Casa abierta al tiempo

UNIVERSIDAD AUTÓNOMA METROPOLITANA

Unidad Iztapalapa

Las nuevas perspectivas del Estado mexicano frente a los retos de la ciberseguridad y ciberdefensa

T E S I N A

Q U E P R E S E N T A

MARIAM CRYSTELL APARICIO GUADARRAMA
MATRICULA: 2163078870

Para acreditar el requisito del trabajo terminal
y optar al título de

LICENCIADA EN CIENCIA POLITICA

DRA. LAURA VERÓNICA CORONADO CONTRERAS

ASESOR

MTRO. MIGUEL GONZÁLEZ MADRID

LECTOR

Alcaldía Iztapalapa, Ciudad de México, 18 de mayo de 2022

Casa abierta al tiempo

UNIVERSIDAD AUTÓNOMA METROPOLITANA – Unidad *Iztapalapa*
DIVISIÓN DE CIENCIAS SOCIALES Y HUMANIDADES
DEPARTAMENTO DE SOCIOLOGIA-COORDINACIÓN DE CIENCIA POLÍTICA

D I C T A M E N

Después de examinar este documento final presentado por la alumna Mariam Crystell Aparicio Guadarrama, matrícula 2163078860 con el título de Las nuevas perspectivas del Estado mexicano frente a los retos de la ciberseguridad y ciberdefensa se consideró que reúne las condiciones de forma y contenido para ser aprobado como conclusión de la Tesina o Trabajo Terminal, correspondiente a la Licenciatura en Ciencia Política que se imparte en esta Unidad.

Con lo cual se cubre el requisito establecido en la Licenciatura para aprobar el Seminario de Investigación III y acreditar la totalidad de los estudios que indica el Plan de Estudios vigente.

Asesor	Lector
Dra. Laura Verónica Coronado Contreras	Mtro. Miguel González Madrid

Fecha 18/05/22 Trim: 22-I No. Registro de Tesina: AGMC/2020-I

Para Enrique. Gracias, papá, por ser siempre la luz en mi camino que me ha inspirado a seguir adelante.

AGRADECIMIENTOS

Agradezco a mi padre, Enrique Aparicio Cuevas, por los sabios consejos que me regaló a lo largo de los años que pasamos juntos y por su amor incondicional.

A Ady, Jaime, Pablo y Uzziel porque con ellos encontré el cariño y comprensión de una familia, gracias por todo el apoyo que me han brindado a lo largo de mi vida y por las aventuras y alegrías compartidas a su lado.

A las mujeres de mi familia, a mi abuela, Matilde Cuevas, que es la persona más valiente que conozco y el pilar de la casa. También agradezco a Ana, Anayelly y Mayte por siempre estar a mi lado.

A Felipe, que se convirtió en mi mejor amigo y quien me ha acompañado en todas esas noches de desvelo. Pero sobre todo por ser un motivo de alegría para vivir el día a día.

A la Dra. Laura Coronado, quien me inspiró a hablar sobre algo nuevo, y quien ha sido una red de apoyo, agradezco la paciencia y el compartirme sus conocimientos para que esta investigación fuera posible.

Agradezco también el apoyo del profesor Miguel González Madrid, por ser mi lector y por el aprendizaje que me dejó en algunas materias a lo largo de la carrera.

A Diana, Fernando, Lizeth, Miguel, Oscar, Tamara y Yaidi, que se convirtieron en mis grandes amigos durante mi trayectoria estudiantil, agradezco los momentos compartidos a su lado y porque siempre han estado ahí cuando los necesito.

CONTENIDO

INTRODUCCIÓN

Hoy en día, gracias a las nuevas Tecnologías de Información y Comunicación (TIC), se dice que vivimos en un mundo que está casi por completo conectado, capaz de transformar la realidad de sus habitantes con un simple *click*. Sin embargo, el mundo, desde aquel 2019, cuando surgió el primer caso del virus SARS-CoV-2, se ha transformado por completo, en todos los ámbitos que van desde lo económico, político, internacional, y social; este último, sobre todo, ha cambiado la manera en que las personas se relacionan, puesto que se tuvieron que adaptar a una nueva forma de socialización, la "realidad virtual", la cual sirvió como un apoyo para trasladar todas aquellas actividades presenciales al ciberespacio.

También, a raíz de esto, se dio un aumento en el porcentaje de personas partícipes en el ciberespacio y, por tanto, se vieron más expuestas a sufrir algún tipo de ciberataque, ya que este riesgo también creció por todo el mundo, en un número inimaginable, dejando múltiples pérdidas económicas para algunos individuos y organizaciones.

Si bien esto a primera vista no se considera como un problema de carácter urgente para todos los gobiernos, debería ser todo lo contrario, puesto que los ciberataques no solo están referidos a la pérdida de bienes tangibles, sino que son capaces de alterar cualquier tipo de infraestructura que sea esencial para el funcionamiento y servicio de la sociedad; tal es el caso del patrimonio nacional, las instituciones bancarias, la industria, los hospitales y las diversas empresas que ofrezcan algún servicio y para ello requieran de medios informáticos.

Algo realmente alarmante, por ejemplo, es que la mayoría de la sociedad no está muy familiarizada con la protección de sus datos personales que proporcionan a través de internet, ni mucho menos saben lo que implica el resguardo y la

ciberseguridad de las infraestructuras críticas de información; o bien, son pocos los que tienen conocimiento en estos temas y lo pasan desapercibido, hasta que ya es demasiado tarde cuando sufren los perjuicios.

Y es ahí donde entra en juego la ciberseguridad y ciberdefensa, ya que ambas persiguen un mismo objetivo, el mantener segura la información que se procesa a través de las tecnologías de la información. El primer concepto puede estar dirigido a la prevención de posibles ciberataques a las entidades privadas, la sociedad y los organismos públicos, mientras que la ciberdefensa por lo regular trata de dar una posible respuesta a ellos, a través de sus mecanismos de defensa, ya sean organismos o herramientas para salvaguardar la integridad de un país, puesto que muchas veces esos ataques se convierten en un riesgo para la seguridad nacional de cualquier nación.

Las ventajas que ofrecen las tecnologías de información son favorables para la sociedad, pero existen otros factores que impiden el pleno desarrollo de una sociedad tecnológica; tal es el caso de la brecha digital, puesto que se requiere de una inclusión social con la que los países no cuentan, ni siquiera los más desarrollados. Aunado a lo anterior, existe una falta de cultura de ciberseguridad y ciberdefensa por parte de la sociedad y del uso consciente en cuanto al uso de internet.

Es tarea de los gobiernos, el Estado y las organizaciones de carácter público y privado, garantizar que todas y todos tengamos un acceso libre y seguro al ciberespacio, donde se respeten los derechos humanos. Y es necesario contribuir también al aumento en el nivel de la ciberseguridad de las infraestructuras críticas y a la mejora de la ciberdefensa para protección de la seguridad nacional y del propio Estado.

En cuanto a la investigación, es de carácter teórico y documental puesto que se busca comprender y tratar de explicar diversos conceptos que emanan del ciberespacio, con base en las definiciones que apenas se están estudiando y que hasta ahora se perfilan para ser socialmente aceptadas. Dichas interpretaciones

son elaboradas con la participación de gobiernos, organismos internacionales y autores especializados en el área de las tecnologías de información.

El objetivo principal de esta investigación consiste en enfatizar la importancia que hoy en día tiene el poner de la ciberseguridad y la ciberdefensa en la agenda pública de todas las naciones, puesto que los ciberdelincuentes están un paso adelante de cualquier gobierno. Además, es pertinente plantear posibles alternativas para mitigar los riesgos en el ciberespacio. Sin embargo, esto sólo es posible con la participación del Estado, la sociedad civil y privada.

La presente tesina está organizada en tres capítulos. El primero trata de dar una definición de las variables de investigación, ciberseguridad y ciberdefensa, incluyendo la del ciberespacio e infraestructuras críticas de información, ya que están estrechamente vinculadas. Como segundo punto, se habla acerca de la importancia que tiene la ciberseguridad y la ciberdefensa analizadas desde la perspectiva del Estado mexicano, esto se ejemplifica con algunos casos de ciberataques ocurridos, no sólo en México sino de manera internacional y que traen consigo consecuencias, como la alteración al funcionamiento de industrias, empresas, hospitales y empresas paraestatales por mencionar algunas, debido a que no cuentan con un nivel adecuado de ciberseguridad. Al término de este capítulo, se discute acerca del gran trabajo que tienen los países para poner en su agenda pública estos temas y la manera en que un mal resguardo a su ciberseguridad y ciberdefensa puede afectar a la Seguridad Nacional. Por último, se aborda la problemática que existe en México en cuanto a su ciberseguridad y ciberdefensa, así como las acciones que el país ha implementado para contrarrestar posibles amenazas a su entorno digital y también en el físico.

El segundo capítulo se basa en un análisis comparativo de la manera en que, tres grandes potencias económicas, Estados Unidos, China y la Unión Europea, manejan su gobernanza en internet y en el ciberespacio, mediante sus órganos encargados de velar por él y también mediante su jurisdicción. Dichas naciones se tomaron como un enfoque de comparación puesto que, si hablamos de Estados

Unidos, este país ha hecho énfasis en la importancia que tiene velar por un ciberespacio de libre expresión, pero sin descuidar su principal objetivo, la supremacía por encima de todos. Por su parte, China ha exigido a sus ciudadanos un control en cuanto a la manera que realizan actividades en el ciberespacio; este país ha encontrado mecanismos efectivos para ejercer el poder mediante medios digitales. En cuanto a la Unión Europea, el modelo implementado tiene una perspectiva que también es de libre expresión, pero que incluye leyes que regulan al ciberespacio y velan por los derechos universales de sus ciudadanos.

En el tercer capítulo, se encuentra una serie de nuevos conceptos que han surgido a raíz de las nuevas tecnologías de información y que se están directamente vinculados con las agendas públicas de los países. Me refiero a las políticas públicas en Internet, parte de ellas relacionadas con las implementadas por algunos países en materia de ciberseguridad y ciberdefensa. Además de esto, se mencionan algunos modelos de estas políticas y demás acciones que han hecho algunas naciones para la protección del ciberespacio. Para finalizar el capítulo, se habla sobre una alternativa a una posible propuesta de política pública en ciberseguridad y ciberdefensa para el caso mexicano.

OBJETIVOS

O.G: Conocer el papel del Estado mexicano en el ámbito de la ciberseguridad y ciberdefensa, así como la participación de otros actores involucrados en el ciberespacio.

O.P.1: Definir los conceptos de ciberseguridad, ciberdefensa y ciberespacio, así como la importancia de estos en la sociedad.

O.P.2: Estudiar las estrategias implementadas en cuanto a la ciberseguridad y ciberdefensa de Estados Unidos, China y la Unión Europea.

O.P.3: Detallar una posible propuesta de política pública en ciberseguridad y ciberdefensa para México.

CAPÍTULO I. LA IMPORTANCIA DE LA CIBERSEGURIDAD Y LA CIBERDEFENSA EN EL ESTADO MEXICANO Y LA SOCIEDAD

1.1 Acercamiento a una conceptualización: ciberespacio, ciberseguridad y ciberdefensa

Como se sabe, hoy en día debido a la globalización, vivimos en un mundo interconectado, el cual nos permite obtener una respuesta casi instantánea a nuestras preguntas. Los seres humanos recurrimos a diversas formas de comunicación, modos revolucionarios que están directamente ligados a las nuevas tecnologías de la información y comunicación (TIC). Quizá el espacio no territorial, al que se acude con frecuencia en la actualidad, que ofrece un sin fin de información, la cual viaja de manera exponencial, y además confiere la apertura a una nueva forma de socialización, es el llamado “ciberespacio”, como menciona Coronado(2015), existe una ventaja entre este espacio y otros medios de comunicación, porque el ciberespacio garantiza la interacción de las personas que se quisiera de forma simultánea, y permite también una constante actualización entre la información que viaja dentro de este metaespacio.

Ahora bien, algunos autores se han percatado de la importancia que tiene el encontrar y/o formular una conceptualización con base en las características que el ciberespacio cuenta; Lévy (1997 p. 70) lo define como: “el espacio de comunicación abierto por la interconexión mundial de los ordenadores de las memorias informáticas”. Mientras que Avogadro (2012, p. 12) ve al ciberespacio como “un nuevo medio de comunicación que surge de la interconexión mundial de los sistemas de datos. Incluye la infraestructura material de la información digital y el universo de informaciones que contiene”.

Si bien Córdoba y Pérez (2020) hablan acerca de la importancia que tiene el ciberespacio como un dominio global, puesto que está compuesto por infraestructuras tecnológicas de la información, internet, telecomunicaciones e incluso sistemas de información, en donde es casi imposible hablar de una "seguridad total". Afirman que el hecho de que en este espacio exista cierta deficiencia en cuanto a su protección, no implica que no se deba buscar, alertar y minimizar las problemáticas involucradas en el ciberespacio.

Si se entiende al ciberespacio desde un enfoque técnico, podemos decir que es un conjunto de redes e infraestructuras tecnológicas. Sin embargo, atendiendo al ámbito social, se logra entender como un nuevo espacio de comunicación que da pauta a una nueva forma de socialización y educación, el cual no conoce una frontera geográfica que establezca un límite a la libertad de expresión, y el cual da cabida a una nueva forma de vida resiliente en la que los seres humanos encuentran un sustituto a las actividades ordinarias y presenciales.

En el año 2016, la OTAN[1] reconoció al ciberespacio como el quinto dominio de guerra al que se debe proteger al igual que se hace en tierra, mar, aire y espacio. Debido a las capacidades y características con las que cuenta este metaespacio, se presenta como un escenario de combate en donde sus acciones y conflictos bélicos pueden ser llevados no sólo a un terreno físico, sino a uno virtual. Con lo que se entiende que el espacio cibernético es una zona de conflicto y un escenario de poder (Ramírez, 2020).

Es relevante estudiar al ciberespacio desde una perspectiva donde se analicen los pros y contras que ofrece; de él derivan una serie de prerrogativas y problemáticas a las que el ser humano se encuentra expuesto al momento de interactuar por este medio. En cuanto a sus ventajas encontramos que, este espacio permite la apertura a una comunicación e interacción más rápidas, acceso y difusión del conocimiento (Herrera, 2020), libertad de expresión, activismo social, comercio

[1] En el año 2016 se llevó a cabo la cumbre de Varsovia con participación de los Jefes de Estado y de Gobierno miembros de la Alianza del Atlántico Norte. La información se encuentra disponible en: https://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber

electrónico, por mencionar algunas. Sin embargo, también presenta ciertas desventajas, que en un futuro suelen generar ciertas problemáticas, las cuales son tomadas muchas veces a la ligera, sin embargo, prevén un riesgo a la seguridad del ciberespacio como por ejemplo: robo de datos personales, ataques y delitos cibernéticos, vulnerabilidad a la privacidad e incluso acciones que cuentan con la capacidad de atentar contra la seguridad de los Estados.

El punto de partida -y quizá el más alarmante- es que este ambiente de comunicación no reconoce una frontera geográfica como tal que lo delimite ni tampoco una restricción en cuanto al manejo de la libertad de expresión e información que proporciona. Una de las tantas causantes, es la falta de una regulación y normatividad en el ciberespacio que atiendan a los nuevos fenómenos alarmantes: ciberataques, el ciberterrorismo, la ciberguerra, los ciberdelitos[2], ciberamenazas, ciberespionaje y hacktivismo, entre otros conceptos que merecen la pena ser estudiados a fondo en futuras investigaciones. Ahora bien, estas consideraciones antes expuestas, tienen que ser mencionadas en esta presentación de resultados de mi investigación, porque las dos variables principales –ciberseguridad y ciberdefensa– tienen, de manera conjunta, la capacidad de dar respuesta a estas problemáticas que se desarrollan en el ciberespacio.

Considerando lo anterior, me gustaría plantear por qué, hoy en día, la ciberseguridad y la ciberdefensa deben ser puestos en la agenda pública de cualquier país, incluso como un tema que concierne directamente a la seguridad nacional. La seguridad de un Estado se ve expuesta a las amenazas que surgen dentro del ciberespacio, sin dejar de lado las cuestiones técnicas y operativas, que deben mantenerse en constante actualización, porque los ciberdelitos cometidos en el ciberespacio van un paso delante de cualquier ley que los regule. También

[2] Si bien los términos de *cibercrimen* y *ciberdelito* se refieren a un conjunto de conductas que vulneran los derechos de terceros en un escenario tecnológico, Coronado (2021) dice que se emplean usualmente como sinónimos. Este autor recalca la importancia de atenderlos de manera distinta, puesto que en el área del derecho el primero se refiere a un fenómeno social, mientras que el concepto de ciberdelito está inmerso en un ámbito jurídico y se enfoca en conductas que están reguladas por algún cuerpo normativo.

están por encima de la protección de los sistemas de seguridad en la red y de quienes atentan contra el ciberespacio.

Por lo tanto, las problemáticas a las que se enfrenta la sociedad adquieren un valor significativo que, si no se les entiende a tiempo, generan un ciberespacio vulnerable y expuesto a amenazas e incapacidades defensivas. Ello ocasionaría que el problema avance de manera exponencial y sin previo aviso. Ospina y Sanabria (2020) han dicho que los problemas de ciberseguridad (como un derivado de la ciberguerra) tienen la característica de no reconocer a bandos de contienda, ya que diversos actores se ven envueltos, como por ejemplo: acciones de gobiernos en contra de los ciudadanos, disputa entre partidos políticos, carreras empresariales, disputa entre ejércitos, entre otros. Arreola (2019) señala que la ciberseguridad[3] debe encargarse de proteger todos los datos inmediatos que entran al ciberespacio, y, especialmente, si estos contienen información sensible. Una característica esencial de la ciberseguridad es que cuenta con sistemas operativos, medios de comunicación, planes nacionales, innovaciones e infraestructura estratégica.

Con lo mencionado en el párrafo anterior, el autor percibe una idea del papel de la ciberseguridad en cuanto a su característica de vigía en el ciberespacio. Por su parte, también ofrece una definición, que puede entenderse como:

> El intento de la sociedad por salvaguardar la continuidad de sus operaciones en el ciberespacio, a fin de garantizar la protección de sus secretos e información, el intercambio seguro de datos y la operatividad de sus sistemas computarizados dentro de la infraestructura de las tecnologías de la información y la comunicación (TIC).

[3] La ciberseguridad, seguridad informática y seguridad de la información, en ocasiones se emplean como equivalentes, ya que de manera conjunta, su función es la de “proteger”, sin embargo es importante mencionar que cada una cuenta con tareas distintas (Becerra y González, 2019), la ciberseguridad se basa en proteger la información digital, la infraestructura crítica y las TIC. Mientras que la seguridad informática solo los datos digitales y recursos de TIC que de estos deriven. La última se enfoca en preservar la confidencialidad, integridad y disponibilidad de la información tanto digital como física.

Simultáneamente existen algunos otros autores que han tratado de encontrar un significado de ciberseguridad, al igual que lo han hecho organismos internacionales, como, por ejemplo, la Unión Internacional de Telecomunicaciones (UIT)[4], quien menciona que la ciberseguridad es:

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

En la Estrategia Nacional de Ciberseguridad (2017), establecida para el caso de México, se define a la ciberseguridad como: “Un 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”. A su vez también apunta que la ciberdefensa es un “conjunto de acciones, recursos y mecanismos del estado en materia de seguridad nacional para prevenir, identificar y neutralizar toda ciberamenaza o ciberataque que afecte a la infraestructura crítica nacional” (ENC, 2017, p.28).

Cárdenas (2015), también ofrece otra concepción de lo significa la ciberdefensa. Él la entiende como la capacidad del Estado para cumplir con las responsabilidades que le permitan prevenir y contrarrestar toda amenaza o ataque

[4] Es un organismo perteneciente a las Naciones Unidas especializado en tecnologías de la información: TIC. Nacido en 1885 con la finalidad de desarrollar la conectividad internacional y herramientas tecnológicas.

de naturaleza cibernética que afecte los valores e intereses nacionales. Con dicha definición se estipula que la función principal de la ciberdefensa es conjuntar y mejorar herramientas tecnológicas para la defensa del ciberespacio (Arreola, 2019), puesto que ésta se orienta a las acciones de un Estado para proteger y controlar las amenazas, peligros o riesgos de naturaleza cibernética, con el fin de permitir el uso del ciberespacio con normalidad, bajo la protección de los derechos, libertades y garantías de los ciudadanos, en apoyo a la defensa de la soberanía y la integridad territorial (Vargas, Recalde y Reyes, 2017 p. 35).

Se entiende, por tanto, que el papel, en conjunto, de la ciberseguridad y la ciberdefensa es el de velar por la protección del ciberespacio. Sin embargo, cada una cuenta con características propias, el Ministerio de Defensa Española (2017), ve a la ciberseguridad como un objetivo y a la ciberdefensa como un medio para alcanzarla. La principal diferencia radica en que, por un lado, encontramos que la ciberdefensa tiene la capacidad de prevenir identificar y neutralizar toda ciberamenaza o ciberataque que afecte a la infraestructura crítica nacional (ENCS, 2017, p.13) y su actor principal es el Estado, el cual implementa mecanismos enfocados en materia de seguridad nacional. Simultáneamente en la ciberseguridad pueden participar ya sean organizaciones públicas o privadas que administren de forma organizada la cantidad de información que manejan objeto de posibles ciberataques.

Sin embargo, según Camacho (2017), se deben trabajar ambos conceptos para entender el contexto en el que se estudian y comprender que son fundamentales para su desarrollo. En el mismo, se ven inmersos, el compromiso internacional, la educación, la doctrina, las capacidades de investigación y la normatividad. Todo ello es de la mayor relevancia ya que son importantes para la evolución y protección de un país de posibles ciberataques.

Pese al esfuerzo que han hecho diversos autores, y algunos organismos internacionales en encontrar un significado a estos nuevos conceptos que emanan de las tecnologías de la información, el problema principal radica en que aún no se

encuentra estipulado como tal una concepción exacta que sirva de base en dichas definiciones. Las tecnologías generan constantes actualizaciones en donde se complejiza el tratar de definir cada concepto sin ambigüedad alguna. La tarea es propia no sólo de las futuras generaciones, sino también de las actuales, para así generar un espacio de comunicación seguro eficaz que vele por sus intereses y sin vulnerar los derechos de los individuos.

Tabla.1 Tipos de ataques y delitos que atiende la ciberseguridad y la ciberdefensa. Elaboración propia con información del Ministerio de Defensa.

Tipos de ataques	**Baja intensidad**	**Alta intensidad**
	Ciberseguridad	*Ciberdefensa*
Objetivos principales	• Vulnerar organismos de carácter público o privado e individuos aislados con diversos fines delictivos. • Presenta dificultades para determinar su origen o procedencia, aprovechando el anonimato. • La reacción que se espera es la adopción o reforzamiento de medidas por parte de los afectados.	• Afectar tanto organismos militares, como las infraestructuras consideradas como críticas de un país. • Mayores facilidades para identificar su origen o procedencia. • La reacción que se espera es una respuesta o acción bélica, ya sea en el ciberespacio o en los otros ámbitos de operaciones.
Jurisdicción	Autoridades policiacas responsables de materializar la Ciberseguridad en el ciberespacio.	Fuerzas Armadas, responsables de materializar la Ciberdefensa en el ciberespacio.
Principales delitos	El robo de identidad o suplantación, ataques a páginas web, ataques a la información bancaria y robo de dinero por vía electrónica.	Inutilización de sistemas de comunicaciones y de defensa antiaérea, extracción de información sensible considerada como confidencial o secreta y hasta ciberterrorismo.

1.2 Infraestructuras críticas y los ciberataques

El actual panorama en el ciberespacio, debido a su fácil acceso, permite la apertura a todo tipo de público. Con ello, se insertan actores que se han encargado de generar inseguridad en internet y que perpetúan los tan famosos "ciberataques." Éstos se entienden como: "cualquier acto que comprometa las expectativas de seguridad de un individuo, organización o nación" (Ghandi *et al*., 2011, citado en Azúa, p.63) y se caracterizan (Gamón, 2018) por el bajo costo que tienen, su fácil ejecución, efectividad y un riesgo reducido para quien lo emprende.

Normalmente los problemas en el espacio virtual se convierten en fenómenos complejos debido a su dimensión, y su forma tan tajante de poder infiltrarse, desde el anonimato, sumado a la facilidad de realizar alguna conducta delictiva en el ciberespacio desde cualquier parte del mundo. Esto genera que cualquier sistema de seguridad o protección sea endeble y provoque un impacto de forma directa en la ciberseguridad y ciberdefensa de los gobiernos e infraestructuras críticas. Éstas engloban tanto a la infraestructura pública y privada, cuyo funcionamiento es de vital importancia para el Estado o sociedad (Algora, 2019), las cuales no permiten soluciones alternativas (Cocchini, 2021), puesto que su destrucción o perturbación generan un grave impacto en los servicios esenciales.

Dichas infraestructuras tienen que ser protegidas en su totalidad debido a que Pages (2019) no se dimensiona de manera exacta la cantidad de ciberataques que se tienen documentados en las infraestructuras críticas que han sido vulnerados. Según el Centro Nacional de Protección de Infraestructura de Estados Unidos[5] (NIPC, 2013 en Pérez p.103), las define como: "aquellos sistemas físicos o cibernéticos esenciales para el mantenimiento vital de la economía, y el gobierno, incluyendo telecomunicaciones, energía, banca y finanzas, transporte,

[5] Redactado en el Plan Nacional de Protección de la infraestructura (NIIP), disponible en: https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

sistemas de agua potable y sistemas de emergencias, tanto públicos como privados".

El año pasado, 2020, debido a la Covid-19, la sociedad, en su mayoría se vio prácticamente obligada a utilizar herramientas tecnológicas y en la necesidad de aprender a sobrevivir en el ciberespacio. Con ello, se ha visto aumentada la cantidad de personas que ahora son cibernautas, puesto que todas las actividades presenciales tuvieron que cambiar su comportamiento.

Es así como las personas fueron asumiendo sus responsabilidades de manera virtual. Este panorama implicó también que aumentaran los ciberataques hacia la sociedad, tanto en el sector público como en el privado. No sólo esto debe considerarse, sino que también se han registrado ciberataques contra las infraestructuras críticas del sector salud y algunos organismos públicos, lo cual ha sido sumamente grave.

En general, los tipos de ciberataques más comunes y que han adquirido un avance considerable en los últimos años, aplicables también para el caso mexicano, son:

- Suplantación de identidad (*phishing*): Consiste en tratar que el usuario proporcione datos personales, por medio de un envío masivo de mensajes aparentemente provenientes de fuentes confiables. Los casos más típicos son por medio de correos electrónicos con mensajes provenientes de alguna institución bancaria (Téllez, 2009).
- *Malware*: Cualquier código maligno o software malicioso, cuyo objetivo es infiltrarse o dañar una computadora (Arias y Celis, 2015). Una vez instalado el virus, puede bloquear el acceso a los componentes clave de la red (ransomware), instalar malware o software dañino adicional, obtener información furtivamente mediante la transmisión de datos del disco duro (*spyware*) o alterar y hacer que el equipo sea inoperable (CISCO, 2020).
- *Rasonware*: Son códigos maliciosos que están diseñados para bloquear un acceso a los archivos electrónicos. Se considera un secuestro de

información, por la que se solicita un rescate para poder restaurar el acceso. (Roca y Torralba en De la Rosa, 2019).

- *Botnets*: Mejor conocidos como robots de la red, (Joyanes, 2015), son empleados para realizar ataques, espionaje contra empresas, spam. Este virus se puede instalar en los ordenadores sin que los usuarios logren percatarse del cometido, manteniendo así una red de alcance con el ciberatacante.
- Ataque distribuido de denegación de servicio (DDoS): El atacante puede controlar cientos de servidores con el objetivo de atacar a una computadora, regularmente estos ataques pretenden derribar algún sitio web. La manera en que opera es enviando paquetes de información al servidor hasta que este no pueda responderlos (Gómez, 2013).

Hoy en día, también se habla de que existen organizaciones ciberterroristas y hacktivistas que pueden ser respaldados por otro Estado y así atentar contra la seguridad y el funcionamiento de las infraestructuras críticas de otro Estado (Cocchini, 2021).

Uno de los primeros ataques cibernéticos que dañó la infraestructura del "mundo real", se registró en el año 2010 cuando un virus llamado Stuxnet se infiltró en una memoria USB, la cual se instaló en el programa nuclear de Natanz de Irán, dicho gusano tomó control de las máquinas centrifugadoras instaladas, ocasionando así que el uranio trabajado por dichos aparatos fuera aumentando su velocidad, provocando así su destrucción, se sabe que este virus fue diseñado especialmente para controlar la velocidad de las centrifugadoras. Lo curioso de este tipo de virus es que pueden insertarse en las computadoras sin alterar el sistema, ya que se registró un segundo ataque un mes después del primero. Si bien no se tiene con certeza quién fue el culpable del atentado, en el año 2011 el experto en seguridad informática Ralph Langner mencionó que el gusano fue creado en un laboratorio de Estados Unidos en conjunto con Israel para averiar el programa nuclear de Irán.

