# UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

## ESCUELA DE RELACIONES INTERNACIONALES

**TEMA DE INVESTIGACIÓN:**

# ESTRATEGIAS DE CIBERSEGURIDAD APLICADAS EN LAS EXPORTACIONES COMERCIALES EN EL PERIODO 2016-2020

MODALIDAD DE TESIS PARA OPTAR POR EL TÍTULO DE LICENCIATURA EN RELACIONES INTERNACIONALES CON ÉNFASIS EN COMERCIO EXTERIOR


**NOMBRE DE LA ESTUDIANTE:**

DAINE PRISCILLA MONGE LÓPEZ

**TUTORA DE LA INVESTIGACIÓN:**

IBEL DÍAZ CALDERÓN



SEDE ARANJUEZ, SAN JOSÉ

MARZO, 2021

# Contenido

# RESUMEN EJECUTIVO

El uso de las tecnologías de información y comunicación se llegó a implementar en la vida cotidiana y se estableció dentro de la sociedad, estas novedades tecnológicas en las que nos desenvolvemos actualmente establecieron nuevos escenarios donde el intercambio informativo y los canales de comunicación se diversificaron de manera inédita. Su desarrollo ha traído consigo muchísimas ventajas en la búsqueda de la eficacia y la innovación tecnológica.

El internet es una realidad que envuelve la sociedad por completo, donde cada vez hay menos espacio que queda a su margen, la globalización del ciberespacio en todas las áreas en las que se han establecido por lo que la podemos observar áreas como el ocio, el trabajo, las comunicaciones entre muchísimos otros más. Podemos decir que absolutamente todas las actividades que desarrollemos tienen consigo la tecnología, así como nos ha permitido gozar de muchísimas ventajas, también se puede escapar del alineamiento y control al que se dirigía, de este modo caer en manos de quienes le den un uso inadecuado e incluso sea utilizado para ejecutar actividades ilícitas.

En la era digital y la evolución tecnológica que se experimenta, principalmente en los países desarrollados, se puede encontrar situaciones donde la implementación tecnológica ha llegado a solventar algunas necesidades importantes de mejora. Sin embargo, hay que tener en cuenta que de igual forma pueden suponer un problema.

Durante los últimos años se han experimentado y presenciado diferentes situaciones, entre ellas la más común que se pueden mencionar es cuando la información sensible escapa del control del usuario e incluso de algunos sectores empresariales de la industria, lo que ha generado una alarma importante dentro de la población. Y es aquí donde la reflexión hacia la importancia de disponer de un ciberespacio seguro para el desarrollo de actividades es fundamental.

Por lo que realizar estrategias de desarrollo y ejecución en materia de ciberseguridad tanto para la prevención como para el resguardo del mismo conlleva la realización de protocolos o convenios que favorezcan a los diferentes actores que

conforman la comunidad internacional, por lo que en esta investigación se tiene como propósito resaltar la importancia de las estrategias de ciberseguridad, brindando una visión y análisis de las estrategias establecidas dentro de las exportaciones comerciales, evaluando algunos de los protocolos de cooperación internacional y realizando una recopilación de recomendaciones y mejores prácticas.

# CAPÍTULO I: INTRODUCCIÓN

La evolución que ha llevado la tecnología de la información y la comunicación a lo largo de la historia ha traído grandes ventajas dentro de las telecomunicaciones para la sociedad y ha llegado a modificar el quehacer en todos los ámbitos del comportamiento y las relaciones sociales. No hay quienes desaprovechen la oportunidad de utilizar las ventajas que proporciona el mundo de la tecnología, y es por esto que no se puede dejar de lado quienes lleguen a cambiar estas oportunidades y las vuelvan desventajas utilizando las nuevas tecnologías de forma negativa.

Las organizaciones de crimen organizado transnacional dedicadas a los actos delictivos han aprovechado cada una de sus aristas para entrar dentro del ciberespacio y realizar sus fechorías. El cibercriminal se ha posicionado y ha estado involucrado dentro de factores sociales, políticos, económicos e históricos, lo cual lo lleva a posicionarse como un actor más del Sistema Internacional.

Aunque el ciberespacio ha regalado grandes herramientas integrales para sacar mayor provecho a las novedades tecnológicas, también ha dado un espacio para nuevas amenazas que van desde el tradicional como el hurto y fraude, hasta amenazas más complejas como el espionaje, daño a la información, y ciberataques. A pesar de que se entiende la evolución constante, y las dinámicas tecnológicas en la creación de herramientas informáticas en la que nos encontramos siendo así una sociedad cada vez más interconectada, no se dimensiona el peligro que esto mismo conlleva.

Es por esto que constantemente se crean defensas capaces de lograr repeler cualquier amenaza de forma integrada coordinando esfuerzos no solo nacionales, sino también internacionales. La ciberseguridad se ha venido posicionando fuertemente en los últimos años a través de las nuevas tecnologías, por lo cual la creación de estrategias de carácter nacional e internacional, buscan de este modo, prevenir las acciones hostiles de actores maliciosos.

Dado todo este panorama, la ciberseguridad se ha caracterizado como un fenómeno de suma importancia, ya que forma parte de la era tecnológica, la información, la comunicación, y por ende sus repercusiones dentro de las relaciones internacionales. Se ha

podido presenciar los efectos negativos y devastadores que pueden ocasionar los ataques cibernéticos. Algunos de los países que han llegado a sufrir de estos ataques han sido Estonia en 2007, Georgia en el 2008, e Irán en el 2010. Cuando sucedieron estos acontecimientos se destacó la necesidad de implementar la ciberseguridad como prioridad en la agenda de seguridad proporcionando nuevas estrategias que lleguen a resguardar la seguridad de las naciones.

De acuerdo con Kshetri (2018 s.p):

> Desde el punto de vista de la seguridad nacional y las relaciones internacionales el ciberespacio añade tres grandes problemas:
>
> 1) éxito limitado en la cooperación en los temas de ciberseguridad, como consecuencia de la falta de normas para la participación en el ciberespacio.
> 2) falta de evidencias fácticasy concluyentes que permitan conocer a ciencia cierta quién es el perpetrador de los ataques, la mayoría de las evidencias son circunstanciales.
> 3) Las violaciones son más frecuentes en el ciberespacio que en el espacio físico; en realidad esto es una consecuencia del segundo, debido a que la naturaleza del ciberespacio hace más fácil desacreditar la evidencia presentada por los adversarios". .

Durante los últimos años, las naciones se han visto obligadas a actualizar los conceptos de seguridad, ampliando el término a diversos niveles dimensionales abarcando así el espacio cibernético, debido a la diversificación de actores y el incremento de riesgos, por lo que, en los últimos años naciones como Estados Unidos empezaron a considerar el ciberespacio como un prioridad dentro de sus agendas, posicionándolo así un como uno de los temas importantes para la implementación y desarrollo dentro de sus estrategias de seguridad nacional. Por tanto, se observa una integra relación entre los actores públicos y privados en busca de fomentar la seguridad, protección y prevención de posibles ciberataques.

Para ello, durante esta última década se ha incrementado la colaboración entre departamentos gubernamentales, como Justicia, el de Comercio, o la Agencia Nacional de

Seguridad. Asimismo, en 2013 se desarrolló una nuevaOrden Ejecutiva: ImprovingCriticalInfrastructureCubersecurity, para reforzar la concienciación, capacitación y trasvase de información. Según (Aina Pou, párr.2, 2020)

De esta forma buscan mantener un liderazgo estratégico que garantice la consolidación política y comercial dentro de un mundo cada vez más competitivo, donde el mercado mundial se expande cada vez más. En este marco se busca además, dar de forma efectiva frente a los diferentes retos que se afrontan en materia de seguridad nacional.

Para poder garantizar este nuevo marco de ciberseguridad, Washington ha calificado de imprescindible optar con la colaboración de empresas aseguradoras para así obtener la provisión de pólizas susceptibles decubrir toda la gama de ciberriesgos que se ciernen sobre las empresas estadounidenses. Las empresas de seguros adquieren un papel central en la armonización, homogeneización y mejora de las ciber capacidades de este sector. Según (Aina Pou, párr.5, 2020)

La trascendencia de las prácticas en el ciberespacio en los últimos años ha logrado integrarse en sectores de suma importancia para la economía de los países como lo es en el ámbito comercial. Hay que tener en cuenta que una de las limitaciones con las que cuentan las entidades son las herramientas de detección de mercancías ilícitas. Las consecuencias más relevantes son las afectaciones que traen consigo los ataques cibernéticos a nivel internacional, pues esto implica grandes afectaciones de forma negativas dentro de las relaciones internacionales así como las relaciones comerciales y la afectación en la imagen país.

## 1.1 Planteamiento del problema

Esta investigación busca ayudar a sus lectores a comprender los puntos que impulsaron la creación de este estudio, evolución y entendimiento de cómo se llega a implementar la ciberseguridad para combatir la criminalidad que se ha implementado incluso en el ciberespacio, por lo que se ha calificado como un mal común entre la comunidad internacional. Debido a que en los últimos años, gracias al acelerado desarrollo de la

tecnología y las telecomunicaciones, este mismo se ha vuelto parte de los actores dentro del Sistema Internacional.

