lugar hay una problemática para delimitar sus áreas de competencia, debido a la constante evolución tecnológica; y en tercer lugar, existen diferentes visiones para definir el concepto de ciberseguridad hechas por Estados o sector privado, que agregan y quitan competencias. Por lo tanto la ciberseguridad, es un término en constante evolución y su definición contará con las características del ente que lo defina, ya que aún falta mucho para homologar dicho concepto a nivel global.

- La ciberseguridad puede moldearse para perseguir intereses particulares de diversos Estados, con la finalidad de usarla para espionaje político, intimidación de medios informativos o robo de información, sustentándose principalmente en la Seguridad Nacional. Por lo tanto es importante crear leyes adecuadas y claras que protejan la privacidad de la población, la democracia y la censura dentro del ciberespacio, ante estas acciones que se han visto cada vez más usadas por parte de diversos Estados.
- Existieron tres sucesos que marcaron a la ciberseguridad a nivel internacional: el primer ataque cibernético a Estonia marcó la pauta del desarrollo de la ciberseguridad de diversos países europeos y demostró cómo un ciberataque es capaz de afectar a un país completamente; el segundo fue Stuxnet, demostrando que los países empiezan a desarrollar armas cibernéticas, empezando a alcanzar objetivos particulares como infraestructuras críticas nacionales; y el tercer ataque fue WannaCry, el cual afectó a México y marcó la pauta donde los ataques cibernéticos empiezan a ser globales y con una propagación rápida.
- En el panorama internacional falta la creación de leyes de alcance global para regular el ciberespacio ante amenazas a la Seguridad Nacional y delitos cibernéticos que atraviesan fronteras; la

problemática de crear tratados de dicho ámbito, recae que toca intereses nacionales y cuestiones de soberanía, dado que cada Estado tiene sus propias leyes internas para regular y castigar delitos dentro del ciberespacio. Pero conforme avanza más la tecnología, no quedará de otra que crear tratados internacionales de alcance global que abarquen dichas cuestiones, ya que en la actualidad solo existen tratados que regulan algunas áreas del ciberespacio y son de alcance regional (como el convenio de Budapest de la Unión Europea); mas no global.

- Los Organismos Internacionales o Regionales son los principales desarrolladores de políticas cibernéticas, ayudando así a sus Estados miembro. La OTAN desarrolló su ciberseguridad notoriamente gracias al ataque de Estonia en el 2007, donde considera al ciberespacio como un dominio operacional (aérea, marítima, terrestre, ultraterrestre y ahora el ciberespacio). Por parte de la Unión Europea, se creó el Tratado de Budapest el cual se enfoca en cuestiones delictivas en el ciberespacio, su desarrollo cibernético se debe tanto al terrorismo como también, que la mayoría de sus miembros pertenecen a la OTAN. Mientras que la Organización de Estados Americanos (OEA) con ayuda de Estados Unidos y otros países europeos ha desarrollado sus políticas regionales de ciberseguridad y asesorando a sus Estados miembros para la creación de Estrategias Nacionales de Ciberseguridad en América Latina, como el caso de México. Esto demuestra que la securitización de la ciberseguridad dentro de las regiones empieza a ser una prioridad en las agendas nacionales, con un dinamismo en la colaboración entre el sector privado y Estado en materia de ciberseguridad.
- En México existen 4 CERT´s que se encargan de monitorear los incidentes de ciberseguridad en el país, uno institucional, perteneciente a la Policía Federal; otro académico por parte de la

UNAM y los últimos dos del sector privado, pero cabe resaltar que no existe uno por parte del sector militar.

- La ciberseguridad en México tiene sus primeras menciones en el Segundo Informe de Gobierno del sexenio de Felipe Calderón, el cual sentó las bases de la ciberseguridad en el país, mientras en el actual sexenio de Enrique Peña Nieto, la ciberseguridad se está desarrollando satisfactoriamente. En caso del sexenio de Vicente Fox, no se mencionada nada relacionado dentro de su Plan Nacional de Desarrollo como en sus Informes de Gobierno, demostrando que la ciberseguridad a inicios de presente siglo no era prioritaria para México.
- En el sexenio de Felipe Calderón se crearon las bases del avance cibernético del país, iniciando en el sector policial, mientras en el sexenio de Enrique Peña Nieto a través de los Programas Sectoriales de las Fuerzas Armadas, como en la de Seguridad Pública, reconoce y da prioridad a prepararse ante los desafíos y amenazas del ciberespacio desarrollando políticas y mecanismos para empezar a sustentar el avance de la ciberseguridad a nivel nacional.
- Las Fuerzas Armadas han llevado a cabo un avance notorio dentro de los aspectos de ciberseguridad y ciberdefensa, aunque existe una diferencia de avance cibernético entre las Secretaría de Marina y la Secretaría de Defensa Nacional, han empezado a trabajar conjuntamente. Aquí se podría recomendar la creación de un Cibercomando unificado dentro de las Fuerzas Armadas, que ayudará a especializar al sector militar en cuestiones relacionadas a la ciberseguridad para proteger mejor las infraestructuras críticas nacionales y crear una mejor coordinación entre ambas dependencias, aunque la cuestión sería a qué institución pertenecería o si sería independiente.
- Dentro del sector policial, también se habla de un avance cibernético, en el caso de la Policía Federal es considerada la más desarrollada

en cuestiones de ciberseguridad, la cual busca coadyuvar a las policiales estatales para su rápida actualización. Un problema es que el área cibernética de la Policía Federal, está limitada dentro de la División Científica, algo que no debería estar sucediendo, dado que debería ser independiente y contar con un reconocimiento para que la Policía Cibernética sea una División más de la Policía Federal, contando con un mayor rango de acción y leyes que le permitan actuar.

- Se necesita crear un marco jurídico relacionado a cuestiones de delitos cibernéticos, y se actualice constantemente. El Código Penal Federal y la Ley de Seguridad Nacional han sido rebasadas por la nueva generación de delitos y amenazas cibernéticas actuales; la importancia de contar con una ley acorde al contexto que se vive es de suma importancia para el país. Por lo tal se recomendaría crear un Código Penal Cibernético a nivel federal, que contenga todo lo relacionado a delitos de dicha índole y conglomere artículos que aparezcan en diversas leyes (juntando todos en una sola ley). Dicho Código deberá de tener una constante actualización de términos, para poder contar con una actualizada base jurídica.
- La ciberseguridad es clave para el completo desarrollo de nuestro país, por tal motivo es considerada un área más dentro de las competencias de la Seguridad Nacional, reconociéndose dentro de la Estrategia Nacional de Ciberseguridad y otros documentos oficiales, pero no se menciona ni se encuentra establecida dentro la Ley de Seguridad Nacional, la cual no se ha actualizado desde el 2005.
- La Estrategia Nacional de Ciberseguridad es un gran paso para México de poner a la mesa a la ciberseguridad como una prioridad y señalar las deficiencias que se tiene; dicha Estrategia contó con la ayuda de la Organización de Estados Americanos (OEA), abarcando aspectos económicos, sociales, políticos y de Seguridad Nacional. La importancia de dicho documento radica que será la base de las

políticas cibernéticas y marcará la pauta para preparar al país ante ataques cibernéticos cada vez más sofisticados y que vulneren a la Seguridad Nacional, a pesar que existen algunas carencias y el documento no sea tan específico, es un paso importante para el país; pero en unos meses habrá elecciones presidenciales, el cual se espera que dichas políticas continúen y se mejoren como una política de Estado y no una política de gobierno, pues su tardía implementación sería catastrófico por las amenazas presentes y futuras provenientes del ciberespacio.