En el año 2020, se registraron algunos intentos de ciberataques realizados por los famosos “piratas informáticos” de algunos Estados, quienes pretendían lanzar ciberataques contra algunas farmacéuticas estadounidenses, surcoreanas y británicas y también a algunas compañías como: Astra Zeneca, Oxford y Johnson & Johnson, enfocadas en la cadena de suministro de vacunas contra el coronavirus. Si bien no se tienen datos oficiales de estos incidentes, con este ejemplo podemos corroborar la importancia que tiene un buen sistema de seguridad informático para proteger a las infraestructuras críticas, puesto que se encuentran en ocasiones muy expuestas y vulnerables.

Como se mencionaba, en el ciberespacio crecen las amenazas en materia de ciberseguridad y ciberdefensa, las cuales evidencian la necesidad de incorporar -y mejorar- nuevas formas de protección a las infraestructuras críticas. Sin embargo, se debe planear que la problemática principal es que los ciberataques crecen de manera exponencial, con lo cual van un paso adelante de las medidas en protección.

Además, existe la dificultad de articular mecanismos de colaboración entre otros actores involucrados como organismos públicos y privados para que puedan colaborar en mejorar a la ciberseguridad y ciberdefensa (Maestre, 2019). Si éstos decidieran colaborar entre sí, se podría construir un modelo eficaz de protección contra ciberataques a las infraestructuras críticas. Dichas amenazas son capaces de exponer y atentar contra la seguridad de un país, sin requerir de un esfuerzo considerable, o bien, sin usar algún tipo violencia física, ya que con un simple *click* los ciberdelicuentes y personajes delictivos de la red, pueden llegar a poner en tela de juicio la palabra “seguridad”, atentando así el bienestar de los Estados y la sociedad civil en el ciberespacio.

Por lo tanto, es importante que se desarrollen políticas públicas que garanticen la ciberseguridad (Blanco, 2016). Asimismo, es trascendental concientizar acerca de la importancia que tienen las infraestructuras críticas para evitar “efectos cascada” que en algún momento colapsen sistemas prioritarios.

Si bien la importancia y valoración que se tiene de las infraestructuras críticas han sido manifestadas en las agendas de los gobiernos en los últimos años, María del Rosario Rodríguez (2019) recomienda que los Estados diseñen un plan para contrarrestar amenazas a dichas infraestructuras, haciendo alusión de algunos elementos básicos que deberían plantearse para su elaboración, y que merecen la pena ser mencionados:

- Los actores que deben intervenir.
- De qué manera se debería actuar y cómo protegerse ante un daño intencionado.
- Los fundamentos que deberían ser foco de atención para los Estados, o bien organizaciones, como por ejemplo: el valor y la importancia de la infraestructura crítica,
- Las políticas, estrategias y la elaboración de un plan de acción estatal, con la capacidad de responder ante las amenazas.

1.3 El papel del Estado mexicano y la Seguridad Nacional en el ciberespacio

Históricamente, cuando se habla de Estado, como un tipo de comunidad política, ha sido delineado desde muchos espacios. Por ejemplo, comúnmente se le analiza como agente y actor protagónico, el cual proporciona seguridad y la propiedad privada. Asimismo, el Estado es indispensable para garantizar el orden de la sociedad y es aquel que procura el bien común. Los componentes del Estado son territorio, población y autoridad política, mientras que el rasgo más característico es la soberanía.

Sin embargo, se necesita de un requisito adicional para que un tipo de organización que tenga los tres elementos anteriores sea considerado un Estado, según Benítez y Chaparro (2008: 16): “tener el reconocimiento internacional; esto se cumple con el hecho de que un Estado ya reconocido reconozca al nuevo, ya

sea declarándolo, estableciendo relaciones diplomáticas o realizando tratados o convenios internacionales. Esta potestad supone la capacidad de decidir su destino con base a sus intereses nacionales".

Para las concepciones clásicas y modernas, estudiadas desde la ciencia política, se retoma la idea de Estado en autores como Weber, Kelsen, Bobbio, Hobbes, quienes lo ven como una entidad jurídico administrativa soberana que tiene el monopolio de la fuerza legítima (Perafán, *et al*, 2020), si bien esta concepción es vigente hasta hoy en día, derivado de las nuevas tecnologías y las transformaciones globales, la concepción clásica de Estado debe reformularse, para crear así, nuevas estrategias (Wendt, 2019,) contra riesgos de carácter global y regional con relación a la sobrevivencia de la población, en la nueva era digital. Tomando en cuenta aquellas acciones que le sigan dando la legitimidad que le es conferida, pero ahora aplicarla a este mundo tan actualizado, tecnológico y cambiante. Por supuesto sin dejar de lado, los principios básicos, como lo son: la seguridad, justicia y derechos fundamentales pero ahora trasladados al nuevo territorio sin fronteras geográficas, el ciberespacio.

En cuanto al concepto de Seguridad Nacional se ubica en la corriente "realista", desarrollada por Thomas Hobbes y Carl Schmitt y, de manera particular, por Hans Morgenthau. Entre los principios del realismo político, Morgenthau (1989: 63) señala que los Estados se encuentran en una lucha constante por el poder, donde la política exterior tiene la finalidad inmediata de mantener, aumentar o demostrar el poder de uno frente otro; además, que la lucha por el poder implica también la lucha por la supervivencia, por lo que la diplomacia, la defensa militar y las alianzas buscan garantizar el poder y la supervivencia del Estado frente a las amenazas del exterior (Buzan, en Montero, 2010).

Ahora bien, las responsabilidades del Estado en materia de Seguridad Nacional radican en preservar la legitimidad, proteger los intereses nacionales, hacer efectiva su soberanía y asegurar el desarrollo nacional. Esto obliga al Estado (Iturria,1980, p. 31) a ser corresponsable de la legitimidad a favor de sus

ciudadanos, mantener el prestigio internacional y la cohesión nacional que garantice paz, justicia y seguridad.

Existen medios e instituciones a cargo del Estado para garantizar la seguridad nacional de la que es responsable (Ministerio de Defensa, 2010). Por ello, podemos mencionar que el gobierno se basa en acciones como: la justicia, diplomacia e inclusive la política económica para protegernos. Y en caso de que fuese necesario, se puede hacer uso de la fuerza que se le confiere puesto que los Estados organizan la defensa de la seguridad.

La ciberseguridad es un componente muy importante de la Seguridad Nacional (Aimar, 2017), sino se controla adecuadamente el ciberespacio, desde allí puede ver una nación como es amenazada su libertad de acción y su seguridad, es decir, no sólo su ciberseguridad sino toda la Seguridad Nacional. La protección de los intereses vitales de una Nación y, especialmente, su supervivencia son los objetivos últimos e indiscutibles de los Estados. La articulación del Estado hoy en día se encuentra condicionada por el funcionamiento del ciberespacio, lo que vuelve a éste un dominio de gran importancia para la Seguridad Nacional (Katicoglu, 2019).

En el ciberespacio persisten cierto tipo de riesgos y amenazas, por ejemplo: causas técnicas, hacking, delincuencia, espionaje, crimen organizado, invasión extranjera, organizaciones terroristas (Pons, 2018), que atentan contra la seguridad nacional de los países. En el contexto que se vive en la actualidad, los Estados serán los encargados de decidir, en el ámbito de la ciberdefensa, si un ataque virtual, a un individuo u organización pública o privada, puede comprometer el desarrollo y la supervivencia de la nación (Vargas *et al*, 2017).

En cuanto a la noción de seguridad, ésta se ha transformado a través de los años y también se ha diversificado puesto que es aplicada en diversas índoles. Hoy en día se habla de la seguridad pública, seguridad jurídica, seguridad ciudadana, seguridad social, seguridad laboral, seguridad informática, etcétera. Por lo tanto, el término compete a distintas áreas de estudio. La seguridad tanto interna como

externa es responsabilidad intrínseca del Estado (Castro y Monteverde, 2018). Sin embargo, su significado se ha tenido que adaptar a las transformaciones de la sociedad y la globalización. Este último punto representa por sí solo un avance a las tecnologías. Dentro de los riesgos que hoy día se contemplan, están los que pueden ser una detonante para atentar contra la seguridad nacional, por ejemplo, aquellas vulnerabilidades que se presentan en el ciberespacio y donde se debe hacer énfasis en analizar a la seguridad nacional desde una perspectiva en la cual se involucre tanto a la ciberseguridad como a la ciberdefensa, puesto que son encargadas de proteger los intereses nacionales (Ministerio de Defensa, 2010).

> De acuerdo a la Estrategia Nacional de Seguridad Pública (DOF 16/05/19) y al Plan Nacional de Desarrollo (DOF 17/07/19), el Gobierno de México entiende a la seguridad nacional como una condición indispensable para garantizar la integridad y la soberanía nacionales, libres de amenazas al Estado, en busca de construir una paz duradera y fructífera (Centro Nacional de Inteligencia, 2018 p.1).

La Estrategia Nacional de Ciberseguridad (2017), en México, establece dentro de sus objetivos prioritarios la importancia de la seguridad nacional en el ciberespacio, donde su función principal es prevenir riesgos y amenazas que surjan en el ciberespacio y puedan alterar la integridad y la soberanía nacional que vulnere a los intereses nacionales (ENC, 2017).

Pese a que en ningún país se debe analizar y estudiar a la ciberdefensa como una problemática que sea ajena a la seguridad nacional, para el caso mexicano, los esfuerzos por garantizar que exista esa salvaguarda requieren de un mayor trabajo, teniendo en cuenta que, según datos del Banco Interamericano de Desarrollo (BID)[6], México cuenta con una puntuación aproximada de entre 2 y 3 en cinco áreas de evaluación con respecto a las etapas de madurez en la

[6] La organización se encargó de elaborar un estudio acerca de las capacidades cibernéticas, evaluando así, que tan preparadas se encuentran América Latina y el Caribe.

capacidad de ciberseguridad[7]. Sin embargo, se aconseja mejorar las estrategias en materia de ciberseguridad y ciberdefensa puesto que existen rezagos.

Por otra parte, no se sabe con exactitud el presupuesto que se destina a la ciberseguridad y la ciberdefensa en México. El Presupuesto de Egresos de la Federación para el ejercicio fiscal 2021, en el Ramo 38B[8], correspondiente a ciencia y tecnología, estipuló la cantidad de 26,573,104,028, sin embargo se debe aclarar que este presupuesto no especifica concretamente la cantidad que se emplea para ciberseguridad y ciberdefensa, pues sólo menciona que se destinará una parte a programas nacionales de ciencia y tecnología que estén vinculados con los sectores públicos y privados.

En los meses de septiembre y octubre de 2020, la policía cibernética de la Guardia Nacional registró 2 mil 218 reportes de ciberataques de ciudadanos, 7 mil 964 incidentes de seguridad a instituciones públicas, privadas y algunas universidades del país (Réyez, 2020).

Adolfo Arreola, experto en ciberseguridad e investigador de la Universidad Anáhuac México, menciona que el costo de un cibercrimen, al menos para el año 2021, tiene un valor aproximado de entre 3 y 6 millones de millones, trillones, trillones de dólares, lo que resulta una cantidad impresionante y preocupante. Además, afirma que México debe renovar su legislación involucrando así los nuevos conceptos que emanan de las tecnologías de la información, respetando los derechos humanos y haciendo frente a una colaboración entre sector gobierno, sector productivo, sociedad y cooperación internacional, también recomienda desarrollar planes de educación digital (Arreola, en Romero, 2020).

---

[7] La cinco etapas son: *inicial (no existe la madurez en ciberdefensa),* formativa (existen las primeras evidencias en este tema), *consolidadas (la etapa comienza a funcionar y está definida), *estratégica (se han realizado algunas acciones por parte del Estado u organizaciones) y *dinámica (rápida toma de decisiones ante posibles amenazas).

[8] El Ramo 38-B está compuesto por el Consejo Nacional de Ciencia y Tecnología, cuyos gastos son referidos principalmente en apoyo a la investigación científica, desarrollo e innovación, becas de posgrado y apoyos a la calidad, además de Programas nacionales de ciencia, tecnología y vinculación con el sector social, público y privado. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/PEF_2021_301120.pdf

De igual manera, ya lo mencionaba el coronel Lira Hernández (2015), que “en México se debe redefinir la estrategia, en coordinación con los sectores públicos y privado, adoptando acciones para detectar las amenazas, establecer sistemas de respuesta y recuperación ante eventualidades; así como fomentar la cooperación internacional”.

1.4 Soberanía en el ciberespacio

Según Von Heinegg (2013), cuando hablamos de soberanía territorial, estamos hablando de independencia. Dicha independencia de un territorio es primordial para ejercer funciones de forma exclusiva ante cualquier otro Estado. Con base en esa definición, se puede decir entonces, que la soberanía que se requiere en el llamado “ciberespacio” ahora se ve permeada y no cumple con esa forma característica de ser “independiente”, como lo menciona (Katicoglu, 2019 p. 26) :

> Los espacios tradicionales donde se desarrollaron históricamente los fenómenos que acechan a la seguridad internacional hoy se han visto complementados por un nuevo espacio en el que es imposible hablar de soberanía territorial en términos clásicos. La inmensidad de lo virtual y sus posibilidades generan que el ambiente informático sea escenario de criminalidad organizada y compleja. Delitos de los cuales antes sólo nos preocupábamos dentro de nuestras fronteras nacionales, hoy terminan sumergiéndose en las posibilidades que ofrece el ciberespacio para su propagación, financiamiento, reclutamiento, propaganda y solidificación.

Por otro lado, la soberanía se refleja en la necesidad de tener habilidades científicas, técnicas y operativas, pero también capacidades industriales. Ya que (Ministerio de Defensa de Francia, 2017), un ataque a los sistemas de información podría plantear una cuestión importante de soberanía en el caso de una toma de control o una parálisis de sectores vitales para el Estado. Con lo que se traduce (Valls, 2015) en que los Estados que no dispongan de la autonomía necesaria en el sector digital verán amenazada y vulnerada a su soberanía.

El Informe de Amenazas y Tendencias (2019), revela que todos los sistemas de información con acceso a internet resultan vitales para las economías nacionales, y pueden dar pauta a una controversia entre los Estados; si estos son alterados o vulnerados, representan riesgos ilimitados a la soberanía de los países, como es el caso de ataques nucleares, satélites espaciales, instalaciones de navegación aérea, industrias y plantas químicas además de ataques con fines políticos, sociales, etcétera.

Simultáneamente, se contemplan varios registros en el pasado de la manera en que un ciberataque puede atentar contra la soberanía de un Estado. Uno de los casos más conocidos fue la ocasión en que se culpó a Rusia por haber utilizado a hackers informáticos, un operador político y el sitio web de WikiLeaks con la finalidad de socavar las elecciones presidenciales de Estados Unidos en el año de 2016, utilizando así estas herramientas para ayudar a ganar a Donald Trump, filtrando información perjudicial contra Hillary Clinton. Para el año 2018 se reabrió la investigación contra dos empresas rusas a las que se les culpaba por el sabotaje en las elecciones, pero a principios del año 2020 el Departamento de Justicia de Estados Unidos retiró los cargos.

Ya se mencionaba con anterioridad que el ciberespacio es visto como un nuevo campo de batalla. Sin embargo, sería importante analizar el caso anterior, tomando en cuenta cuatro perspectivas que se deben considerar cuando se tiene este tipo de problemáticas, haciendo alusión a la Teoría de la Guerra (Aguilar, 2021), y son las siguientes:

a) Ver al ciberespacio como un campo de batalla.
b) Confrontar la idea de que existen varios actores involucrados.
c) Existen ciberarmas que cuentan con categorías de espacio, tiempo y fuerza.
d) Establecer la idea central para darle un enfoque al ciberespacio como un teatro de guerra o de operaciones.

Si bien estas ideas anteriores permiten construir un nuevo escenario capaz de establecer los mecanismos principales que se presentan ante los fenómenos que surgen en el ciberespacio, aún sigue pendiente la variable principal a resolver, es decir: cuál es el organismo, el ordenamiento jurídico y la autoridad responsable a las que se les confiere la habilidad y capacidad para resolver este tipo de nuevas disputas, que, lejos de ser vistas como algo lejano a la realidad, hoy en día presentan nuevos panoramas que dan cabida a nuevos conflictos derivados de las tecnologías de la información.

Considerando que el organismo autónomo auténtico tiene que ser el Estado, es importante mencionar que, sin perder su capacidad de ente legítimo, podemos contemplar la idea de que este puede apoyarse de la sociedad civil y privada, además de un modelo jurídico (Robles, 2015) que se construya en un contexto normativo y aplicable para el ámbito global de manera autónoma, que permitan una mejor distribución en los poderes, y así tener capacidad para contrarrestar los factores que no permiten un ciberespacio seguro y eficaz.

Muchas veces se subestiman estas problemáticas que surgen a raíz del ciberespacio. Sin embargo, es fundamental recalcar que es una urgencia a la soberanía de los Estados, puesto que a medida que la sociedad se expande y se vuelve más dependiente del ciberespacio, se deben crear nuevos mecanismo de defensa que permitan salvaguardar y proteger dicha soberanía. Pareciera que se retoma aquel paradigma internacional que hace alusión a garantizar la paz y disuadir las guerras, pero esta vez en un nuevo territorio, el ciberespacio.

El gran problema del ciberespacio es precisamente que “rompe” con muchos conceptos tradicionales como territorio y soberanía, ya que no existen límites geográficos establecidos, no hay un compromiso internacional (un tratado) que señale que ley se debe seguir, ni cuáles son los límites para la defensa.

Si hacemos una analogía con respecto a las nuevas tecnologías y lo trasladamos a conceptos jurídicos, políticos y sociales, podemos decir que la ciberseguridad y la ciberdefensa, son consideradas hoy en día por los nuevos investigadores

sociales como aquellos elementos fundamentales (Perafán *et al*, 2020) a través de los cuales los Estados ejercen su soberanía.

Ahora bien, cuando se estudia a la soberanía desde el enfoque de la teoría política y el derecho, podemos retomar a uno de sus clásicos precursores, Jean Bodin, en una de sus grandes obras, *Los seis libros de la República*, donde, entiende a la soberanía como "el poder absoluto y perpetuo de una República"; o bien, a Hobbes, en *El Leviatán*, que refiere la función del soberano como el que procura la seguridad del pueblo, legítimo trabajo y sin peligro para el Estado. Mientras que Rousseau, en *El Contrato Social*, habla del soberano, cuyo poder recae en un conjunto de ciudadanos, es decir, el pueblo mismo. Sin embargo, nos encontramos con la problemática de estudiar la soberanía desde la perspectiva de las nuevas tecnologías, además de que existe la cuestión de focalizar la atención en *quién es ahora el soberano en este llamado ciberespacio*.

De forma similar, en consideración las ideas de dos grandes pensadores, Hans Kelsen y Carl Schmitt, el primero menciona que la soberanía tiende a ser una propiedad característica que emana de un ordenamiento jurídico que es aceptado por la sociedad y además es vigente, donde si bien la soberanía está en el pueblo, una vez trasladado a ese orden jurídico, el poder soberano recae ahora sobre el cuerpo normativo o Constitución; el segundo retoma la idea de estudiar a la soberanía desde la coyuntura o el momento histórico en el que la sociedad se encuentra. Podría decirse entonces, *que Kelsen se enfoca en tratar de explicar el concepto de soberanía*, mientras que *Schmitt quién es el soberano* (Montoya y Montoya, 2015). Anteriormente, ya se mencionaba *lo importante que es encontrar aquellos mecanismos que nos indiquen quién será ahora el nuevo soberano legítimo, con la capacidad de juzgar las conductas delictivas perpetradas en el ciberespacio.*

En el año de 1996 se redactó la Declaración de Independencia del Internet por John Perry Barlow; se hizo un llamado a los gobiernos para que no se asumiera que dentro del ciberespacio existía una soberanía (Arreola, 2021).

A medida que transcurre el tiempo, existen autores interesados en temas tecnológicos, estudiados desde el ámbito social, político y jurídico, los cuales hacen alusión a la importancia que tiene una regulación en el ciberespacio, como por ejemplo, Laura Coronado (2017b) y Emilio Suñé (2015), quienes proponen dos acciones fundamentales y necesarias: una Declaración de los Derechos del Ciberespacio y una Constitución del Ciberespacio.

En concreto, sin dejar de lado a los elementos constituyentes de la soberanía, pero ahora aplicados al ciberespacio, se debe considera que (Sanz, 2010):

1. Es fundamental la protección del espacio sobre los que el Estado ejerce su respectiva jurisdicción y soberanía.
2. Se debe hacer frente a la capacidad que tiene el Estado para ejercer su autonomía y efectividad desde las acciones tomadas en el gobierno.
3. Reconocer la identidad que tiene la soberanía, donde se agrupan recursos que son intangibles del Estado, que permitan la cohesión en los valores y derechos fundamentales de la sociedad.

1.5 Caso mexicano: problemática en ciberdefensa y ciberseguridad

Si bien México, en el año 2018, según datos de la UIT, se encontraba en la posición número 63 en el índice de Ciberseguridad Global (GCI)[9], en cuanto al nivel estratégico en materia de ciberseguridad. Para el año 2020, México se sitúo en el lugar 52, con una puntuación de 81.68, en una muestra representativa de 182 países analizados. Sin embargo, pese a los esfuerzos empleados, estos son decadentes, puesto que se ha visto que en los últimos años los ciberataques y delitos informáticos han ido incrementando. Pese a los intentos realizados, y como se menciona anteriormente, la red maneja un sin fin de información y datos personales que pueden originar algún tipo de inconveniente si la información es mal utilizada.

A pesar de las ventajas que ofrece el ciberespacio, también puede ser un medio de riesgo, con lo cual se debe prever que exista un sistema de defensa que permita la colaboración del gobierno, las empresas y el público en general. Cano y Rocha (2019) hablan acerca de las amenazas, riesgos y disrupciones en el ciberespacio, y donde surgen a su vez nuevos retos para la ciberdefensa y la ciberseguridad, porque ya no es suficiente entender las amenazas, sino que se necesita una constante actualización en cuanto a las propuestas que permitan proteger, asegurar, defender la información que se encuentra en este espacio virtual, para así generar una respuesta eficiente a una serie de escenarios desconocidos e inciertos a los que se enfrentan los países y organizaciones.

El primer documento creado en México en materia de tecnologías de la información fue la Agenda Digital de México (2009) que estableció como primer objetivo unificar los conceptos relacionados con el mundo digital y con las TIC. Esta agenda se basa en cuatro apartados principales: marco político y jurídico

[9] Sus objetivos principales se basan en identificar las brechas, incentivar y fomentar prácticas que proporcionen herramientas e información para que los países se transformen y creen mecanismos necesarios para la seguridad cibernética (UIT, 2021).

para el desarrollo del entorno digital, acceso digital, gobierno electrónico, desarrollo empresarial y las TIC.

Anteriormente se hizo mención sobre la importancia de establecer mecanismos de defensa para que los ciberataques no atenten contra la seguridad nacional de un país mediante una estrategia de ciberseguridad y ciberdefensa. Sin embargo, debido a que los seres humanos se encuentran expuestos en el ciberespacio, en México se han creado organizaciones y autoridades encargadas de contrarrestas la ciberdelincuencia, entre los que se encuentran:

- División Científica de la Coordinación para la Prevención de Delitos Electrónicos. Es un organismo que opera el equipo de respuesta e incidentes de seguridad informática en México. Se encarga de "prevenir, investigar y perseguir conductas antisociales e ilícitas en internet. (De la Rosa, 2019).
- SEDENA, que entre sus funciones se encuentra la de fortalecer las capacidades del Centro de Operaciones del Ciberespacio en contra de incidentes de ciberseguridad hacia la infraestructura crítica de la Secretaría de la Defensa Nacional.

Además de algunos documentos expedidos en los últimos años de carácter oficial que ofrecen breves descripciones y actos implementados en materia de tecnologías de la información, ciberseguridad y ciberdefensa:

- Programa Sectorial de Marina (2013-2018): pretende fortalecer la Seguridad de la información y del Ciberespacio, así como consolidar la inteligencia Naval para identificar, prevenir y contrarrestar riesgos y amenazas que afecten a la Seguridad Nacional:

1. Elaborar el diagnostico Insitucional de Seguridad de la Informacion, Ciberdefensa y Ciberseguridad (DISICC).
2. Elaborar e implementar las Estrategias Institucionales de Seguridad de la Información, CIberdefensa y Ciberseguridd (EISICC).

3. Modernizar con equipamiento, capacitación y tecnologías el Sistema Integral de Seguridad de la Información Institucional acorde a la Estrategia Nacional.
4. Construir un Centro de Control de Ciberdefensa y Ciberseguridad para fortalecer la cuarta dimensión de Operaciones de Seguridad.
5. Fortalecer la coordinación interinstitucional para impulsar la Estrategia Nacional de la Seguridad de la Información.

- Estrategia Nacional de Ciberseguridad (2017), cuyos objetivos principales son:

1. Identificar y establecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas.

2. El uso y aprovechamiento de las tic de manera responsable para el desarrollo sostenido del Estado Mexicano.

3. Si bien, en el marco internacional, las Estrategias Nacionales de Ciberseguridad, se consideran para los países, un avance en la protección ante amenazas en el ciberespacio, y que se deben fundamentar como asuntos prioritarios. Hay que mencionar que, en el actual gobierno de López Obrador, no se han realizado modificaciones o bien no se ha concretado de manera oficial si va a proseguir con dicha estrategia, sin embargo, sigue siendo de carácter vigente.

- Programa para un Gobierno Cercano y Moderno (PGCM) prevé la necesidad de: contar con un gobierno orientado a resultados, eficiente, con mecanismos de evaluación que permitan mejorar su desempeño y la calidad de los servicios; que simplifique la normatividad y trámites gubernamentales, rinda cuentas de manera clara y oportuna a la ciudadanía, que optimice el uso de los recursos públicos, y que utilice las nuevas tecnologías de la información y comunicación. Establecer una

Estrategia Digital Nacional para fomentar la adopción y el desarrollo de las tecnologías de la información y la comunicación, e impulsar un gobierno eficaz que inserte a México en la Sociedad del Conocimiento.

- Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI, 2018) ,las dependencias y entidades de la Administración Pública Federal están obligadas a comunicar al Centro Nacional de Inteligencia (CNI), para efectos de su registro los datos de los servidores públicos que designen como Responsables de la Seguridad de la Información, de los Enlaces responsables de mantener comunicación con los Equipos de Respuesta a Incidentes de Seguridad en TIC, y de las personas autorizadas para conocer información de seguridad nacional, en razón de su empleo, cargo o comisión, relación contractual o de cualquier otra naturaleza, así como el nivel de diseminación al que tengan acceso.

- Estrategia Digital Nacional (2013-2018): guía todas las acciones del Gobierno de la República en materia de digitalización, y a partir del cual se medirán los avances, logros y retos en este ámbito. El propósito fundamental de la Estrategia es lograr un México Digital en el que la adopción y uso de las TIC maximicen su impacto económico, social y político en beneficio de la calidad de vida de las personas.

- Estrategia Digital Nacional (2021-2024): se fundamenta en la capacidad del gobierno en atender los requerimientos para una gobernanza tecnológica, mejorar y optimizar servicios digitales, así como disminuir la brecha digital, basada en cinco principios fundamentales:

    1. Principio de Austeridad
    2. Principio de combate a la corrupción
    3. Principio de Eficiencia en los Procesos Digitales
    4. Principio de Seguridad de la información
    5. Principio de Soberanía Tecnológica

- Plan Nacional de Desarrollo (2019-2024): en cuanto a las funciones de las FF.AA. Repensar la seguridad nacional y reorientar a las Fuerzas Armadas. El Ejército Mexicano y la Armada de México conservarán sus tareas constitucionales en la preservación de la seguridad nacional y la integridad territorial del país, la defensa de la soberanía nacional y la asistencia a la población en casos de desastre; asimismo, los institutos armados seguirán aportando a diversas esferas del quehacer nacional: aeronáutica, informática, industria, ingeniería, entre otras.

- Programa Sectorial de Marina 2020-2024: su estrategia prioritaria, es fortalecer las capacidades de seguridad en el ciberespacio para coadyuvar con la seguridad nacional y seguridad interior, alude a la importancia en:

- Desarrollar el fortalecimiento de las acciones institucionales en materia de ciberseguridad para la integridad y permanencia del Estado mexicano.
- Promover el marco jurídico con la finalidad de actuar para el establecimiento conforme a derecho en materia de ciberseguridad.
- Reducir la vulnerabilidad cibernética con la cooperación del sector público, privado, académico y con otras FF. AA. con la finalidad de salvaguardar la seguridad nacional e interior.