La constante evolución de los fenómenos que impactan la esfera internacional hace necesaria la comprensión de los mismos, el análisis de comportamiento de los actores, los medios en el entorno que se llega a operar, conocer el desarrollo y la implementación de la ciberseguridad, con base especialmente en Estados Unidos la cual nos ayudará a tener una visión más precisa de la complejidad que conlleva el mundo digital incluyendo herramientas como el internet. Todas estas herramientas llegan a modificar el concepto de seguridad como tradicionalmente lo conocemos y los retos que este se llega a imponer en el mundo actual.

Todo esto se debe a que en los últimos años se ha visualizado un enorme aumento de las afectaciones de los sistemas que comprenden el espacio cibernético dentro de las industrias ilegales dedicadas al cibercrimen que interfieren en los Estados, perjudicando principalmente las relaciones comerciales entre las diferentes naciones, y viéndose así los países cada vez más afectados.

En el mundo globalizado en el que vivimos, las amenazas al orden requieren protagonismo y dimensiones globales, ya que su expansión ha logrado establecerse dentro de toda estructura pública y privada, comprendiendo temas sensibles como procesos de fiscalización, eficiencia, control y cumplimiento de todas las políticas existentes en el amplio tema de la seguridad. Por eso, se ha hecho referencia desde sus bases históricas, hasta llegar a la ciberseguridad como forma de neutralización contra las organizaciones dedicadas a implementar ataques cibernéticos contra las industrias comerciales.

Con el desarrollo explosivo de las tecnologías de la información, comunicación y de las telecomunicaciones (TIC), las nuevas tecnologías se han sabido posicionar como una figura activa dentro de actividades comerciales y económicas que llegan a desenvolverse en el ciberespacio, incluso se puede utilizar de forma negativamente las estructuras que componen los entornos sociales, económicos, políticos y comerciales del Estado**.** Por la estructura comercial que engloba el mismo en el aparato estatal, sector comercial y político, se dificulta el desligue del crimen organizado del entorno lícito, con el propósito de legitimar y enmascara su accionar.

La forma en la que tradicionalmente se conoce la seguridad en el espacio físico y su aplicación de normas, es muy diferente a la hora de hablar en el ámbito del ciberespacio, ya que el ciberespacio no cuenta con un espacio determinado por lo que hace difícil sus delimitación en cuanto a ubicación, y geografía intangibles, por lo cual se carece de estudios suficientes para su comprensión a nivel internacional.

En este siendo expresa Rodríguez (2018, pág.10) lo siguiente: "Estados Unidos ha sido consistente en la creación de diferentes estrategias de ciberseguridad, las constantes amenazas cibernéticas y el robo de información y propiedad intelectual, ponen de manifiesto la necesidad de que crear estrategias que trascienden las fronteras estatales".

La ciberseguridad empezó a ocupar un lugar importante dentro del estudio de las relaciones internacionales, como consecuencia de pertenecer a una sociedad cada vez más interconectada, en donde muchas de las oportunidades que nos brinda las tecnologías de la comunicación han sido aprovechadas para realizar actividades criminales que se ejecutan dentro del ciberespacio. La ciberseguridad ha sido creada como aliada en la aplicación de medidas preventivas ante actividades que puedan ser utilizadas maliciosamente.

Ante este panorama se puede decir que el problema de investigación se basa en la siguiente interrogante: ¿Cuál ha sido el impacto de las estrategias de ciberseguridad estadounidenses en las exportaciones comerciales en el periodo 2016 al 2020?

## 1.2 OBJETIVOS

### 1.2.1 Objetivo general

Estudiar las estrategias de ciberseguridad en las exportaciones comerciales estadounidenses en el periodo 2016-2020.

### 1.2.2 Objetivo específicos

- Describir el concepto y la relevancia de los elementos históricos de ciberseguridad.
- Examinar las propuestas de cooperación internacional en temas de ciberseguridad
- Determinar las regulaciones de las exportaciones en materia de seguridad nacional en Estados Unidos
- Analizar el impacto comercial de las estrategias de ciberseguridad estadounidense en el mercado global.

## 1.3 Justificación

Este proyecto se realiza en virtud de conocer aspectos actuales del acontecer internacional, que pueden llegar afectar a la sociedad en algún momento; es importante adentrarse en este tipo de temas con el fin de promover una armonía de la cual tienen derecho a gozar integralmente las naciones. Por tanto, es necesario investigar a fondo la problemática de la ciberseguridad ya que ha llegado a influir mucho en el desarrollo de la sociedad actual.

La era digital y la interconexión han logrado llegar a facilitar las tareas que por muchos años atrás requerían de mayor tiempo y recursos para su realización. La llegada del internet ha suministrado una amplia gama de oportunidades a la sociedad en general, sin embargo, ha sido lugar de actividades criminales como espionaje, ataques, robos, entre otros que llegan a poner en riesgo la seguridad de los Estados.

Las diferentes actividades de forma positiva o negativa que se desarrollen en el ciberespacio son igual de importantes que aquellas que conocemos tradicionalmente en el ámbito físico, viéndose así las naciones forzadas a enfrentar las nuevas amenazas en la búsqueda de mitigar el impacto que esta pueda producir, la ciberseguridad aunque se visualice como un fenómeno complejo y distante, se debe percibir como un ejemplo de evolución constante en las Tecnologías de Información y Comunicación y su importancia dentro de las relaciones internacionales como un actor más del Sistema Internacional.

Sin dejar de lado la importancia que esta presenta dentro del sistema comercial, y que, esta es fundamental para el desarrollo comercial interno y externo de una nación. Al igual aplica para el sector público y privado, en este caso nos dará la oportunidad de echar un vistazo en el ámbito empresarial y las posibles implicaciones que comprende este ámbito.

Por lo que esta investigación busca realizar un análisis que permita profundizar en la seguridad informática, adquiriendo los conceptos necesarios para la aplicación en términos comerciales, que se vuelven fundamentales para el desarrollo de un país. De este modo comprender la dinámica a la que nos enfrentamos con las diferentes posibles

vulnerabilidades y las debidas fortalezas para adecuarnos a los diferentes cambios y evolucionar con ellos de forma continua.

De acuerdo con Data BreachInvestigationsReports de Verizon 14, la mayoría de las empresas ha demostrado ser simple y llanamente incapaces de detectar cuando un hacker se introduce en sus sistemas de información. Esta encuesta fue realizada por los servicios empresariales de Verizon en colaboración con los servicios secretos de Estados Unidos, la Policía Nacional Holandesa y la Unidad de los delitos cibernéticos de la Policía del Reino Unido, informó de que un promedio del 62% de las intrusiones contra empresas tardaba aproximadamente dos meses en detectarse, Según (Data BreachInvestigationsReports, 2013).

Por esta razón, es crucial fomentar la investigación de las nuevas tecnologías dentro todos los ámbitos posibles, principalmente en los menos tradicionales como lo es el comercio. Ya que, es uno de los que se pueden ver no solo con beneficios notables sino que además con posibles consecuencias no tan favorables representando así uno de los campos que mayormente son apetecidos para realizar diferentes crímenes cibernéticos.

Por otro lado, debemos remarcar que si bien es cierto es un tema que ha llegado para quedarse, y evolucionar en el tiempo. La nueva forma de vida que despertó el Covid-19 incrementó considerablemente esta transformación de la era digital, la ciberseguridad y las nuevas formas de trabajo como el teletrabajo y la implementación de nuevos conceptos como ¨los nómadas digitales¨ que se han convertido en estándares donde las herramientas digitales se han vuelto herramientas habituales entre las empresas y las personas.

De la misma forma, tenemos que recordar que en esta nueva modalidad de interacción digital, para un país representa de forma relevante mantener las estrategias posibles de ciberseguridad. Ya que, frente a la normatividad es importante, porque las personas pueden conocer los retos a los que se enfrentan de manera digital, en el cual, a diario se está relacionando el mundo principalmente ahora en medio de una pandemia, todo esto llega a representar la estabilidad, credibilidad, el desarrollo económico, y comercial de un país.

Esta investigación busca analizar la implementación de las estrategias realizada por los Estados Unidos en el marco de la ciberseguridad y que esa investigación sirva como precedente para el enriquecimiento del conocimiento de sus lectores y de este modo los mismos tengan mayor referencia de este tipo de temas que se encuentran en la vanguardia del desarrollo en la actualidad, así como obtener las bases necesarias y suficientes para la creación de nuevas perspectivas para la difusión de la información.

Por otra parte, este estudio busca ser de beneficio para todas aquellas personas que deseen ampliar el tema, además, esta investigación servirá como un antecedente para la sociedad que quiera sacar provecho de para el desarrollo de nuevas investigaciones en el ámbito comercial y tecnológico.

## 1.4 Antecedentes

En el transcurso de la historia, del desarrollo del comercio y de las relaciones internacionales, la ciberseguridades uno de los fenómenos más importantes que ha traído consigo el fenómeno de la globalización y el intercambio al libre mercado. La aparición y expansión de nuevos actores internacionales con la facilidad de movimientos monetarios, transferencias, bienes y servicios de personas de un lugar a otro en casi todo el mundo, la conexión directa en las comunicaciones, la llegada de transnacionales han generado nuevas oportunidades de mercados entre ella el cibercriminal, la implementación y el desarrollo de la ciberseguridad.