- La creación de una Agencia Nacional de Ciberseguridad a cargo de la Secretaría de Gobernación, propuesta por el sector empresarial, no sería la solución adecuada, debido a tres factores: el primer factor, existe una centralización por parte de la Secretaría de Gobernación en materia de seguridad, lo cual limitaría la acción de la dependencia que llevará acabo la supervisión e implementación de la Estrategia Nacional de Ciberseguridad; el segundo factor es el tratar centralizar la función del desarrollo cibernético del país, ya que debería de haber una diversificación de la ciberseguridad en el ámbito académico, institucional, empresarial y militar como es el caso de otros países; y el tercer factor, es que la dependencia que llevará a cabo el seguimiento de dicha Estrategia sea un organismo autónomo separada de las secretarías de Estado, pues solo logrará así ser más efectiva y enfocada en intereses nacionales y no de intereses políticos.

México atraviesa por un proceso riguroso de estructuración en materia de ciberseguridad, al admitir que no se está preparado para ataques cibernéticos de escala global. Dentro de la próxima década, el avance de la Estrategia Nacional de Ciberseguridad marcará una diferencia entre sufrir grandes daños por ataques cibernéticos o controlar y mitigar esos daños.

El sector más importante para que se desarrolle la ciberseguridad radica en las Fuerzas Armadas e otras Instituciones de Seguridad Nacional, ya que

son la última capa que protegerá al Estado Mexicano de ataques cibernéticos y le otorgará las habilidades de hacerle frente. Muchos expertos en ciberseguridad han llamado a los países a desarrollar ésta área, pues se está viendo que los Estados que son potencia empiezan a desarrollar armas cibernéticas cada vez más avanzadas y de mayor alcance; pero a México aún falta camino que recorrer, ya que se espera para finales del 2030, el país ya sea capaz de defenderse de ciberataques de dichas proporciones.

FUENTES

Bibliografía:

- Bartlett, Jamie, (2017), *La Red Oculta,* (Franco Mundo Velázquez, Trans.), (pág. 28), Ciudad de México, México: PAIDÓS. (Trabajo original publicado en 2014).

- Buzan, Barry, (1991), *People, States and Fear (2nd ed.): An Agenda for International Security in the Post-Cold War Era,* Colorado, United States of America: LYNNE RIENNER PUBLISHERS.

- Buzan, Barry. & Waever, Ole., (2003), *Regions and Powers The Stucture of International Security*, New York, United States of America: Cambridge University Press.

- García Mexía, Pablo, (2012), *Historias de Internet Casos y Cosas de la Red de Redes*, Valencia, España: TIRANT HUMANIDADES.

- Secretaría de Marina & Centro de Estudios Superiores Navales, (2015), *Seguridad y Defensa en el Ciberespacio*. México: Secretaría de Marina & Centro de Estudios Superiores Navales.

- Segura Serrano, A., Gordo García, F., (Coords.), (2013), *Ciberseguridad Global Oportunidades y Compromisos en el Uso del Ciberespacio*, España: Editorial Universidad de Granada & Campus Universitario de Cartuja. Granada.

Hemerografía:

- Francisco Javier García Lorente. (2017, Segundo Cuatrimestre). Seguridad Aeroportuaria. *SEGURILATAM.* (N° 5).

- Humberto Guerrero García & Staff Seguridad en América. (2017, Septiembre-Octubre). Seguridad en tiendas minoristas. *Seguridad en América.* (N° 104).

- Jenaro Villamil. (2016, Agosto). Las redes sociales vértigo y pasión. *Proceso. (Edición Especial 53).*

- Newsweek. (2017, Marzo, 10). Conciencia y compromiso: el destino de la seguridad. *Newsweek.* (Edición Especial).

- Pablo Corona Fraga. (2017, Primer Cuatrimestre). Infraestructuras críticas. *SEGURILATAM.* (N°4).

- XTREM SECURE. (2017, Marzo-Abril). Novedades Tecnológicas en Seguridad*. XTREM SECURE*.

Cibergrafía:

- Internet World Stats. (30 de junio de 2017). Estadísticas mundiales de uso y de la población en internet. Recuperado 10 de noviembre de 2017, de: http://www.internetworldstats.com/stats.htm

- Rouse Margaret & Wigmore Ivy. (enero de 2017). Internet de las cosas (IoT). *TechTargetES*. Recuperado 09 de noviembre de 2017, de: http://searchdatacenter.techtarget.com/es/definicion/Internet-de-las-cosas-IoT

- Gobierno Federal. (2017). *Estrategia Nacional de Ciberseguridad*. [Archivo PDF]. Recuperado 29 de junio de 2017, de: https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad

- Gabriela Chávez. (15 de mayo de 2017). Este es el país de Latinoamérica más afecto por el ciberataque WannaCry. *CNN en Español*. Recuperado 29 de junio de 2017, de: http://cnnespanol.cnn.com/2017/05/15/este-es-el-pais-de-latinoamerica-mas-afectado-por-el-ciberataque-wannacry/

- DARPA. Where the Future Becomes Now*. DARPA.* Recuperado 29 de junio de 2017, de: https://www.darpa.mil/about-us/darpa-history-and-timeline

- DARPA. ARPA Changes Names. *DARPA.* Recuperado 29 de junio de 2017, de: https://www.darpa.mil/about-us/timeline/arpa-name-change

- DARPA. ARPANET and the Origins of the Internet*. DARPA.* Recuperado 29 de junio de 2017, de: https://www.darpa.mil/about-us/timeline/arpanet

- Barry M. Leiner, Vinton G. Cerf, David D. Clarck, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts & Stephen Wolff. (1997). Breve Historia de Internet. *Internet Society*. Recuperado 29 de junio de 2017, de: https://www.internetsociety.org/es/breve-historia-de-internet#Origins

- Raúl Rivero. (2002). Evolución de ARPANET/Internet. *EL MUNDO*. Recuperado 30 de junio de 2017, de: http://www.elmundo.es/imasd/docs/cursos/masterperiodismo/2002/rivero-master01-usa.html

- Álef. (2 de noviembre de 2014). ¿Una broma cibernética? El primer gusano de internet salió el 2 de noviembre de 1988. *Álef.* Recuperado 23 de noviembre de 2017, de: http://alef.mx/wp/una-broma-cibernetica-el-primer-gusano-de-internet-salio-el-2-de-noviembre-de-1988-2/