Por otra parte, no sólo en México, sino alrededor del mundo, los ciberataques se incrementaron a causa principalmente por la Covid-19, ya que las actividades de común asistencia se trasladaron ahora al ciberespacio, como fue el *Home Office*, el aumento de servicios públicos y privados que se ofrecen por internet, clases virtuales, etcétera. Aunado a esto, la falta de una cultura de seguridad digital hace que las personas se vuelvan objeto de sufrir algún tipo de ciberataque. Actualmente, el Centro de Operaciones del Ciberespacio Mexicano (COCEM) que opera la Sedena, a partir del año 2016, así como el Centro Nacional de Respuesta

a Incidentes Cibernéticos, que está a cargo de la Guardia Nacional, han sumado sus esfuerzos para así prevenir y contrarrestar los ciberataques (Camacho, 2021).

Es relevante mencionar que, si bien las estrategias implementadas requieren una constante actualización y mejoras debido a que el panorama en el ciberespacio se dificulta, puesto que las amenazas crecen y cada día existen nuevas formas de atentar contra la seguridad de un país, México debe implementar leyes que regulen los ciberdelitos, porque no existe una legislación específica que los castigue y sancione (Coronado, 201b). Sin embargo, cuenta con los siguientes ordenamientos jurídicos que se encargan de las faltas cometidas en el ciberespacio o bien en medios electrónicos:

- Código Penal Federal
- Ley Federal de Telecomunicaciones
- Ley de Instituciones de Crédito
- Ley General de Títulos y Operaciones de Crédito
- Ley del Mercado de Valores
- Ley Federal de Derechos de Autor
- Ley de Protección a la Propiedad Intelectual
- Reglamento de la Ley Federal de Derechos de Autor
- Ley Federal de Protección de Datos
- Códigos Penales de las entidades federativas.

1.5.1 Marco internacional, estrategias, lineamientos jurídicos en materia de ciberseguridad y ciberdefensa

Como se mencionó anteriormente, el desarrollo de las nuevas tecnologías de la información y la comunicación permite la apertura a ciertas ventajas que facilitan la vida y acciones del ser humano, pero a la vez presentan algunas problemáticas de carácter social, ético, cultural, político etcétera, que no solo tienen un impacto de manera local sino global, debido a la velocidad en la información y datos que

viajan en el ciberespacio es importante (Fernández, 2014), por lo que los países y las organizaciones internacionales deben reflexionar sobre la mejor manera de hacer frente a los desafíos que enfrentan. Teniendo en cuenta que la mejor manera de contrarrestarlos es con bases sólidas en cuanto a sus estrategias de ciberseguridad y en conjunto con la ciberdefensa de cada estado. Puesto que es un tema complejo de tratar debido a que se encuentra en constante cambio, se presenta también como un desafío que enfrentan los Estados (Vercelli, 2009).

Si bien estos conceptos son relativamente recientes, algunos países han visualizado la importancia de hacer frente a los ciberataques y ciberdelitos elaborando mecanismos estratégicos para contrarrestarlos. Sin embargo, pese a los esfuerzos, aún falta mucho por hacer, ya que los problemas que estas amenazas presentan generan que en el ciberespacio persista en ser un lugar incompletamente seguro expuesto a todo tipo de amenazas.

Actualmente, se han creado herramientas internacionales que, si bien son muy generales, dan pauta a un avance en materia de ciberseguridad y ciberdefensa; las principales son:

Tabla 2. Reglamentos internacionales en el ámbito de la ciberseguridad y la ciberdefensa. Elaboración propia con base al autor Coronado (2021).

Documento	Vigor	Objetivos
Convenio sobre ciberdelincuencia del Consejo Europeo (Convención de Budapest)	1 de julio 2004	• Combatir el crimen organizado. transnacional de los delitos informáticos. • Establecer una legislación penal para proteger a la comunidad internacional. • Fortalecer el Estado de Derecho en el ciberespacio. • Lucha contra el racismo, discriminación racial, xenofobia e intolerancia en internet.
	8 de junio de	• Incrementar la seguridad de las redes e

Resolución AG/RES 2004 (XXXIV-O/04) de la Asamblea General de la Organización de Estados Americanos.	2004	internet, para proteger a los usuarios, la seguridad nacional y las infraestructuras críticas. • Establecer grupos nacionales de "vigilancia y alerta": Equipos de Respuesta a Incidentes de Seguridad en Computadoras (CSIRT).
Decisión 587 de la Comunidad Andina	10 de julio de 2004	• Prevenir, erradicar y combatir las amenazas a la seguridad a través de la cooperación y coordinación que hagan frente a los desafíos hacia la comunidad.
Consejo en materia de Ciberseguridad de la Unión Internacional de Telecomunicaciones	3 de noviembre 2010	• Promoción del examen de los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones
Resolución 64/25. «Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional»	2 de diciembre 2010	• Mantener una inteligencia gubernamental y militar contra ataques cibernéticos tanto internos como externos y mantener vigilancia permanente en la red, implementar aplicaciones inteligentes cibernéticas en materia de seguridad.
Exhortación de la Asamblea General a los Estados Miembros	18 noviembre 2020	• Promover el examen multilateral de las amenazas reales y potenciales en el ámbito de la seguridad de la información y de posibles medidas para limitar las amenazas que surjan en ese ámbito, de manera compatible con la necesidad de preservar la libre circulación de información.

Para el caso de América, solamente hay 13 países que se han encargado de la creación de *equipos de respuesta a incidentes o emergencias de seguridad cibernética* (CSIRT); el término proviene de las siglas en inglés Computer Emergency Response Team, y define a un equipo de personas (CN-CERT, 2020) dedicado a la implantación y gestión de medidas preventivas, reactivas y de gestión de la seguridad, con el objetivo de mitigar el riesgo de ataques contra las redes para ofrecer soluciones de cualquier incidente y sus efectos, en el menor tiempo posible. También es conocido por las siglas CSIRT (Computer Security and Incidente Response Team) y tiene muchas similitudes con el Centro de Operaciones de Seguridad (SOC, en inglés).

Los países en el continente americano que cuentan con un CSIRT son: Argentina, Bahamas, Barbados, Bolivia, Brasil, Canadá, Chile, Colombia, Costa Rica, Ecuador, Estados Unidos, Guatemala, Guyana, Jamaica, Panamá, Paraguay, Perú, Surinam (en proceso), Trinidad y Tobago, Uruguay y Venezuela. Y, mundialmente, se encuentran reconocidos 55 grupos de respuesta a emergencias cibernéticas nacionales (Coronado, 2021), los cuales, con ayuda del gobierno, se han enfocado en construir nuevas Estrategias Nacionales, las cuales pueden contribuir en cierta medida a fortalecer un marco normativo en el cual los países puedan organizar sus iniciativas de ciberdefensa y ciberseguridad.

CAPÍTULO II. GOBERNANZA EN EL CIBERESPACIO, COMPARATIVA DE LOS MODELOS DE CIBERSEGURIDAD Y CIBERDEFENSA EN CHINA, ESTADOS UNIDOS Y LA UNIÓN EUROPEA

2.1 Gobernanza en el Internet

El mundo, desde aquel noviembre del año 2019, cuando se dio a conocer al paciente cero de la pandemia provocada por el virus SARS-CoV-2, se convirtió en un escenario de incertidumbre, sumado a los problemas sociales que nos acomplejan como, por ejemplo, al cambio climático, la pobreza, la desigualdad, inseguridad, delincuencia, discriminación, machismo y violencia contra la mujer, entre muchos más. Una de las consecuencias que ha provocado la pandemia es que los seres humanos buscarán otro estilo de vida, el cual se encontró, convirtiéndonos en cibernautas. Aunque claro, el espacio en el que habitamos ya estaba inmerso en la tecnología y las relaciones sociales virtuales (Bartolomé y Monteiro, 2020), estas han crecido en última década, y debido a la pandemia, acrecentaron de manera exponencial, para así formar parte de la vida cotidiana y la rutina presencial, convirtiendo al ciberespacio en un lugar común para el trabajo, la educación, la salud, la economía, el entretenimiento social, entre muchos más campos de actividad humana.

En la actualidad, según datos de la Asociación de Internet MX[10] se menciona que existen 87.4 millones de usuarios conectados a internet en México, es preciso seguir recalcando, que debido a la Covid-19, este número se incrementó en un porcentaje de 74% en cuanto a la injerencia de la población con actividad en internet, los datos se construyen a partir de un rango de 6 años en adelante.

[10] Dicha asociación se encarga de afiliar empresas con alguna actividad en línea, además elabora de manera anual estudios en temas tecnológicos como por ejemplo: redes sociales, comercio electrónico, hábitos en internet, protección de datos personales, entre otros.

Por otro lado, el Banco Mundial informa que el porcentaje de usuarios conectados a internet de manera global, hasta el año pasado, 2020 era de 56.72%. Mientras que, para el primer trimestre de 2021, Internet World Stats (IWS) en su análisis, muestra un porcentaje al alza, dando como resultado un 69.9% de usuarios en internet. Si bien este parámetro, indica un acercamiento a lo que implica estar interconectados socialmente, a simple vista se aprecia como una ventaja para el desarrollo y alcance de las tecnologías de la información. Se pensaría entonces, que el mundo se está volviendo un lugar que aproveche cada vez más las tecnologías.

Sin embargo, existen ciertos fenómenos contradictorios, que refutan lo anteriormente mencionado como por ejemplo, la brecha de acceso a internet, además de que (Pisanty y Velasco, 2021), la expansión de Internet, más allá de favorecer al ámbito gubernamental y académico, puede ocasionar litigios costosos y responsabilidades que no se sabe con exactitud si el gobierno por sí solo podría enfrentar, puesto que en internet no se tiene noción sobre quién gobierna a esos muchos en el ciberespacio, ni mucho menos se tiene un control sobre las actividades que operan las reglas del juego en él.

Las tecnologías de Información y la Comunicación e Internet han facilitado el funcionamiento de los sistemas políticos democráticos, (Galindo, 2012), tal es el caso del proceso electoral[11], ofrecer servicios públicos[12] mediante plataformas digitales, apoyo en el funcionamiento del poder judicial, entre muchas otras actividades.

Según lo mencionado por Esterhuysen (2015), la Red tiene que ser regulada como si fuese un bien público global. Lo que en años anteriores se veía como una forma de comunicación elitista entre instituciones académicas y militares estadounidenses principalmente, hoy en día, el ciberespacio se transformó en un

[11] El uso de las TIC no solo funciona como uso de propaganda electoral, sino que algunos países han implementado el ya tan popular voto electrónico.
[12] Lo que se conoce como Gobierno Electrónico (GE), que según la CEPAL, es una transformación de todo el gobierno hacia un paradigma en gestión gubernamental que utiliza a las TIC para mejorar sus servicios y fundamenta su aplicación en la Administración Pública.

recurso público y global que requiere de la participación de los gobiernos. Lo que conlleva a que estos busquen la manera de ejercer un control en su utilización y gobernanza de la propia red.

Lo aludido anteriormente trae consigo también la apertura a conflictos de carácter público y político, y que, si bien no son asuntos recientes, debido al coronavirus (Cornejo y Segura, 2021), la palabra gobernanza ha adquirido de nuevo relevancia para problemas complejos que se presentan en las nuevas Tecnologías de la Información. Así mismo, “Tanto políticos como politólogos, en numerosos subcampos y contextos político-administrativos, se han acogido a la idea de gobernanza como una nueva manera de pensar sobre las capacidades estatales y las relaciones entre el Estado y la sociedad” (Peters y Pierre, 2005 p. 37).

En el capítulo previo, se mencionaba la importancia del Estado en su papel protagónico en el ciberespacio, sin embargo, hoy en día, sabemos que debido a los fenómenos tan complejos que se presentan en él, se debe hacer alusión a la idea de que es fundamental y necesaria la participación de otros actores que se involucren en la protección y seguridad de la sociedad dentro de este metaespacio, para así lograr contrarrestar de manera considerable los problemas sociales, políticos, económicos, entre muchos más que surgen a raíz del territorio sin fronteras, mejor conocido como ciberespacio.

Por otro lado, el interés de los Estados en el ámbito tecnológico se basa principalmente en su capacidad de intervenir en la administración del internet, analizando sus perspectivas a nivel local y global, buscando siempre que los beneficios que éste ofrece sean equitativos para sus ciudadanos. Sin embargo, se debe tomar en cuenta que la visión que se tiene sobre gobernanza de internet puede cambiar su perspectiva dependiendo del enfoque político o el tipo de Estado que se desee analizar (Barzallo, 2012).

A la par, se han creado nuevos conceptos que tratan de explicar sucesos surgidos por las nuevas Tecnologías de la Información. Por ejemplo, tenemos el caso de la "gobernanza en el internet", cuya concepción, fue abordada por primera vez, de manera internacional, en el año 2003, cuando la Asamblea General de las Naciones Unidas, con sede en Ginebra, aprobará la celebración de la Cumbre Mundial sobre la Sociedad de la Información (CMSI)[13]. El objetivo principal de esta fase fue establecer un tipo de voluntad política, para que se tomaran medidas y así, preparar una Sociedad de la Información al alcance de todos.

Dicha conmemoración se dividió en una segunda parte, inaugurada en Túnez en noviembre del año 2005, el fin importante, fue llevar a cabo el Plan de Acción de Ginebra, para así, hallar soluciones a nivel gobierno de Internet, además de mecanismos de financiación y aplicación de algunos documentos de los países en cuestión (UIT, 2006).

En esta segunda fase, la Cumbre Mundial sobre la Sociedad de la Información, estableció una definición acerca del concepto de gobernanza de internet:

> El desarrollo y aplicación de los gobiernos, el sector privado y la sociedad civil, en el desempeño de sus respectivos papeles, de principio, normas, reglas, procedimientos de toma de decisiones y programas comunes que dan forma a la evolución y a la utilización de Internet (CMSI, 2005).

A su vez, Pérez y Olmos (2009), ofrecen una definición similar a la anterior, puesto que ellos entienden a la gobernanza de Internet como, "el desarrollo y la aplicación por los gobiernos, el sector privado y la sociedad civil, en las funciones que les competen respectivamente, de principios, normas, reglas, procedimientos de adopción de decisiones y programas comunes que configuran la evolución y utilización de Internet" (citado en Aguirre, 2016).

[13] Dicha cumbre fomento a la creación del Foro para la Gobernanza de Internet (FGI), cuyo objetivo es impulsar el debate de gobiernos, organismos internacionales, profesionales de internet, empresas y organizaciones de la sociedad civil, para reconocer la igualdad de condiciones en el desarrollo del internet, así como la interacción con otros sectores de la administración pública (UNESCO, 2021).

Mientras que la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, la interpreta como, “un conjunto de principios, normas, reglas, procesos de toma de decisión y actividades que, implementados y aplicados de forma coordinada por gobiernos, sector privado, sociedad civil y comunicación técnica, definen la evolución y el uso de la Red” (UNESCO, 2021).

Además, en la Declaración de principios de dicha organización, se alude a la importancia que tiene la gestión de Internet, para las cuestiones técnicas y de política pública, así como a la importancia de la cooperación en el ámbito internacional y gubernamental, dichos ideales se enfocan en cinco puntos fundamentales (Secretaría de Comunicaciones y Transportes, 2019, p.3):

- La autoridad de política en materia de política pública relacionada con Internet es un derecho soberano de los Estados. Ellos tienen derechos y responsabilidades en las cuestiones de política pública internacional relacionadas con Internet;
- El sector privado ha desempeñado, y debe seguir desempeñando, un importante papel en el desarrollo de Internet, en los campos técnico y económico;
- La sociedad civil también ha desempeñado, y debe seguir desempeñando, un importante papel en asuntos relacionados con Internet, especialmente a nivel comunitario;
- Las organizaciones intergubernamentales han desempeñado, y deben seguir desempeñando, un papel de facilitador en la coordinación de las cuestiones de política pública relacionadas con Internet;
- Las organizaciones internacionales han desempeñado, y deben seguir desempeñando, una importante función en la elaboración de normas técnicas y políticas pertinentes relativas a Internet.

Con base en esa serie de principios antes mencionados, se puede inferir entonces sobre la importancia que tiene la Gobernanza de Internet (Galindo 2012), puesto que la gobernanza no juega solamente un papel en cuestiones políticas, sino que hoy en día se debe emplear el concepto de manera distinta y mucho más incluyente, que preste debida atención a su manifestación en otros ámbitos sociales. También, considerar que se encuentran presentes nuevas herramientas que han sido creadas por diversos actores del ciberespacio, que son aceptados legitimante hasta ahora por la sociedad virtual, a los cuales, se les adjudica la

capacidad de establecer reglas básicas que permiten el funcionamiento dentro de él, estás van más allá sólo del conocimiento y uso de las tecnologías, ya que han dado como resultado una serie de normas análogas a las que operan en el mercado y dentro de una sociedad, pero dándole siempre premura al ámbito tecnológico en beneficio de las personas.

Por otro lado, en cuanto a la perspectiva de la teoría política en este tema de la gobernanza en internet, se podría mencionar primero, al vínculo que tiene la concepción clásica que tenía Gramsci acerca del Estado, puesto que él lo entendía más allá de sólo ser un conjunto de instituciones legales que configuran al gobierno, sino que también incluía en su pensar, a la relación de dependencia recíproca en la que participan la sociedad civil y la sociedad política (Ruiz, 2016), es decir, ahora con este mundo tan globalizado se debe fomentar a la participación de otros actores de carácter institucional sin perder de vista a la legitimidad del Estado. Algunos autores coinciden en que el término de gobernanza hoy en día va de la mano con esta definición, puesto que "las instituciones estatales y no estatales, actores públicos y privados, participan y cooperan en la formulación y aplicación de políticas públicas" (Mayntz, 1993, citado en Cornejo y Segura, 2021).

Aunque, si bien el argumento refutado de la idea antes mencionada radica en el peso que ahora tendría el Estado, puesto que se dejaría de ver cómo aquel ente de voluntad fuerte y arbitrio, puesto que la gobernanza pretende (De la Garza y Barredo, 2017) dar cauce a la colaboración de ciertos grupos de la sociedad civil. Ya que podría pensarse que la unión de los poderes públicos y la cooperación entre esos grupos sociales puede contraponerse con las corrientes teóricas originales. Sin embargo, De la Garza y Barredo, también mencionan que el argumento a favor de la implementación de la gobernanza recae en el hecho de que su reconocimiento parte de una realidad hacia la contribución entre instituciones públicas y diversos actores sociales que pueden fomentar la democratización en diversos espacios establecidos.

Sin embargo, se manifiesta una problemática mayor en el escenario de gobernanza global de Internet , puesto que aún falta establecer una conceptualización completa, y también conlleva una laguna legal, ya que falta una marco jurídico universal que regule las conductas dentro del ciberespacio, además, uno de los problemas principales, es que no se cuenta con una entidad de gobernanza global hasta ahora con la capacidad de ratificar acuerdos para el desarrollo de políticas de justicia, equidad social, y derechos humanos, lo que da pauta a un campo abierto a los actores involucrados en el juego del poder dentro de él, dichas problemáticas pueden ser la base para que se visualicen los retos a los que se enfrentan los Estados, ya que las problemáticas que se presentan en el ciberespacio engloban entre otros factores a los derechos humanos y a la equidad, según menciona Burch (2015), la expansión de Internet ha mostrado con sí que hay ciertos conflictos que no son capaces de resolverse en el plano nacional, con lo cual es fundamental la creación y el reforzamiento de acuerdos internacionales de gobernanza de Internet y del ciberespacio. El propio autor también menciona que hoy en día existe una urgencia por fomentar el debate público nacional e internacional, cuyo fin sea avanzar en una definición de principio, derechos, políticas públicas con perspectiva de la gobernanza de Internet, que permitan un diálogo abierto entre Gobierno y ciudadanía y así crear un ciberespacio libre y seguro.

Por otro lado, como menciona (Pérez, 2008) la definición de gobernanza de Internet debe incluir también una serie de referentes clave que permitan un modelo adecuado, en cuanto a las autoridades involucradas, la soberanía compartida, además de hacer énfasis en la importancia que tienen las relaciones entre agentes nacionales e internacionales, puesto que se deben abarcar cuestiones técnicas, políticas, sociales y económicas para el desarrollo de internet.

Por su parte, ya se mencionaba que existen otras perspectivas desde las que se le podría estudiar a la Gobernanza en el Internet, ya que por ejemplo (Gelbstein, 2005), los especialistas en telecomunicaciones, la pueden entender a través de un enfoque técnico, en informática se centrarán en un desarrollo de aplicaciones y

estándares, los activistas de los derechos humanos, hablarían de la importancia que tiene la libertad de expresión en el internet, derechos sociales, privacidad, o también están los abogados cuyo enfoque es acerca de una jurisdicción y resolución de conflictos que surjan en internet (en Pérez, 2008).

Se necesita también (Esterhuysen, 2015), un enfoque multilateral visto con un medio para alcanzar el fin de la gobernanza democrática del ciberespacio, estos procesos deben tener en común perspectiva de índole democrática, establecer los roles e intereses de los actores internacionales y por supuesto ser flexibles y resilientes. Además de que se debe brindar seguridad y confianza a los ciudadanos en el uso de las tecnologías de la información y las comunicaciones. Para mejorar la seguridad se debe buscar también la participación de los interesados y la creación de una cultura de ciberseguridad por parte de sociedad civil y privada (Barzallo, 2012), y por parte del Estado una que promueva a la ciberdefensa.

La lista podría crecer dependiendo del enfoque que se dé en cada área de estudio; sin embargo, considero que desde el ámbito politológico, lo que se esperaría, es una Gobernanza en Internet incluyente, capaz de crear modelos que incorporen la participación e injerencia de otros actores a nivel internacional con capacidad de crear nuevas reglas que sirvan para operen en el ciberespacio, buscando como siempre, la garantía de los derechos humanos, la seguridad y libertad, y que legitimen el papel fundamental de los Estados, apoyados por la sociedad civil y privada.

2.2 Estrategias de ciberseguridad y ciberdefensa en China

China es el país con la mayor población, cuenta con 1.402 miles de millones de habitantes, de los cuales 1.011 millones forman parte del ciberespacio. No es novedad que, a lo largo de los años, el país ha logrado posicionarse como una de las primeras potencias mundiales, sus grandes resultados van desde el desarrollo económico, científico y tecnológico, por mencionar algunos.

Aunque el avance tecnológico y científico en China, crece de manera exponencial, trae consigo una fuerte dependencia a las nuevas tecnologías de información, entre ellas, la sujeción del internet por parte de sus ciudadanos. Por ende, a mayor población en el ciberespacio, se vuelve menos seguro debido a la casi nula capacidad de poder controlar de manera segura ese espacio, es por esto que el gobierno, de China, debe organizar arduamente la lucha contra posibles ciberataques para su población y mejorar consigo los mecanismos de ciberseguridad y ciberdefensa.

Es relevante mencionar, que sí bien esta tarea es compleja, China, es uno de los países que ha hecho hincapié en la importancia de mejorar sus sistemas de seguridad informática. Sin embargo, pese a los esfuerzos, según un estudio publicado por el Instituto Internacional de Estudios Estratégicos (IISS, por sus siglas en inglés) refiere que la ciberdefensa en China sigue siendo permeable comparada con la de Estados unidos, puesto que la protección a sus infraestructuras nacionales críticas está apenas en las primeras fases de desarrollo. La investigación también afirma, que al menos durante la próxima década Pekín no podrá igualarse a las capacidades cibernéticas de su mayor adversario (Haro, 2021).

Lo que sí es de reconocer, es que, al menos en China las sanciones que fueron creadas en las leyes para la protección de internet, se cumplen a la par con base en la legalidad, algo que ejemplifica lo anteriormente mencionado es que, en mayo de 2021 a unos universitarios de Jiangsu se les sentenció a dos años y medio en

prisión al aprovechar que la cadena de comida KFC tuviera algunas vulnerabilidades en su sistema informático, lo que ocasionó que los estudiantes obtuvieron comida gratuita y que la empresa perdiera aproximadamente 311 mil 740 dólares (lo que equivale a 200 mil yuanes). Este es un claro ejemplo de que Beijing tiene un control sobre la información de su población y economía (Zimbrón, 2021).

También, la ciberseguridad en aras de su territorio ha sido ejecutada para su beneficio. Hoy en día, el país asiatico trabaja con la llamada "ciberseguridad alimentaria", ésta se refiere basicamente al impulso por parte del gobierno para desarrollar nuevas soluciones tercnológicas aplicadas al sector agroalimentario, las cuales facilitan el monitoreo del comercio de dicha industria, el proceso es llevado a cabo mediante las blockchain[14] que son puestas en marcha mediante una plataforma capaz de monitorear el origen y trazabilidad de los productos cárnicos, para afianzar al proveedor el estado de sus productos, además de que a través de estas nuevas tecnologías se logra controlar las transacciones comerciales de manera segura (Martínez y Feijoo, 2021).

Con lo mencionado en el párrafo anterior, se pensaría entonces, que el país utiliza a la ciberseguridad en conjunto con la ciberdefensa, no sólo para proteger a las infraestructuras críticas, sino para agilizar las relaciones comerciales, entre otros mercados más. No obstante, nos encontramos con la otra cara en la moneda, puesto que en recientes publicaciones se lee a China como una entidad que controla el internet de manera exhaustiva (Rubal, 2018), debido a que las autoridades competentes, se han encargado de realizar un monitoreo sobre las actividades que realizan sus ciudadanos dentro del ciberespacio. El ejemplo es claro, cuando por parte del gobierno chino, se indaga en correos privados, se impide el acceso a páginas extranjeras y demás contenidos. El régimen chino hoy en día está más preocupado por mantener el orden de la Seguridad nacional, la

[14] Según la International Business Machines (IBM), define a tecnología de blockchain como un libro mayor compartido e inmutable que agiliza un proceso de transacciones y de activos (que pueden ser rastreados y comercializados) en una red de negocios, a través de la red de blockchain se reducen los riesgos y posibles costos implicados.

estabilidad social y la injerencia extranjera, en lugar de una protección de datos personales para sus ciudadanos.

Pese a que con estas acciones se infringe a la libre circulación en el ciberespacio, como ya lo mencionaba Meservey ”el gobierno chino lo enmarca como una cuestión de soberanía, pero de lo que realmente se está hablando es de la capacidad de un estado para controlar la libertad flujo de información en línea” (como se citó en Mackinnon, 2019).

En el año de 1994, con la llegada del internet a territorio chino, el gobierno comunista tomó el control de la red informática, para mantener “el orden” en el país, (Lukyanov, 2019), y se encargó de crear el proyecto Escudo Dorado, en el año de 1998, dicho sistema es mejor conocido como el “Gran Cortafuegos chino”, que hace alusión a la Gran Muralla china, que como se sabe, a lo largo de la historia se consideraba un escudo impenetrable con la capacidad de impedir las invasiones.

La autora, Lukyanov, también menciona que ahora la “Nueva Gran Muralla del siglo XXI” es el Escudo Dorado, puesto que sirve para “proteger” a la población china de cuestiones de índole negativo e invasivo provenientes de internet, puesto que evita la injerencia de invasores.

También es relevante mencionar que actualmente la ciberseguridad en China (Patiño, 2021), tiene un enfoque socio-político, más que técnico, además de que promueven la restricción de ciertas libertades en el ciberespacio, justificándose como una puerta a la permanencia de la legitimidad, así como a los órdenes de carácter político y jurídico en el ciberespacio.

Cuando el presidente Xi llegó al poder, el régimen chino, (Vidal, 2017), se encargó de aumentar la censura en el internet, e incluso remarcó la importancia de la soberanía nacional en el ciberespacio, puesto que, para él, “no hay seguridad nacional sin ciberseguridad”.

Ahora bien, retomando el tema de interés, sobre ciberdefensa y ciberseguridad, los primeros intentos para la salvaguarda en este ámbito (Reuters, 2015), y el control del internet, se encaminan principalmente en la protección bancaria y en la regulación de un ciberespacio “seguro y controlable”. Sin embargo, en los últimos años, se han elaborado normas y leyes con respecto a temas de protección en internet y de datos personales, que hacen un ciberespacio más seguro, pero claro está que, debido a la gran potencia de este país, su intención siempre ha sido velar por sus interés nacionales y económicos primordialmente. Lo anterior mencionado, se traslada al resumen de los siguientes estatutos creados a lo largo de la carrera china contra posibles ciberataques y también para mejorar sus sistemas de seguridad y de información en el ciberespacio:

- Un primer intento sobre la norma en temas que respecta a la ciberdeliencuencia, fue la que se promulgó por el Consejo de Estado, Ordenanza sobre protección de la seguridad del sistema informático de información (Decreto del Consejo de Estado No. 147, 18 de febrero de 1994). Cuya base legal se fundamenta en cinco principales responsabilidades; Violar o amenazar los sistemas informáticos de información nacionales e internacionales, no alertar sobre el daño ocurrido a dichos sistemas, así como negarse a contribuir con la seguridad aún despúes de tener conocimiento de su alteración (Rodríguez y Cordero, 2018).