Según Oscar Pastor Acosta (2009):

> La guerra cibernética ya hacía furor a finales de los años 90, pero se desvaneció desde el 11-S y con el terrorismo islámico. Ese interés de EE.UU. se debía a que concebía la guerra moderna cada vez más dependiente de ordenadores avanzados y a que ningún ejército de otro país dependía tanto de la era de la información como el de Estados Unidos. (pág.13)

La Guerra fría y la globalización han sido un factor de suma importancia para el fortalecimiento de organizaciones ilícitas, así como las intercomunicaciones y el mercado negro, ya que este fenómeno viene a interconectar cada vez con mayor fuerza al mundo, esto a su vez hace que surjan cada vez más actores dentro de la comunidad internacional.

Para nadie es un secreto que dentro de la esfera gubernamental y el ámbito empresarial también se llega a determinar diferentes disputas a través de internet, ya que se ha implementado el uso de espionaje en ambos ámbitos, por ejemplo en la intercepción de comunicaciones, robo de datos, minería, estafas entre muchas otras acciones que se han ligado en esta materia; por lo que muchos actores del sistema han optado por el reforzamiento estratégico de ciberseguridad, en busca de respaldar sus intereses.

Graham Wright, director de Operaciones de Información y Objetivos (Director of Targeting&InformationOperations) del Ministerio de Defensa del Reino Unido, llega incluso más allá, sugiriendo una perspectiva estratégica de la ciberguerra, en la que se presenta la necesidad de implementar una ciberfuerza como cuarto ejército. El momento de prestar atención a la amenaza cibernética es ahora. Además, esta atrae a los Gobiernos y a diferentes actores, incluyendo a los terroristas, porque es de bajo coste, puede ser muy eficaz y permite realizar acciones de forma anónima. (2009, pág.14).

En la actualidad el ciberespacio es una de las mayores fuerzas dispuesta a intervenir en la sociedad incluso si eso se refiere a la cooperación política, económicay militar, mientras estas le brindan espacios de participación. Es fundamental en nuestra actualidad analizar los criterios de políticas y estrategias utilizadas para el combate criminal de este tipo.

Por otro lado, la historia deja visualizar lo que ha dejado como consecuencia el mal uso de la tecnología teniendo en consideración que un ataque informático puede tener grandes repercusiones como virus que provoquen caídas de sistemas, la corrupción de datos, reproducir y distribución de información falsa, interferencia en mandos y control de forma efectiva, afectar las comunicaciones, la inteligencia, navegación e incluso logísticas de operaciones importantes de un país entero.

Según datos históricos de seguridad nacional y ciberdefensa:

> Estonia se puede considerar como el primer ataque a una nación. Posteriormente, se han registrado incidentes similares en otros países; así, el conflicto armado entre Georgia y Rusia, en agosto de 2008, fue acompañado de ciberataques sobre Georgia orientados a afectar al funcionamiento de algunas infraestructuras críticas del país. Este

> hecho supuso un hito nuevo en la ejecución de acciones militares ya que fue la primera vez que una invasión terrestre fue coordinada con una acción ciber ofensiva on-line. (Acosta, 2009, pág.15)

En relación con lo anterior, existen momentos específicos de la historia que cuentan el desenlace de las operaciones criminales en el ciberespacio, el primero corresponde a los ataques dirigidos a Estonia, es el momento en donde por primera vez se suscita un enfrentamiento relacionado con los ataques cibernéticos entre Rusia y Estonia. Europa perseguía la apertura de mercados y ventajas asociadas al conflicto, y limitaba su introducción de recursos debido a que este ataque bloqueó todos los insumos de la población causándole efectos negativos.

### 1.5 Proyecciones

Esta investigación busca dar una visión internacional sobre los grandes problemas que atraviesa la evolución de la ciberseguridad, desarrollando los diferentes hechos históricos desde su origen hasta los actuales. También se pretende desarrollar la importancia de los intereses de los actores en materia política, económica, comercial, cooperativa, estratégicas y las recomendaciones que puedan llegar a realizarse desde la comunidad internacional.

Una delimitación adecuada permite enfocar los esfuerzos hacia problema que nos interesa (Muñoz C. I., 2015). En la investigación científica, las proyecciones muestran al lector como la guía que permitirá conocer las aspiraciones, pretensiones y restricciones que se encontraron en el abordaje del tema.

Se determinaron dos variables que definen las proyecciones de este trabajo, estas son los alcances y las limitaciones, a su vez, permiten comprender la finalidad y el propósito de la investigación. En los alcances se puntualiza los principales elementos que pretende abordarse en la investigación: Se pretende buscar y analizar la situación actual de las estrategias implementadas desde sus vértices en el desarrollo de las tecnologías de información y comunicación (TIC) como medio de protección, denominada como

ciberseguridad. Se busca reflejar las estrategias definidas en las iniciativas específicas en el sector de las relaciones internacionales y el comercio exterior.

En la investigación se desarrolla el papel que juegan los Estados Unidos como potencia, por su relevancia regional, mundial, y de las posibilidades de acceso a la información relacionada con los aspectos abordados en la investigación. Por último, se incluye un análisis de la situación actual utilizando información pública, reflejando el desarrollo y la implementación de las nuevas tecnologías.

Por otro lado, las limitaciones pretenden nombrar algún obstáculo que se presume pueda entorpecer el logro de las metas (Barrantes, 2013). En este apartado se señalan los elementos no incorporados para efectos investigativos.

### 1.5.1 Alcances

- La presente investigación pretende analizar la dinámica de la ciberseguridad en Estados Unidos como punto geoestratégico, por su presencia a nivel internacional como potencia.
- La investigación pretende dimensionar el impacto generado en la implementación de estrategias de ciberseguridad en las exportaciones comerciales.
- El trabajo persigue determinar las responsabilidades de diferentes actores que interactúan en el amplio espacio cibernético. Esto implica analizar la labor de instituciones estatales y organizaciones privadas en procesos de control, fiscalización y seguridad.
- Se busca conocer el rol estratégico de Estados Unidos en los procesos de ciberseguridad.
- Además, pretende analizar la proyección de la imagen y reputación de los Estados Unidos en relación con la ciberseguridad, como clave para el desarrollo del país ante el tema de seguridad.

### 1.5.2 Limitaciones

- La investigación se centra en las estrategias de ciberseguridad aplicadas en las exportaciones comerciales de Estados Unidos, con base principalmente, en el uso de las TIC.
- Por lo tanto, no contempla las exportaciones de un producto como tal.
- La investigación se enfoca en el uso de las TIC y los desafíos que tienen las instituciones gubernamentales en materia de aplicación de controles efectivos contra diversos crímenes cibernéticos.
- Únicamente se estudiará la estructura logística de exportación comercial estadounidense donde interviene el uso de ciberseguridad.
- Se analizarán los casos relacionados con la aplicación de estrategias de ciberseguridad procedentes de Estados Unidos durante un período de cuatro años, a partir del año 2016 al año 2020.

# CAPÍTULO II. MARCO TEÓRICO

Para efectos de comprensión, los lectores podrán recurrir a este capítulo con el fin de obtener la mayor cantidad de información y datos recopilados. La creación de este apartado de Marco Teórico se ha desarrollado a partir de la revisión de diversos materiales de sustento infalible para la amplitud de este tema, se busca desarrollar las perspectivas teóricas encargadas de contextualizar las bases y las teorías necesarias para respaldar los diferentes aspectos que se expondrán a lo largo de esta investigación y que busca ayudar a facilitar la comprensión de la información plasmada en esta investigación, asa como el contexto histórico inmerso.

**Marco histórico**

## 2.1 Ciberseguridad

A finales de la década del 2000 empezó el siguiente nuevo y gran desafío de la ciberseguridad, que fue cuando se empezó a implantar el internet de las cosas (“Internet of Things” o IoT). Esto supuso un problema debido a que se tratan de dispositivos domésticos, cámaras o incluso juguetes capaces de conectarse a internet (para obtener nuevas ventajas y comodidades) lo que se convirtió en una puerta de entrada para los ciberdelincuentes con la que tenían la oportunidad de acceder a los hogares, así como un incremento de los dispositivos que los ciberdelincuentes pueden utilizar para realizar sus ataques. Según (Sergio López, párr.5. 2020)

La seguridad informática, también conocida como ciberseguridad, nace con la llegada del internet y el avance de la tecnología y su evolución; aun cuando la ciberseguridad se ha logrado desarrollar de forma continua todavía existen quienes siguen en la búsqueda de pequeños vacíos o portales en los que puedan ingresar para violentar la seguridad de los dispositivos y de este manera realizar sus fechorías, por lo que es necesario mantenerse precavidos con el uso de la tecnología y los aparatos electrónicos principalmente los de uso diario.

### 2.1.1 Origen de la ciberseguridad

La evolución de la ciberseguridad brinda un contexto más amplio de cómo fue la transformación al mundo digital y los riesgos que surgieron con este cambio, además que nos sitúa el orden de los acontecimientos que da camino a la llegada y creación de lo que hoy conocemos como seguridad informática o ciberseguridad.

Por esta razón es importante recordar algunos acontecimientos importantes en la historia que permiten entender cómo se da paso a estas nuevas regulaciones que nacen a consecuencia de diferentes acciones ilícitas.