- Carnegie Mellon University. About Us. *Instituto de Ingeniería de Software*. Recuperado 13 de agosto de 2017, de: https://www.cert.org/about/

- CERN. About CERN. *CERN*. Recuperado 02 de julio de 2017, de: http://home.cern/about

- UNESCO. (27 de febrero de 2017). Los idiomas importan. *UNESCO.* Recuperado 10 de noviembre de 2017, de: http://www.unesco.org/new/es/communication-and-information/wsis-10-review-event-25-27-february-2013/feature-stories/languages-matter/

- TeleGeography. Submarine Cable Frequently Asked Questions. *TeleGeography*. Recuperado 11 de julio de 2017, de: http://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions

- Internet World Stats. (30 de junio de 2017). Usuarios de Internet al nivel mundial. *Internet World* Stats. Recuperado 02 de julio de 2017 de: http://www.internetworldstats.com/stats.htm

- Diario Oficial de la Federación. (14 de julio de 2017). Ley Federal de Telecomunicaciones y Radiodifusión. *SEGOB*. Recuperado 06 de julio de 2017, de: http://www.dof.gob.mx/nota_detalle.php?codigo=5352323&fecha=14/07/2014

- Asociación de Internet.mx. ¿Qué es la asociación de internet.mx?. *Asociación de Internet.mx.* Recuperado 05 de julio de 2017, de: https://www.asociaciondeinternet.mx/es/que-es/descripcion

- Estadística Digital. (18 de mayo de 2017). 13° Estudio sobre los Hábitos de los Usuarios de Internet en México 2017. *Asociación de internet.mx & INFOTEC*.

[Archivo PDF]. Recuperado 23 de noviembre de 2017 de: https://www.asociaciondeinternet.mx/es/estudios

- We are Social. (2017). Digital 2017. Global Overview. *We are Social.* Recuperado 06 de diciembre de 2017, de: https://wearesocial.com/uk/special-reports/digital-in-2017-global-overview

- BETA de INEGI. Sala de Prensa. *INEGI*. Recuperado 06 de julio de 2017, de: http://www.beta.inegi.org.mx/app/saladeprensa/

- BETA de INEGI. Quiénes somos. *INEGI*. Recuperado 06 de julio de 2017, de: http://www.beta.inegi.org.mx/inegi/quienes_somos.html

- BETA de INEGI. (2016) Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2016. *INEGI.* Recuperado 06 de julio de 2017, de: http://www.beta.inegi.org.mx/proyectos/enchogares/regulares/dutih/2016/

- INEGI. (14 de marzo de 2017). Aumentan uso de internet, teléfonos inteligentes y TV digital: Encuesta Nacional sobre Disponibilidad y uso de Tecnologías de la Información en los Hogares, 2016. [Archivo PDF]. Recuperado 10 de noviembre de 2017, de: http://www.inegi.org.mx/saladeprensa/boletines/2017/especiales/especiales2017_03_02.pdf

- CONEVAL. (2014). Medición de la Pobreza. *CONEVAL.* Recuperado 06 de julio de 2017, de: http://www.coneval.org.mx/Medicion/MP/Paginas/AE_pobreza_2014.aspx

- CONEVAL. ¿Quiénes somos?. *CONEVAL.* Recuperado 06 de julio de 2017, de: http://www.coneval.org.mx/quienessomos/Conocenos/Paginas/Quienes-Somos.aspx

- Expansión. (14 de marzo de 2017). 10 puntos que debes conocer sobre el internet en México. *EXPANSIÓN*. Recuperado 06 de julio de 2017, de: http://expansion.mx/tecnologia/2017/03/14/10-puntos-que-debes-conocer-sobre-el-internet-en-mexico

- IFT. Las telecomunicaciones a 3 ½ años de la Reforma Constitucional en México*. IFT*. [Archivo PDF]. Recuperado 06 de julio de 2017, de:

http://www.ift.org.mx/sites/default/files/contenidogeneral/estadisticas/a3anosreforma-vf6.pdf

- IFT. ¿Qué es el IFT?. [Archivo PDF]. Recuperado 06 de julio de 2017, de: http://www.ift.org.mx/sites/default/files/que-es-ift.pdf

- IFT. Principales beneficios para los usuarios y las audiencias. *IFT.* [Archivo PDF]. Recuperado 06 de julio de 2017, de: http://www.ift.org.mx/que-es-el-ift/principales-beneficios-para-los-usuarios-y-las-audiencias

- Internet World Stats. (30 de junio de 2017). Usuarios de Internet de Centro Américas y Población. *Internet World Stats.* Recuperado 17 de noviembre de 2017, de: http://www.internetworldstats.com/stats12.htm#central

- RAE. Definición de "Seguridad". *RAE.* Recuperado 12 de octubre de 2017, de: http://dle.rae.es/?id=XTrIaQd

- RAE. Definición de "Ciber". *RAE.* Recuperado 12 de octubre de 2017, de: http://dle.rae.es/?id=98ULSyc

- UIT. Acerca de la UIT. *UIT.* Recuperado 10 de julio de 2017, de: http://www.itu.int/es/about/Pages/default.aspx

- UIT. (2010). Ciberseguridad. *UIT.* [Archivo PDF]. Recuperado 13 de julio de 2017, de: https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf

- ISACA. Sobre ISACA. *ISACA.* Recuperado 13 de julio de 2017, de: http://www.isaca.org/about-isaca/Pages/default.aspx

- Miguel Ángel Mendoza. (16 de junio 2015) ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia. *Welivesecurity*. Recuperado 13 de julio de 2017, de: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

- ISO. Sobre ISO. *ISO.* Recuperado 14 de julio de 2017, de: https://www.iso.org/about-us.html

- 27001 Academy. ¿Qué es norma ISO 27001? *ADVISER.* Recuperado 14 de julio de 2017, de: https://advisera.com/27001academy/es/que-es-iso-27001/

- Diccionario de Oxford. Definición de "Ciberseguridad". *OXFORD.* Recuperado 13 de agosto de 2017, de: https://en.oxforddictionaries.com/definition/cybersecurity

- Diccionario de Cambridge. Definición de “Ciberseguridad”. *Cambridge.* Recuperado 13 de agosto de 2017, de: http://dictionary.cambridge.org/es/diccionario/ingles/cybersecurity#translations

- Ministerio de Defensa de España. (26 de febrero de 2013). Boletín Oficial del Ministerio de Defensa Núm. 40. [Archivo PDF]. Recuperado 14 de julio de 2017, de: http://www.emad.mde.es/Galerias/MOPS/novoperaciones/multimedia/documentos/20130226_CIBERDEFENSA.pdf

- Ministerio de la Presidencia y para las Administraciones Territoriales de España. (28 de septiembre de 2015). Ley de Seguridad Nacional. Recuperado 24 de noviembre de 2017, de: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10389

- Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (14 de julio de 2011). Lineamientos de Política para Ciberseguridad y Ciberdefensa. *CONPES.* [Archivo PDF]. Recuperado 13 de agosto de 2017, de: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