- Ley Penal de China de 1997 : “proporcionó criterios y directrices esenciales para establecer la condena de los ciberdelincuentes, apoyada de otras leyes estatutarias y reglamentos (Rodríguez y Cordero, 2018).

- Ley Antiterrorismo publicada en el año 2015. En términos generales, el texto busca (Fontdeglòria, 2015), mantener la seguridad en el mundo y controlar el terrorismo en el país. Sin embargo, la ley fue fuertemente

criticada por algunos defensores de la libertad de información y protección de datos, puesto que el borrador de la ley suscitó una polémica en algunas cláusulas donde obligaba a empresas tecnológicas a entregar información, que ante los ojos del gobierno chino se consideraba sensible, además de instalar puertas traseras[15] en algunos productos. También fue juzgada por el poder excesivo de algunos medios estatales a los cuales se les otorgaba una autorización expresa, para que ellos, desde su arbitrio consideraran lo que es o no el terrorismo. Sin embargo, según los legisladores fue para "restringir información relacionada con el terrorismo que puedan publicar los ciudadanos en las redes sociales" (Fontdeglòria, 2015).

- Ley de Seguridad Nacional presentada en el año 2015, cuya base legal fue exigir a las infraestructuras y sistemas de información que sean seguras y controlables (Sánchez, 2015). Además de reforzar la infraestructura y el sistema financiero.

- Los datos que emanan de la regulación integral de China, con respecto a temas de privacidad y seguridad digital, se fundamentaron con la creación de la Ley de Seguridad Cibernética[16] (CSL), entró en vigor el 1 de junio de 2017 (Edwards, 2019). Cuyo objetivo principal es, "salvaguardar la soberanía en el ciberespacio, la seguridad nacional y el interés público, así como los derechos y los intereses de los ciudadanos" (Administración del Ciberespacio de China, en Vidal, 2017). Además de la regulación de ciertas actividades comerciales que operan las empresas en el ciberespacio chino (PwC, 2017).

[15] Mejor conocidas como "backdoors", estas permiten saltarse los sistemas de seguridad que dan acceso a los sistemas informáticos, en términos más simples, son entradas secretas con la capacidad de controlar los sistemas, saltándose protocolos de seguridad. Diversas agencias de seguridad nacional y gobiernos piden a expertos informáticos instalar este tipo de software para así poder espiar a posibles atacantes cibernéticos (Universidad de Alicante, 2020).
[16] Anteriormente se hizo mención sobre la tecnología blockchain, y es relevante mencionar que en el año 2018 se reguló legalmente bajo está ley.

- Ley de Seguridad de Datos (DSL), con vigencia a partir del 1 de septiembre de 2021, Su enfoque se refiere a la clasificación de la protección y seguridad de datos críticos en el ámbito de seguridad nacional e interés público. Su elemento más distintivo se complementa con el sistema de clasificación de datos, en el cual el gobierno tiene la capacidad de establecer los datos conforme al nivel de importancia que considere (Patton, 2021).

- Reglamento sobre la protección de la seguridad de la infraestructura de información crítica, vigente a partir del 1 de septiembre de 2021, es una norma que complementa a la Ley de Ciberseguridad de La República Popular China, para este texto se especifica quienes son las autoridades encargadas de la seguridad en el ciberespacio, así como las obligaciones de seguridad de operadores de la infraestructura crítica (CII)[17], cuya función es, almacenar información personal y datos sujetos a revisión de la seguridad nacional que le competen al gobierno del país (The National Law Review, 2021).

- La Ley de Protección de Datos Personales (LPDP), entró en vigor el 1 de noviembre de 2021. Si bien, es la más reciente, como lo menciona Colacci (2021), dicha ley se coloca como, la primera que protege datos integrales, dentro del país asiático. La LPDP se fundamenta (Marval, 2021), principalmente en la regulación del tratamiento de la información personal (IP) de personas físicas[18] (ya sea por cualquier tipo de información recopilada por medios electrónicos en su mayoría).

[17] Entre las obligaciones correspondientes a los operadores de CII se encuentran: nombrar a la autoridad correspondiente para el análisis de riesgos que vulneren la ciberseguridad, así como la protección de la CII, proporcionar fondos operativos suficientes para velar por la ciberseguridad y agilizar el proceso de servicios en línea priorizando a proveedores confiables y seguros.

[18] La ley también aplica si fuese el caso de que la IP las personas físicas que residen en la República Popular se procesa fuera de la misma, con respecto a lo siguiente, si se proporciona

Según el Gobierno de Canadá (2021), el régimen de ciberseguridad de China cuenta con cinco elementos principales que están enfocados en la seguridad de la red y protección de datos en el país, en primer lugar, se encuentra la Ley de Ciberseguridad (LCS), los cuatro restantes son:

- Sistema de protección multinivel (SPPN): Es un sistema que se encarga de clasificar las redes de China[19], así como los requisitos para protección y supervisión de la ciberseguridad, este modelo se divide en cinco niveles que van desde el menos crítico, hasta llegar al que necesita mayores requisitos de seguridad.
- Infraestructura de información crítica (CII): Existen reguladores del sector chino encargados de identificar a las infraestructuras críticas[20] para así dar importancia al tipo de instalación que opera en redes y sistemas de información con actividad industrial u otras. Entre las demás funciones, se encuentran también, estudiar el impacto y el tipo de daño que pueden ocasionar los ataques contra dichas infraestructuras.
- Protección de datos importantes: Los operadores chinos deben tener la capacidad, no sólo de garantizar la seguridad de datos importantes, sino de también de contemplar las amenzas que se puedan presentar contra la seguridad nacional y económica, estabilidad social, salud y seguridad pública, que son los filtros principales de donde se podría obtener información confidencial de la población en cuestión.

servicios y productos a personas físicas dentro de China, así como también la evaluación de las actividades dentro dichas fronteras.

[19] Este sistema no clasifica para redes de uso personal o doméstico, ni tampoco para servidores que se encuentran fuera del territorio chino.

[20] En el capítulo previo se hizo mención sobre los ejemplos de infraestructuras críticas. Para el caso China centran su atención en: servicios públicos de comunicación e información, transporte, energía, gobierno electrónico, industria de tecnología de defensa, entre las principales.

- Protección de la información personal: Los operadores de red[21] tienen la obligación de velar por la información personal de los ciudadanos (apellido, geolocalización, fecha de nacimiento, datos biométricos, cuentas bancarias, etc). Además de que no pueden recopilar información de uso personal que no sea de interés en los servicios que puedan ofrecer, puesto que en caso de filtrar "información personal sensible" se expondría a la seguridad de las personas o sus bienes activos, que podrían terminar en algún delito cibernético o estafa.

Por otro lado, la ciberseguridad en China (Patiño, 2021), tiene un enfoque socio-político más que técnico, puesto que en el país se justifican haciendo referencia a la importancia que tiene la permanencia de la legitimidad y los órdenes de carácter político y jurídico en el ciberespacio, sin embargo ante los ojos de la sociedad, lo que se ve es una restricción a la libertad de expresión y una vulneración a la privacidad de datos personales y de ciertas actividades en el ciberespacio.

Algunos expertos como Ramírez (2019), menciona que existe una limitante en cuanto a la implementación de la Ley de Seguridad Cibernética para que sirva como una referencia al marco normativo de otros países, esto se debe a la distancia que separa a la cultura oriental de la occidental, además de que dicha Ley por sí sola es escasa para lo complejo que resulta la regulación en el ciberespacio, aunque si bien está alineada con otras que se aplican de manera global para la protección de sistemas de información y comunicación, el problema radica en el momento en que se debe determinar a la autoridad correspondiente para imponer las leyes y en los órganos a quienes se les confiere la capacidad de garantizar los derechos y obligaciones.

Sin embargo, también dichas leyes que se justifican como acciones que velan la seguridad y el bienestar del Estado, (Sánchez, 2015), tienen otro significado

[21] Dentro de las normas que operan para los operadores se encuentra la de no poder recopilar información personal de niñas y niños menores de 14 años sin el consentimiento de sus tutores.

puesto que se presentan como una amenaza contra la ya de por sí limitada libertad de información y expresión de la población en el ciberespacio.

En un artículo titulado ”La otra Muralla China: el control de Internet”, que fue publicado por Lucía (2016), menciona, que si bien China no busca en sí un control total de toda la red, si lo ha hecho alrededor y dentro de las conexiones que tienen acceso directo a sus fronteras, y en el intento de esa gobernanza global de internet, y en la búsqueda de lograr la supremacía por encima de Estados Unidos, se ha convertido en un país que aprueba la censura y el control a la libertad de expresión de los ciudadanos que residen en el ciberespacio, priorizando así las actividades comerciales de libre injerencia extranjera por encima de los derechos civiles y políticos, sin importar que su objetivos económicos atenten contra la propia seguridad de sus ciudadanos dentro del ciberespacio. Vendiéndose, así como un país con un discurso nacionalista, defensivo y controlador, que atenta contra los principios de privacidad de datos personales de sus ciudadanos. Inclusive el propio Consejo de Estado del país chino anunciaba que el ciberespacio debe cumplir la finalidad de promover y legitimar la educación sobre el Partido Comunista para que internet sea civilizada y centrada en valores socialistas (Forbes, 2021).

Por otro lado, gracias a la modernización y demás avances, ha permitido que China se convirtiera en un país capaz de posicionarse en el sistema internacional, que ha sabido acortar la distancia tecnológica, económica y militar con los demás países (Oviedo,2021). Sin embargo pese a dicho ascenso internacional, sigue siendo un país con tendencia monopolística y paradójicamente a pesar de tener un Estado que es “legítimamente aceptado” en la sociedad, no se cumple con la premisa de que sea políticamente correcto, puesto que no protege y defiende la libertad de sus ciudadanos en el ciberespacio.

Para un país desarrollado como lo es China, su meta principal y a su vez la más compleja, es entonces, garantizar un ciberespacio libre y seguro, así como mejorar sus mecanismos de ciberseguridad y ciberdefensa y crear nuevos acuerdos

internacionales. Además de (Burch, 2014), buscar alternativas que permitan disminuir los problemas de operación y gobernanza en internet sin ejercer un control total para sus ciudadanos.

2.3 Estrategias de ciberseguridad y ciberdefensa en Estados Unidos

Desde aquel trágico suceso del 11 de septiembre de 2001, la gran potencia mundial, Estados Unidos de América, se vio en la necesidad de tomar medidas para salvaguardar su territorio frente a posibles ataques terroristas, mejorando así, no sólo la seguridad en sus fronteras, sino incluyendo el resguardo a sus sistemas de seguridad de información y reforzado con sí la seguridad nacional para incrementar las capacidades ofensivas y defensivas de su propio Estado.

El ciberespacio en Estados Unidos se rige a partir de ciertas vertientes que lo vuelven un lugar libre y sin censura. Es un país (Morelli, 2013), que se proclama a favor de un ciberespacio libre de interferencias políticas, donde se busca garantizar la libertad de expresión e información. Sin embargo, también se ha encargado de tener la mayor participación dentro del mismo.

Previamente se mencionó, que para China es más importante focalizar sus objetivos en analizar el papel que juega la ciberseguridad y la ciberdefensa para mantener un orden social y político. Sin embargo, en el caso de Estados Unidos, encontramos a un país que centra su atención en "fortalecer una concepción de ciberseguridad bajo un lente más técnico" (Patiño, 2021: 111), lo que implica la búsqueda hacia un nuevo posicionamiento internacional, es decir, ya no sólo demanda ser la primer potencia en el ámbito económico, político y social, sino ahora lo que quiere es convertirse en un nuevo ente con la capacidad y los recursos necesarios para salvaguardar sus intereses a partir de una ciberseguridad y ciberdefensa autosuficientes.

Existe cierta presión que se ejerce por parte del gobierno de los Estados Unidos y la guerra comercial contra su contrincante, ya que, actualmente involucran nuevos temas tecnológicos que van desde la propiedad intelectual, inteligencia artificial, guerra cibernética, hasta el dominio de la tecnología 5G, por mencionar algunos. Sin embargo, ambos países están conscientes que el desarrollo en este ámbito

parte de la proposición de que el ciberespacio está lleno de amenazas, lo que implica un atentado contra la ciberseguridad y ciberdefensa de cada país.

Las disputas entre Estados Unidos y China, debido al contexto histórico que viven, es sumamente notorio en diversos ámbitos, entre los que se encuentran, el económico, político, social y tecnológico, este último, que está estrechamente vinculado al ciberespacio, trae consigo disputas entre las grandes potencias por querer controlar quién o quiénes están al mando de este metaespacio. Actualmente, se sabe que el liderazgo mundial en él está gobernado por dos bloques principales: Estados Unidos por un lado y por el otro, China y Rusia. El primero se enfoca en tratar de hacer válida la aplicación del derecho internacional dentro del ciberespacio, así como de garantizar que la libertad de expresión en el mismo se cumpla, mientras que el segundo bloque presupone que los tratados internacionales tienen la encomienda de dar un mayor control a los Estados sobre la soberanía en el ciberespacio (Haro, 2021). Es decir, existe una competencia para imponer valores, principios e ideales entre ambas potencias que buscan una hegemonía en el ciberespacio correspondiente a sus propios intereses. Y que si bien ambos países se reconocen como interdependientes uno del otro, se asume que, por un lado ambos bloques se benefician puesto que existe la cooperación internacional y permite una expansión e interconexión para ambos, sin embargo, por otro lado, también se encuentran con una problemática donde el ciberespacio se convierte en un espacio de conflicto para ambos Estados. (Patiño, 2021). Esto último representa diversos problemas, puesto que a medida que crece la participación de estos países dentro del ciberespacio sus intereses se ven más expuestos y vulnerables a sufrir algún tipo de ataque cibernético o bien, algún tipo de enfrentamiento dentro del mismo.

Aunado a lo anterior, se dice que, existe un efecto red, mejor conocido como “network effect”, cuyas posturas económicas y comerciales conllevan a la formación de monopolios naturales en el ciberespacio, que se forman a partir de la

clasificación que les otorgan los usuarios en el ciberespacio, las ponderaciones van desde un pésimo servicio, hasta el mejor calificado o bien de mayor utilidad, tal es el caso de Facebook, Google, Amazon, etc. Si bien existen ya leyes antimonopolio, al menos la postura que hasta ahora se ha hecho presente en EE.UU. no se ha inclinado a favor de ellas para poner un límite a esas empresas, sin embargo, incluso han mejorado las negociaciones de acuerdos comerciales y estrategias geopolíticas para su crecimiento y expansión[22] (Bustamante, Riquelme y Salinas, 2015).

Según las convicciones de EEUU, es reforzarse de manera sólida para buscar la prosperidad económica, recuperar el liderazgo tecnológico, y de la inteligencia artificial (García, 2018). Si el país logra esos avances a nivel mundial, tendría que demostrar también, que cuenta con la capacidad de mantener a sus sistemas de información lejos de estar expuestos a posibles ciberataques, además de que una buena ciberseguridad y ciberdefensa lo colocaría en una nueva esfera mundial que esté mejor posicionada en comparación de sus demás contrincantes.

Previamente se mencionó que China es un país que vigila constantemente la manera en que sus ciudadanos navegan en el ciberespacio. Sin embargo, según menciona Marina (2021), existen otros países como Estados Unidos, Francia, Reino Unido y Rusia que se han encargado de espiar mensajes de texto y otras actividades que se realizan en el ciberespacio con la justificación de que lo hacen para prevenir el terrorismo y mejorar la seguridad interior. Lo que conlleva a la premisa de que Estados Unidos, lejos de proclamarse como un país a favor de la libertad de expresión en el ciberespacio, busca expandir a toda costa sus fronteras comerciales irrumpiendo así la privacidad de sus ciudadanos en internet, y ejerciendo con sí un control en las actividades que se operan dentro del mismo.

[22] En el Plan Nacional de acción sobre Ciberseguridad (2016), se estableció que el Gobierno de Estados unidos sumaria fuerzas con empresas líderes en tecnología como Google, Facebook, DropBox y Microsoft para crear una campaña sobre concientización sobre ciberseguridad, que ayudaría a los usuarios a prevenir y enfrentar los retos cibernéticos.

El siguiente punto a tratar, es acerca de los primeros intentos del país en materia legislativa de seguridad cibernética, según una página web que se encarga de enunciar leyes respecto a temas de ciberseguridad en diversos países, menciona que, en caso de Estados Unidos, en años anteriores, se hizo mención a la importancia de regular las organizaciones de atención médica, instituciones financieras y agencias federales, para proteger sus sistemas de información. A nivel federal las leyes prescritas eran: Ley de Responsabilidad del Seguro de Salud (1996), Ley Gramm-Leach-Bliley (1999) y la Legislación de Seguridad Nacional (2002).

No obstante, en una de las páginas oficiales del gobierno de Estados Unidos, Cybersecurity and Infrastructure Security Agency (CISA), que es la Agencia de Seguridad de Infraestructura y Ciberseguridad, por su traducción al español, proporciona información de los registros de seguridad cibernética a partir del año 2012, con la creación de programas para la concientización sobre ciberseguridad, tanto en la sociedad, como en las empresas y entes gubernamentales, además de la publicación de una revisión de la política del ciberespacio, publicada en 2009.

Para los años posteriores, el país ha logrado grandes avances en cuanto a su legislación, puesto que, según informes, la gama es un tanto amplia, por ejemplo, la Agencia de Seguridad de Infraestructura y Ciberseguridad y algunos otros autores señalan los siguientes textos de carácter oficial y normativo, así como la mención a la creación de algunos organismos con la tarea de salvaguardar el ciberespacio:

- Estrategia Nacional para Asegurar el Ciberespacio (2003): fue publicada por la Casa Blanca para proteger a las infraestructuras de información, prevenir ataques cibernéticos y reducir y minimizar los daños y la

vulnerabilidad de la nación frente a dichos ataques (Rodríguez y Cordero, 2018).

- Equipo de preparación para emergencias informáticas de los Estados Unidos (US-CERT), fue fundado en 2003 con el objeto de coordinar una respuesta a los posibles ciberataques en el país, trabaja en apoyo de algunos sectores públicos y privados.

- Centro Nacional de Integración de Comunicaciones y Ciberseguridad (NCCIC): creado en 2009 , actúa como una herramienta para la mitigación de posibles ciberataques, con la cooperación de algunas entidades civiles, privadas y estatales.

- Ley de Compartición de Información de Ciberseguridad de 2015, según informó el periodico, El mundo (2015), esta ley fue elaborada con la finalidad de que el gobierno destinará su protección para aquellas empresas que voluntariamente compartan datos que consideren podrían presentar una amenaza cibernética al Gobierno Federal." Facilitan que las empresas privadas compartan información sobre amenazas cibernéticas con el Gobierno" (La casa Blanca, 2016).

- El Plan Nacional de Protección de Infrestructura 2016 (NIPP)[23]: fue elaborado por expertos de infraestrcutura critica, agencial federales, gubernamentales estatales y locales, y algunas más del sector privado.

[23] Anterior a este Plan, se elaboraron la NIPP de los años 2009 y 2013 que fueron sustituidas por la del año 2016.

Cuya finalidad era generar alianzas para la seguridad y resilencia de la infraestructrua crítica[24] (CISA, 2013).

- El Programa EINSTEIN, con fecha del 17 de abril de 2015, tiene la finalidad de proporcionar a la CISA, conocimiento sobre la salud del Gobierno Federal en el ciberespacio, y también puede instalar sistemas que recopilen datos de flujo de la red (CISA, 2015).

- EINSTEIN 1, 2 Y 3. Son tres programas publicados en 2015, el número 1, cumple la función de analizar información de flujo de las redes de agencias del Poder Ejecutivo civil Federal, y proporcionar información sobre cualquier posible actividad maliciosa en las redes. Mientras que EINSTEIN (2), se basa en recopilar información dañina en la red e informar a la Agencia, mientras que el último programa EINSTEIN (3), detecta y evita el tráfico malicioso dirigido a las redes del Gobierno Federal (CISA, 2015).

- Plan Nacional de Acción sobre Ciberseguridad (CNAP). Publicado en 2016 durante la administración del ex presidente Obama, cuya base se fundamenta en: "la protección de la seguridad cibernética, proteger la privacidad, mantener la seguridad pública. Así como la seguridad económica y nacional, y empoderar a los estadounidenses para que tomen un mejor control de su seguridad digital" (La casa Blanca, 2016).

- Estrategia cibernética del Departamento de Defensa-2017. Según lo establecido por este organismo, entre sus principales estrategias estaban:

[24] Según CISA, en marzo de 2014 se reunieron los cinco países críticos (Australia, Canadá, Nueva Zelanda, Reino Unido y Estados Unidos), para publicar una narrativa sobre "forjar un entendimiento común para la infraestructura crítica".

acelerar el desarrollo de las capacidades cibernéticas, disuadir las actividades maliciosas en el ciberespacio, aumentar la resiliencia de las infraestructuras críticas, construir asociaciones confiables con el sector privado, fomentar la cooperación internacional, reforzar las normas de comportamiento responsables del Estado en el ciberespacio e incorporar una cultura de conciencia cibernética en su cultura institucional.

- Estrategia de Seguridad Nacional (ESN) 2017. Según lo analizado por la investigadora Carlota García (2018), lo que se busca en este documento es:

  > "Involucrarse en una dura competición global en la que EEUU recupera terreno en el ámbito de las nuevas tecnologías y la innovación y adaptarse a la competición que ha llegado al ciberespacio y al espacio. Y siempre tratando de priorizar los intereses de EEUU bajo el concepto de 'América primero' y de competir más que colaborar".

- Estrategia CISA 5G. Se llevó a cabo el 19 de agosto de 2020, cuya finalidad es la implementación de una infraestructura de quinta generación que sea segura y resistente, para poder así promover a la seguridad nacional, integridad de datos, innovación tecnológica y el desarrollo de la economía en Estados Unidos(CISA, 2020).

- Ley de Mejora de la Ciberseguridad del Internet de las Cosas (Iot) de 2020: el objetivo de dicha ley es: asegurar que la compra de dispositivos hecha por el gobierno cumpla con los requisitos mínimos de seguridad que serán propuestos por el Instituto Nacional de Estándares y Tecnología (NIST). También, los fabricantes tienen la obligación de cumplir con los estándares

de seguridad para continuar con los contratos de adquisición con el gobierno (Legal Army, 2020).

Por otro lado, el actual gobierno del presidente Joe Biden ha hecho hincapié en la importancia de mejorar los sistemas de información y proteger a las infraestructuras críticas, mediante el fortalecimiento de la ciberseguridad, puesto que, un daño o invasión a estos tiene la capacidad de generar un impacto negativo en diversas índoles como las que ya se han mencionado anteriormente. Todo esto de la protección a los sistemas de información, surgió a raíz del ataque de ransomware que sufrió la mayor red de oleoductos del país, la Colonial Pipeline en mayo de 2021, EUA tuvo que declararse en estado de emergencia, ya que los ciberdelincuentes desconectaron y robaron más de 100 GB de información del Oleoducto Colonia, el cual transporta más de 2.5 millones de barriles por día, el impacto generado trajo consecuencias inéditas que afectan al suministro de gasolina, combustible para aviones y otros derivados del petróleo según informó BBC.

Con el ejemplo anterior, se puede ver que a pesar de que Estados Unidos sea líder en ciberseguridad a nivel mundial, los ciberdelincuentes siguen estando un paso de cualquier gobierno y que si estos no tienen un plan de acción bien estructurado o estrategias para contrarrestar posibles ciberataques, el riesgo que corren es muy alto.

En lo que a mi parecer respecta, Estados Unidos tiene el potencial, el desarrollo económico, político, y tecnológico para mejorar aún más sus sistemas de información, los cuales deben incluir como hasta ahora, la proclamación a favor de la libertad de expresión y la no censura en sus tecnologías de información. A pesar de que el país cuenta con un considerable nivel técnico y diplomático que hasta ahora han sabido manejar dentro de lo que cabe, se deben incorporar mejoras a la ciberseguridad y ciberdefensa, ya que considerando que Estados Unidos es primer potencia, se requiere de mayores esfuerzos, puesto que su

nación siempre se ha visto envuelta en posibles ataques y vulneraciones a su seguridad nacional, y hoy en día, debido a los avances tecnológicos, estos crecen de manera exponencial y se propagan con un simple click.

Sin embargo, lo que hace falta también, es un análisis exhaustivo en cuanto a contemplar la noción de que hoy en día la cooperación internacional no es una opción sino algo necesario y que el buscar la monopolización y el interés nacional antes que el bienestar internacional, al menos en el ciberespacio, no es una opción viable para Estados Unidos, ni para ninguna nación, puesto que en este metaespacio nadie es dueño de nada, e incluso en ocasiones se vive en la propia anomia.

2.4 Estrategias de ciberseguridad y ciberdefensa en la Unión Europea

Se estima que derivado de la pandemia por Covid-19, durante el 2020 el 40% de los trabajadores de la UE se convirtieron en teletrabajadores y también durante ese año las ciberamenazas se expandieron generando vulneraciones a sistemas críticos, como por ejemplo en hospitales y centros de investigación en vacunas (Tesoro, 2021).

Aunado a lo anterior, algunos gobiernos de la Unión Europea han creado mecanismos de defensa referentes a conservar un status quo, en cuanto a la ciberseguridad y ciberdefensa y también de la gobernanza del ciberespacio, estudiando para sí lo referente a la seguridad de información. A su vez apoyan al enfoque estadounidense con las tendencias al reparto de responsabilidades en diversos actores involucrados en el ciberespacio, como por ejemplo, privados, civiles y militares. (Patiño, 2021).

Como se sabe, la Unión Europea, a lo largo de la historia se ha transformado en un eje de estados soberanos y también en una organización compuesta por instituciones y elementos normativos comunes, es decir, la base institucional de la normativa europea permite ver que la aplicación de las leyes ejerce una influencia en todo el territorio y una puerta para la regulación internacional (Wegener, 2014).

Pese a que el conjunto de países que la conforman se caracterizan por respetar y garantizar que las leyes se cumplan conforme a lo establecido, existen aún ciertas deficiencias en cuanto a la protección de sistemas de información e infraestructuras críticas, sin embargo es importante señalar que la Unión Europea es una de las entidades más desarrolladas en el ámbito jurídico que compete a temas de esta índole.

Una nota publicada por el Parlamento Europeo (2021), revela que las empresas y organizaciones de la UE invierten un 41% menos en ciberseguridad que Estados Unidos, sin embargo, se busca el liderazgo en materia de ciberseguridad y

ciberdefensa puesto que los ataques en línea, la desinformación y la presión económica principalmente, han puesto en tela de juicio a la resiliencia de los Estados democráticos y a la seguridad de la Unión Europea.

Según Alessandro Demurtas (2020), la evolución en la ciberseguridad en la UE ha tenido dos enfoques principales, el primero se basa en que los actores políticos europeos se han dado a la tarea de poner en la agenda pública cuestiones derivadas de dimensiones cibernéticas, ya que se encuentran estrechamente interconectadas con actores en el sistema internacional: población, instituciones públicas y privadas, entre otros. La segunda razón, es necesaria analizarla desde un contexto de interdependencia, porque debido a la cooperación intergubernamental entre los miembros[25] de la Unión Europea, estos comparten intereses comunes que logran fortalecer sus relaciones diplomáticas que les permite contrarrestar las amenazas en el ciberespacio.

Otra característica fundamental de la UE es que para mantener la cohesión, su tarea principal ha sido la mejora y la garantía de trasladar al ciberespacio aquellos derechos fundamentales, la democracia y el Estado de derecho para que sean protegidos y cumplan con la finalidad de brindar a sus ciudadanos un lugar abierto y libre. Además de ser una de las naciones que tiene la iniciativa de fomentar una colaboración de un ámbito público-privado, para llevar a cabo uno de sus objetivos primordiales, que el ciberespacio sea un lugar libre y seguro.

A partir de los atentados terroristas en Francia y Bruselas, ministros de justicia y Asuntos de Interior, insistieron en la necesidad de buscar soluciones políticas que permitieran no sólo explorar el ciberespacio, sino también de hacer frente a la

[25] España como miembro perteneciente, es uno de los países que más ha trabajado en temas de ciberseguridad y ciberdefensa, como por ejemplo con la creación de la Estrategia de Seguridad Nacional (2017) y la Estrategia de Ciberseguridad Nacional (2019) que van encaminadas a estos temas y acorde con la normativa aprobada por la EU.

lucha contra actividades delictivas en él, con la finalidad de mejorar la justicia penal en el ciberespacio (Consejo de la Unión Europea, 2016).