El primer *hacker* de la historia fue NevilMaskelyne. En 1903, interceptó la primera transmisión de telégrafo inalámbrico, mostrando las vulnerabilidades de este sistema desarrollado por Marconi. Por otro lado John Draper fue el primer ciberdelincuente, mejor conocido como *CaptainCrunch*. Draper, descubrió que el sonido emitido por un silbato que se obsequiaba en las cajas de cereal de Cap'nCrunch, podía engañar a la señal de la central telefónica y así poder realizar llamadas gratis. (Vázquez Pesina, párr. 9, 2021)

Toda esta información producida y recopilada a lo largo de la historia, nos permite visualizar el desarrollo imparable en materia tecnológica en el que nos encontramos actualmente llegando así impactar puntos esenciales de las relaciones humanas, que llena a la sociedad de oportunidades, pero que a su vez debe hacer frente a enormes retos.

En los años 70 apareció el primer *malware* de la historia: Creeper, un programa que se replicaba así mismo. Este *malware* mostraba el mensaje "I'm a creeper, catch me ifyou can!". A partir de ahí, nace el primer antivirus llamado Reaper, cuya función era la de eliminar las infecciones por Creeper. Con el paso de los años y los avances tecnológicos, la información en red iba cada vez en aumento, y con ello, su valor e importancia tanto para las organizaciones como para los ciberdelincuentes; el malwareen los años 80 incrementó su presencia y a la par se desarrollaron antivirus más eficientes. En la actualidad, se utiliza una plataforma de detección y respuesta de endpoint (EDR) para proteger los equipos de un ataque de malware debido a su gran evolución (Vázquez párr.11, 2021).

Dada estas circunstancias nace la nueva era tecnológica donde la forma de desarrollo muestra un mundo virtual absolutamente interdependiente con el mundo real, del cual dependemos cada vez más. Por lo que se busca establecer un panorama reestructurado de las operaciones industriales, políticas e incluso las formas tradicionales de operación dentro de la sociedad civil.

**2.2 ¿Quién propone?**

A finales de esta década,Kevin Mitnick utilizó ingeniería social para tener acceso a información personal y confidencial; este tipo de ciberataque, que comenzó a tener mayor uso en aquella época, sigue siendo una de los métodos más populares para vulnerar los activos de una empresa; sin embargo, se pueden prevenir y reducir con una buena estrategia, formación a colaboradores y protocolos de securityawareness. (Info México, párr.12, 2020)

En la cibercultura, existen diferentes conceptos que llegan a surgir con la llegada de la era digital y con ello diferentes formas de uso y manipulación de la información. Cuando muchas de las actividades que se ejecutan en internet y se realizan con mala intención hacen que la seguridad de los sistemas informáticos se vuelvan vulnerados y con ello el contenido de la información. Quienes vulneran los sitios dentro del internet se perciben como ciber rebeldes los cuales utilizan sus habilidades en materia informática en la búsqueda de recolección de datos para dialogar, jugar y transgredir en el ciberespacio; todo esto con el fin de llegar a democratizar el uso de la información.

En el portal  InfoMéxicose puede leer la siguiente información:

> La regulación de la Internetes uno de los temas más desafiantes al que se deben enfrentarse cada uno de los ejecutantes debido a su carácter internacional, la variedad en su contenido y su carácter intangible dentro del ciberespacio. Es por esto que a principios de los 90s surgió la necesidad de hacer frente a los ataques cibernéticos que llegaron a causar múltiples disturbios. Las primeras acciones para crear mecanismos legales frente a los ciberdelitos fueron locales. En 1986, en

> Estados Unidos se creó la ComputerFraud and Abuse Act, sin embargo, su capacidad se vio sobrepasada por la transformación tecnológica" (párr.15, 2020)

Históricamente, cuando se empezaba hablar de la llegada del internet se explicaba el surgimiento de toda una revolución alrededor de la tecnología, el tema del internet y el descubrimiento del espacio cibernético. En general, dentro de lo bueno y lo malo que rodea todo este tema, los Estados empiezan a desarrollar herramientas y planes en los cuales puedan resguardar sus intereses, por esta razón se empieza a ejecutar comités expertos, acuerdos y regulaciones que buscan dar ese respaldo.

Aproximadamente en 1995, se llegó a formar en Europa un comité de expertos en delitos informáticoscon el fin de ejecutar estrategias que ayudarán a contrarrestar los ataques que se daban a través de Internet. La comunidad internacional, convencida de la necesidad de buscar aplicaciones que fortalezcan la seguridad política-social, amplían y aplican una política penal para proteger a la sociedad frente a la ciberdelincuencia. Por la importancia de fortalecer la cooperación internacional, alrededor del 2001 se aprobó y firmó el Convenio de Budapest, que hoy en día es integrado por aproximadamente 56 países como se puede observar en la siguiente imagen.

IMAGEN #1


Fuente: Banco Interamericano de Desarrollo (BID) & Organización de Estados Americanos (OEA)

IMAGEN #2


Fuente: Banco Interamericano de Desarrollo (BID) & Organización de Estados Americanos (OEA)

Dentro de esta imagen se puede observar cada uno de los países miembros y observadores, además indica el año en el que participan y datos relevantes para la investigación, como qué territorios cuentan con estrategias nacionales en temas de ciberseguridad y quiénes trabajan para su desarrollo.

El convenio que regula el tema de cibercriminalidad, llamado Convenio de Budapest fue creado en el año 2001 este convenio tiene tres ejes esenciales en temas de delitos informáticos, esto con el fin de dar el respaldo necesario en tema de legislación en el ámbito de la ciberseguridad, ya que, esta área resulta bastante compleja principalmente cuando se habla de las posibles regulaciones aplicadas en diferentes países que no están alineados a nivel jurídico.

De acuerdo con el Comité del Consejo de Europa:

> El primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, que se ocupa especialmente de las infracciones de los derechos de autor, el fraude informático, la pornografía infantil y las violaciones de la seguridad de la red. También contiene una serie de poderes y procedimientos, como la búsqueda de redes informáticas y la intercepción. *(CETS No.185)*

Este instrumento se confeccionó con el fin de establecer una política penal común y que establezca el alineamiento a seguir en política penal entre los países, de este modo obtener y brindar protección a la sociedad que les permita como instrumento internacional la ejecución bajo protocolos estandarizados de desarrollos en temas de legislaciones nacionales alineados en la lucha contra el cibercrimen.

Brindando además mayor eficacia en la implementación en las normativas procesales y con ello como resultado colateral una mejor armonía en la cooperación internacional. Facilitando así el ajuste de medidas y protocolos a seguir cuando se presenten violaciones de las leyes adoptadas a la lucha contra la delincuencia cibernética.

Según las estipulaciones del convenio de Budapest se establece lo siguiente: El convenio tiene cuatro capítulos, en los que además de definirse una serie de terminologías en común, se establecen tres ejes esenciales para hacer frente a los delitos informáticos:

En el primer eje se aborda el tema de los delitos informáticos y tiene como objetivo establecer un catálogo de figuras dedicadas a pensar las modalidades de criminalidad informática. Es decir, en este capítulo **se** definen los delitos y se los clasifica en 4 categorías:

- Delitos que tienen a la tecnología como fin: son aquellos que atentan contra la confidencialidad, integridad o disponibilidad de la información. Por ejemplo, el daño informático, el acceso ilícito a un sistema, etc.
- Delitos que tienen a latecnología como medio: se refiere a delitos ya conocidos, que se cometen a través de un sistema informático. Son delitos comunes, que ya se encuentran tipificados en la mayoría de las legislaciones, ampliados a los medios digitales. Por ejemplo, el fraude informático o la falsificación de datos digitales.
- Delitos relacionados con el contenido: establece como delitos diversos aspectos de la producción, posesión y distribución electrónica de pornografía infantil.
- Delitos relacionados con infracciones a la propiedad intelectual: se refiere a la reproducción y difusión en Internet de contenido protegido por derechos de autor, sin la debida autorización. Por ejemplo: infracciones a la propiedad intelectual, piratería, etc.

En el segundo eje se abordan las normas procesales: aquí se establecen los procedimientos para salvaguardar la evidencia digital, así como también las herramientas relacionadas con la manipulación de esta evidencia. El alcance de esta sección va más allá de los delitos definidos en el punto anterior, ya que aplica cualquier delito cometido por un medio informático o cualquier tipo de evidencia en formato electrónico. Entre otras cosas determina la obtención y conservación de datos digitales para ser utilizados como pruebas.

El último eje contiene las normas de cooperación internacional, que son reglas de cooperación para investigar cualquier delito que involucre evidencia digital, ya sean delitos tradicionales o informáticos. Incluye, entre otras, disposiciones acerca de la localización de

sospechosos, recolección o envío de evidencia digital, e incluso lo referente a extradición. Según (Pastorino, párr.6-13, 2017)

En concordancia con Pastorino (2017), cada eje establecido por el convenio ha sido para los países una guía óptima para dar frente ante eventos de delitos informáticos a los que se enfrentan diariamente la comunidad internacional y la sociedad civil en general, brindando así un respaldo consciente y armónico entre los Estados, además de dar un paso importante en materia de investigación brindando las herramientas, procedimientos, concientización y prevención hacia las amenazas diarias y futuras en materia informática.