- Comité del Sistema Nacional de Seguridad. (6 de abril de 2015). *Committee on National Security Systems (CNSS) Glossary*. [Archivo PDF]. Recuperado 13 de agosto de 2017, de: https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf

- Homeland Security. Cybersecurity Overview. *Homeland Security.* Recuperado 14 de julio de 2017, de: https://www.dhs.gov/cybersecurity-overview

- Comando Estratégico de los Estados Unidos. *U.S. Cyber Command (USCYBERCOM).* Recuperado 13 de agosto de 2017, de: http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/

- Secretario General de la Comisión Europea. (8 de febrero de 2013). Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro. *Consejo de la Unión Europea*. Recuperado 16 de julio de 2017, de: http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=es

- GCHQ. *Who we are*. Recuperado 24 de julio de 2017, de: https://www.gchq.gov.uk/

- Proceso. (21 de octubre de 2013). Calderón se indigna por espionaje en su contra: es un agravio a instituciones, dice. *Proceso.* Recuperado 20 de julio de 2017, de: http://www.proceso.com.mx/356019/calderon-se-indigna-por-espionaje-en-su-contra-es-un-agravio-a-instituciones-dice

- MILENIO. (31 de julio de 2014). Las Principales Revelaciones de Snowden. Recuperado 24 de julio de 2017, de: http://www.milenio.com/internacional/principales-revelaciones-Snowden_0_345565796.html

- Sandra Fernández Moreno. (12 de octubre de 2015). ¿Qué es spyware? Definición y tipos. *ValorTOP.* Recuperado 13 de octubre de 2017, de: http://www.valortop.com/blog/que-es-un-spyware

- R3D: Red en Defensa de los Derechos Digitales. (19 de junio de 2017). Informe: Gobierno Espía: Vigilancia Sistemática a Periodistas y Defensores de Derechos Humanos en México. *R3D*. Recuperado 19 de julio de 2017, de: https://r3d.mx/2017/06/19/gobierno-espia/

- R3D. Quiénes somos / Qué hacemos. Recuperado 19 de julio de 2017, de: https://r3d.mx/nosotros/

- THE CITIZEN LAB. About the citizen lab*. THE CITIZEN LAB.* Recuperado 19 de julio de 2017, de: https://citizenlab.ca/about/

- Jorge Carrasco & Mathieu Tourliere. (24 de junio de 2017). Pegasus, el arma peñista para espiar. *Proceso.* Recuperado 19 de julio de 2017, de: http://www.proceso.com.mx/492358/pegasus-arma-penista-espiar

- Thomas Fox-Brewster. (18 de abril de 2017). NSO Group: Los espías israelíes que hackean iphone con un solo SMS. *Forbes México.* Recuperado 19 de julio de 2017, de: https://www.forbes.com.mx/nso-group-los-espias-israelies-que-hackean-iphones-con-un-solo-sms/

- R3D: Red en Defensa de los Derechos Digitales. (11 de febrero de 2017). Destapa la vigilancia: promotores del impuesto al refresco, espiados con malware gubernamental. *R3D.* Recuperado 19 de julio de 2017, de: https://r3d.mx/2017/02/11/destapa-la-vigilancia-promotores-del-impuesto-al-refresco-espiados-con-malware-gubernamental/

- El Poder del Consumidor. (13 de febrero de 2016). El espionaje del gobierno de México contra defensores del derecho a la salud no debe quedar impune: OSC. [Archivo PDF]. Recuperado 19 de julio de 2017, de: http://elpoderdelconsumidor.org/wp-content/uploads/2017/02/b-el-espionaje-del-gobierno-de-mexico-a-activistas-no-debe-quedar-impune.pdf

- Ernesto Aroche Aguilar. (3 de julio de 2017). Gobierno duplica en 4 años sus solicitudes de datos sobre usuarios de Facebook, Twitter y Google. *Animal Político.* Recuperado 19 de julio de 2017, de: http://www.animalpolitico.com/2017/07/datos-solicitudes-redes-gobierno/

- Universidad de Oxford. (2017). Troops, Trolls and Troublemakers: A Gblobal Inventory of Organized Social Media Manipulation.Oxford Internet Institute. Oxford*. Oxford.* [Archivo PDF]. Recuperado 18 de julio de 2017, de: http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf

- Adam Satariano. (17 de julio de 2017). Gobierno mexicano, entre los que "meten mano" a redes para influir en opinión pública: estudio. *El Financiero.* Recuperado 18 de julio de 2017, de: http://www.elfinanciero.com.mx/tech/mexico-entre-gobiernos-que-manipulan-facebook-y-redes-sociales-estudio.html

- Jordan Robertson, Michael Riley & Andrew Willis. (31 de marzo de 2016). Cómo Hackear una Elección. *Bloomberg Businessweek.* Recuperado 19 de julio de 2017, de: https://www.bloomberg.com/features/2016-como-manipular-una-eleccion/

- Reuters Staff. (7 de septiembre de 2017). *ECB´s Draghi rejects Estonias´s virtual currency idea. Reuters.* Recuperado 12 de septiembre de 2017, de: http://www.reuters.com/article/us-ecb-bitcoin-estonia/ecbs-draghi-rejects-estonias-virtual-currency-idea-idUSKCN1BI2BI?feedType=RSS&feedName=technologyNews

- Ricardo Martínez de Rituerto. (18 de mayo de 2017). Los "ciberataques" a Estonia desde Rusia desatan la alarma en la OTAN y la UE. *El País.* Recuperado 31 de agosto de 2017, de: https://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html

- CERT-UNAM. Diccionario. *CERT-UNAM.* Recuperado 13 de octubre de 2017, de: https://www.seguridad.unam.mx/taxonomy/term/1030

- Norton. Bots y botnets: Una amenaza creciente. *Norton.* Recuperado 13 de octubre de 2017, de: https://mx.norton.com/botnet

- Álvaro Fernández. (12 de agosto de 2015). Estonia, baluarte de la ciberseguridad europea. *El Orden Mundial en el S.XXI.* Recuperado 31 de agosto de 2017, de: http://elordenmundial.com/2015/08/12/estonia-ciberseguridad-europea/

- BBC Mundo. (11 de octubre de 2015). El virus que tomó control de mil máquinas y les ordenó autodestruirse. *BBC Mundo.* Recuperado 31 de agosto de 2017, de: http://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

- Lucía Luna. (5 de julio de 2013). Stuxnet: La filtración de un ciberataque. *Proceso.* Recuperado 31 de agosto de 2017, de: http://www.proceso.com.mx/346707/stuxnet-la-filtracion-de-un-ciberataque

- Documental *Zero Days.* (2016). Directo Alex Gibney. Recuperado 25 de noviembre de 2017, de: YouTube: https://www.youtube.com/watch?v=J50bUcf8gfc

- Panda. (15 de noviembre de 2013). ¿Qué es un Ransomware?. *Panda.* Recuperado 13 de octubre de 2017, de: https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/