El Consejo de la Unión Europea (2021), refiere que las medidas que ha tomado la propia EU para contrarrestar las problemáticas en materia de ciberseguridad y ciberdefensa, engloban seis principales aspectos: mejorar la ciberresilencia, luchar contra la ciberdelincuencia, impulsar la ciberdiplomacia[26], reforzar la ciberdefensa, fomentar la investigación e innovación y proteger las infraestructuras críticas. En cuanto al desarrollo de los documentos legales, y otros mecanismos que acción que permiten la regulación en estos ámbitos se ha elaborado lo siguiente[27]:

- Agencia de la Unión Europea para la Ciberseguridad (ENISA): fue creada en 2004; según el sitio web de la agencia, cumple funciones como, lograr un alto nivel de ciberseguridad en Europa, contribuir a la política cibernética, mejorar la confiabilidad de los productos, servicios y procesos de TIC y cooperar con los Estados miembros para los futuros retos cibernéticos (ENISA, 2021).

- Estrategia de Ciberseguridad de 2013: Entre las estrategías propuestas para este documento se encuentran, la implementación de una Marco político de Ciberdefensa (MPCD), que establezca la protección a las infraestructuras de sistemas de información y comunicación, apoyar y fomentar a los Estados Miembros para la aplicación en el desarrollo de capacidades de ciberdefensa, así como promover la cooperación cívico-militar y la unión con otros actores internacionales (Fojón, 2015). Además,

[26] Según Ramón (2021), la ciberdiplomacia europea es entendida como un instrumento intrínseco de la política internacional de la UE con relación al ciberespacio.
[27] Existen otros espacios creados para la discusión de riesgos cibernéticos y cuestiones relacionadas con el ciberespacio, como lo son, el Consejo de Transporte, Telecomunicaciones y Energía (2017), Consejo sobre la ciberdiplomacia (2015).

entre sus estrategias prioritarias se encuentra, la resilencia contra ciberataques y el desarrollo de una política de ciberdefensa (Wegener, 2014).

- Directiva 2016/1148: Instaura las medidas que garantizan un nivel elevado de seguridad y sistemas de información, y establecer las capacidades de los Estados miembros para minimizar los riesgos que se planteen en la seguridad de las redes y sistemas de información (Alarcón, 2017).

- El Conjunto de instrumentos de ciberdiplomacia: adoptado por el Consejo el 19 de junio de 2017, para prevenir conflictos y mitigar amenazas cibernéticas. Además de fomentar a la cooperación internacional (Consejo de la UE, 2019).

- El Reglamento sobre la Ciberseguridad, adoptado el 9 de abril de 2019, tiene como objetivo mejorar la ciberresilencia a partir de la creación de una marco de certificación a escala de la UE para productos y servicios provenientes de las TIC, así como sustituir a la Agencia de Seguridad de las Redes y de la Información de la EU (ENISA) por una Agencia de la UE para la Ciberseguridad.

- El 17 de mayo de 2019, se estableció un marco normativo[28] para que en la unión Europea puedan imponer medidas restrictivas para contrarrestar los ciberataques, que sean expresados como una amenaza a sus Estados miembros, o bien proveniente del exterior. En resumen, el reglamento permite imponer sanciones que comentan o pretendan lanzar algún tipo de ciberataque (Consejo de la UE, 2019).

- A través de un acuerdo interinstitucional con fecha del 20 de diciembre de 2017, se creó un equipo de respuesta a emergencias informáticas (CERT-

[28] Los ciberataques merecedores de una sanción serán los que; tengan origen desde el exterior de la UE, sean cometidos por personas u organizaciones fuera de la UE o bien utilicen infraestructura no proveniente de la UE.

EU), que colabora con otros equipos y miembros de seguridad informática cuya finalidad es dar una respuesta ante posibles ciberataques.

- Estrategia de Ciberseguridad de 2020 : permite el liderazgo de las normas internacionales que rigen al ciberespacio, para que el país pueda potenciar la cooperación con otros países, con la finalidad de "promover un ciberespacio global, abierto, estable y seguro, basado en el Estado de Derecho, derechos humanos, libertades fundamentales y valores democráticos".(Comisión Europea, 2020). También representa un elemento clave para el marco legal y parámetros que tienen que ver con la resiliencia física y la ciberresilencia de infraestructuras críticas.

- Creación del Centro de Competencia en Ciberseguridad: Este nuevo organismo tendrá su sede en Bucarest "para poner en común inversiones en investigación, tecnología y desarrollo industrial en materia de ciberseguridad", según informó el Consejo. También la ministra de Estado y de la presidencia de Portugal, Mariana Vieira da Silva (2021), mencionó que: El nuevo Centro de Competencia, en conjunto con la Red de Centros Nacionales de Coordinación tendrán una función clave para contribuir a la seguiridad de las infraestructuras digitales y a las críticas. Además de reforzar la competitividad de la industria de ciberseguridad de la UE, para las pymes y aumentar el liderazgo en dicha materia.

Aunado a lo anterior, el 23 de junio de 2021, la Comisión publicó una recomendación para la creación de una Unidad Cibernética Conjunta con la capacidad de hacer frente a incidentes de un alto nivel que involucran a servicios públicos, empresas y ciudadanos, además de actuar de manera conjunta con otras unidades cibernéticas de la UE. También, en diciembre de ese mismo año, el Consejo de Transporte, Telecomunicaciones y Energía, se posicionó a favor de la propuesta a la nueva Directiva SRI2, cuyos objetivos son: mejorar la resiliencia y

la capacidad ante posibles accidentes. Además, el ministro de Administración Pública de Eslovenia dijo que esta medida podrá reforzar la ciberseguridad, puesto que las ciberamenazas tienen la capacidad de afectar a la sociedad, economía y democracia en la Unión Europea, también, de que con esto se demostrará la capacidad que tiene esta para considerarse un líder en la legislación en materia de este índole (Kirtnik, 2021).

Un ejemplo muy próximo que se tiene en cuanto a la implementación de las leyes elaboradas en la UE, fue cuando, el 30 de junio de 2020 el Consejo impuso medidas restrictivas a seis personas y tres organizaciones que fueron actores de algunos ataques informáticos, por el intento de ciberataque contra OPAQ (Organización para la Prohibición de las Armas Químicas), WannaCry, NotPetya y Operation Cloud Hopper, según informó el Consejo.

Por otro lado, en cuanto al nivel de ciberseguridad, el informe publicado por la UIT en 2020, revela que de los países miembros de la unión Europea, se encuentran entre los primeros 20 lugares los siguientes:

Tabla 3. Nivel de ciberseguridad en la Unión Europea. Elaboración propia con base a los datos proporcionados por la UIT.

País	Índice	Posición
Estonia	99.5	3
España	98.5	4
Francia	97.6	9
Luxemburgo	97.4	13

Alemania	97.4	13
Portugal	97.3	14
Letonia	97.3	15
Bélgica	96.3	19
Italia	96.1	20

Mientras que los países restantes van de un rango desde el 95% el más alto, hasta el 67% que le corresponde a Bulgaria.

Como se ha mencionado anteriormente, el ciberespacio suele ser complejo y de carácter amenazante, y si lo que se busca es garantizar la seguridad, el hecho de que la UE sea una de las entidades más desarrolladas en temas de ciberseguridad y ciberdefensa, lo posiciona en un papel importante en el ámbito internacional. Algunos investigadores como Machín y Gazapo (2016), aluden a la importancia que se tiene sobre crear nuevos mecanismos de defensa para garantizar un ciberespacio libre y abierto que es lo que se busca desde la perspectiva de la Unión Europea. Entre las vertientes que estos autores toman como referente para analizarla están: construir una Unión Europea resiliente a nivel cibernético, fomentar la participación público-privada en materia de ciberseguridad, impulsar la cooperación con otros actores internacionales sólidos, como es el caso de Estados Unidos y la OTAN, por último adoptar estrategias y mecanismos de defensa enfocados a largo plazo con la finalidad de garantizar un nivel alto de seguridad en sus redes y sistemas de información. Sin embargo, es relevante mencionar el esfuerzo que han hecho los países miembros de la UE, puesto que hoy en día se cuenta con un total de 22 actores distribuidos en tareas enfocadas en tareas que tienen que ver con la ciberseguridad y ciberdefensa (Demurtas, 2020), estos componen el mapa europeo de la ciberseguridad, lo cual representa una expansión pertinente en ciertos ámbitos como lo son, el normativo y el político principalmente, y en cuanto a la distribución del poder por parte de las autoridades a las que se les confiere la tarea de velar por el ciberespacio.

También, la investigadora Andrea García (2021), menciona que la Unión Europea logró posicionarse como un líder en la gobernanza digital, durante la pandemia, puesto que ha mostrado la capacidad que tiene de extender algunas de sus normas en el mundo, las cuales fueron creadas durante la contingencia sanitaria, estas son:

The Digital Services Package, se compone de tres preceptos principales, el primero dirigido a la lucha contra la desinformación (Democracy Action Plan), después el (Digital Markets Act) encaminado hacia los monopolios digitales y el (Digital Aervices Act) que combate el contenido ilícito en línea. Es de reconocerse que la evolución legislativa y la creación de mecanismos de defensa en materia de ciberseguridad y ciberdefensa que ha tenido en los últimos años la Unión Europea ha logrado contrarrestar ciertos riesgos cibernéticos, pero aún falta mucho camino por recorrer.

En cuanto a la relación China-Unión Europea, en materia legal, se dice que la Ley de Seguridad de Datos (DSL) y la Ley de Protección de Datos (PIPL), antes mencionadas, logran que China se posicione en un nivel de protección similar (visto desde un ámbito jurídico), al que se encuentran algunas leyes que regulan la seguridad en internet de la Unión Europea. Ya que dichas normativas, hasta ahora son caracterizadas por permitir una “libre circulación” en el ciberespacio, preocupada por la protección de datos personales. Sin embargo, dichas leyes tendrían que ser analizadas desde otro ámbito de comparación, puesto que existe una gran diferencia entre ambas culturas, que van desde lo social, hasta lo económico y político, por mencionar algunos. Además de que como ya se había referido, el sistema que rige a China es más controlador en comparación al estadounidense y europeo.

Por último, según menciona Marina (2021), Europa cuenta con empresas tecnológicas de carácter competitivo, pero no con el nivel que tienen Estado Unidos y China, y esa fuerte competencia económica hace que Europa se

encuentre desprotegida en cuanto al nivel de una guerra ciberpolítica en el ámbito tecnológico. La historia que engloba a China, EEUU, es un juego cibergeopolítico, donde la Unión Europea tiene un papel importante para el equilibro de poder en ambos Estados, y dicho poder podría definir qué tanto influyen esas potencias es sus estrategias de ciberseguridad y ciberdefensa. Sin embargo, la historia nos ha enseñado que su postura sea conforme a su aliado americano.

Una vez analizados los tres esquemas, el chino, el estadounidense y el de la Unión Europea, se puede inferir entonces, que los Estados han encontrado en la ciberseguridad y la ciberdefensa, herramientas que confieren la apertura a una nueva forma de recuperar aquellos espacios de acción e influencia social (Patiño, 2021), en la que los gobiernos antes no se habían adentrado y los que permite también una posición en el ámbito internacional y un control mundial, en términos tecnológicos y estratégicos.

Tabla 4. Comparativa de los esquemas de ciberseguridad y ciberdefensa de: China, Estados Unidos y la Unión Europea. Elaboración propia.

País	China	Estados Unidos	Unión Europea
Objetivos	* Regulación del contenido de Internet, seguridad del ciberespacio. *Resguardar la confidencialidad de datos personales como un medio estratégico para fortalecer a la seguridad del ciberespacio. *Estudiar a la ciberseguridad y a la ciberdefensa desde un enfoque socio político más que técnico.	*Fortalecer a la ciberseguridad y ciberdefensa para hacer crecer al ejercicio gubernamental. *Crear nuevas estrategias técnicas con el fin de liderar en el ciberespacio	*Impulsar la ciberdiplomacia. *Aumentar la ciberresiliencia. *Combatir la ciberdelincuencia y proteger las infraestructuras críticas. *Crear un ciberespacio seguro y confiable, aumentando su ciberseguridad para reforzar el liderazgo digital.

Nivel en ciberseguridad y ciberdefensa	Medio	Alto	Alto
Autoridades responsables y departamentos de protección en el ciberespacio	Administración del Ciberespacio de China (ACCh) Ministerio de Seguridad Pública Ministerio de Industria y Tecnología de la Información	*Agencia Central de Inteligencia *Centro Nacional de Coordinación de Telecomunicaciones (NCC) Comando Cibernético (Uscrybercom) *Comisión Militar Central Departamento de Defensa *Equipo de preparación para Emergencias Informáticas de EE.UU. (US-CERT) *Equipo de Respuesta a Emergencias Cibernéticas de Sistemas de Control Industrial (ICS-CERT) *Oficina General de Investigaciones *Servicio Secreto de EE-UU. *Unidad contra Delitos	*Agencia de la Unión Europea para la Ciberseguridad (ENISA) *Agencia Europea de Defensa (AED) *Centro Europeo de la Ciberdelincuencia (Europol) *Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad *Equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la Unión Europea (CERT-EU) *Supervisor Europeo de Protección de Datos (SEPD)

		Cibernéticos del C3	
Principales mecanismos de defensa	Apoyo de un marco jurídico Control por parte del gobierno para resolver problemáticas en el ciberespacio. Un alto nivel en el desarrollo de tecnologías	Contar con el apoyo de empresas públicas y privadas en beneficio de mejorar la seguridad informática. Control y liderazgo del comercio electrónico	División de tareas por parte de las distintas autoridades encargadas de velar por la seguridad en el ciberespacio. Constante actualización en cuanto a la normativa que regula al ciberespacio.
Similitudes	• Se han creado leyes, normas y reglas para la salvaguarda del ciberespacio para lograr sus objetivos. • Creación de organizaciones que tomen acciones en la gobernanza del ciberespacio. • Búsqueda de la prevención de ataques cibernéticos, así como la protección de las infraestructuras críticas. • Relaciones de interdependencia en el ámbito internacional • Buscan la supremacía y el liderazgo en el ciberespacio.		

Diferencias	Proyecto de ciberseguridad con una mayor injerencia Estatal. Idea de una comunidad en el ciberespacio basada en el respeto a la soberanía cibernética de cada nación. Modernización económica y control político	Interponen los intereses nacionales propios antes que los de otros Estados. Énfasis en proteger las redes de información de posibles ataques terroristas y el cibercrimen	Participación y distribución de tareas de las distintas instituciones del ciberespacio, así como el desarrollo en áreas principales y herramientas que contrarresten los riesgos de ciberseguridad.

CAPÍTULO III. PROPUESTA DE UNA POLÍTICA PÚBLICA EN CIBERSEGURIDAD Y CIBERDEFENSA PARA EL CASO MEXICANO

3.1 Política pública en Internet

En los últimos años, las políticas públicas de manera general han adquirido cierta importancia desde el enfoque de las ciencias sociales, este campo estudia (Méndez, 2010), aspectos que están relacionados con los procesos de definición de los objetivos del Estado en el ámbito público, el desarrollo de las organizaciones y programas que se encargan de alcanzar dichos objetivos y también, tratan de estudiar el impacto que pueden generar los programas implementados.

Ahora bien, el término que se le da a las políticas públicas hace la distinción entre politics (política) y policies (políticas). El primero se entiende como las relaciones de poder, los procesos electorales y las confrontaciones entre organizaciones sociales con el gobierno. Mientras que el segundo se refiere a las acciones, decisiones y omisiones de los actores que se ven envueltos en actos de carácter público (Aguilar, 2017).

En palabras de Aguilar (2010, p.13), las políticas públicas son: “las acciones de gobierno que tienen como propósito realizar objetivos de interés público y que los alcanzan con eficacia y aun eficiencia”.

Para que una política pública se lleve a cabo debe constar de un proceso o ciclo durante su desarrollo, que consta de al menos los siguientes pasos: entrada en la agenda gubernamental, definición del problema, diseño, implementación y evaluación (Arellano y Blanco, 2013).

Por otro lado, el fenómeno de “política pública en internet”, es un tema aún más reciente, los objetivos de ésta, se podría decir que se enfocan principalmente en: disminuir la brecha digital, crear un ciberespacio libre y seguro, disminuir los delitos en internet, la apertura al gobierno electrónico (e-gobierno)[29], educación digital, por mencionar algunas. Sin embargo, el avance de las nuevas tecnologías, en especial del ciberespacio, requiere la actualización próxima a cada agenda de gobierno para la regularización en estos asuntos, y más aún en cuestión a la ciberseguridad y ciberdefensa, que son incluso tópicos menos concurridos.

Esta nueva tarea de generar políticas públicas enfocadas en la seguridad del mundo digital debe ser puesta en la agenda pública, no solamente por el incremento en el uso de las TIC, sino debido a las amenazas que sufren los sistemas informáticos estatales, ya que muchos regulan redes de distribución y servicio gubernamentales a través de internet. (Macuaran, 2019).

Según apunta Paniagua (2015), la importancia de analizar a las políticas públicas en Internet radica a partir de los resultados que se desee obtener, puesto que las decisiones públicas que se tomen siempre deben tener como objetivo el bienestar de la sociedad. Además de que la integración de estas políticas depende en cuestión, del diseño, la articulación de sus instrumentos, servicios y acciones que facilitan la implementación y su evaluación.

Ya que como menciona Martínez (2001), el poder que tienen las políticas públicas es que, son vistas como una herramienta potencial cuya capacidad radica en buscar soluciones a los problemas sociales, mientras que internet sirve para fortalecer esa capacidad de las políticas públicas y así lograr calidad, oportunidad y transparencia en la resolución de problemas.

[29] Según mencionan Criado y Gil (2913), el e-gobierno funge como un accesorio dentro de la administración pública que se deriva de la utilización de las TIC en distintas áreas de la acción pública.

El promover políticas públicas en internet enfocadas también en la ciberseguridad y ciberdefensa respectivamente, es un acto intrínseco de la gobernanza de internet, puesto que estos temas surgen como fenómenos recientes que parten de la premisa que de internet es una herramienta global y que no cuenta con la capacidad de ser regulado por un solo actor, sino que requiere la participación de otros miembros con influencia internacional, regional y nacional, para promover un espacio pluralista, democrático y de discusión (Palacio y Cabrera, 2017).

De modo que, es importante definir el concepto en sí de lo que es la política pública en internet, ya que como bien menciona Concha (2006), hoy en día, más que fijar un plan estratégico enfocado en la construcción de políticas públicas en este ámbito, se debe fomentar a la participación de instituciones públicas y privadas que interactúen con los ciudadanos, para que el internet sea un espacio colectivo capaz de generarlas y que permita también que los ciudadanos se conviertan en sujetos activos en esta área.

> Las políticas públicas de Internet, para que puedan concretarse y sostenerse no pueden enfocar exclusivamente lo tecnológico y lo económico, y acentuar solamente en el acceso y la conectividad. Deben privilegiar el factor humano, es decir enfatizar en la capacitación, para que las personas y los colectivos identifiquen para qué les pueden servir las TIC y puedan generar sus propios usos, apropiarse de ellas y crear aplicaciones y contenidos (Albornoz, 2006, p. 107).

Además, como bien menciona Ríos (2021), las políticas públicas implementadas en internet tienen que estar orientadas a crear un uso productivo de Internet y el desarrollo de habilidades tecnológicas.

Sin embargo, Palacio y Cabrera (2017), identifican que, las políticas públicas, implementadas en internet, que tienen como fin la cobertura mundial y un desarrollo en la calidad de la educación a través de las TIC, siguen siendo precarias, puesto que se necesita que la gobernanza en internet permite la apertura a otros espacios de debate y una mayor participación entre sus actores. Y peor aún, el desarrollo de políticas públicas enfocadas en ciberseguridad y ciberdefensa, son aún temas inexistentes incluso en algunos lugares del mundo.

Es decir, se trata de que internet sea visto como una herramienta potencial, sin embargo, el verdadero desafío es lograrlo, y encontrar la manera de generar políticas públicas en internet para que éstas provoquen un verdadero impacto social positivo que responda mejor a las demandas del sector de la población al que van dirigidas (Martínez, 2001).

Alrededor del mundo, los gobiernos y otros organismos tanto públicos como privados se han interesado en temas que competen a la ciberseguridad, en conjunto con la ciberdefensa, debido a los riesgos que existen en el ámbito de la seguridad nacional, y en el financiero. Por tanto, es un deber que se elaboren políticas públicas que busquen la protección al patrimonio de la sociedad como a las actividades de la administración pública (Aguirre, 2022).

3.2 Los modelos de políticas públicas y otras acciones implementadas para la protección del ciberespacio, fomento a la ciberseguridad y ciberdefensa alrededor del mundo.

A nivel internacional el Centro de Excelencia de la OTAN para la Ciberdefensa, se ha colocado hasta ahora como el organismo mejor preparado en cuestión gracias a la cooperación y transmisión de información entre los Estados miembros de la OTAN. Mientras que en España se ha creado el Instituto Nacional de Ciberseguridad (INCIBE), que se ha encargado de generar una confianza digital de sus ciudadanos y empresas (Huete, 2021).

También, las iniciativas en ciberseguridad se producen con distintos alcances, que van desde, lo global, pasando por Naciones Unidas, en conjunto con la Unión Internacional de Telecomunicaciones (Ramirez, 2015). Como ya se había mencionado previamente, este organismo antes mencionado se ha encargado de realizar una evaluación en cuanto al nivel de ciberseguridad de sus países miembros. Al igual que la Unión Europea, la Organización de Estados Americanos y la Unión de Naciones Suramericanas, han sumado esfuerzos para comprometerse a mejorar la ciberseguridad de sus naciones.

Tal es el caso de la política internacional de ciberseguridad de la Unión Europea, cuyo objetivo es abordar los desafíos y promover la estabilidad cibernética global (Herczynski, 2020).

Las naciones de Europa y Norteamérica, que pertenecen a la OTAN, han priorizado que el ciberespacio se convierta en un mercado negociable y de alto valor, y por tanto se enfoque en la seguridad el Estado Nación. Sin embargo, existen otras naciones que aún se encuentran en aras del desarrollo legal o bien de documentos actualizados en materia de ciberseguridad y ciberdefensa, tal es el caso de, América Latina, África y el Medio Oriente, que trae consigo una

desventaja internacional puesto que no permite que estas regiones desarrollen las capacidades necesarias para enfrentar ciberamenazas (Aguilar, 2020).

Como menciona Leyva (2021), en el caso de los países de Latinoamérica, los problemas a los que se enfrenta traen consecuencias devastadoras, puesto que muchos de los países pertenecientes a esta región no cuentan con estrategias dignas de protección ante posibles ciberataques, ni tampoco con planes que protejan a sus infraestructuras críticas, o bien un organismo con la capacidad de controlar dichos conflictos que se presentan, y en el peor de los casos, tampoco se cuenta con una fiscalía con los instrumentos legales para dar seguimiento a los delitos informáticos. Como consecuencia de ello, se tiene una falta de legislación actualizada en estos temas pertenecientes a las nuevas tecnologías de la información.

Si bien, para el caso de América Latina, los países que se han adentrado en la formación de políticas públicas en temas de internet, el ciberespacio, ciberseguridad y ciberdefensa, siguen siendo casos aislados, pero que no demeritan el esfuerzo implementado, como por ejemplo los países que ya cuentan con una política o Estrategia Nacional de Ciberseguridad son: Chile, Colombia, Costa Rica, Guatemala, Jamaica, México, Panamá, Paraguay, República Dominicana y Trinidad y Tobago (Álvarez, 2018).

En Panamá (Masís, 2019), se redactó la Declaración de Panamá sobre la protección de la infraestrcutura crítica en el hermifesferio frente al terrorismo, en ella se habla acerca de la importancia que tiene la cooperación internacional, estatal y el sector privado para hacer frente a la protecciión de sus infraestructuras.

Mientras que en Argentina en el año 2011 se creó el “Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad” (ICIC), adjuntando a los organismos interjurisdiccionales, organizaciones civiles y sector privado, que requieran proteger e identificar sus infraestructuras críticas (Masís, 2019).

En palabras de Hiram (2022), hace alusión a la “seguridad de papel” a aquellos países que cuentan con una normativa en cuanto al ámbito tecnológico pero que no llevan a cabo ningún mecanismo para su implementación. Haciendo referencia sobre todo a los países de América Latina, puesto que, en 2021 en esta región y el Caribe los ciberataques aumentan en un 600% según datos de Fortinet, una empresa líder en ciberseguridad, es decir se llevaron alrededor de 289.000 millones de intentos de ciberataques (Vera, 2022).

Pero, por otro lado, en Colombia (Cortés, 2015), existe una política pública líder en cuanto al papel del Estado como actor principal para enfrentar desafíos que plantean la ciberseguridad y la ciberdefensa. Si bien, en el capítulo primero se mencionó que ya existen en Latinoamérica algunas instituciones o CERT que se encargan de velar por la seguridad en el ciberespacio. En Colombia (Palacio y Cabrera, 2017), el escenario de la gobernanza de Internet comienza a ser un tema en el papel del Estado, éste ha tenido influencia en cuanto a políticas públicas en materia de educación a través de las TIC.

También, en el año 2017 en Chile se creó la Política Nacional de Ciberdefensa, como respuesta al Estado para generar las capacidades de defensa nacional, en cuanto a su información, infraestructura y operaciones que se emplean, dicho documento establece sus objetivos para ser cumplidos en el presente año, 2022, estos fueron propuestos por parte de las instituciones de Defensa Nacional (Álvarez, 2018).

Para el año de 2020, el Gobierno de Canadá, apoyo a la Junta Interamericana de Defensa (HID) para lanzar el Programa de Ciberdefensa[30], que respalda a 29

[30] Si bien esta guía se basa en la ciberdefensa desde el ambito militar, también proporciona algunos conceptos básicos que se relacionan con ese fenómeno, como por ejemplo: el

países miembros, entre ellos México, para fomentar a la creación, planificación, diseño, desarrollo y despliegue de políticas en el ámbito de la ciberdefensa (José, 2020).

Mientras que Suiza ha implementado algunas políticas públicas para contrarrestar los riesgos de la ciberseguridad donde se habla incluso de la red 5G, uno de los objetivos de esa nación es formar especialistas cuya capacidad radique en atender emergencias en el ciberespacio (Aguirre, 2022).

Si bien, lo mencionado en párrafos anteriores, sólo hacen menciones de algunos países, estos muestran claramente cómo cada nación ha construido esas políticas públicas, estrategias, organismos y mecanismos de defensa para proteger su entorno digital conforme a sus intereses, y sin desatender a las herramientas necesarias para una eficaz ciberseguridad y ciberdefensa. Estas medidas se adoptan dependiendo a las necesidades de cada nación y si bien, hasta ahora no se ha fijado un modelo ejemplar a seguir, se sabe que existen países más avanzados en estos temas. Sin embargo, con ayuda de la cooperación internacional se podría construir una base sólida que permita disminuir la brecha entre países y para concientizar que el ciberespacio, es ahora también un nuevo mundo al que tenemos que cuidar y proteger.

---

ciberespacio, la ciberseguridad, ámbito de operaciones ciberespacial, ciberdefensa militar, fuerza ciberespacial, ciberamenaza, ecosistema ciberespacial, por mencionar algunos.

3.3 Política pública en ciberseguridad y ciberdefensa en México

En el primer capítulo, ya se argumentaba acerca de la problemática que se tiene en México en cuanto a la ciberseguridad y a la ciberdefensa, puesto que si bien, son temas que ya se han puesto en la agenda pública de diversos países, sobre todo en los más desarrollados en el ámbito tecnológico, en México se requiere de una mayor y mejor organización para mitigar los riesgos en el ciberespacio. Existe un sin fin de inconvenientes que imposibilitan que esta política pública se lleve a cabo, pero el hecho de que no se haga hincapié en su desarrollo no quiere decir que no sea importante su implementación.

En países como México, el hecho de pensar en la elaboración de políticas públicas requiere de retos trascendentales, puesto que la tendencia al cambio no suele ser de manera general, y mucho menos el proceso de la modernización. Además de que desde la perspectiva del gobierno, siempre existirán distintas concepciones en cuanto a la prioridad de asuntos sociales, por resolver (Sánchez, 2008), tal es el caso de los problemas que emanan del ciberespacio, puesto que debido a la polaridad tan marcada en la que se encuentra la sociedad se sabe que hay conflictos más urgentes a resolver, que caracterizan a cualquier sociedad y que parecen nunca tener fin, la pobreza, asesinatos, corrupción, desigualdad social, por mencionar algunos.

Sin embargo, la sociedad parece estar más conectada con la realidad virtual, que en el mundo real, ya que en los últimos años la interacción en el ciberespacio ha crecido de manera inmensurable, que desde la perspectiva de una política pública en internet, esto es algo beneficio, puesto que da apertura incluso a la democratización por esta vía e influye en la manera en que nos relacionamos con el propio gobierno y el alcance que tenemos hacia él.

Por ejemplo, como menciona Castañeda (2020), para el caso mexicano, si lo que se busca es implementar la economía digital, se deben tomar en cuenta los siguientes aspectos, enfocados en la elaboración de las políticas públicas en

internet; brindar servicio de internet total a la población mexicana, la reducción de los costos de banda ancha, el Internet de las Cosas (IoT), las redes 5G, la Inteligencia Artificial (IA) y la ciberseguridad.