Este tratado, consensuado durante más de cinco años, fue aprobado en 2001 y reflejaba no sólo las preocupaciones del momento, sino también dos aspiraciones europeas muy concretas: la necesidad de estandarizar los sistemas penales de justicia y, más importante aún, la urgencia de crear mecanismos de cooperación internacional contra la cibercriminalidad. (Hiperderecho, párr.6 ,2018)

En la actualidad, necesariamente hay que visualizar de forma crítica el rol en que se desenvuelve el ciberespacio, además de la evolución que la misma tiene a la hora de acondicionarse a nuevos paradigmas con la llegada del convenio, ya que, modifica las bases o estructuras con las que se llegó a desarrollar en un principio, sin dejar de lado que si bien es cierto la creación de una estandarización brinda un guía de ejecución, cada país tiene sus puntos fuertes en donde hacer mayor hincapié.

El apunte hacia el futuro de la **s**eguridad cibernéticaestá en la cooperación internacional, por esta razón la creación de convenios como el de Budapest se ha convertido en un tema importante para los diferentes Estados. Por esta razón este mismo convenio ha adquirido un éxito importante en la generación en conjunta de normas, además de dar una mayor visualización panorámica en temas de mejoras, prioridades e importancia que se requiere en servicios de control sobre el tema de ciberseguridad y los temas adyacentes al mismo.

Trabajar el análisis de riesgos se vuelve imprescindible ya que se comparten espacios comunes entre sí, lo que se vuelve un crucial para la protección y la

administración de la información. Por medio de la cooperación se puede visualizar cómo las directrices, y las estrategias en temas de ciberseguridad comparten planes de alcance institucional o nacional dentro de la comunidad internacional.

## Marco conceptual

### 2.2.1 ¿Qué es la ciberseguridad?

La Real Academia Española define la ciberseguridad como un conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos. (RAE, s.f.). La ciberseguridad hace referencia a la protección que se le puede brindar a los sistemas informáticos de posibles ataques maliciosos.

De acuerdo a los expertos de InformationSystemsAudit and Control Association (ISACA), la ciberseguridad se define como "una capa de protección para los archivos de información". También, para referirse a la ciberseguridad, se utiliza el término **s**eguridadinformática o seguridad de la información electrónica. (Vázquez párr.1, 2021)

Como se ha mencionado antes, gracias a la evolución tecnológica en las últimas décadas se ha llegado a elaborar un proceso continuo de digitación social sin precedentes, que ha llegado a impactar a la sociedad en general desde la parte personal hasta la parte laboral. Por lo que para las industrias que se dirigen hacia una producción cada vez más automatizada y que su finalidad es la búsqueda de la eficacia, así como la productividad manufacturera, llega la ciberseguridad a ser parte de importante, dejando así como objetivo principal la generación de confianza entre clientes, proveedores y el mercado en general.

En un mundo hiperconectado, donde la mayoría de las actividades se hacen a través de la red y dispositivos electrónicos, garantizar la seguridad de las operaciones es una necesidad imperante.

Desde otro punto de vista, la empresa Kaspersky define la ciberseguridad como la práctica que tiene como objetivo "defender los ordenadores y servidores, dispositivos móviles, sistemas electrónicos, redes y datos frente a ataques maliciosos". Esta definición

deja claro que la ciberseguridad no es una práctica limitada únicamente a asegurar los equipos informáticos, sino que se dirige a cualquier dispositivo o sistema que pueda estar conectado a internet o hacia cualquier material de valor almacenado.  Reinares Párr.4, 2020)

El concepto integral que se le da a la ciberseguridad se ha vuelto fundamental para entender lo amplio en lo que órbita las generalidades de este tema, principalmente en el área comercial donde los empresarios y líderes mundiales llegan a considerar a los ataques cibernéticoscomo uno de los principales riesgos a los que se enfrentan en la actualidad y a la ciberseguridad como su mayor reto de desarrollo para su propia protección.

Esto implica mayor dinamismo con las tecnologías emergentes y la mayor exposición a la información. Pese a la vasta llamada de prevención a este tipo de temas y la importancia que este mismo emana, son pocas las industrias comerciales que tienen un abordaje claro de la ruta a seguir a la hora de enfrentar los posibles peligros que se encuentran alrededor del mundo cibernético.

Por esta situación según El Centro Criptológico Nacional de España denomina ciberseguridad al conjunto de actuaciones orientadas a asegurar, en la medida de lo posible, las redes y sistemas de que constituyen el ciberespacio: detectando y enfrentándose a intrusiones; detectando, reaccionando y recuperándose de incidentes; preservando la confidencialidad, disponibilidad e integridad de la información. (pág.20, 2017)

Se puede inferir que el concepto de ciberseguridad nace con la necesidad de las compañías por mantener protegido sus sistemas e información de posibles ataques que busquen violentar o comprometer su correcto funcionamiento, así como también el uso inadecuado de la información que puedan causar daños irremediables. Por lo que para el comercio y la industria se vuelve primordial no solo tener sistemas de defensa, sino que más allá de esto busca la educación a sus usuarios en la prevención de riesgos que puedan resultar innecesarios.

### 2.2.1 Relaciones comerciales.

Las relaciones comerciales entre los diferentes países han recorrido un holgado camino. Por lo que, a continuación se mencionan algunas de las etapas más importantes del comercio.

El trueque fue la primera actividad comercial de la historia (Mun, 1995). En donde se intercambiaban los bienes por algún otro. Esto lograba que las diferentes culturas satisficieran sus necesidades e incluso sus gustos por medio del intercambio comercial.

El mercantilismo duró aproximadamente tres siglos, desde el siglo XV hasta mediados del siglo XVIII, el cual afirma que el oro y la plata son la base fundamental de la economía de los países. El principio de esta corriente es que cada país debe tener un excedente en el comercio y este solo se puede efectuar mediante las exportaciones y disminución de importaciones. Tuvo su auge hasta que se publicaron las teorías de Adam Smith en 1776, el cual siempre abogó por la libertad de intercambios internacionales ya que vio que entre más amplios fueran los mercados mayores son las oportunidades de especialización.

En 1880 surge otro modo de comercio, en el que se usaban las monedas hechas de oro. Esta época se conoce como la ¨Época del Patrón de Oro¨. En esta época se procedía a realizar los intercambios comerciales de bienes por monedas de oro o plata. Dado lo difícil y pesado del transporte de los metales es aquí donde surge el uso del papel como el nuevo medio de tipo de cambio, de este modo se logró estabilizar las conversiones de los intercambios comerciales de bienes y servicios ya que las monedas tenían el mismo equivalente dando como resultado una balanza comercial cada vez más equilibrada.

Además, David Ricardo desarrolló su teoría de la ventaja comparativa, la cual habla que un país debe especializarse en lo que mejor sabe hacer y comprar el bien o producto del que carece de producción (Ledesma, 1993).

El comercio internacional continuará siendo un punto importante para la economía mundial. Una de los principales focos de atención es la importancia que brinda el comercio ya que ofrece soluciones a la faltante de algún bien o producto gracias a que todos los

países cuentan con el acceso necesario al intercambio comercial de bienes para suplir sus necesidades de diferentes productos.

### 2.2.2 Economía

Para empezar el siguiente apartado se define qué es la economía y seguidamente se desarrolla el enlace de las exportaciones comerciales y la economía en general. La economía es la ciencia social encargada de administrar los recursos disponibles para satisfacer las necesidades humanas. También se encarga de estudiar el comportamiento y las acciones de los seres humanos.

"Como ciencia, es la disciplina que estudia las relaciones de producción, intercambio, distribución y consumo de bienes y servicios, analizando el comportamiento humano y social en torno de éstas fases del proceso económico." (Bembibre, 2008, párr.1) Tal y como lo describe Bembibre, la economía viene hacer una recolección y análisis del comportamiento de los individuos para su producción, intercambio así mismo como su respectiva distribución de cualquier bien o producto necesario.

La economía también interactúa con el análisis del comportamiento y reacción del ser humano con el entorno cuando se modifican su desarrollo. Sus efectos ante diferentes cambios serán percibidos de variadas formas por lo que por lo general se contemplan principalmente en la variación de precios, productos, producción, riqueza y el consumo que se registre.

Por esta razón se le atribuye su vínculo con las exportaciones, ya que influye en la percepción y manejo del dinero y por ende en las consecuencias económicas de uno o más países. Se menciona esta referencia porque las relaciones comerciales y las exportaciones pueden modificar la dinámica económica y el accionar de los Estados en la búsqueda del balance.

### 2.2.3 Comercio internacional

De acuerdo con Torres (1990), el comercio es el sustrato de la economía capitalista, pues este se encuentra en todos los aspectos de la vida, como lo es la fuerza laboral, el dinero, el comercio de mercancías y el comercio de divisas. Estos elementos generales se relacionan

con procesos en donde los productores elaboran mercancías mediante las cuales los consumidores satisfacen sus necesidades, este intercambio o relación comercial se produce a través del mercado.

La Real Academia Española define el comercio como "compraventa o intercambio de bienes o servicios" (RAE, s.f.). El comercio internacional se refiere a la relación comercial entre países y regiones. Se caracteriza por la diferenciación de precios y la distribución de los recursos de los países, aquí se produce la misma dinámica del intercambio comercial, pero a una escala global.