- Boletín de Seguridad UNAM-CERT-2017-001. (12 de mayo de 2017). Alerta por ransomware WannaCry. *CERT-UNAM.* Recuperado 02 de septiembre de 2017, de: https://www.seguridad.unam.mx/node/355

- El País. (17 de agosto de 2016). Un grupo de hackers filtra programas de espionaje robados a la NSA. *El País.* Recuperado 03 de septiembre de 2017, de: https://elpais.com/internacional/2016/08/17/actualidad/1471436554_088389.html

- Secuelist. (22 de diciembre de 2017). Estados Unidos acusa de forma frontal y sin tapujos a Corea del Norte por los ataques de WannaCry. *Securelist.* Recuperado 28 de diciembre de 2017, de: https://securelist.lat/estados-unidos-

acusa-de-forma-frontal-y-sin-tapujos-a-corea-del-norte-por-los-ataques-de-wannacry/85880/

- Forbes Staff. (15 de mayo de 2017). Microsoft acusa de negligencia a la NSA por hackeo masivo. *Forbes México.* Recuperado 02 de septiembre de 2017, de: https://www.forbes.com.mx/microsoft-acusa-negligencia-la-nsa-hackeo-masivo/

- BBC Mundo. (13 de mayo de 2017). MalwareTech, el joven que detuvo el ciberataque que secuestró computadoras en caso 100 países. *Animal Político*. Recuperado 25 de noviembre de 2017, de: http://www.animalpolitico.com/2017/05/malwaretech-ciberataque-100-paises/

- Rosa Jiménez Cano. (6 de agosto de 2017). La caída del héroe que paró el virus WannaCry. *El País.* Recuperado 02 de septiembre de 2017, de: https://elpais.com/internacional/2017/08/06/actualidad/1502011078_699717.html

- OMPI. ¿Qué es la OMPI?. Recuperado 10 de agosto de 2017, de: http://www.wipo.int/about-wipo/es/

- Chema Flores. (20 de julio de 2017). Estados Unidos y Europa tumban los mercados ilegales más grandes de la dark web. *El Economista America.com* Recuperado 06 de diciembre de 2017, de: http://www.economiahoy.mx/telecomunicacion-tecnologia-mx/noticias/8510839/07/17/Operacion-policial-sin-precedentes-EEUU-y-Europa-tumban-los-mercados-ilegales-mas-grandes-de-la-dark-web.html

- Chris Baraniuk. (20 de julio de 2017). Duro golpe contra los traficantes de armas y drogas en la internet oscura: FBI y Europol cierran los mercados AlphaBay y Hansa. *BBC Mundo.* Recuperado 06 de diciembre de 2017, de: http://www.bbc.com/mundo/noticias-internacional-40674538

- KATEHON. (20 de junio de 2017). La Ciber Política de China. *KATEHON.* Recuperado 25 de noviembre de 2017, de: http://katehon.com/es/article/la-ciber-politica-de-china

- RSA Conference. Recuperado 10 de agosto de 2017, de: https://www.rsaconference.com/

- Microsoft. (14 de febrero de 2017). The need for a Digital Geneva Convention. *Microsoft.* Recuperado 10 de agosto de 2017, de: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

- Centro de Excelencia de Cooperación de Ciberdefensa. (18 de julio de 2017). Geneva Conventions Apply to Cyberspace: No Need for a "Digital Geneva Convention*". CCDCOE.* Recuperado 10 de agosto de 2017, de: https://ccdcoe.org/geneva-conventions-apply-cyberspace-no-need-digital-geneva-convention.html

- Securelist. (7 Septiembre 2017). Hackers adquieren conocimientos y habilidades para controlar las operaciones de plantas de energía en Europa y Estados Unidos. *Securelist.* Recuperado 07 de septiembre de 2017, de: https://securelist.lat/hackers-adquieren-conocimientos-y-habilidades-para-controlar-las-operaciones-de-plantas-de-energia-en-europa-y-estados-unidos/85503/

- Rhett Jones. (9 de junio de 2017). *Hackers Have Reportedly Gained "Operational Access" to US Power Grids, But Dont´Freak Yet. GIZMODO.* Recuperado 07 de septiembre de 2017, de: http://gizmodo.com/hackers-have-reportedly-gained-operational-access-to-us-1800755045

- Jon Henly. (31 de agosto de 2017). Denmark and Sweden boost defence ties to fight Russian cyber-attacks*. The Guardian.* Recuperado 14 de septiembre de 2017, de: https://www.theguardian.com/world/2017/aug/31/denmark-and-sweden-boost-defence-ties-to-fight-russian-cyber-attacks

- Keith Griffith. (22 de agosto de 2017). Were they hacked? US Navy to investigate wether BOTH warships that crashed into much larger merchant vessels with deadly results were the victims of a cyber attack. *Daily Mail.* Recuperado 14 de septiembre de 2017, de: http://www.dailymail.co.uk/news/article-4811516/amp/US-Navy-consider-crashed-warships-hacked.html

- Ellen Nakashima. (12 de junio de 2017). Russia has developed a cyberweapon that can disrupt power grids, according to new research. *The Washington Post.* Recuperado 15 de septiembre de 2017, de: https://www.washingtonpost.com/world/national-security/russia-has-developed-a-

cyber-weapon-that-can-disrupt-power-grids-according-to-new-research/2017/06/11/b91b773e-4eed-11e7-91eb-9611861a988f_story.html?hpid=hp_hp-top-table-main_russiascyber-810a%3Ahomepage%2Fstory&utm_term=.a942776d6e98

- BBC News. (10 de agosto de 2017). Ukrainian postal service hit by 48-hour cyber-attack. *BBC News.* Recuperado 15 de septiembre de 2017, de: http://www.bbc.com/news/technology-40886418

- Schneier. (2016). Someone is learning how to take down the internet. *Blog Personal.* Recuperado 15 de septiembre de 2017, de: https://www.schneier.com/blog/archives/2016/09/someone_is_lear.html

- OTAN. What is NATO. *OTAN*. Recuperado 23 de julio de 2017, de: http://www.nato.int/nato-welcome/index.html

- OTAN. Member countries. *OTAN.* Recuperado 23 de julio de 2017, de: http://www.nato.int/cps/en/natolive/topics_52044.htm

- Centro de Excelencia de Cooperación de Ciberdefensa. Recuperado 31 de julio de 2017, de: https://ccdcoe.org/index.html

- OTAN. NATO Nations to boost cyber defence cooperation. *OTAN.* Recuperado 28 de julio de 2017, de: http://www.nato.int/cps/en/natolive/news_70519.htm

- OTAN. NATO Defence Ministers adopt new cyber defence policy. *OTAN.* Recuperado 28 de julio de 2017, de: http://www.nato.int/cps/en/SID-4DC51D3F-30C063BB/natolive/news_75195.htm

- MN CD2. About the MN CD Project. *MN CD2.* Recuperado 28 de julio de 2017, de: https://mncd2.ncia.nato.int/pages/about.aspx