Actualmente, la protección de la seguridad en el ciberespacio tiene que ser una prioridad en la agenda pública de cualquier gobierno, y esto exige el desarrollo de políticas públicas enfocadas en la prevención y evaluación a las futuras amenazas en el mundo virtual. Como se ha mencionado con anterioridad, el papel fundamental que tiene el Estado como actor principal en el ámbito de la ciberseguridad y la ciberdefensa, y en palabras de Pizarro (2002), éste sigue siendo el actor político clave en la sociedad y la expresión más aceptada del interés colectivo. Lo verdaderamente significativo, por tanto, no es su presencia en el proceso político general, sino la transformación de su rol, que pasa a estar fundamentado en la coordinación y la falta de discernimiento entre las esferas pública y privada (Pizzarro, 2002, p. 2), por tanto, la presencia del Estado en los procesos de gobernanza puede ir desde su contemplación como coordinadores hasta ser uno tan sólo de los actores políticos más relevantes del proceso de gobernanza.

La protección de la seguridad en el ciberespacio también se ha convertido en una prioridad para los poderes públicos, que exige el desarrollo de políticas adecuadas para prevenir y contrarrestar las amenazas que se materializan en el mundo virtual. Como menciona Martínez (2020), en algunos Estados, se plantea el debate sobre el alcance de las competencias de las entidades estatales en materia de ciberseguridad, sobre todo porque los gobiernos, organismos y servicios públicos son un posible objeto de ataque en el ciberespacio.

Por lo tanto, es necesario contar con el apoyo de políticas nacionales cuya capacidad sea coordinar una ruta clara para el diseño e implementación de medidas que permitan proteger la seguridad y derechos de los ciudadanos en el ciberespacio (Viollier, 2017).

Una política pública en ciberseguridad y ciberdefensa no sólo puede prevenir y sancionar actos ilícitos cometidos en el ciberespacio o bien a las infraestructuras críticas de información, sino también a través de ellas se puede generar confianza en los cibernautas empleando incluso el uso de las TIC. Las políticas públicas también, ofrecen a su vez la ventaja de adoptar medidas y soluciones técnicas para aumentar la seguridad en el ciberespacio (Gobierno de Chile, 2020), convirtiendo así al ciberespacio en un lugar confiable, de libre expresión y que valide el cumplimento de los derechos humanos en el ciberespacio.

Como tal, no existe hoy en día la definición exacta de los que sería una política pública en ciberseguridad y ciberdefensa, pero si recordamos que una política pública es una acción del Estado que está dirigida a cumplir algunos objetivos, se podría decir entonces, que esta política pública estaría enfocada en: las acciones del Estado, en conjunto con la sociedad civil y el sector privado para minimizar los riesgos que se presenten en el ciberespacio y para proteger las infraestructuras críticas de información, así como garantizar la protección de la soberanía nacional a través de sus mecanismos y recursos con los que cuenta.

Con el apoyo de algunos textos elaborados por gobiernos e instituciones de carácter público y privado de distintos países, se presentan a continuación, posibles alternativas que bien podrían ser aplicadas al caso mexicano para el desarrollo de una política pública en ciberseguridad y ciberdefensa.

3.3.1 Inclusión digital y disminución de la brecha digital

La desigualdad del acceso a internet y demás tecnologías de información, es uno de los temas emergentes hoy en día en las agendas públicas de la mayoría de los países. El acceso a internet es fundamental para entender la interacción del ser humano con respecto a la ciberseguridad y a la ciberdefensa, ya que, sin esta, el esfuerzo por fomentar una política pública en estos temas, sería considerada innecesaria.

El trabajo que se tiene sobre disminuir la brecha digital es el que implica un mayor esfuerzo, no sólo en México, sino en todo el mundo, incluso en los países más desarrollados, el problema de la brecha y desigualdad digital sigue sin resolverse. Sin embargo, el problema emana de diversos aspectos, no sólo en el ámbito tecnológico, sino principalmente en el económico, se sabe que el acceso a internet no es de manera equitativa en ningún lugar del mundo. Existen diversos factores que determinan esto, por ejemplo, el área geográfica, el nivel socioeconómico de las personas, la edad, el género, por mencionar algunos.

Internet (Martínez, 2001), por un lado, agrava las desigualdades sociales, económicas y políticas, es decir, desde esos ámbitos intensifica a la brecha digital, puesto que se convierte en un factor más de exclusión, pero por el otro lado, facilita la vida a los cibernautas e incluso al gobierno.

Por ejemplo (Criado y Gil, 2013), en el caso de la implementación del “e-gobierno”, se prevé que el objetivo de interconectar a la administración pública y al gobierno por medio de medios digitales, se intensifique o sea de mayor interacción, todo esto mediante la creación de políticas públicas que se orienten a grupos más vulnerables con acceso limitado a internet. Pero bien, lo anterior antes mencionado, está muy ligado con la tarea que el gobierno y el Estado tienen para fomentar a las prácticas de participación en ciberseguridad y ciberdefensa.

El gobierno también ha hecho hincapié en la importancia que tiene el uso de internet en nuestros días, no obstante, no existe aún la respuesta para que este servicio sea accesible para todos.

Por ejemplo, en el caso de México, el Instituto Nacional de Estadística y Geografía (INEGI), desde el año 2015, se encarga de la captación de datos sobre las tecnologías digitales en el sector social, que recibe el nombre de: la Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares (ENDUTIH)[31], dicha muestra representativa, reveló que para el año 2020, de un total de 20 millones 059 mil 794, un 59.7% no cuenta con una computadora disponible por falta de recursos económicos, mientras que de los 1 millón, 368 mil 244 hogares que sí disponen de una computadora, el 56.67 % no cuenta con conexión a Internet por los mismos motivos. Además que, 21 millones, 641 mil 607 hogares, que equivale al 60.6%, cuentan con Internet.

Según informo la Asociación de Internet.mx (2019), en el año 2018 el informe de Evaluación de la Política de Desarrollo Social de la Coneval, mencionó que en México existen alrededor de 53.4 millones de personas en situación de pobreza, de los cuales, Guerrero (23%), Oaxaca (26.9%) y Chiapas (28.1%) son los que mayor pobreza concentran, dichos estados coinciden también en ser los que menor penetración tienen de internet y telefonía móvil, el mismo informe, apoyado por la ENDUTIH 2018, menciona que de los 70 millones de usuarios de teléfonos inteligentes (smartphones) en el país, los tres estados antes mencionados son los que menos usuarios de telefonía cuentan. Además, que de 82.7 millones de internautas, Chiapas y Oaxaca son los que menos usuarios de internet tienen. Sin embargo, en la zona Centro Sur (Ciudad de México, Estado de

[31] El dominio es a nivel nacional, nacional ámbito urbano, nacional ámbito rural, por entidad federativa y por estrato socioeconómico. Mientras que la cobertura temática se basa en: Equipamiento de TIC, medios de conexión a Internet, las limitantes de acceso, capacidad de uso de computadora, Internet y telefonía celular, comercio electrónico, formas de uso de Internet, radio y tv abierta.

México y Morelos), la zona Noroeste (Baja California, Baja California Sur, Chihuahua, Durango, Sinaloa y Sonora) y el Oeste (Colima, Jalisco, Michoacán y Nayarit), son las zonas donde existe una mayor presencia de internautas.

Como lo menciona De la Cruz (2021), en América Latina, existe una urgencia de modificar todas las tecnologías, así como en desarrollar habilidades, ya que de nada servirá que tanto las industrias como el gobierno trabajen de manera conjunta para mejorar las condiciones de regulación, sino existe la capacidad de proveer a las personas habilidades digitales para que puedan aprovechar las nuevas tecnologías.

Hoy en día, al menos en la Ciudad de México, se han creado redes de internet con acceso libre, lo que permite que cualquier dispositivo electrónico, logre estar conectado de manera gratuita a internet, si bien, esta alternativa es eficaz, aún se debe buscar la manera en que todas y todos estén conectados incluso desde sus hogares, sin embargo, la contratación a este servicio es de paga, lo que imposibilita que la sociedad cuente con esta tecnología.

Para que una sociedad tecnológica funcione, como bien mencionan Torres y Vila (2014), el acceso universal a un internet libre y abierto debe coadyuvar a los principios de apertura, libertad, colaboración y democracia basado en las políticas y el desarrollo que lo regulan. Ya que, se debe entender que Internet es un bien común, y esto, por tanto, “es el fundamento para contrarrestar las distintas formas de dominación (incluyendo la dominación política), las subordinaciones culturales, las dependencias tecnológicas, la consolidación del modelo de apropiación privada del conocimiento y de centralización”.

Por tanto, se debe apuntar a mejorar la cobertura e incentivar a la apertura de los servicios sociales, como por ejemplo, a través de la educación en línea o la telemedicina, e incluso se pueden mejorar los procesos de

participación ciudadana como la formulación, ejecución, monitoreo y evaluación de posibles políticas públicas (Martínez, 2001).

3.3.2 Participación consciente de los ciudadanos en el ciberespacio

Al hablar de participación ciudadana, se piensa inmediatamente en el papel que juega la democracia en este ámbito (Carrión, 2007), no obstante, la premisa a resolver con respecto a esto es la manera en que los ciudadanos toman las decisiones, pero en el ciberespacio, puesto que esto influye en las acciones que realizan dentro de él. Un punto importante es que las instituciones tienen que tomar en cuenta que el oír, consultar y hacer partícipe a los ciudadanos mejora el ejercicio en los derechos y responsabilidades, al igual que fomenta la transparencia e incentiva a la democracia (Carrión, 2007), y todo esto es importante para el abrir camino hacia la construcción de las políticas públicas. Por tanto, lo antes mencionado, es aplicable también en el ciberespacio.

Por otro lado, y para entender un poco más el contexto de este apartado sobre la importancia que tiene el saber utilizar de manera correcta las tecnologías de la información, y tratando siempre de que se sea en beneficio para de la población, es que, por ejemplo, en la ENDUTIH, también se analizó que dentro de esa parte de la población que no cuenta con una computadora o algún otro dispositivo con conexión a internet, se tiene que el 11.5% de la población no sabe utilizar este tipo de tecnologías.

Se podría hacer una encuesta donde incluya preguntas con respecto a la concientización del uso de esta tecnología, y que atienda a otros aspectos importantes que emana sobre todo del empleo de internet, como es el caso de la ciberseguridad en sus medios digitales. Ya que la mayoría de la

población con acceso a internet no tiene idea de lo vulnerable que es su privacidad, una vez ingresada cualquier tipo de búsqueda por este medio.

Sin embargo, esta tarea resulta complicada debido a que estos temas pasan a segundo plano, una vez se entra al mundo de internet, puesto que la mayoría de la población encuentra en el ciberespacio, un lugar de entretenimiento, incluso antes que un medio educativo, es decir, anteponen su comodidad, antes que su privacidad, sin darse cuenta de lo expuestos que se encuentran.

En el año 2013, INEGI, realizó la Encuesta sobre Tecnologías de la información y las Comunicaciones (ENTIC 2013), cuyo objetivo fue recabar información acerca de los recursos humanos, financieros y de infraestructura que las empresas del sector privado emplean a través de las tecnologías de información, como apoyo para elaborar políticas públicas en el desarrollo de esos ámbitos. Aunque dentro de sus variables a considerar, no se aborda el tema de ciberseguridad, a pesar de que sí hace mención a aquellas empresas que detectaron un problema de seguridad informática o bien, se les pregunto si contaban con algún tipo de seguridad informática, también se contemplaron datos acerca de la capacitación que recibe el personal en cuanto a las TIC´S. Si bien esta herramienta resulta útil, considero que esa encuesta debe ser actualizada y con una nueva formulación de preguntas, o bien, se podría crear una encuesta que radique alrededor de estos nuevos conceptos que emanan del ciberespacio, en especial de las variables que competen a esta investigación, la ciberseguridad y la ciberdefensa.

Entre las preguntas, se podrían considerar las siguientes: ¿Qué tan segura me siento en el ciberespacio?, ¿Conoces los riesgos de proporcionar datos de carácter privado a cualquier sitio web?, ¿Me siento segura cuando introduzco datos bancarios o de índole personal?, ¿Qué tan familiarizada estoy con los conceptos de ciberseguridad y ciberdefensa?

También se puede contemplar la creación de talleres con fines educativos en el área de ciberseguridad y ciberdefensa, ya sea que sean impartidos por organismos públicos y/o privados, esto puede ser un primer paso para hacer una llamado de atención a que la población se ocupe de salvaguardar sus datos personales. E incluso en educación básica, las materias como computación, uso de TIC o que estén relacionadas con la rama de la informática, debería ser prioridad enseñar a las alumnas y alumnos de qué manera pueden protegerse en el ciberespacio.

Otra alternativa que propone Mendez (2015), para la concientización es, diseñar planes de capacitación especializada de ciberseguridad y ciberdefensa a través de mensajes, volantes, encuestas o incluso juegos interactivos. Claro, haciendo uso de las tecnologías de la información.

Como menciona Araya (2007), Internet por sí solo no genera ciudadanía, ni tampoco aumenta la participación ciudadana de manera automática, ya que, una sociedad que no es participativa, no tiende a serlo por sí sola, incluso a pesar de contar con los medios necesarios para incorporar herramientas tecnológicas, sin la interacción de las instituciones o autoridades correspondientes esto no sería posible, es decir, la importancia de esto radica entonces, en el papel que tienen las autoridades para fomentar la participación ciudadana como parte de la retroalimentación.

Las medidas de prevención en concientización sobre el uso de las tecnologías de información son necesarias para que se evite la pérdida de bienes, robo de datos personales, al mismo tiempo que ayuda a mitigar la delincuencia organizada en el ciberespacio (Aguirre, 2022), he ahí la importancia de crear conciencia sobre la importancia que tiene el saber proporcionar información en este medio.

3.3.3 Creación de un ciberespacio libre de expresión e intercambio comercial seguro

Ya se mencionaba que el ciberespacio tiende a ser un lugar donde la población puede expresarse con toda libertad, y que sus fronteras no delimitadas lo permiten. En la mayoría de los casos esa libertad de expresión no es censurada, pero no siempre es así, ya que muchas veces cuando la idea no es afín con cierto sector de la población o incluso con el propio gobierno de cualquier país, se censura.

En concreto, la libertad de expresión esta se debe garantizar sobre todas las cosas, siempre y cuando no vulnere la integridad de otro ser humano, pero hoy en día se sabe que el expresarse de manera “libre” en el ciberespacio ha traído consecuencias no tan favorables, ya que, debido a lo expuestos que estamos en internet, se han encontrado las herramientas e información necesaria para ser usada en contra de otro cibernauta, lo que da origen a un nueva problemática a la que nos enfrentamos los ciudadanos, entonces, de qué manera sí se podría respetar esa libertad de expresión sin que sea censurada ni usada para vulnerar la integridad de otro ser humano, esa sigue siendo una variable aún sin atender, puesto que el ciberespacio siempre puedes atacar a otro ser, inclusive desde el anonimato.

Si bien, hasta ahora la policía cibernética y otras autoridades encargadas de velar por el ciberespacio, han salido adelante con algunas situaciones alarmantes, como por ejemplo, el ciberbullying, el acoso cibernético, la pornografía infantil en internet, tráfico de órganos por internet, entre demás delitos cibernéticos, se sabe que el trabajo a realizar por parte de las autoridades correspondientes aún es inmensurable, puesto que en

repetidas ocasiones no se les da la importancia que merece este tipo de conductas y se deja pasar como muchos otros delitos impunes que son característicos en México. Por eso, es importante atender a la cuestión de la regularización en el ciberespacio, contar con la legalidad autónoma y suficiente que pueda atender aquellos delitos cometidos en internet, dicha normatividad, tiene que ser actualizada constantemente, puesto que las tecnologías crecen de manera exponencial, y con ello los conflictos que traen consigo.

Ahora bien, pasando a otro punto de interés, que es el intercambio comercial por internet, o mejor conocido como comercio electrónico, se sabe que, hoy en día, cualquier producto de utilidad para la sociedad, puede ser encontrado de manera automática por medio de internet, esto ha ayudado a aumentar las ventas, agilizar la compraventa, facilitar la vida de las personas y disminuir egresos para las empresas. No obstante, ese intercambio comercial ya establecido, debe tener con sí un carácter de "mercancía segura", es decir, un espacio donde los cibernautas no sólo se sientan satisfechos con el producto adquirido, sino también con la plena seguridad de que su mercancía les será entregada en tiempo y forma, dicho de otro modo, lo que un comprador busca es no ser estafado, es decir, se deben encontrar los medios necesarios para que las páginas web sean confiables.

Una posible alternativa podría ser, que el gobierno cree un sitio web en donde se registren a las páginas que ofrezcan algún tipo de producto o servicio en línea, para comprobar el carácter fidedigno al momento de la compra venta, donde además los compradores o interesados puedan dejar una recomendación acerca del producto, ya sea sobre el precio, la calidad, etc. En la que incluso esto podría ayudar a los ciudadanos a detectar posibles fraudes o algunas irregularidades, además esto beneficiaría a los vendedores a incrementar sus ventas, pero por otro lado también los obligaría a aumentar su ciberseguridad en sus empresas.

En contraste, este proyecto sí tendría que ser financiado en parte por inversión privada a las que les interese se participe, tal es el caso también de las instituciones bancarias, puesto que hoy en día, México es considerado como uno de los países con más fraudes electrónicos, robo de datos, entre otros. Los cibernautas, deben tener la plena seguridad de que sus transacciones electrónicas están protegidas y son confidenciales.

Por ejemplo, Chile, en su Estrategia Nacional de Ciberseguridad (2017-2020), establece que se le debe exigir un nivel adecuado de ciberseguridad tanto al sector público como al privado, de acuerdo a algunos estándares como lo son: “la confidencialidad, integridad y disponibilidad de información y de los sistemas que operan” (pág. 18), también donde se identifiquen los riesgos y posibles amenazas.

Un gran avance en el ámbito comercial internacional es que, con la entrada del Tratado de Libre Comercio entre México, Estados Unidos y Canadá (T-MEC), ha incluido entre sus preceptos a la ciberseguridad, donde los países se comprometen a trabajar de manera conjunta para construir capacidades de respuesta ante posibles incidentes cibernéticos. Además de garantizar la privacidad de los datos entre sus consumidores (American Chamber México, 2020).

Mientras que en el ámbito nacional (Ríos, 2021), la Secretaría de Economía (SE), ha trabajado de manera conjunta con la Procuraduría Federal del Consumidor (PROFECO), en una Norma Mexicana para regular el Comercio Electrónico, cuya base servirá como una guía entre clientes y proveedores al momento de establecer algún tipo de intercambio comercial en línea. Además de que se considera necesario delimitar el ámbito geográfico de los mercados digitales, así como fomentar la cooperación internacional y dar solución a posibles problemáticas en este ámbito.

En el mes de abril del presente año, el Senado de la República, instaló en su sede un cajero de Bitcoin[32], y a pesar de que el país ya cuenta con 11 cajeros de esta criptomoneda[33] y que esto se considere un avance en cuanto a la implementación del uso de las tecnologías, a la par ya se tendría que estar creando entonces, una ley[34] que regule este tipo de operaciones y que a través de su normativa garantice la transparencia y seguridad en esta índole.

Según menciona Lecuit (2019), hoy en día, se debe implantar un nivel adecuado de ciberseguridad al sector privado, como requisito indispensable para aquellas empresas que se dediquen al comercio, compra pública de bienes y servicios, instalaciones e infraestructuras, además de las empresas que participen en cadenas de suministro, dicha regulación debe establecer un marco que permita el control en ámbitos como la organización y deliberación de las responsabilidades.

La demanda actual de las necesidades en la sociedad tecnológica, ha generado que el intercambio comercial y de servicios se puedan generar con un solo "click", sin embargo, se deben reforzar las medidas de seguridad ante el comercio electrónico y exigir a todo tipo de empresa que vele por su propia ciberseguridad, para que sus clientes sigan escogiendo a esa empresa por encima de las demás y donde se garantice que su mercancía llegue tal y como la imagino, sin ningún inconveniente. Además de que esta actividad trae consigo nuevos retos, como el de crear un marco normativo a nivel nacional como primer punto e internacional, de carácter sólido capaz de responder a las demandas de los sujetos interesados.

[32] Es considerada la primer criptomoneda y es la de mayor uso hoy en día, pero también ya existen otras como por ejemplo, Ethereum, Litecoin y Ripple.
[33] Según la empresa experta en ciberseguridad Kaspersky, menciona que una criptomoneda es un sistema de pago de tipo digital, el cual no depende de algún tipo de insitución bancaria que verifique la transaccion.
[34] En México existe la Ley Fintech que se encarga de regular las Insituciones de Tecnología Financiera, y sí bien, es un marco de referencia que hasta ahora ha sido eficaz, esta debe ir adecuandose a medida que las industrias financieras digitales se modifiquen o expandan.

3.3.4 Fomento a la información y concientización a los ciudadanos en materia de ciberseguridad y ciberdefensa

Según Araya (2006), existen criterios asociados a la incorporación de Internet en la gestión pública, él los resume en tres aspectos, una mayor eficiencia, transparencia en la gestión y cercanía con los ciudadanos. Mientras que a nivel gobierno, se esperaría que las tecnologías de información jueguen un papel importante, no solo para su beneficio, sino para establecer una nueva relación política, cuyos objetivos, serían: participar en el diseño de las políticas públicas, atender a la retroalimentación, dudas, quejas y sugerencias por parte de los ciudadanos y una mejor fiscalización.

El autor, también menciona que por parte de la ciudadanía se asumen que esas promesas traen consigo beneficios, como, por ejemplo, el acceso a la información sobre servicios públicos, lo que conlleva a la transparencia de los procesos gubernamentales, además que los ciudadanos esperarían un servicio de calidad.

Tal es el caso del voto electrónico por Internet en México, que se aprobó para las elecciones locales 2020-21, para que los ciudadanos que residen en el extranjero pudieran ejercer su voto. Esto da paso a una nueva materia en sustentabilidad democrática, ya que no sólo reduce costos, y agiliza el proceso, sino que genera un menor impacto ambiental, sin embargo, sigue siendo un tema pendiente, ya que debido al contexto histórico, la sociedad desacredita estas prácticas, y no lo ven como un proceso realmente confiable, y es aquí donde sobre todo la ciberseguridad juega un papel importante, puesto que si se demuestra que las instituciones autónomas encargadas de este ejercicio, contarán con un sistema de seguridad

confiable, se tendría otro tipo de panorama que pinta a ser favorable, y que sí bien, la inversión es de alto costo, los beneficios que ofrece el voto electrónico se vislumbran en un futuro próximo.

Cortés (2015), menciona que las políticas públicas en materia de ciberseguridad y ciberdefensa deben contar con los organismos y demás instrumentos jurídicos, que permitan que los países cuenten con una seguridad cibernética con la capacidad de garantizar a las instituciones públicas y privadas la salvaguarda de sus derechos, patrimonio e información. Dicho autor también enuncia que es fundamental la suma y el esfuerzo no sólo del sector privado y el público, sino incluir al sector militar, la academia y la ciudadanía, que ayuden a la creación de una ciudadanía bien educada en el mundo cibernético. En palabras de Mariano (2021), aumentar la concientización pública en ciberseguridad, y agregaría ciberdefensa también, puede elevar el nivel general de inmunidad contra posibles ciberataques. Puesto que los ciudadanos conocerán los riesgos a los que se exponen al compartir su información en internet.

Una de las problemáticas que también se presenta, es la falta de consenso global en cuanto al vocablo relacionado con el ciberespacio, y citando a la Junta Interamericana de Defensa (2020), es que, los términos que emanan de la palabra “ciber”, son de carácter controversial, puesto que no existe un único glosario para estas nuevas definiciones, y mucho menos una taxonomía actualmente aceptada. Lo que trae consigo desinformación no solo en la sociedad sino que también repercute a la visión que se debe tener a nivel gobierno y demás instituciones encargadas de la ciberseguridad y ciberdefensa, por tanto, esto dificulta la cooperación nacional e internacional, ya que las tareas que se asigna a las diferentes autoridades quedan incompletas puesto que muchas de ellas no son precisas y generan un esfuerzo doble, y además, no se sabe con exactitud para quién o quiénes tendrían que ser asignadas esas tareas en realidad.

3.3.5 Regularización del ámbito jurídico en el ciberespacio

Retomando a Fonfría (2020), menciona que la gobernanza de la ciberseguridad es un concepto establecido para alcanzar un objetivo, cuyo enfoque trata acerca de la gestión de riesgos que se basan en el seguimiento, la medición y el control de procesos en internet. Para esto, el término regulación, es un concepto clave, ya que engloba diversos temas como lo son: gobernanza, normas industriales, legislaciones nacionales, acuerdos internacionales, por mencionar algunos. Esa regulación en el ciberespacio debe tener la capacidad de generar confianza y mantener la estabilidad dentro de este.

Como bien menciona Porrúa (2019), un marco jurídico flexible y actualizado, permite perseguir los delitos informáticos cometidos por cibercriminales, que cada vez encuentran métodos más sofisticados para llevar a cabo sus objetivos. Él mismo autor propone la idea acerca de la construcción de una legalidad fragmentada, es decir no una sola ley global de ciberseguridad y ciberdefensa, ya que esa división permite hacer frente a la versatilidad de los delitos informáticos con una eficiencia mayor.

El Convenio de Budapest sobre la ciberdelincuencia, se considera hasta ahora el documento de carácter internacional más actual y completo sobre el marco legal ante ciberdelitos. Además de servir como guía para los países que estén en aras de desarrollar una legislación nacional en este ámbito (Consejo de Europa, 2021). Y a pesar de que México es un país invitado, aún no ha formalizado su adhesión a la Convención (Piña, 2019). Esto representaría un avance significativo en cuanto al fortalecimiento de los marcos regulatorios de ciberseguridad y ciberdefensa ya que se tendría un excelente intercambio de información a nivel mundial (Mendez, 2015).

Además de que reforzar la agenda de ciberdefensa de las instituciones regionales, es una estrategia para que las naciones colaboren de manera conjunta para su fortalecimiento en este ámbito, como también lo es un marco regulatorio eficaz, puesto que permite elevar el nivel de confianza en ciberseguridad entre los miembros (Mariano, 2021).

Además de que contar con los organismos especializados en esta materia es un gran avance para cualquier sociedad, sobre todo en México, puesto que muchos de los delitos informáticos que son cometidos no se les da seguimiento debido a que la persecución resulta un tanto compleja debido a que no se cuenta con los recursos y medios adecuados para detener a los culpables y como ya se ha repetido en diversas ocasiones a lo largo de esta investigación, el ciberespacio es un lugar complejo que no conoce fronteras.

> La importantísima labor que desempeñan otros operadores jurídicos, como es el caso de los abogados, especialista en materia de TIC y las instancias encargadas de la administración de justicia, es decir, de los litigantes, peritos particulares y los jueces que intervengan en los casos en que se busque enjuiciar a los presuntos responsables, pues por una parte, serán quienes en primera instancia analizarán y dictaminarán sobre la autenticidad y validez de indicios y pruebas vinculadas a crímenes informáticos, y en segunda, los que habrán de juzgar sobre el bien jurídico protegido, y en su caso, imponer la sanción que conforme a la legislación penal corresponda (Piña, 2019, pág. 14).

La falta de organización y regulación, por parte del gobierno, que se encarga de elaborar este tipo de política públicas, ha impulsado a que los ciberdelincuentes puedan cometer todo tipo de actos ilícitos sin recibir una sanción (Mendez, 2015), ya que, en primer lugar existen vacíos legales o incluso inexistentes en los lugares donde cometen los actos que imposibilita aún más la búsqueda, y peor aún no se cuenta con la cooperación internacional eficaz para perseguir el caso o bien mitigar el riesgo. A veces

esto es posible en sociedades donde sí cuentan con los medios y recursos suficientes para llegar al ciberdelincuente, o bien, cuando son actos que vulneran o atentan contra su seguridad nacional.

En México, como ya se ha mencionado hace falta una actualización a su normativa que contemple aquellos conceptos que emanan de las nuevas tecnologías de información (Arreola, 2018), aunado a esto, hace falta una definición clara y precisa sobre lo que es la ciberseguridad y la ciberdefensa. Y sobre todo hace falta una política pública de largo alcance que sirva de apoyo en estos temas tan complejos, la regulación jurídica permitirá que los actos delictivos cometidos en el ciberespacio no queden impunes y reciban la sanción correspondiente y sobre todo que la sociedad tenga la seguridad de que puede ejercer sus derechos y libertades en él.

3.3.6 Distribución equitativa de funciones de las autoridades encargadas de la seguridad en el ciberespacio

Hoy en día, se estudia a la ciberseguridad y ciberdefensa, como un ámbito de análisis en la esfera política, no solamente como parte de la seguridad nacional, sino que esto se convierte ahora en un tema de suma importancia, puesto que las autoridades deben tener la formación profesional necesaria para desarrollar habilidades educativas en sistemas de ciberseguridad (Fonfría, 2020).