El objetivo principal es cubrir las necesidades de los Estados y regiones promoviendo el beneficio mutuo de posicionar sus productos en mercados internacionales. El intercambio entre naciones y bloques regionales está sujeto a regulaciones que establecen los mismos Estados involucrados y sus Gobiernos.

El comercio internacional es una de las alternativas ante la saturación del mercado interno, promueve la diversificación y permite que el país se especialice en la producción de un bien o servicio en el que tiene una ventaja sobre los demás países, esto a su vez deriva al aumento de la competencia y la oferta de productos o bienes en el plano internacional.

### 2.2.4 Exportaciones

Sobre este término se puede decir que:

> La exportación es un medio más común de que sirven las compañías para iniciar sus actividades internacionales. Es decir, que las empresas que se introducen a la exportación lo hacen sobre todo para incrementar sus ingreso de ventas, para conseguir economías a escala en la producción y diversificación de sus sedes de ventas (Daniels y Radebaugh, pág.714, s.a)

Por lo que se podría deducir que la exportación es la acción de enviar o vender bienes, productos, o servicios de un país a otro. Es decir, es un término que describe las operaciones donde un bien, producto o mercancía se lleva fuera del país residente para su utilización comúnmente con fines comerciales.

Teniendo en cuenta que para el desarrollo de este proceso existe un organismo encargado de su regulación conocida como aduanas, ellas se responsabilizan del tráfico de los bienes y servicios que se mueven de un país a otro. Por esta razón, a lo largo de la historia el tema de las exportaciones llega a jugar un papel importante dentro de la economía de los Estados; ya que esto representa un gran dinamismo en la demanda de los productos nacionales.

Se señala como alternativa de expansión comercial las exportaciones, por lo que Según Martínez y Cateora (1996): "Una empresa puede ofrecer su exceso de capacidad productiva en otros países por medio de la exportación. Es la forma más común y sencilla de incursionar en los mercados internacionales pues los riesgos son mínimos". (pág.2)

La importancia de las exportaciones radica en que llega a formar parte importante de los ingresos de un país y por ende llega a promover la economía interna de un Estado, permitiendo de este modo fomentar el crecimiento de fuentes de empleo a la población. Además, es importante recalcar que las exportaciones brindan a los países variedad de productos para solventar el déficit de productos o servicios faltantes en un país, permitiendo evitar inestabilidad de mercados internos y por ende debilita posibles problemas macroeconómicos en los Estados.

En las últimas décadas, la llegada de las nuevas tecnologías, la evolución de los servicios electrónicos, así el desarrollo de las redes de comunicación se ha incorporado cada vez más a nuestra vida diaria. Por lo que, a medida de que la sociedad se empezó a volver cada vez más dependiente es cuando se volvió un tema de interés primeramente nacional y después se desplaza a nivel global, esto cuando todos los Estados empiezan a enfrentar los diferentes cambios.

En el área de las exportaciones es muy común visualizar que con la expansión de las nuevas tecnologías. Dentro de las exportaciones comerciales se visualizan gran cantidad de exportaciones de bienes y servicios de parte de todos los Estados donde hay una creciente demanda en materia tecnológica tanto física como intelectual.

### 2.2.5 Globalización

El fenómeno de la globalización se ha adentrado en temas sociales, políticos, culturales, y económicos de los Estados. Además se debe tener en cuenta que se obtienen tanto benéficos como también inconvenientes, por lo que hay una disputa entre aspectos de beneficio al estado en el acercamiento entre países por medio del intercambio comercial de bienes, servicios, productos, información y acceso al conocimiento. Mientras que en otro extremo existe la idea de los diferentes desafíos que conlleva todo el proceso de globalización y consecuencias importantes dentro de la comunidad internacional. Sobre este tema se entiende también que:

> La globalización es un fenómeno que se ha dado a lo largo de la historia y que ha acercado al mundo en todos los sentidos. Tanto en el intercambio de bienes y productos, como en información, conocimientos, cultura, telecomunicaciones, etc. Como es lógico, y dados los avances tecnológicos, estos últimos años la globalización ha sido mucho mayor y ha llegado y llega más rápido. Pero es un proceso cuya base han sido todos estos años atrás. Es la consecuencia de la integración mundial, del progreso humano. Pero todo esto cambia y hay que adaptarse a ello. También supone multitud de problemas, que se deben resolver. (Finanzas y Economía, párr. 9, s.f)

Un elemento importante a tomar en consideración es que la globalización tiene la facilidad de adherencia en múltiples ámbitos, por lo que se llega a la conclusión de que la globalización ha estado presente en los humanos desde los primeros asentamientos ya que la historia nos deja saber la evolución comercial entre los diferentes pueblos y tribus de la antigüedad que se fue desarrollando como un proceso de avance continuo en los años trayendo un auge debido a los avances tecnológicos que llegaron apresurar este proceso.

Como consecuencia de ello los Estados, y los diferentes actores internacionales han tenido que buscar alternativas necesarias para el desarrollo de estrategias que permitan el avance uniforme y adaptable a la realidad en la que se presenta.

Ander-Egg (2010) define globalización como:

> (…) una palabra de moda que se suele utilizar con diferentes alcances, pero con significaciones semejantes. Pero el uso más corriente con el que se suele utilizar el término es para designar el proceso de universalización de la economía y des territorialización conforme con el cual las distancias físicas y las fronteras han perdido buena parte del significado que habían tenido en los últimos siglos. (p.16)

Como se demuestra anteriormente podemos decir que la globalización tiene un concepto sumamente amplio, pero que en concordancia con el autor se le da mayor enfoque a este concepto en el ámbito económico y comercial. Por último y no menos importante, Ander-Egg (2010) recalca un punto importante de conexión con la investigación citando así que las distancias y fronteras físicas han llegado a modificar su connotación a lo largo de los años y dando así facilidad de intercambio comercial de bienes y servicios a los diferentes actores internacionales.

Al ser este un punto fundamental para el desarrollo y el avance tecnológico dentro de las sociedades, se brindan cambios importantes a nivel mundial. Es por esto que podemos vincular no solo el hecho de la notable evolución comercial que se da gracias a la degradación conceptual de termino fronteras físicas sino que también al alcance tecnológico, su expansión y la absorción de información sin importar los obstáculos como: distancias entre remitente y receptor, por lo que para efectos de investigación es de suma importancia entender este proceso de cambio que se encuentra a la tente como consecuencia de la globalización.

## Marco referencial

### 2.3 Teoría neorrealista

El neorrealismo es la escuela postmoderna de pensadores que proponen el punto de vista de la evolución del realismo político donde los cambios enfatizan el análisis de las estructuras de mecanismos de cambio y continuidad de su propio sistema.

Las concepciones neorrealistas e institucionalistas de las instituciones, consideran que estas son necesidades funcionales para generar orden, según Koremenos, Lipson and

Snidal (pág. 761, 2001). Sin embargo, ni la teoría neorrealista ni tampoco la institucionalista tratan adecuadamente las variaciones de tiempo y espacio.

Es por esta razón que el pensamiento neorrealista es estático de los sistemas internacionales, esto quiere decir no hay mayor dinamismo en las estructuras por lo que busca el beneficio propio, mas no colectivo solo con la excepción a las posibles alianzas contra amenazas en común que se pueda presentar.

Por su parte, Waltz (1964) define la estabilidad como durabilidad del sistema y lo pacifico de sus ajustes internos. Además, la estabilidad implica como factores el endeudamiento de la organización de la anarquía, y la ausencia de variaciones consecuenciales en el número de partes principales o polos que constituyen el sistema. Según (pág.887).

La evolución de las sociedades a lo largo del tiempo hizo que este concepto tenga muchísimas alternativas para ejercerlo, como lo da el comercio, la economía, el desarrollo científico y tecnológicos. Sin embargo, el neorrealismo sostiene que, en vez de analizar las capacidades, deben comprenderse las relaciones de los Estados por lo que al ser estas relaciones multilaterales, el mundo necesariamente debe ser multipolar.

El actual proceso de gestación del orden internacional presenta características de un sistema multipolar que facilita la dispersión del poder y la disminución de los problemas a los que pueda aplicarse, de manera única, el uso de la fuerza. Como resultado de este proceso de dispersión de poder, existe una única superpotencia militar hegemónica, la de Estados Unidos, con una multipolaridad económica, cultural y política.

### 2.3.1 Cooperación internacional

Cuando se habla del origen de la cooperación internacional para el desarrollo implica comprender dos puntos importantes el primero es la parte histórica donde a lo largo de la historia ocurren distintos sucesos que llegan a establecer un contexto para su origen. Y por otro lado, está el enfoque teórico, pues aquí es donde surgen los diferentes pensadores que exponen sus teorías a partir de temas económicos para el desarrollo y la dependencia del mismo.

Gran parte surge a partir de la Segunda Guerra Mundial esto en 1939-1945 donde se llegan a forjar las condiciones que hacen posible el origen de la cooperación internacional y donde nace además la necesidad consciente de llegar a desarrollar herramientas necesarias para fomentar la paz, equilibrio y seguridad internacional, así es como nace la cooperación internacional dentro los diferentes actores mundiales.