- NATO Industry Cyber Partnership. Recuperado 31 de julio de 2017, de: http://www.nicp.nato.int/objectives-and-principles/index.html

- OTAN. NATO and European Union enhance cyber defence cooperation. *OTAN.* Recuperado 28 de julio de 2017, de: http://www.nato.int/cps/en/natohq/news_127836.htm

- OTAN. Collective defence-Article 5. *OTAN.* Recuperado 29 de julio de 2017, de: http://www.nato.int/cps/cn/natohq/topics_110496.htm

- OTAN. (13 de marzo de 2012). NATO Rapid Reaction Team to fight cyber attack. *OTAN.* Recuperado 28 de julio de 2017, de: http://www.nato.int/cps/en/SID-CF294941-345E723F/natolive/news_85161.htm

- OTAN. (10 de noviembre de 2017). Cyber defence. *OTAN.* Recuperado 12 de octubre de 2017, de: http://www.nato.int/cps/en/natohq/topics_78170.htm

- Unión Europea. Todos los países de la UE. *Unión Europea.* Recuperado 01 de agosto de 2017, de: https://europa.eu/european-union/about-eu/countries/member-countries_es

- Unión Europea. Agencia de Seguridad de las Redes y de la Información de la Unión Europea. *Unión Europea.* Recuperado 01 de agosto de 2017, de: https://europa.eu/european-union/about-eu/agencies/enisa_es

- Unión Europea, (13 de marzo de 2004). Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. Recuperado 01 de agosto de 2017, de: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

- Unión Europea. (18 de junio de 2013). Reglamento (UE) N° 526/2013 del Parlamento Europeo y del Consejo, relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA). [Archivo PDF]. Recuperado 01 de agosto de 2017, de: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32013R0526&from=EN

- ENISA. (2016). ENISA Strategy 2016-2020. *ENISA.* [Archivo PDF]. Recuperado 01 de agosto de 2017, de: https://www.enisa.europa.eu/publications/corporate/enisa-strategy

- Zeljka Zorz. (14 de septiembre de 2017). European Commission wants ENISA to introduce EU-wide cybersecurity certification scheme. *HELPNETSECURITY.* Recuperado 16 de septiembre de 2017 de: https://www.helpnetsecurity.com/2017/09/14/eu-wide-cybersecurity-certification-scheme/?ct=t()

- EUROPOL. Acerca de EUROPOL. *EUROPOL.* Recuperado 01 de agosto de 2017, de: https://www.europol.europa.eu/es/about-europol

- EUROPOL. European Cybercrime Centre-EC3. *EUROPOL.* Recuperado 01 de julio de 2017, de: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

- Unión Europea. Agencia de la Unión Europea para la Formación Policial (CEPOL). *Unión Europea.* Recuperado 01 de agosto de 2017, de: https://europa.eu/european-union/about-eu/agencies/cepol_es

- Unión Europea. Oficina del Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE). Unión *Europea.* Recuperado 01 de agosto de 2017, de: https://europa.eu/european-union/about-eu/agencies/berec_es

- Unión Europea. Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA). *Unión Europea.* Recuperado 01 de agosto de 2017, de: https://europa.eu/european-union/about-eu/agencies/eu-lisa_es

- Unión Europea. Agencia Europea de Seguridad Aérea (AESA). *Unión Europea.* Recuperado 01 de agosto de 2017, de: https://europa.eu/european-union/about-eu/agencies/easa_es

- Presidencia y para las Administraciones Territoriales de España. (19 de julio de 2016). Directiva (EU) 2016/1148 del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión. [Archivo PDF]. Recuperado 01 de agosto de 2017, de: https://www.boe.es/doue/2016/194/L00001-00030.pdf

- OEA. Artículo 1 De la Carta de la Organización de Estados Americanos. [Archivo PDF]. Recuperado 02 de agosto de 2017, de: http://www.oas.org/es/sla/ddi/docs/tratados_multilaterales_interamericanos_A-41_carta_OEA.pdf

- OEA. Estados Miembros. Recuperado 02 de agosto de 2017, de: http://www.oas.org/es/estados_miembros/default.asp

- OEA. (8 de junio de 2004). Adopción de una estrategia interamericana integral de seguridad cibernética: un enfoque multidimensional y multidisciplinar para la creación de una cultura de seguridad cibernética. *OEA.* [Archivo PDF]. Recuperado 02 de agosto de 2017, de:

http://www.oas.org/es/sms/cicte/documents/asambleas/AG-RES.%202004%20(XXXIV-O-04)_SP.pdf

- OEA. Seguridad Cibernética. Recuperado 02 de agosto de 2017, de: https://www.sites.oas.org/cyber/ES/Paginas/default.aspx

- OEA. Informe Anual del Secretario General 2016. *OEA*. [Archivo PDF]. Recuperado 30 de noviembre de 2017, de: http://www.oas.org/es/centro_informacion/informe_anual.asp

- Observatorio de la Ciberseguridad en América Latina y el Caribe. Recuperado 02 de agosto de 2017, de: http://observatoriociberseguridad.com/country/mx

- FIRST. Recuperado 02 de agosto de 2017, de: https://www.first.org/

- Página Oficial del INAI. Misión, Visión y Objetivos. Recuperado 03 de agosto de 2017, de: http://inicio.ifai.org.mx/SitePages/misionViosionObjetivos.aspx

- OEA. (20 de junio de 2017). Comunicado de Prensa. *OEA.* Recuperado 05 de agosto de 2017, de: http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-049/17

- Julio Sánchez Onofre. (15 de mayo de 2017). Policía Federal ha identificado sólo 4 infecciones de WannaCry en México. *El Economista.* Recuperado 05 de agosto de 2017, de: http://eleconomista.com.mx/tecnociencia/2017/05/15/policia-federal-ha-identificado-solo-4-infecciones-wannacry-mexico

- Joan Faus. (14 de septiembre de 2017). EEUU veta el uso del software Kaspersky a las agencias gubernamentales por miedo al espionaje ruso. *El País.* Recuperado 30 de noviembre de 2017, de: https://elpais.com/tecnologia/2017/09/13/actualidad/1505330916_156194.html

- Mauricio Hernández Armenta. (15 de mayo de 2017). México es el país más afectado por el virus WannaCry en AL. *Forbes México.* Recuperado 05 de agosto de 2017, de: https://www.forbes.com.mx/mexico-es-el-pais-mas-afectado-por-el-virus-wannacry-en-al/

- Mauricio Hernández Armenta. (12 de junio de 2017). México, vulnerable ante más ataques cibernéticos. *Forbes México.* Recuperado 05 de agosto de 2017, de: https://www.forbes.com.mx/mexico-vulnerable-ante-mas-ataques-ciberneticos/

- Jair López. (1 de junio de 2017). Especialistas ven impunidad en ciberseguridad en México. *Expansión*. Recuperado 05 de agosto de 2017, de: http://expansion.mx/tecnologia/2017/06/01/especialistas-ven-impunidad-en-ciberseguridad-en-mexico