La diplomacia cibernética permite contrarrestar algunas amenazas presentes en el ciberespacio que no conocen fronteras (Porrúa, 2019), por tanto, contar con las autoridades nacionales que hagan frente a dichas amenazas, no es suficiente sino se cuenta con la cooperación internacional donde diversas naciones trabajen de manera conjunta compartiendo conocimientos y avances tecnológicos en estos temas para hacer del ciberespacio un lugar seguro y armónico.

Según Violler (2017), existen ciertas tareas de carácter oficial a las que podrían dedicarse las instituciones públicas u otras organizaciones con la capacidad de salvaguardar el ciberespacio, y que a la hora de colaborar con el gobierno, las autoridades correspondientes podrían:

1. Asesorar al Presidente de la República en el análisis y definición de la política pública en ciberseguridad y ciberdefensa, que debe contener planes, medidas y programas de acción que verifiquen su ejecución y cumplimiento.

2. Identificar e ir actualizando las amenazas a las que se expone el ciberespacio, así como proponer alternativas para su solución.

3. Estudiar y mantenerse al tanto de la legislación vigente en materia de las nuevas tecnologías de información, sobre todo en el ciberespacio, además de proponer algunas modificaciones legales que consideren pertinentes.

4. Promover la colaboración de otras formas de organización y coordinación entre entes públicos y privados.

Sin embargo, existe una brecha entre la cantidad de recursos humanos y económicos disponibles y los que exige la demanda de ciberseguridad y ciberdefensa, tanto en el ámbito público como en el privado (Lecuir, 2019). Y esto podría solucionarse mediante el refuerzo a los programas de capacitación y de tipo educativos, la formación profesional encaminada a crear expertos en seguridad informática, además de que, se debe exigir la obligatoriedad y cumplimento de sus funciones a las autoridades correspondientes.

Debido a lo compleja y dinámica que es la ciberseguridad y ciberdefensa, se atiene como un problema público, el cual da pauta a crear nuevas estrategias, como lo es una política pública en estos temas que sea elaborada a diferentes niveles de gobierno, lo cual implica que exista la participación de otros actores (Nieves, 2019).

3.3.7 Participación del Estado en el ciberespacio

Como primer punto, se debe tener en cuenta que en el ciberespacio hay potenciales enemigos, los cuales buscan atentar contra el Estado, por tanto, la ciberseguridad y la ciberdefensa deben ser prioridades para la seguridad nacional, y para esto se requiere de ciertas estrategias políticas para lograr un alto grado de ciberseguridad y ciberdefensa (Arreola, 2018).

También, el Estado ha sido el encargado de potenciar el uso de internet y de promover una mejor conectividad a nivel nacional para estar al alcance de la población, es por esto que también se ha visto en la necesidad de ampliar el marco de regulación jurídico, y hoy en día tiene la tarea de crear uno nuevo para la sociedad virtual, sin perder de vista el resguardo de su soberanía (Nieves, 2019).

Si bien, las políticas públicas de ciberseguridad y ciberdefensa engloban diversos ámbitos, el papel de los agentes estatales, económicos y sociales son fundamentales para esclarecer de qué manera se vislumbran los objetivos, con la finalidad de identificar el papel del Estado en las diversas funciones que le serán conferidas en este tema (Fonfría, 2020).

El Estado debe promover e impulsar medidas para alcanzar un nivel suficiente de ciberseguridad, para proteger a los más vulnerables y permitir

también un mejor desarrollo económico (Departamento de Seguridad Nacional, 2019, pág. 37).

Hoy en día, al menos en la Ciudad de México, se han creado redes de internet con acceso libre, tal es el caso de la red “CDMX-Internet para todos”, que permite la conexión desde los postes del Centro de Comando, Control, Cómputo, Comunicaciones y Contacto Ciudadano (C5). Según la Agenda Digital e Innovación Pública, la Ciudad de México cuenta con 21500 zonas de acceso a wifi (Santos, 2021), lo que permite que cualquier dispositivo electrónico, se conecte de manera gratuita a internet, si bien, esta alternativa resulta positiva, la conexión no es tan estable, lo que imposibilita una navegación rápida, aunado a esto, muchos usuarios no se sienten seguros conectándose a esta red, puesto que en ocasiones se solicita algunos datos personales como el correo electrónico o número telefónico. Además de que no en todos lados existe esa conectividad.

Se debe buscar la manera en que todas y todos estén conectados incluso desde sus hogares, sin embargo, la contratación de este servicio es de paga, lo que imposibilita que la sociedad cuente con esta tecnología. La participación del Estado en este aspecto es fundamental, ya que como se mencionaba anteriormente, se debe crear un internet universal que sea accesible a todos o al menos subsidiar el mayor porcentaje posible del costo por este servicio.

Algo que sí es importante aclarar es que, el Estado debe asegurar primero sus redes civiles y militares ante cualquier posible ataque cibernético, puesto que, para poder salvaguardar su ciberseguridad en las infraestructuras críticas, debe contar con la participación del sector privado, ya que la ciberseguridad no es tarea de un solo miembro, sino que es en parte responsabilidad de todos los que interactúan en el ciberespacio.

La colaboración público-privada engloba a muchos sectores de la sociedad, que van desde las entidades del Estado, organismos autónomos,

empresas, escuelas, centros de investigación, asociaciones, fundaciones, por mencionar algunos, y sí bien, la gobernanza de internet incentiva a la participación de estos (Lecuit, 2019), en las decisiones a favor de fortalecer la seguridad en el ciberespacio, la creación de un organismo que facilite un asesoramiento, supervisión y evaluación de la política de ciberseguridad y ciberdefensa permite una mejor distribución entre las diversas organizaciones, así como un mejor desarrollo de las mismas.

Por tanto, el éxito que tenga el Estado está estrechamente vinculado en la confianza que le da a los distintos sectores de la sociedad, y en este ámbito (Arreola, 2018), las mejores prácticas de ciberseguridad y ciberdefensa que podrían llevar a cabo los Estados, se basan en los planes, programas, estrategias y previsiones para mitigar los riesgos en el espacio virtual.

3.3.8 Protección a las infraestructuras críticas de información

Las infraestructuras críticas, cuentan con la característica de ser aquellos sistemas que tanto físicos como virtuales tienden a facilitar las funciones y servicios considerados esenciales para la sociedad, ya sea por su impacto económico, social, medioambiental y político. En consecuencia, una alteración a esta puede generar una amenaza para quienes las utilizan y también afectar de manera directa a cualquier Estado, debido a que imposibilita su normal funcionamiento (Instituto de Seguridad y Bienestar Laboral, 2020). Peor aún cuando estas infraestructuras son dependientes una de otra, tan sólo una pequeña falla, podría tener inclusive un efecto cascada.

En particular, la elaboración de un plan eficaz podría ayudar a proteger todas las infraestructuras críticas. Si se propone a cada entidad, ya sea de carácter público o bien privado que construya su propia Estrategia de Ciberseguridad, se sabe que un programa bien estructurado, capacita el

contrarrestar futuros daños y sobre todo sirve como una guía para conocer de qué manera actuar ante cualquier amenaza de tipo cibernética. Las estrategias de ciberseguridad son parte también esencial de la categoría que emana de las políticas públicas, puesto que integran aspectos militares, económicos y sociales (Macuaran, 2019).

En consecuencia, las infraestructuras críticas de información deben estar diseñadas con una alta arquitectura resiliente, capaz de hacer frente a los ataques que la puedan vulnerar, y que se adapte a fenómenos de la naturaleza, modificaciones humanas o bien ciberataques (Gobierno de Chile, 2020).

Por ejemplo, el logro más reciente en México, es que en el año 2021, la Secretaría de Marina[35], planteo la Estrategia Institucional para el Ciberespacio 2021-2024, cuyo objetivo es:

Coadyuvar de forma más eficiente, al mantenimiento de la integridad, estabilidad y permanencia del Estado mexicano, al disminuir el riesgo institucional en el ámbito marítimo nacional y coadyuvar en el esfuerzo nacional para mantener la continuidad de los servicios críticos que se proporcionan a la sociedad mexicana, a través de las instalaciones estratégicas del país. (pág. 3)

En efecto, mediante este texto se deja en claro la importancia que tiene para esta institución proteger su infraestructura tecnológica, en cuanto a las Operaciones Navales en mar, aire, tierra, y agrega uno más, el ciberespacio, la defensa de este último, ayuda a contrarrestar los riesgos

[35] En el año 2013 se elaboró un glosario de términos SEDENA-MARINA en materia de Seguridad en el Ciberespacio, el cual se ha ido actualizando conforme a los nuevos términos relacionados al ciberespacio. Se encuentra disponible en: https://www.gob.mx/semar/documentos/glorario-de-terminos-de-ciberseguridad?state=published

cibernéticos marinos y portuarios y mitigar los riesgos de Seguridad Nacional desde el entorno marítimo.

Sin embargo, en México no se cuenta con un órgano autónomo especializado en materia de protección a las infraestructuras críticas, a pesar de que algunas instituciones públicas y privadas se han encargado de elaborar un plan ante posibles riesgos, no hay un centro especial que atienda este ámbito. Por ejemplo, en España, se tiene al Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), cuyas funciones son: coordinar y supervisar las políticas y actividades que estén relacionadas con la protección de sus infraestructuras críticas y con la ciberseguridad del Ministerio del Interior.

Por otra parte, no se puede separar a la ciberseguridad y a la ciberdefensa, puesto que si bien, ambas se relacionan con la capacidad de un Estado-Nación, para hacer frente a posibles amenazas en el ciberespacio, el primer término engloba a diversos sectores de la sociedad, con capacidad de generar políticas públicas, legislación, normas y demás controles tecnológicos para la protección de las infraestructuras críticas, mientras que la ciberdefensa debe generar acciones, recursos y mecanismos en materia de Seguridad y Defensa nacional para neutralizar dichas amenazas, incluidas las que atentan contra las instalaciones estratégicas de un país (Arellano y Villa, 2021).

Como lo menciona Márquez (2017), no existe como tal una protección de infraestructura crítica de información única que se ajuste a cada país, puesto que la naturaleza del proceso para su protección depende más del perfil del riesgo en el que se encuentre la nación, sus capacidades de mitigar el riesgo y las necesidades que tenga. Sin embargo, la responsabilidad de mantenerlas a salvo también depende del interés que le pongan las partes involucradas y sobre todo de las capacidades que cada estado tiene a su disposición para que las propias partes interesadas

trabajen de manera conjunta hacia esos niveles de protección a sus infraestructuras.

Por último, y resumiendo este apartado, un experto mexicano en seguridad informática, Vásquez Cruz (2016), propone una serie de recomendaciones a los que se tiene que hacer frente desde al ámbito público y privado para la protección de las infraestructuras críticas:

- Estudiar ataques del pasado hechos a las infraestructuras críticas, para generar conciencia sobre la magnitud de las amenazas, a fin de diseñar un plan estratégico.
- Contar con una estrategia de ciberseguridad en cada país, que permita identificar y alertar sobre posibles vulnerabilidades y amenazas para actuar de manera eficaz y lo más rápido posible.
- Mejorar las capacidades de inteligencia, incluyendo a la protección de las infraestructuras críticas con ayuda de los Centros Nacionales de Respuesta a Incidentes Cibernéticos (CERT).
- Implementar un manual general en materia de tecnologías de la información, comunicación y seguridad. Así como continuar actualizando el catálogo de las infraestructuras críticas.
- Realizar auditorías regulares que permitan, además de revisar en nivel de seguridad de la infraestructura, percibir el nivel de conocimiento en cuanto a la cultura de seguridad informática.
- La protección de las infraestructuras críticas debe incluir tres áreas fundamentales, infraestructura empresarial de las tecnologías de

información, sistemas SCADA[36] (supervisión, control y adquisición de datos), y sistemas de control industrial.

Mientras que Masís (2019), enuncia algunas herramientas que son de gran ayuda a la hora de proteger a las infraestructuras:

- Capacitación y participación en simulacros en caso de desastres, además de proteger y garantizar los puestos de trabajo de quienes investigan los fallos de seguridad, pero exigirles también su constante actualización en temas de seguridad a las infraestructuras críticas.

- La educación y la cooperación pública y privada es fundamental para crear alianzas y programas de fomento a la capacidad preventiva de protección contra amenazas a las infraestructuras críticas.

[36] Es un acrónimo de Supervisory Control and Data Acquisition, este tipo de sistema ayuda a las empresas a controlar sus equipos y demás maquinaria para tener un registro de sus operaciones.

CONCLUSIONES

El ciberespacio se ha convertido en un nuevo lugar que juega una doble partida, por un lado, ofrece un sinfín de herramientas que ayudan a mejorar y facilitar nuestra vida, y por el otro, se ha convertido en un campo de batalla, en el cual todos buscan su control pero que nadie hasta ahora lo ha conseguido.

Sin embargo, las grandes potencias ya se han encargado de ejercer su dominio en el ciberespacio a través de la población, puesto que han creado para su beneficio nuevas herramientas y aplicaciones para hacer su interacción gobierno-sociedad más fácil, tal es el caso del gobierno electrónico, el voto electrónico, ciberespionaje, o bien el desprestigio o apoyo a las campañas políticas por medios digitales, sólo por mencionar algunos.

Pero por otro lado, los gobiernos se han olvidado de la problemática que surge a raíz de actos mal intencionados que realizan los ciberdelincuentes, puesto que pareciera que para ellos es más importante el mantener un status quo en el ciberespacio, antes que salvaguardar los intereses de la nación, o de proteger a sus ciudadanos. Dejando a la ciberseguridad y a la ciberdefensa como segundo plano.

Ahora bien, a lo largo de la investigación se expusieron distintas concepciones de “ciberseguridad y ciberdefensa”, sin embargo, lo se debe recordar y tener siempre presente que la diferencia entre ambas radica en que, la primera se refiere a las acciones que puede implementar el Estado, el sector privado y público para poder aplicar políticas públicas, normas y leyes que puedan mitigar los ciberataques y demás amenazas en el ciberespacio, así como las acciones para la protección de las infraestructuras críticas. Mientras que la ciberdefensa hace alusión a protección de la soberanía nacional, al fomento en el uso de fuerzas llámense,

militares, marítimas, aéreas y demás inteligencias, para que puedan prevenir, identificar y contrarrestar dichas amenazas y dar posibles soluciones a estas.

Por otro lado, en cuanto al nivel que se encuentra México para las capacidades de ciberdefensa y seguridad, se sabe que aún no es el adecuado como para decir que sus infraestructuras críticas de información se encuentran a salvo de cualquier posible vulneración o ciberataque. Pero es de reconocerse, que el país ha realizado un esfuerzo por mejorarlo, como por ejemplo con la creación de su policía cibernética, algunas modificaciones a las leyes y normativas que competen a los delitos informáticos, la creación de su Centro de Respuestas a Incidentes Cibernéticos de la Dirección General Científica de la Guardia Nacional (CERT-MX), y que si bien aún falta mucho por hacer ningún esfuerzo hasta ahora hecho se demerita.

Sin embargo, considero que se debe tomar en cuenta la participación de otros organismos internacionales que sirvan de apoyo en la creación de leyes para la protección y garantía de los derechos humanos en el ciberespacio.

El papel que puede jugar México para los próximos años, en materia de ciberseguridad y ciberdefensa es de suma importancia, ya que visto desde el ámbito nacional, podría generar para el gobierno mexicano y el Estado una cierta credibilidad, puesto que los ciudadanos se sentirían seguros en el ciberespacio. Pero en el ámbito internacional lo podría colocar como un actor principal en la toma de decisiones, pero sí y sólo sí hace énfasis en la mejora de la ciberseguridad y la ciberdefensa a sus infraestructuras críticas de información.

Sin embargo, por ahora, se tiene un reto muy grande por aumentar esos niveles en cuanto a la protección y seguridad de los ciudadanos en el ciberespacio y de sus infraestructuras críticas de información. Debido a que se tienen que atender diversos factores para su desarrollo como, la falta de infraestructura, financiamiento, la falta de organización entre sus instituciones, y en el ámbito

social, se encuentra que, existe una ausencia de cultura en ciberseguridad y cibefensena en los ciudadanos mexicanos, y también, una deficiencia en cuanto al apoyo de entes privados y públicos, pero sobre todo, la falta de participación del Estado para atender esta índole.

En cuanto a las problemáticas principales que se encontraron en la investigación es que, existe una falta de consenso para aquellas definiciones que emanan del ciberespacio, y que sí bien los organismos internacionales son lo que más han trabajado en su elaboración, aún falta la colaboración de instituciones privadas y de los gobiernos de todos los países.

También, la falta de un orden jurídico universal que sea capaz de regular al ciberespacio, ha generado una laguna legal en las normativa de los demás países. Esa falta de organización, ha dado lugar a que muchos ciberdelincuentes cometan sus actos sin miedo a la persecución, debido a que su rastreo resulta aún más complicado que en el terreno físico. Por tanto, hace falta una regulación que garantice la plena permanencia en el ciberespacio y la actualización constante de la misma, ya que incluso muchos países tienen un doble rezago en este ámbito o peor aún, no cuentan con una legislación vigente para castigar dichos actos.

Una primera y posible alternativa ante esta situación, es que los países deben contar con una Estrategia Nacional de Ciberseguridad, y que los organismos encargados de la Defensa Nacional se ocupen de crear sus propios mecanismos de ciberdefensa para la protección de sus infraestructuras críticas. Además, es importante contar con una policía cibernética o cualquier otro tipo de organización que atienda los delitos y faltas cometidas en el ciberespacio.

Por último, si bien, uno de los objetivos principales de esta investigación, fue abordar la propuesta de una política pública de ciberseguridad y ciberdefensa para el caso mexicano, este no es un caso aislado, puesto que bien podría ser aplicado en algunos países de Latinoamerica, que es donde menos estamos preparados

para un ciberataque y donde más hace falta la creación de leyes que regulen el ciberespacio, y la participación del Estado, sociedad civil y privada. Las políticas públicas que se implementen en estos temas podrían ser con base en modelos de otras sociedades más avanzadas en cuanto al nivel de ciberseguridad y ciberdefensa, pero se tendría que estudiar bien de qué manera funciona o si esta podría aplicarse dependiendo el tipo de país.
Puesto que los países se benefician, ya que se incrementa en cierto punto la credibilidad del gobierno, se fortalece a la democracia y se podrían construir instituciones de carácter fuerte y legítimas, para fortalecer al Estado en el mundo virtual.

Pero no está de más aclarar que ningún país aún está completamente preparado para contrarrestar amenazas en el ciberespacio, y que si bien existen ciertas diferencias en cuanto a la implementación de sus mecanismos de defensa y sobre todo en la capacidad que tienen estos de hacer frente a los ciberataques, no se debe trabajar de manera individual, sino conjunta, debido a que el ciberespacio no conoce fronteras, y los ciberdelincuentes no conocen los límites. Sin embargo, si se trabaja conjuntamente se puede garantizar un espacio libre de expresión y donde se respeten los derechos humanos a sus cibernautas.

Todos estos conceptos son nuevos y un tanto técnicos, se pensaría que no tienen una relación con las ciencias sociales, en este caso, con la ciencia política, pero no es así puesto que la ciberseguridad y la ciberdefensa, como la lo vimos a lo largo de la investigación, no atiende sólo asuntos informáticos o de carácter tecnológico, sino que se trata también de construir una concientizacion y educacion en la sociedad participe del ciberespacio.

REFERENCIAS

Álvarez Valenzuela, D., 2018. Ciberseguridad en América Latina y ciberdefensa en Chile *Revista chilena de derecho y tecnología*, [revista electrónica] 7(1), pp. 1-2. http://dx.doi.org/10.5354/0719-2584.2018.50416 **.**

Amoroso Fernández, Y., 2014. Infoética, Ciberespacio y Derecho. *Bibliotecas anales de investigación*, [en línea]. Disponible en: <http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199> [Acceso 22 mayo 2021].

Aguilar Antonio, JM., 2020. La brecha de ciberseguridad en América Latina frente al contexto global de amenazas. *Revista de Estudios en Seguridad Internacional,* [revista electrónica]. Disponible en: <https://seguridadinternacional.es/resi/html/la-brecha-de-ciberseguridad-en-america-latina-frente-al-contexto-global-de-ciberamenazas/ > [Acceso 19 febrero 2022].

Aguilar Antonio. JM., 2021. Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. *Estudios Internacionales,* [revista electrónica] 53(198), pp. 169-197. https://doi.org/10.5354/0719-3769.2021.57067.

Aguirre, D., 2015. *El ciberespacio y las relaciones internacionales en la era digital*. [pdf]. Disponible en: https://www.researchgate.net/profile/Daniel-Aguirre-8/publication/327392167_El_ciberespacio_y_las_relaciones_internacionales_en_la_era_digital/links/5b8c96c0299bf1d5a73a05ec/El-ciberespacio-y-las-relaciones-internacionales-en-la-era-digital.pdf [Acceso 11 diciembre 2021].

Aguirre Ramírez, JL., 2021. *La integración del ciberespacio a las operaciones multidominio.* [en línea]. Centro Latinoamericano de Estudios Interdisciplinarios.

Disponible en: <https://celaei.org/2020/07/03/la-integracion-del-ciberespacio-a-las-operaciones-multidominio/> [Acceso 22 junio 2021].

Arellano Gault, D. y Blanco, F., 2013. *Políticas Públicas y Democracia.* [pdf] México, D.F.: Instituto Federal Electoral. Disponible en: <https://archivos.juridicas.unam.mx/www/bjv/libros/8/3565/11.pdf> [Acceso 22 enero 2022].

Arreola García, A., 2019. Ciberseguridad: *¿Por qué es importante para todos*? [libro electrónico] Ciudad de México: Siglo XXI Editores México. Disponible a través del sitio web de Amazon < https://www.amazon.com.mx/Ciberseguridad-%C2%BFPor-importante-para-todos-ebook/dp/B082NM3RSZ> [Acceso 30 marzo 2021].

Arreola García, A., 2021. *Ciberespacio: ¿El salvaje oeste?* [pdf]. Disponible a través de: Sitio web de ResearchGate < https://www.researchgate.net/> [Acceso 10 agosto 2021].

Asociación de Internet MX, 2019. *Los 10 estados menos conectados a internet.* [en línea] Disponible en: <https://www.asociaciondeinternet.mx/prensa-ssig-habitos-los-10-estados-menos-conectados-a-internet> [Acceso 19 abril 2022].

Asociación de Internet MX, 2021. *Estudio sobre los hábitos de los usuarios de internet en México 2020*. [pdf] Disponible en: <https://irp-cdn.multiscreensite.com/81280eda/files/uploaded/16%20Estudio%20sobre%20los%20Hábitos%20de%20los%20Usuarios%20de%20Internet%20en%20México%202020%20versión%20pública.pdf> [Acceso 15 noviembre 2021].

Avogadro, M., 2012. Reinventando las palabras en el ciberespacio: de la arroba al Smartphone informaciones de millones por millón. *Razón y palabra*. [en línea] Disponible en:

<http://www.razonypalabra.org.mx/comunicarte/2012/012012_Comunicarte.html> [Acceso 18 mayo 2021].

Azócar Aguirre, D., 2016. La gobernanza global de Internet y sus alcances para Chile. *Estudios internacionales (Santiago),* [revista electrónica] 48(186), pp. 183-197. http://dx.doi.org/10.5354/0719-3769.2016.44538 .

Banco Interamericano de Desarrollo, 2020. *Ciberseguridad riesgos, avances y el camino a seguir en América Latina y el Caribe*. [pdf] Disponible en: <https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf> [Acceso 04 mayo 2021].

Banco Mundial, 2021. *Personas que usan Internet*. [en línea] Disponible en: https://www.internetworldstats.com/stats.htm [Acceso 19 noviembre 2021].

Bartolomé, M. y Monteiro Lima, AG., 2021. El ciberespacio, durante y después de la pandemia Covid-19. *Revista de la Academia de Guerra del Ejército Ecuatoriano*, [en línea]. Disponible en: https://journal.espe.edu.ec/ojs/index.php/Academia-de-guerra/article/view/VOL14ART6/pdf [Acceso 14 diciembre 2021].

BBC , 2015. *El virus que tomó control de mil máquinas y les ordenó autodestruirse* [en línea] (2022) Disponible en: <https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet [Acceso 11 octubre 2021].

Biblioteca del Congreso Nacional, s.f. *Convenio Nº 185, del Consejo de Europa, sobre la Ciberdelincuencia (Convenio de Budapest).* [pdf] Disponible en: <https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20810/5/Convenio%20N%20185%20del%20Consejo%20de%20Europa%20sobre%20la%20Ciberdelincuencia%20(Convenio%20de%20Budapest).pdf> [22 mayo 2021].

Bodin, J., 1997. *Los seis libros de la República.* [libro electrónico] Tecnos. Disponible en: WordPress <https://esepuba.files.wordpress.com/2013/10/1er-enc-bodino-jean-los-seis-libros-de-la-republica.pdf> [Acceso 08 agosto 2021].

Borrero Cortés, R., 2015. Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia. *Revista de Derecho Comunicaciones y Nuevas Tecnologías,* [en línea] Disponible en: <https://derechoytics.uniandes.edu.co/components/com_revista/archivos/derechoytics/ytics227.pdf> [Acceso 14 febrero 2022].

Burch, S., 2015. La Gobernanza mundial de Internet. *Línea Sur 9 Revista de política exterior*, [en línea] 3(9), pp. 23-36. Disponible en: <https://www.cancilleria.gob.ec/wp-content/uploads/2016/12/linea_sur_9.pdf#page=25> [Acceso 03 2021].

Camacho, Z., 2021. México, en el “top 5” de ciberataques. *Contralínea* [blog] 14 de septiembre. Disponible en: < https://contralinea.com.mx/interno/semana/mexico-en-el-top-5-de-ciberataquesad-cibernetica/> [Acceso 14 agosto 2021].

Cano M., JJ. y Rocha A., 2019. Ciberseguridad y ciberdefensa. Retos y perspectivas en un mundo digital. *Revista Ibérica de Sistemas y Tecnologías de Información*, [revista electrónica] (32), pp.VII-IX. http://dx.doi.org/10.17013/risti.32.0 .

Cárdenas Moreno, W., 2015. *Ciberdefensa y ciberseguridad en el sector defensa de Colombia.* [pdf] Universidad Piloto de Colombia. Disponible en: <http://polux.unipiloto.edu.co:8080/00002590.pdf> [Acceso 14 junio 2021].

Centro Criptológico Nacional, 2019.*Informe de Amenazas y Tendencias. Edición 2019* [en línea] Disponible en: <https://www.ccn-cert.cni.es/informes/informes-ccn-

cert-publicos/3776-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-edicion-2019-1/file.html>[Acceso 18 mayo 2021].

Centro Superior de Estudios de la Defensa, 2012. *Ciberespacio. Nuevo escenario de confrontación*. [pdf] Ministerio de Defensa.Disponible en: <https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_126.pdf > [Acceso 09 febrero 2021].

Centro Tecnológico de Seguridad, Ministerio del Interior y Gobierno de España, 2022. *¿Qué es el CETSE?*. [en línea] Disponible en: https://cetse.ses.mir.es/publico/cetse [Acceso 27 marzo 2022].

Cerbino, M. y Richero, A. Eds., 2006. *Gobernanza, políticas públicas y aplicaciones de Internet*. [libro electrónico] Quito, Ecuador: Facultad Latinoamericana de Ciencias Sociales. Disponible en: FLACSO <https://biblio.flacsoandes.edu.ec/libros/digital/48767.pdf> [Acceso 27 enero 2022].

Cisco, 2021. *¿Cuáles son los ciberataques más comunes?* [en línea]. Disponible en: < https://www.cisco.com/c/es_mx/products/security/common-cyberattacks.html> [Acceso 14 agosto 2021].

Cocchini, A. 2021. Los ciberatauqes de los actores no estatales y la "ciberdiligencia debida" de los estados. *Revista UNICSI*, [en línea] Disponible en: < http://www.unisci.es/los-ciberataques-de-los-actores-no-estatales-y-la-ciberdiligencia-debida-de-los-estados/> [Acceso 17 junio 2021].

Comisión Económica para América Latina y el Caribe, 2011. *El gobierno electrónico en la gestión pública.* [en línea] Disponible en: <https://www.cepal.org/es/publicaciones/7330-gobierno-electronico-la-gestion-publica> [Acceso 02 noviembre 2021].

Consejo de la Unión Europea, 2021 *Cronología-Ciberseguridad.* [en línea]. Disponible en: <https://www.consilium.europa.eu/es/policies/cybersecurity/timeline-cybersecurity/> [Acceso 11 enero 2022].

Consejo Permanente a la Asamblea General, 2004. *Adopción de una estrategia interamericana integral de seguridad cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética.* [pdf] Disponible en: <https://www.oas.org/es/sms/cicte/documents/asambleas/ag-res.%202004%20(xxxiv-o-04)_sp.pdf> [Acceso 19 mayo 2021].