Las políticas de ayuda externa y la cooperación internacional para el desarrollo han sido uno de los elementos constitutivos del sistema internacional de posguerra, e incluso su rasgo histórico singular. Antes de 1945 las políticas de ayuda no existían como tales. Su evolución desde ese año responde, en gran medida, a las transformaciones que ha experimentado dicho sistema (Sanahuja, s.p. 2001).

En este sentido, se entiende como una vía de desarrollo de los países en la transformación del crecimiento económico, el aumento del volumen de los bienes y servicios. Todo esto como componente del desarrollo y progreso tecnológico para la industria y la búsqueda de la urbanización con el fin de producir ingresos y bienestar a los Estados que se establecen de tal catástrofe.

Algunos ejemplos de cooperación en el tema de ciberseguridad y/o comercio, establecidas por los Estados Unidos en busca de cooperación y normativas para la aplicación de estrategias de seguridad que permitan un bienestar común.

A través de la Alianza por la Conectividad Digital y la Ciberseguridad*(*Digital Connectivity and CybersecurityPartnership, DCCP), Estados Unidos está brindando formación y desarrollo de capacidades en la región con socios como el U.S. Telecommunications Training Institute y la Comisión Federal de Telecomunicaciones. Esta capacitación y asistencia técnica favorece el crecimiento y la expansión de redes de comunicaciones abiertas, confiables, seguras y con interoperabilidad, alienta la adopción de políticas sobre comercio digital y TIC que posibilitan el crecimiento sostenible a largo plazo y promueve las inversiones del sector privado. (StateDepartment, 2020)

A medida que los integrantes de la comunidad internacional y sus diferentes actores incluyendo la sociedad civil se sumergen en las comunicaciones digitales en busca de

establecer, construir, y ejecutar redes del futuro, Estados Unidos trabaja en la establecer colaboración con sus socios en América Latina y el Caribe para promover el crecimiento digital. Y de esta forma impulsar el desarrollo del potencial regional en temas propios de la era digital que brinden seguridad, privacidad y la inclusión dentro de la conectividad y la ciberseguridad.

El Programa de Desarrollo del Derecho Comercial del Departamento de Comercio reúne a expertos jurídicos para que brinden guías sobre mejores prácticas, conferencias y asistencia técnica bilateral en una variedad de temas relativos a la DCCP, que incluyen las subastas de espectro, la reglamentación de las telecomunicaciones, las contrataciones públicas, las redes de arquitectura abierta y la legislación sobre telecomunicaciones. (StateDepartment, 2020)

Este tipo de programas busca aplicar los conocimientos en una cooperación de carácter técnica para desarrollar las guías necesarias para impulsar la transformación digital y la implementación de las buenas prácticas brindando normativas bilaterales que busquen respaldo legislativo en temas de tecnologías. Así como la debida reglamentación de las mismas en ámbitos de las tecnologías de la información y comunicación

La Iniciativa de USAID relativa a la Promoción de las Visiones Estadounidenses sobre Políticas y Reglamentaciones de TIC (Promoting American Approachesto ICT Policy and Regulation, ProICT) brinda asistencia específica sobre políticas bajo la modalidad de asistencia técnica, expertos a préstamo, desarrollo de capacidades y capacitaciones. A través de la Corporación Financiera de Desarrollo Internacional de EE. UU., el Banco de Exportación e Importación y la Agencia de Comercio y Desarrollo de Estados Unidos, la DCCP ofrece una variedad de herramientas para apoyar el financiamiento de proyectos y brindar garantías de préstamo. (StateDepartment, 2020)

Como se puede ver, todas estas iniciativas implementadas buscan brindar una cooperación tanto financiera, como técnica. Se habla de la unión entre ambos esfuerzos que permiten la participación e integración de todas las áreas de trabajo del Gobierno

estadounidense de indagar y proporcionar una superior conectividad y un ciberespacio con internet abierto, confiable y seguro para la sociedad con un carácter hacia la inclusión digital.

Este tipo de programas busca aplicar los conocimientos en una cooperación de carácter técnico para desarrollar e impulsar la transformación digital brindando de este modo mayor atracción e inversión del sector privado, así como estimular el crecimiento empresarial en todos sus ángulos, de forma que permita impulsar iniciativas como la llamada América crece establecida por los Estados Unidos en busca de que este sector se oriente a invertir capital en temas de energía y otras infraestructura, incluidas las telecomunicaciones, en América Latina y el Caribe.

El Gobierno estadounidense brinda o facilita un amplio espectro de programas de desarrollo de capacidades vinculados con cuestiones cibernéticas, destinados a países socios en el hemisferio occidental. Algunos ejemplos son la formación sobre mejores prácticas en ciberseguridad que imparte el Instituto Nacional de Normas y Tecnología *(*NationalInstitute of Standards and Technology, NIST), asistencia técnica, capacitación e intercambio de información a través de la Agencia de Ciberseguridad y Seguridad de la Infraestructura *(*Cybersecurity and Infrastructure Security Agency, CISA), la colaboración entre fuerzas militares, la capacitación de agentes de la ley para el combate al ciberdelito y esfuerzos conjuntos para promover la seguridad internacional y la estabilidad en el ciberespacio a través de la cooperación bilateral y regional. (U.S Mission Chile, 2020)

La cooperación técnica que ha brindado Estados Unidos ha sido bastante amplia esto con el fin de reforzar temas de seguridad dentro del ciberespacio, ya que se establece que entre mayor intercambios de conocimientos en el ámbito del ciberespacio se vuelve cada vez más baja la probabilidad de vulnerabilidades existentes o que puedan llegar a surgir y presentarse como una amenaza futura.

El Departamento de Estado financia a dos asesores internacionales del Departamento de Justicia sobre hackeo informático y propiedad intelectual *(*International

Computer Hacking and IntellectualPropertyAdvisors, ICHIPS) que trabajan en Sao Paulo, Brasil, y la Ciudad de Panamá, en el país homónimo, para fortalecer la cooperación internacional y brindar capacitación para la aplicación de la ley y la asistencia técnica contra el ciberdelito y actividades conexas de robo de propiedad intelectual. Como ejemplo de esta asistencia, cabe mencionar el taller sobre seguridad y ciberdelincuencia que se llevó a cabo en MontegoBay, Jamaica, en diciembre de 2019. También se dictan cursos sobre ciberdelincuencia a través de la Academia Internacional para el Cumplimiento de la Ley (International LawEnforcementAcademy, ILEA) apoyada por el Departamento de Estado, en San Salvador, El Salvador. Según (U.S Mission Chile, 2020)

El empoderamiento regional en términos importantes como la ciberseguridad establecidos en los ámbitos cruciales como lo es el ciberespacio vuelve menos vulnerables a las regiones que no son tan fuertes en estos temas. Por lo que, la implementación del desarrollo técnico especializado se vuelve un tema fundamental para darle frente a los posibles ataques que se presenten dentro de sus vulnerabilidades.

Por medio del Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos (OEA), Estados Unidos ha brindado apoyo y proporcionado oradores especializados con el fin de incrementar la capacidad técnica y de políticas en la región, ha favorecido el desarrollo y la implementación de estrategias sobre cuestiones cibernéticas a nivel nacional y ha respaldado la implementación regional de medidas que fomenten la confianza con respecto a la cibernética. Estados Unidos financia talleres regionales de capacitación sobre ciberdelitos que dicta el Departamento de Cooperación Jurídica de las Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas (REMJA) de la OEA. Según (StateDepartment, 2020)

Es aquí donde se puede evidenciar la importancia que recae sobre el área tecnológica y que se hace presente con mayor fuerza en el transcurso del tiempo, por lo que en temas de cooperación de todas las índoles tanto financieras, técnicas e incluso bilaterales y multilaterales, se vuelve fundamental para contrarrestar los peligros que se esconden dentro del ciberespacio.

Por esta razón, es común ver no solo la presencia de todos los actores de la comunidad internacional trabajando en conjunto para desarrollar cada una de las áreas que establece las nuevas tecnologías. Dado este motivo vemos la participación de organismos internacionales destacados como por ejemplo de la mano con la cita anterior se refleja la participación de la Organización de Estados Americanos, y así como este hay muchos que se integran en la labor de proporcionar cooperaciones que permitan la armonía en el desarrollo que vivimos en esta era digital.

Un claro ejemplo de cooperación en el tema de ciberseguridad es el proceso que se ha obtenido a partir del Convenio de Budapest, y uno de ellos es América Latina. Según Derechos digitales de América Latina, el convenio de Budapest en Latinoamérica y Perú expresa lo siguiente:

> Este proceso, que en el norte global ha durado décadas, ha sido bastante más corto en otras regiones como América Latina, en donde, luego de la implementación (tardía) de leyes de delitos informáticos o la suscripción del Convenio de Budapest, se ha empezado inmediatamente a trabajar en Planes Nacionales de Ciberseguridad. Muchas veces esto responde no solo a las necesidades apremiantes que produce el crimen globalizado, sino también al hecho de que en muchos casos la organización institucional que soporta el plan se ha tenido que replantear porque la anterior no estaba centralizada, era obsoleta o inexistente. (s.p, 2018).