- Itzel Castañares. (20 de julio de 2017). Ciberataques en México afectan a sector financiero: Cisco. *El Financiero.* Recuperado 05 de agosto de 2017, de: http://www.elfinanciero.com.mx/tech/ciberataques-en-mexico-afectan-a-sector-financiero-cisco.html

- Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF). ¿Qué son las fintech?. Recuperado 05 de agosto de 2017, de: http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/educacion-financiera/763-que-son-las-fintech

- Policía Federal. Directorio. Recuperado 06 de agosto de 2017, de: https://www.gob.mx/policiafederal

- Diario Oficial de la Federación. (17 de mayo de 2010). Reglamento de la Ley de la Policía Federal. *SEGOB*. Recuperado 06 de agosto de 2017, de: http://www.dof.gob.mx/nota_detalle.php?codigo=5143004&fecha=17/05/2010

- UNAM-CERT. Acerca de la Coordinación de Seguridad de la Información (CSI). *DGTIC.* Recuperado 12 de agosto de 2017, de: https://www.seguridad.unam.mx/

- Mnemo. Nosotros. *Mnemo.* Recuperado 12 de agosto de 2017, de: https://www.mnemo.com/nosotros/

- Scitum. ¿Quiénes somos?. *Scitum.* Recuperado 30 de noviembre de 2017, de: https://www.scitum.com.mx/ScitumCSIRT

- Plan Nacional de Desarrollo 2007-2012. [Archivo PDF]. Recuperado 30 de noviembre de 2017, de: http://pnd.calderon.presidencia.gob.mx/index.php?page=documentos-pdf

- Primer Informe de Gobierno de Felipe Calderón. [Archivo PDF]. Recuperado 30 de noviembre de 2017, de: http://calderon.presidencia.gob.mx/informe/primer/descargas/index.html

- Segundo Informe de Gobierno de Felipe Calderón. [Archivo PDF]. Recuperado 30 de noviembre de 2017, de: http://calderon.presidencia.gob.mx/informe/segundo/descargas/index.html

- Tercer Informe de Gobierno de Felipe Calderón. [Archivo PDF]. Recuperado 30 de noviembre de 2017, de: http://calderon.presidencia.gob.mx/informe/tercer/descargas/index.html

- Cuarto Informe de Gobierno de Felipe Calderón. [Archivo PDF]. Recuperado 30 de noviembre de 2017, de: http://calderon.presidencia.gob.mx/informe/cuarto/informe-de-gobierno/

- Quinto Informe de Gobierno de Felipe Calderón. [Archivo PDF]. Recuperado 30 de noviembre de 2017, de: http://calderon.presidencia.gob.mx/informe/quinto/descargas/

- Sexto Informe de Gobierno de Felipe Calderón. [Archivo PDF]. Recuperado 30 de noviembre de 2017, de: http://calderon.presidencia.gob.mx/informe/sexto/sexto_informe.html

- Diario Oficial de la Federación. (13 Julio 2010). Acuerdo por el que se expide el Manual Administrativo de Aplicación General en materias de TIC y de Seguridad de la Información. *SEGOB.* Recuperado 14 de agosto de 2017, de: http://dof.gob.mx/nota_detalle.php?codigo=5151475&fecha=13/07/2010

- Secretaría de la Función Pública. (4 de febrero de 2016). Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad dela información, así como el Manual Administrativo de Aplicación General en dichas materias. *Secretaría de la Función Pública.* [Archivo PDF]. Recuperado 30 de noviembre de 2017, de: https://www.gob.mx/cms/uploads/attachment/file/79205/MANUAL_ADMINISTRATIVO_DE_APLICACION_GENERAL_EN_MATERIA_DE_TECNOLOGIAS_DE_LA_INFORMACION_Y_COMUNICACIONES.pdf

- Plan Nacional de Desarrollo 2013-2018 de Enrique Peña Nieto. [Archivo PDF]. Recuperado 01 de diciembre de 2017, de: http://pnd.gob.mx/

- Programa para la Seguridad Nacional 2014-2018. *Enrique Peña Nieto* [Archivo PDF]. Recuperado 01 de diciembre de 2017, de: https://www.gob.mx/presidencia/articulos/programa-para-la-seguridad-nacional-2014-2018

- Programa Sectorial de Defensa Nacional 2013-2018. *Enrique Peña Nieto* [Archivo PDF]. Recuperado 01 de diciembre de 2017, de: http://www.sedena.gob.mx/archivos/psdn_2013_2018.pdf

- Programa Sectorial de Marina 2013-2018. *Enrique Peña Nieto* [Archivo PDF]. Recuperado 01 de diciembre de 2017, de: http://www.semar.gob.mx/informes/programa_sectorial_13.pdf

- Diario Oficial de la Federación. (30 de abril de 2014). Programa Nacional de Seguridad Pública 2013-2018. *SEGOB.* Recuperado 01 de diciembre de 2017, de: http://dof.gob.mx/nota_detalle.php?codigo=5343081&fecha=30/04/2014

- Primer Informe de Gobierno de Enrique Peña Nieto. [Archivo PDF]. Recuperado 30 de noviembre de 2017, de: http://www.presidencia.gob.mx/primerinforme/

- CCO Noticias. (17 de enero de 2013). Sedena y Marina niegan robo de datos; reestablecen sitios. *CCO Noticias.* Recuperado 27 de diciembre de 2017, de: https://cconoticias.com/2013/01/17/sedena-y-marina-niegan-robo-de-datos-reestablecen-sitios/

- Segundo Informe de Gobierno de Enrique Peña Nieto. [Archivo PDF]. Recuperado 30 de noviembre de 2017, de: http://www.presidencia.gob.mx/segundoinforme/

- Tercer Informe de Gobierno de Enrique Peña Nieto. [Archivo PDF]. Recuperado 30 de noviembre de 2017, de: http://www.presidencia.gob.mx/tercerinforme/

- Cuarto Informe de Gobierno de Enrique Peña Nieto. [Archivo PDF]. Recuperado 30 de noviembre de 2017, de: http://www.presidencia.gob.mx/cuartoinforme/

- Quinto Informe de Gobierno de Enrique Peña Nieto. [Archivo PDF]. Recuperado 30 de noviembre de 2017, de: http://www.presidencia.gob.mx/quintoinforme/

- Notimex. (05 Septiembre 2017). PGR crea la Unidad de Investigaciones Cibernéticas. *El Economista.* Recuperado 08 de septiembre de 2017, de: http://eleconomista.com.mx/tecnociencia/2017/09/05/pgr-crea-unidad-investigaciones-ciberneticas

- Mauricio Hernández Armenta. (08 de agosto de 2017). Cisco prevé destrucción de servicios y más ciberataques. *Forbes México.* Recuperado 23 de agosto de 2017, de: https://www.forbes.com.mx/cisco-preve-destruccion-de-servicios-y-mas-ataques-ciberneticos/