Copa-data, s.f. *¿Qué es SCADA?.* [en línea] Disponible en: https:<//www.copadata.com/es/productos/zenon-software-platform/visualizacion-control/que-es-scada/> [Acceso 22 marzo 2022].

Cornaglia, S. y Hernán Vercelli, A., 2017. La ciberdefensa y su regulación legal en Argentina (2006-2015). *Revista Latinoamericana de Estudios de Seguridad*, [revista electrónica] (20), pp. 45-62. https://doi.org/10.17141/urvio.20.2017.2601 .

Cornejo Paz, E. y Cuenca Segura, MC., 2021. Gobernanza colaborativa y nuevos modelos de aprendizaje. En: M. Pallarès Piquer, J. Gil-Quintana y A. Santiesteban Espejo, coords. 2021. *Docencia, ciencia y humanidades: hacia una enseñanza integral en la universidad del siglo XXI.* [libro electrónico]. Madrid: Dykinson S.L. págs.400-417. Disponible a través del sitio web de ResearchGate <https://www.researchgate.net/publication/355348433_Gobernanza_colaborativa_y_nuevos_modelos_de_aprendizaje> [Acceso 04 enero 2022].

Coronado Contreras, JE., 2021. *Ciberterrorismo, ciberdelincuencia y cooperación internacional.* [libro electrónico] Ciudad de México: Bosch México Disponible a través del sitio web de Amazon <https://www.amazon.com.mx/Ciberterrorismo-

ciberdelincuencia-y-cooperaci%C3%B3n-internacional-ebook/dp/B08YCYRS7Q> [Acceso 03 abril 2021].

Coronado Contreras, LV., 2015. *La libertad de expresión en el ciberespacio.* Tesis doctoral. Universidad Complutense de Madrid.

Coronado Contreras, LV., 2017. *La regulación global del ciberespacio*. Ciudad de México: Porrúa.

Criado, JI e Gil-García, JR., 2013. Gobierno electrónico, gestión y politicas publicas: Estado actual y tendencias futuras en América latina. *Gestión y política pública*, [en línea] Disponible en: <http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-10792013000400001> [Acceso 26 febrero 2022].

Cueto, H., 2021. Los intentos de ciberataques triplicaron en México. *Business Insider México,* [en línea] 4 de marzo. Disponible en: < https://businessinsider.mx/intentos-ciberataques-triplicaron-mexico-durante-2020/> [Acceso 13 agosto 2021].

De la Garza Montemayor, D. y Barredo Ibáñez, D., 2017. Gobernanza en el contexto contemporáneo: un análisis crítico de la perspectiva liberal. *Consensus*, [revista electrónica] 22(2), pp. 87-96. Disponible a través: Sitio web de ResearchGate
< https://www.researchgate.net> [Acceso 09 enero 2022].

De la Peña Muñoz, J., 2021. Biden marca su `hoja de ruta ‘en política cibernética con una Orden Ejecutiva que busca aplicar la `Confianza Cero’ y el mayor presupuesto. *Revista Ciberseguridad, seguridad de la información y privacidad*, [en línea] Disponible en: <https://revistasic.es/sic145/revistasic145.pdf> [Acceso 19 noviembre 2021].

De la Rosa Rodríguez, PI., 2019. *Las tecnologías, el ciberespacio y el derecho penal.* Ciudad de México: Porrúa.

Departamento de Seguridad Nacional, 2019. *Estrategia Nacional de Ciberseguridad 2019.* [en línea] Disponible en: <https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019> [Acceso 19 febrero 2022].

Department of Defense, 2018. *Cyber Strategy*. [en línea] Disponible en: <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan> [Acceso 14 noviembre 2021].

Edwards, J., 2019. Todo lo que necesitas saber sobre la nueva ley de Ciberseguridad en China. *Progress*, [blog] 9 de mayo. Disponible en: <https://www.ipswitch.com/es/blog/todo-lo-que-necesitas-saber-sobre-la-nueva-ley-de-ciberseguridad-en-china> [Acceso 01 enero 2022].

El Mundo, 2015.El Senado de Estados Unidos aprueba una ley de ciberseguridad. *El Mundo,* [en línea] 28 de octubre. Disponible en: <https://www.elmundo.es/internacional/2015/10/28/5630219e46163f29348b4595.html> [Acceso 17 noviembre 2021].

Equipo Nizkor, 2019. *El Gran Hermano te vigila: el impenetrable Escudo Dorado de China que `protege´ su internet de EEUU.* Disponible en: <https://www.derechos.org/privacy/doc/chn1.html> [Consultado 02 diciembre 2021].

Europapress, 2015. *China incluye el ciberespacio en su nueva ley de seguridad nacional.* [en línea] (2022). Disponible en:

<https://www.europapress.es/internacional/noticia-china-incluye-ciberespacio-ley-seguridad-nacional-20150508185813.html> [Acceso 22diciembre 2021].

Faraday News, 2012. *Programa Nacional de Infraestructuras Críticas y Ciberseguridad en Argentina*. [en línea] Disponible en: <https://medium.com/faraday/programa-nacional-de-infraestructuras-cr%C3%ADticas-y-ciberseguridad-en-argentina-5790ffd3007> [Acceso 17 marzo 2022].

Fernández Fernández, M., Fernández-Alameda, CM. y Tardivo, G., 2019. Creación de opinión y percepción sobre China en redes sociales occidentales. *Revista de Comunicación*, [revista electrónica] 18 (2), pp. 117 -138. Disponible a través de: SciELO <http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S1684-09332019000200006&lang=es> [Acceso 18 diciembre 2021].

Fontdeglòria, X., 2015. China aprueba su primera ley antiterrorista y el segundo hijo. *El País*, [en línea] 27 de diciembre. Disponible en: <https://elpais.com/internacional/2015/12/27/actualidad/1451209980_254853.html> [Acceso 17 diciembre 2021].

Forbes, 2020. *Rusia interfirió en elecciones de 2016 para ayudar a Trump: Senado de EU.* [en línea] *(2014-2022)* Disponible en: <https://www.forbes.com.mx/rusia-interfirio-en-elecciones-de-2016-para-ayudar-a-trump-senado-de-eu/> [Acceso 09 agosto 2021].

Fronfría, A. y Duch-Brown, N., 2020. *Elementos para una política de ciberseguridad efectiva.* [en línea] Real Instituto Elcano. Disponible en: <https://www.realinstitutoelcano.org/analisis/elementos-para-una-politica-de-ciberseguridad-efectiva/> [Acceso 25 marzo 2022].

Galindo Ayuda, F., 2020. Democracia, Internet y Gobernanza: una concreción. *Seqüência Estudos Jurídicos e Políticos*, [revista electrónica] 33(65), pp.34-56. Disponible en: http://dx.doi.org/10.5007/2177-7055.2012v33n65p33 .

García-Córdoba, J. y Herrero-Pérez L., 2021. La ciberdefensa en los sistemas de información sanitarios militares. *Sanidad Militar*, [en línea] Disponible en: < https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1887-85712020000300140> [Acceso 27 junio 2021].

García Encina, C., 2018. La Estrategia de Seguridad Nacional de la Administración Trump. *Real Instituto Elcano*, [pdf] 9 de abril. Disponible en: https://www.realinstitutoelcano.org/wp-content/uploads/2018/04/dt6-2018-garciaencina-estrategia-de-seguridad-nacional-administracion-trump-2.pdf [Acceso 28 diciembre 2021].

Gobierno de México, 2017.*Estrategia Nacional de Ciberseguridad*.[pdf] Disponible en: <https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf> [Acceso 14 abril 2021].

Gutiérrez Gómez, AC., 1981. Sistema y coyuntura: el concepto de soberanía en Kelsen y Schmitt. *Estudios de Derecho,* [revista electrónica] 72(159), pp.15-40. https://doi.org/10.17533/udea.esde.v72n159a02 .

Herrera Carpintero, P., 2020. El enfoque de género en la Política Nacional de Ciberseguridad de Chile. *Revista Chilena de Derecho y Tecnología*, [revista electrónica] 9(1), pp. 5-32. https://rchdt.uchile.cl/index.php/RCHDT/article/view/51577 .

IMF Smart Education, 2022. ¿Cuáles son los principales organismos relacionados con la ciberseguridad? *Blog de Tecnología.* [blog] Disponible en: <https://blogs.imf-

formacion.com/blog/tecnologia/organismos-ciberseguridad-201904/> [Acceso 20 abril 2022].

Instituto de Seguridad y Bienestar Laboral, 2020. *¿Qué son las Infraestructuras Críticas?* [en línea] Disponible en: <https://isbl.eu/2020/03/que-son-las-infraestructuras-criticas/> [Acceso 20 abril 2022].

Instituto Español de Estudios Estratégicos, 2010. *Ciberseguridad. Retos y amenazas a la Seguridad Nacional en el ciberespacio*. [pdf] Ministerio de Defensa.Disponible en: <https://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf> [Acceso 22 febrero 2021].

Instituto Nacional de Estadística y Geografía, s.f. *Disponibilidad y Uso de TIC*. [en línea] Disponible en: <https://www.inegi.org.mx/temas/ticshogares/> [Acceso 20 febrero 2022].

Instituto Nacional de Estadística y Geografía, s.f. *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2020*. [en línea] Disponible en: <https://www.inegi.org.mx/programas/dutih/2020/#Tabulados> [Acceso 20 febrero 2022].

Instituto Nacional de Estadística y Geografía, s.f. *Encuesta sobre Tecnología de la información y las Comunicaciones (ENTIC 2013)*. [en línea] Disponible en: <https://www.inegi.org.mx/programas/entic/2013/#Tabulados> [Acceso 20 febrero 2022].

Instituto Nacional Electoral, 2020. *Implementará INE voto electrónico por Internet para las y los mexicanos residentes en el exterior en elecciones 2021*. [en línea] Disponible en: <https://centralelectoral.ine.mx/2020/08/26/implementara-ine-voto-

electronico-internet-las-los-mexicanos-residentes-exterior-elecciones-2021/> [Acceso 31 marzo 2022].

Internet World Stats, 2022. *Internet Users Distribution in the World-2021* Disponible en: <https://www.internetworldstats.com/stats.htm> [Accceso 13 noviembre 2021].

Joyanes Aguilar, L., s.f. *Introducción. Estado del arte de la ciberseguridad.* [pdf] Disponible en: <https://www.pensamientopenal.com.ar/system/files/2015/01/doctrina38717.pdf> [Consultado el 22 agosto de 2021].

Junta Interamericana de Defensa, 2020. *Guía de ciberdefensa orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar.* [pdf] Disponible en: https:<//www.iadfoundation.org/wp-content/uploads/2020/08/Ciberdefensa10.pdf> [Acceso 22 febrero 2022].

Krawchik, M., 2021. *Las políticas públicas en la era digital deben ser inclusivas y estar basadas en la conectividad*. [en línea] Congreso Latinoamericano de Transformación Digital. Disponible en:< https://cltd.lat/2021/10/27/las-politicas-publicas-en-la-era-digital-deben-ser-inclusivas-y-estar-basadas-en-la-conectividad/> [Acceso 05 marzo 2022].

Legal Army, 2020. *Estados Unidos avanza hacia un marco de ciberseguridad iniciado. ¿En qué consiste la Ley de Mejora de la Ciberseguridad del IoT?* [en línea] Disponible en: <https://www.legalarmy.net/estados-unidos-avanza-hacia-un-marco-de-ciberseguridad-unificado-en-que-consiste-la-ley-de-mejora-de-la-ciberseguridad-del-iot/> [Acceso 11 noviembre 2021].

Legal Army, 2021. *China y su cambio de paradigma en materia de privacidad*. [en línea] Disponible en: <https://www.legalarmy.net/china-y-su-cambio-de-paradigma-en-materia-de-privacidad/> [Acceso 14 noviembre 2021].

Leyva-Méndez, AE., 2021. Análisis de políticas públicas de seguridad cibernética. Estudio del caso ecuatoriano, *Polo del Conocimiento*, [en línea] Disponible en: <https://polodelconocimiento.com/ojs/index.php/es/article/view/2431> [Acceso 26 marzo 2022].

Mackinnon, M., 2019. For Africa, Chinese-Built Internet Is Better Than No Internet at All. *Foreing*, [en línea] 19 de marzo. Disponible en: <https://foreignpolicy.com/2019/03/19/for-africa-chinese-built-internet-is-better-than-no-internet-at-all/> [Acceso 15 octubre 2021].

Maestre, E., 2019. La importancia de ser infraestructura crítica. *Red Seguridad,* [en línea] Disponible en: < https://www.redseguridad.com/revistas/red/087/72/index.html#zoom=z> [Acceso 16 junio 2021].

Mariano Díaz, R., 2021. *Estado de la ciberseguridad en la logística de América Latina y el Caribe*. Santiago:Comisión Económica para América Latina y el Caribe. Disponible en: <https://repositorio.cepal.org/bitstream/handle/11362/47240/1/S2100485_es.pdf> [Acceso 28 febrero 2022].

Martí de Gidi, L., 2018. *La seguridad nacional y el acceso a la información pública en México.* [pdf] Disponible en: <https://cdigital.uv.mx/bitstream/handle/1944/51453/MartideGidiLuz.pdf?sequence=1&isAllowed=y> [Acceso 08 agosto 2021].

Martínez, Algora, A., 2019. La importancia de asegurar las infraestructuras críticas. *Red Seguridad,* [en línea] Disponible en: < https://www.redseguridad.com/revistas/red/087/68/index.html#zoom=z> [Acceso 16 junio 2021].

Martínez, J., 2001. Internet y políticas públicas socialmente relevantes: ¿Por qué, cómo y en qué incidir? En: Bonilla, M. y Gilles, C. Eds. *Internet y sociedad en América latina y el Caribe*. [libro electrónico] Quito, Ecuador: Facultad Latinoamericana de Ciencias Sociales. Disponible en: <https://biblio.flacsoandes.edu.ec/libros/digital/44947.pdf> [Acceso 05 marzo 2022].

Masís Solís, J., 2019. La protección de las infraestructuras críticas en la era digital en el contexto de Costa Rica. *Revista de la Facultad de Derecho de México*, [revista electrónica] 60 (274-1), pp. 464-503. http://www.revistas.unam.mx/index.php/rfdm/article/view/69957.

Monge, Y. e Sahuquillo, MR., 2020. La justicia de EE UU retira los cargos contra dos empresas acusadas de financiar la injerencia rusa en las elecciones de 2016. *El País*, [en línea] 17 de marzo. Disponible en: <https://elpais.com/internacional/2020-03-17/la-justicia-de-ee-uu-retira-los-cargos-contra-dos-empresas-acusadas-de-financiar-la-injerencia-rusa-en-las-elecciones-de-2016.html> [Acceso 06 agosto 2021].

Monteverde Sánchez, A. y Castro Valdebenito, HJ., 2018. Seguridad hemisférica latinoamericana adaptada a las nuevas tecnologías: Ciberseguridad y avances de cooperación regional e internacional para la sanción del ciberdelito. *Revista Espacios,* [en línea] Disponible en: < http://revistaespacios.com/a18v39n39/18393931.html> [Acceso 22 agosto 2021].

Nava Garcés, A.E., coord., 2013. El derecho en la era digital. México DF: Porrúa.

Nava Garcés, A.E., coord., 2019. Ciberdelitos. Ciudad de México: Tirant Lo Blanch.

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, 2021. *Gobernanza de internet*. [en línea] Disponible en: <https://www.itu.int/net/wsis/basic/about-es.html> [Acceso 17 noviembre 2021].

Organización para la Cooperación y el Desarrollo Económicos, 2021. *Biblioteca.* [en línea] Disponible en: < https://ccdcoe.org/library/publications/> [Acceso 18 mayo 2021].

Ospina Díaz, MR. Y Sanabria Rangel, PE., 2020. Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad*, [en línea] Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199> [Acceso 14 julio 2021].

Pages, J., 2019. Cuando un ciberataque puede paralizar un país: seguridad en infraestructuras críticas. *Red Seguridad,* [en línea] Disponible en: < https://www.redseguridad.com/revistas/red/087/58/index.html#zoom=z > [Acceso 16 junio 2021].

Palacio Puerta, M. y Peña Cabrera, KI., 2017. La gobernanza de internet como plataforma para impulsar políticas en la educación con TIC. El caso de Colombia*. Revista Opera*, [revista electrónica] (21), pp. 5- 23. https://doi.org/10.18601/16578651.n21.02 .

Palacios Moguel, R., s.f. *El voto electrónico en México, un modelo de sustentabilidad democrática*. [pdf] Disponible en:

<https://comisiones.senado.gob.mx/justicia/docs/nombramientos/magistrados/CHIAPAS/RMP/anexo_6.pdf> [Acceso 08 abril 2022].

Paniagua, G., 2015. Políticas públicas y el uso del internet para el acceso y eficiencia en la presentación de los servicios públicos: caso del Portal de Servicios del Registro Nacional de Costa Rica. *Revista Estudios de Políticas Públicas*, [en línea]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/6067316.pdf [Acceso 07 abril 2022].

Patiño Orozco, GA.,2021. Una comparativa de los esquemas de ciberseguridad de China y Estados Unidos. *Oasis*, [en línea] 34, pp. 107-126. Disponible en: <https://revistas.uexternado.edu.co/index.php/oasis/article/view/7166> [Acceso 12 diciembre 2021].

Pierre, L., 2007. *Cibercultura. Informe al Consejo de Europa.* [libro electrónico] Rubí (Barcelona): Anthropos. México: Universidad Autónoma Metropolitana. Disponible en: <https://antroporecursos.files.wordpress.com/2009/03/levy-p-1997-cibercultura.pdf> [Acceso 20 febrero 2021].

Prieto Madrid, M., 2020. Los piratas informáticos disparan contra las vacunas Covid. *Expansión,* [en línea] 15 de diciembre. Disponible en: <https://www.expansion.com/economia-digital/companias/2020/12/15/5fd79f73468aeb4d708b4630.html> [Acceso 26 agosto 2021].

Pons Gamón, V. 2018. *Ciberterrorismo: amenaza a la seguridad. Respuesta operativa y legislativa, nacional e internacional.* Tesis doctoral. Escuela Internacional de Doctorado. Disponible en: < http://e-spacio.uned.es/fez/eserv/tesisuned:ED-Pg-DeryCSoc-Vpons/PONS_GAMON__Vicente_Tesis.pdf> [Acceso 20 marzo 2021].

Porrúa, MA., 2019. Gobiernos y cibermuros: Los ladrillos de una buena política de ciberseguridad", *Banco Interamericano de Desarrollo*, [blog] 30 de abril. Disponible en: <https://blogs.iadb.org/administracion-publica/es/ladrillos-de-una-buena-politica-de-ciberseguridad/> [Acceso 28 enero 2022].

Ramírez Morán, D., 2015. *La visión internacional de la ciberseguridad*. [pdf] Disponible en: https://www.ieee.es/Galerias/fichero/docs_informativos/2015/DIEEEI02-2015_VisionInternacional_Ciberseguridad_DRM.pdf [Acceso 25 enero 2022].

Ramírez Morán, D., 2017. Ciberseguridad en China. *Revista del Instituto Español de Estudios Estratégicos*, [en línea]. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=6057663> [Acceso 20 noviembre 2021].

Red Seguridad, 2020. *El Senado de Estados Unidos da un paso adelante en materia de ciberseguridad IoT*. [en línea] Disponible en: <https://www.redseguridad.com/actualidad/el-senado-de-estados-unidos-da-un-paso-adelante-en-materia-de-ciberseguridad-iot_20201203.html> [Acceso 14 diciembre 2021].

Réyez, J., 2020. México: 10 mil ciberataques al mes. *Contralínea* [blog] 22 de noviembre. Disponible en: < https://contralinea.com.mx/portada/mexico-10-mil-ciberataques-al-mes/> [Acceso 14 agosto 2021].

Riquelme, R., 2020. Internet universal, 5G y ciberseguridad, políticas públicas prioritarias para impulsar la economía digital: Axon Partners Group. *El Economista*, [en línea] 26 de febrero. Disponible en: <https://www.eleconomista.com.mx/tecnologia/Internet-universal-5G-y-ciberseguridad-politicas-publicas-prioritarias-para-impulsar-la-economia-digital-Axon-Partners-Group-20200226-0076.html> [Acceso 07 abril 2022].

Rivas, SM., 2021. El ciberespacio como zona de control geopolítico y papel de las potencias por la supremacía cibernética: China y Estados Unidos. *Revista Relaciones Internacionales*, [revista electrónica] (III), pp. 89–107. Disponible en: <https://revistas.ues.edu.sv/index.php/reinter/article/view/2069> [Acceso 20 diciembre 2021].

Robles Carrillo, M., 2015. *El ciberespacio y la ciberseguridad: consideraciones sobre la necesidad de un modelo jurídico.* [pdf]. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=7688324> [Acceso 20 agosto 2021].

Rodríguez Cuitiño, MR., s.f. *La protección de infraestructuras críticas como un aspecto de la seguridad integral del Estado*. Disponible en: < https://www.gub.uy/ministerio-defensa-nacional/sites/ministerio-defensa-nacional/files/2020-03/Revista_Estrategia_6.pdf#page=9> [Acceso 28 agosto 2021].

Rodríguez, MA., 2018. *Introducción al concepto de soberanía*. [pdf] Disponible en: <https://repositorio.unne.edu.ar/handle/123456789/28188> [Acceso 22 agosto 2021].

Romero, G., 2020. Sin presupuesto y autoridad, México pierde 9 mil mdd por ciberataques. *ContraRéplica*, [en línea] 27 de septiembre. Disponible en: <https://www.contrareplica.mx/nota-Sin-presupuesto-y-autoridad-Mexico-pierde-9-mil-mdd-por-ciberataques202027944> [Acceso 25 agosto 2021].

Rubal Thomse, M., 2019. Internet en China: acceso limitado. *La Vanguardia*, [en línea] 13 de septiembre. Disponible en: <https://www.lavanguardia.com/vida/junior-report/20180213/44754795638/internet-china-acceso-limitado-censura-escudo-dorado-gran-cortafuegos.html> [Acceso 10 octubre 2021].

Ruiz Sanjuán, C., 2016. Estado, sociedad civil y hegemonía en el pensamiento de Gramsci. *Revista de Filosofía y Teoría Política*, [en línea] Disponible en: <https://www.rfytp.fahce.unlp.edu.ar/article/view/RFyTPe002/html> [Acceso 12 diciembre 2021].

Sánchez Gutiérrez, A., 1993. El proceso de diagnóstico en la elaboración de políticas públicas. *Perfiles latinoamericanos*. [en línea] Disponible en: <https://perfilesla.flacso.edu.mx/index.php/perfilesla/article/view/472/425> [Acceso 29 febrero 2022].

Sanz Alisedo, Gonzalo., s.f. *Intereses que afectan a la Soberanía Nacional.* [pdf] Disponible en: < https://dialnet.unirioja.es/descarga/articulo/4547898.pdf> [Acceso 20 agosto 2021].

Schreiber, C., 2019. *El futuro de China y Rusia como Aliados en el Ciberespacio.* [en línea] Disponible en: <http://www.seguridadinternacional.es/?q=es/print/1606> [Acceso 11 mayo 2022].

Secretaría de Energía, s.f. *Estrategia Nacional de Ciberseguridad*. [pdf] Disponible en: https: <//www.energypartnership.mx/fileadmin/user_upload/mexico/Events/03_Marquez_Cybersecurity.pdf> [Acceso 13 marzo 2022].

Secretaría de la Defensa Nacional y Secretaría de Marina, 2021. *Glosario de Términos SEDENA-MARINA en Materia de Seguridad en el Ciberespacio.* [pdf] Disponible en: https: <//www.gob.mx/cms/uploads/attachment/file/661790/Glosario_de_Terminos_SD-_SM_compressed.pdf> [Acceso 05 marzo 2022].

Secretaría de Marina, 2020. *Programa Sectorial Derivado del Plan Nacional de Desarrollo 2019-2024*. [pdf] Ciudad de México: Secretaría de Marina. Disponible en: <https://www.dof.gob.mx/nota_detalle.php?codigo=5596130&fecha=03/07/2020> [Acceso 10 septiembre 2021].

Secretaría de Marina, 2021. *Estrategia Institucional para el Ciberespacio 2021-2024*. [pdf] Disponible en: <https://www.gob.mx/cms/uploads/attachment/file/661788/Estrategia_Institucional_Ciberespacio_SM.pdf> [Acceso 30 marzo 2022].

Sistema de Información sobre Comercio Exterior, 2021. *Decisión 587 Lineamientos de la Política de Seguridad Externa Común Andina.* [en línea] Disponible en: <http://www.sice.oas.org/trade/junac/decisiones/dec587s.asp#:~:text=Prevenir%2C%20combatir%20y%20erradicar%20las,amenazas%20para%20la%20Comunidad%20Andina.> [Acceso 31 julio 2021].

Suñe, E. coord., 2015.La constitución del Ciberespacio. México: Porrúa.

Téllez Valdés, J., 2009. Derecho Informático. 4ta ed. México, D.F.: McGraw-Hill.

The White House, 2016. *FACT SHEET: Cybersecurity National Action Plan.* [en línea] Disponible en: <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan> [Acceso 23 noviembre 2021].

Thomson Reuters, 2022. *Cyberspace Administration of China (CAC) (国家互联网信息办公室)*. [en línea] Disponible en: https://uk.practicallaw.thomsonreuters.com/8-618-

2325?transitionType=Default&contextData=(sc.Default)&firstPage=true [Acceso 12 enero 2022].

Trend Micro, 2022. *United States Computer Emergency Readiness Team (US-CERT).* [en línea] Disponible en: <https://www.trendmicro.com/vinfo/us/security/definition/united-states-computer-emergency-readiness-team-us-cert> [Acceso 14 diciembre 2021].

Unión Internacional de Telecomunicaciones, 2010. *Ciberseguridad*. [en línea] Disponible en: < https://www.itu.int/net/itunews/issues/2010/09/20-es.aspx> [Acceso 14 mayo 2021].

Unión Internacional de Telecomunicaciones, 2017. *Cumbre mundial sobre la sociedad de la información*. [en línea] Disponible en: <https://www.itu.int/net/wsis/basic/about-es.html> [Acceso 10 octubre 2021].

Unión Internacional de Telecomunicaciones, 2018.*Global Cybersecurity Index (GCI)*. [pdf] Disponible en: < https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf > [Acceso 29 mayo 2021].

Unión Internacional de Telecomunicaciones, 2021. *Sobre la Unión Internacional de Telecomunicaciones (UIT)*. [en línea] Disponible en:
< https://www.itu.int/es/about/Pages/default.aspx> [Acceso 14 mayo 2021].

Universidad de Alicante, s.f. *Backdoors o puertas traseras.* [en línea] Disponible en: <https://moodle2020-21.ua.es/moodle/pluginfile.php/298195/mod_resource/content/9/backdoors_o_puertas_traseras.html> [Acceso 22 diciembre 2021].

Vargas Borbúa, R., Reyes Chicango, RP. y Recalde Herrera, L., 2017. Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de

gobernanza en ciberdefensa. *Revista Latinoamericana de Estudios de Seguridad*, [revista electrónica], (20), pp. 31-45. https://revistas.flacsoandes.edu.ec/urvio/article/view/2571 .

Vásquez Cruz, E., 2016. *Crítica, una tarea fundamental en ciberseguridad nacional en México*. [en línea] Diario TI. Disponible en: <https://diarioti.com/proteger-la-infraestructura-critica-una-tarea-fundamental-en-ciberseguridad-nacional-en-mexico/98990#:~:text=Las%20infraestructuras%20cr%C3%ADticas%2C%20son%2C%20de,estratégicas%2C%20por%20estar%20relacionadas%20con> [Acceso 14 abril 2022].

Velasco Sánchez, E. Pisanty Baruch, A., 2021. Cuarta Revolución Industrial: gobierno y buena gobernanza. *Revista Latinoamericana de Economía y Sociedad Digita*l, [revista electrónica] 2. https://revistalatam.digital/article/210228/

Vera, G., 2022. *La ciberdefensa en América Latina, entre el peligro y la indiferencia.* [en línea] Colombia: El Tiempo. Disponible en: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberataques-america-latina-muy-vulnerable-por-indiferencia-de-gobiernos-662478#:~:text=En%202021%2C%20los%20ciberataques%20aumentaron,Brasil%20con%2030%2C6%20%25> [Acceso 14 abril 2022].

Vidal M., 2017. La polémica ley de ciberseguridad entra en vigor en China. *El País*, [en línea] 31 de mayo Disponible en: <https://elpais.com/internacional/2017/05/31/actualidad/1496241283_691973.html> [Acceso 25 noviembre 2021].

Viollier, P., 2017. *La participación en la elaboración de la Política Nacional De Ciberseguridad: hacia un nuevo marco normativo en Chile*. [pdf] Derechos Digitales. Disponible en: https://www.derechosdigitales.org/wp-<content/uploads/ciberseguridad.pdf> [Acceso 14 marzo 2022].

TABLAS