- Rodrigo Riquelme. (18 de noviembre de 2017). Cibercrimen como servicio, la industria de los ataques digitales. *El Economista.* Recuperado 06 de diciembre de 2017, de: https://www.eleconomista.com.mx/tecnologia/Cibercrimen-como-servicio-la-industria-de-los-ataques-digitales-20171118-0010.html

- Código Penal Federal. [Archivo PDF]. Recuperado 05 de diciembre de 2017, de: https://docs.mexico.justia.com/federales/codigo_penal_federal.pdf

- Proceso. (30 de marzo de 2017). Policía Cibernética de la CDMX alerta sobre el reto suicida “Ballena azul”. *Proceso.* Recuperado 23 de agosto de 2017, de: http://www.proceso.com.mx/480180/policia-cibernetica-la-cdmx-alerta-reto-suicida-ballena-azul

- Proceso. (11 de mayo de 2017). Ubican en Iztapalapa el primer caso del reto suicida de la “Ballena azul”. *Proceso.* Recuperado 23 de agosto de 2017, de: http://www.proceso.com.mx/486162/ubican-en-iztapalapa-primer-caso-del-reto-suicida-la-ballena-azul

- Senadores del PAN LXIII Legislatura. (15 de diciembre de 2017). Aprueba Senado propuesta del senador Victor Hermosillo para sancionar la “porno-venganza”. *Senadores del PAN LXIII Legislatura.* Recuperado 27 de diciembre de 2017, de: http://www.pan.senado.gob.mx/2017/12/aprueba-senado-propuesta-del-senador-victor-hermosillo-para-sancionar-la-porno-venganza/

- Gloria Reza M. (07 de septiembre de 2017). Penalizan en Jalisco el sexting, grooming y los retos suicidas. *Proceso.* Recuperado 23 de agosto de 2017, de: http://www.proceso.com.mx/502292/penalizan-en-jalisco-sexting-grooming-los-retos-suicidas

Notimex. (12 de diciembre de 2017). Tipificar delitos informáticos en Código Penal Federal, plantea diputado. *20 MINUTOS*. Recuperado 06 de diciembre de 2017, de: http://www.20minutos.com.mx/noticia/296447/0/tipificar-delitos-informaticos-en-codigo-penal-federal-plantea-diputado/

- El Economista. (20 de julio de 2017). Condusef alerta de nuevo caso de phishing de HSBC. *El Economista.* Recuperado 07 de septiembre de 2017, de: http://eleconomista.com.mx/finanzas-personales/2017/07/20/condusef-alerta-nuevo-caso-phishing-hsbc

- Edgar Juárez & Fernando Gutiérrez. (24 de octubre de 2017). Crean frente nacional sobre Ciberseguridad. *El Economista.* Recuperado 05 de diciembre de 2017, de: https://www.eleconomista.com.mx/sectorfinanciero/Crean-frente-nacional-sobre-ciberseguridad-20171024-0002.html

- Comisión Nacional Bancaria y de Valores. (23 de octubre de 2017). Foro de Ciberseguridad. *CNBV.* Recuperado 05 de diciembre de 2017, de: https://www.gob.mx/cnbv/articulos/foro-de-ciberseguridad

- Ley de Seguridad Nacional. [Archivo PDF]. Recuperado 17 de julio de 2017, de: http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac.pdf

- Diario Oficial de la Federación. (02 de enero de 2009). Ley General del Sistema Nacional de Seguridad Pública. *SEGOB.* Recuperado 18 de julio de 2017, de: http://www.dof.gob.mx/nota_detalle.php?codigo=5076728&fecha=02/01/2009

- Kaspersky. (31 de agosto de 2017). Oculto a simple vista: el grupo “Saguaro” ataca América Latina utilizando técnicas sencillas, pero eficaces. *Kaspersky.* Recuperado 07 de septiembre de 2017, de: https://latam.kaspersky.com/blog/oculto-a-simple-vista-el-grupo-saguaro-ataca-america-latina-utilizando-tecnicas-sencillas-pero-eficaces/7589/

- Gabriela Chávez. (16 de agosto de 2016). A México le faltan expertos para cubrir la demanda de empleos en ciberseguridad. *Expansión.* Recuperado 30 de

septiembre de 2017, de: http://expansion.mx/tecnologia/2016/08/16/a-mexico-le-faltan-expertos-para-cubrir-la-demanda-de-empleos-en-ciberseguridad

- Tania Campos. (07 de septiembre de 2017). La página gob.mx es blanco frecuente de ataques cibernéticos. *XATAKA México.* Recuperado 30 de septiembre de 2017, de: https://www.xataka.com.mx/otros-1/la-pagina-gob-mx-es-blanco-frecuente-de-ataques-ciberneticos

- Gabriela Chávez. (13 de mayo de 2016). La débil ciberseguridad en México pone en riesgo a Estados Unidos. *Expansión.* Recuperado 30 de septiembre de 2017, de: http://expansion.mx/tecnologia/2016/05/13/la-debil-ciberseguridad-en-mexico-pone-en-riesgo-a-estados-unidos

- Life and Style. (08 de septiembre de 2017). México es el quinto país con más ciberataques en el mundo. *Life and Style.* Recuperado 30 de septiembre de 2017, de: https://lifeandstyle.mx/tech/2017/09/08/mexico-es-el-quinto-pais-con-mas-ciberataques-del-mundo

- Julio Sánchez Onofre. (28 de septiembre de 2017). Las infraestructuras críticas de México ya están bajo ciberataques. *El Economista.* Recuperado 01 de octubre de 2017, de: http://eleconomista.com.mx/tecnociencia/2017/09/28/las-infraestructuras-criticas-mexico-ya-estan-bajo-ciberataques

- Secretaría de Relaciones Exteriores. (2017). México Presentó Estrategia Nacional de Ciberseguridad desarrollada con el apoyo de la OEA. *SER.* Recuperado 07 de diciembre de 2017, de: https://mision.sre.gob.mx/oea/index.php/actividades/25-avisos-2017/420-mexico-mexico-presento-estrategia-nacional-de-ciberseguridad

- Documentos. (13 de noviembre de 2017). Estrategia Nacional de Ciberseguridad. *Gob.mx.* [Archivo PDF]. Recuperado 07 de diciembre de 2017, de: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

- Diario Oficial de la Federación (09 de diciembre de 2005). Acuerdo que tiene como objeto crear en forma permanente la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico. *SEGOB.* Recuperado 07 de diciembre de 2017, de: http://www.dof.gob.mx/nota_detalle.php?codigo=2101617&fecha=09/12/2005

- Claudia Juárez Escalona. (06 de septiembre de 2017). Canieti busca que la ciberseguridad sea discuta en el TLCAN. *El Economista.* Recuperado 03 de octubre de 2017, de: http://eleconomista.com.mx/industrias/2017/09/06/canieti-busca-que-ciberseguridad-sea-discuta-tlcan

- Carla Martínez. (07 de septiembre de 2017). Piden a Segob coordinar ciberseguridad. *El Universal.* Recuperado 03 de octubre de 2017, de: http://www.eluniversal.com.mx/cartera/economia/piden-segob-coordinar-ciberseguridad