En este contexto, se logra visualizar que este tratado de Budapest que se llegó a consensuar refleja la preocupación, así como lo que se debía realizar para obtener la protección adecuada a los intereses comunes dentro de los sistemas judiciales, la importancia y urgencia de mecanismos de cooperación internacional, así como dentro del sistema de manejo de información, para resguardar el desarrollo estatal, lo que le permite a los diferentes países participantes e incluso a los que simplemente observan es poder hacer un escáner interno que les permita observar y detectar cómo la idiosincrasia, el pasado

común, y sus propias necesidades les permite avanzar en una mejora continua en la búsqueda de obtener la excelencia en un sistema cada vez más eficiente así como útil.

#### 2.3.1.1 Convenio de Budapest

Hay que hacer una mención especial al Convenio del Consejo de Europa, sobre cibercriminalidad, firmado en Budapest el 23 de noviembre de 2001, el cual tiene como propósito el lograr una mayor cooperación entre los Estados, así como el desarrollo de una legislación armonizada y apropiada para contener, en la mayor medida posible, este tipo de delincuencia.

En lo que respecta a los comportamientos que necesariamente han de ser configurados como ilícitos penales en las correspondientes legislaciones internas, se estructuran en las siguientes categorías:

- Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos informáticos (Tít. 1). En este grupo se deben describir como infracciones penales las siguientes conductas: a) acceso ilícito doloso y sin autorización a sistemas informáticos (art. 2); b) la interceptación dolosa e ilícita, sin autorización, a través de medios técnicos, de datos informáticos, en el destino, origen o en el interior de un sistema informático (art. 3); c) los atentados contra la integridad de los datos, consistente en dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos (art. 4); d) los atentados contra la integridad del sistema, esto es, la obstaculización grave, dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos (art. 5); e) el abuso de equipos e instrumentos técnicos, que comporta la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición de dispositivos principalmente concebidos o adaptados para cometer las infracciones antes referidas; la de una palabra de paso (contraseña), de un código de acceso o de datos similares que permitan acceder a un sistema informático; y la

posesión de alguno de los elementos antes descritos (art. 6)(22).

- Infracciones informáticas (Tít. 2). Entre ellas, según este convenio, deben sancionarse penalmente los siguientes comportamientos:

  a) las falsedades informáticas, que contienen la introducción, alteración, borrado o supresión dolosa y sin autorización, de datos informáticos, generando datos no auténticos (art. 7).

  b) estafa informática, que precisa la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de la introducción, alteración, borrado o supresión de datos informáticos, o de cualquier otra forma de atentado al funcionamiento de un sistema informático, siempre con la intención fraudulenta de obtener un beneficio económico (art. 8) (23).

  C) Infracciones relativas al contenido. Sin embargo, dentro de este apartado únicamente se describen conductas relativas a pornografía infantil (art. 9). D) Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines (art. 10) (24). (González Cussac, pág.101)

El convenio también contiene disposiciones técnicas respecto a la sanción de la complicidad, la tentativa (art. 11), la responsabilidad de las personas jurídicas (art. 12) y las sanciones y medidas a imponer (art. 13).

El convenio de Budapest brinda el primer instrumento normativo en el ámbito de la ciberseguridad, lo cual lo convierte en un paso decisivo hacia la armonización de las legislaciones en materia de ciberseguridad. Ahora bien, tenemos que tener en cuenta que no se debe confundir el término armonización con unificación, pero en cualquier caso constituye el presupuesto necesario para la cooperación internacional y para el avanzar hacia una mayor integración legal y regulatoria en esta área.

Dentro del área regulatoria, es de conocimiento que toda norma internacional, establece los mínimos comunes que los Estados miembros están obligados a incorporar a sus ordenamientos. Sin embargo, se faculta a los Estados para que instaurar procedimientos

o procesos específicos para la investigación de las acciones ilícitas penales antes descritos; además para procesos de delitos informáticos, e incluso recolección de pruebas.

Este convenio pretende armonizar la legislación de los diversos países que lo ratifiquen, no solo en materia de derecho penal sustantivo, sino también de derecho procesal para hacer frente a ese tipo de delincuencia. El Convenio define los delitos informáticos agrupándolos en cuatro grupos:

- Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos. Engloba las conductas de acceso ilícito, interceptación ilícita, interferencia de datos, interferencia de sistemas y el abuso de dispositivos.
- Delitos por su contenido. comprende las conductas que se engloban en los delitos relacionados con la tenencia y distribución de contenidos de pornografía infantil en la Red.
- Delitos relacionados con la informática. Se definen dos tipos penales, la falsificación informática y el fraude informático.
- Delitos relacionados con las infracciones de la propiedad intelectual y de los derechos afines.

En este grupo el Convenio hace una remisión normativa a los tratados y convenios internacionales sobre propiedad intelectual. En un Protocolo adicional al Convenio, de enero de 2003, se incluyeron las conductas de apología del racismo y la xenofobia a través de Internet, como delitos de contenido. (SalomClotet, pág.137)

Este convenio y los sus protocolos adicionales, hicieron eco en las realidades de las problemáticas sociales que se transfieren al entorno cibernético, para hacerle frente a los delitos que se transfieran a este sitio. Conductas que hasta entonces existían en el mundo real, y que pasaron a ser conductas prácticamente exclusivas del mundo virtual, es decir, que entran dentro de la categoría ¨delitos informáticos¨, puesto que es el único medio que existe dentro del ciberespacio el ámbito tecnológico.

La importancia del Convenio no está tanto en el número de países que lo han firmado y ratificado sino en que se ha constituido en el referente internacional a la hora de hablar de la delincuencia informática, y de aproximarnos a una legislación global. Esto provoca que

gran número de países se inspiran en el convenio de Budapest para la creación y el fomento de leyes especializadas en el tema de ciberseguridad.

Es importante indicar que para el desarrollo de esta investigación, se procederá a determinar las regulaciones de las exportaciones en materia de seguridad nacional, y además, se analizará el impacto comercial de las estrategias de ciberseguridad estadounidense en el mercado global esto con el fin de tener una visión panorámica del acontecer actual.

# CAPÍTULO III. MARCO METODOLÓGICO

En el marco metodológico es donde se toman las decisiones operativas de la investigación y donde se exponen las herramientas utilizadas para su realización como la aplicación de los instrumentos, la recolección de los datos y su interpretación. Por esta razón, la descripción clara de los mecanismos utilizados es fundamental para el desarrollo del tema a investigar y, por consiguiente, logran reforzar el trabajo investigativo.

La información recolectada mediante los diferentes procesos da una mejor interpretación de los resultados de la investigación, estableciendo una relación y una comparación de todos los puntos para una mejor exploración política, comercial, socioeconómica etc., con la finalidad de evaluar y extraer datos de importancia sobre el tema de interés para llegar conclusiones verdaderas sobre la situación actual, estudiando cada fenómeno por el cual no se ha llegado a ninguna solución.

El estudio de las estrategias de ciberseguridad se fundamenta en la consulta de fuentes primarias y secundarias confiables y la vinculación de este problema en la exportación comercial estadounidense se centra en el escudriño de fuentes secundarias que permitirán el análisis desde una óptica mucho más amplia.

Los métodos seleccionados corresponden al enfoque cualitativo y al diseño descriptivo con el fin de analizar la problemática del crimen cibernético desde una perspectiva integral, en donde su expansión por elementos de la esfera estatal surge a partir de la complicidad de sectores que facilitan su propagación en actividades como la exportación.

## 3.1. Enfoque de la investigación

Mediante el enfoque cualitativo, descriptivo para un mayor alcance. Las fuentes primarias buscarán una conexión del tema a investigar, el análisis de las estrategias de ciberseguridad implementadas en las exportaciones comerciales ayudarán a entender las

implicaciones del mismo tomando en cuenta desde aspectos históricos en los últimos años hasta lo que actualmente se desenvuelve en este tema.

De acuerdo con Hernández, Fernández, & Baptista (2014), a lo largo de la historia de la ciencia han surgido diversas corrientes de pensamiento y diversos marcos interpretativos, como el realismo y el constructivismo, que han abierto diferentes rutas en la búsqueda del conocimiento; sin embargo, y debido a las diferentes premisas que las sustentan, desde el siglo pasado tales corrientes se "polarizaron" en dos aproximaciones principales de la investigación: el enfoque cuantitativo y el enfoque cualitativo.

En el enfoque cualitativo hay una variedad de concepciones o marcos de interpretación, que guardan un común denominador: todo individuo, grupo o sistema social tiene una manera única de ver el mundo y entender situaciones y eventos, la cual se construye por el inconsciente, lo transmitido por otros y por la experiencia, y mediante la investigación, debemos tratar de comprenderla en su contexto, es por esta razón que las investigaciones cualitativas se basan más en una lógica y proceso inductivo. Van de lo particular a lo general (Hernández, Fernández, Baptista, 2014).

Por otra parte, las variables dan diferentes conceptos de los hechos más importantes durante el proceso histórico, así como las consecuencias de cada medida estratégica adoptada por los Estados, enlazar cada problema con los objetivos y llegar a conclusiones positivas o negativas, así como establecer un acercamiento y las posibles direcciones de las políticas hechas por los diferentes Gobiernos. Se analizará cada una de forma específica para permitir un mejor enfoque con argumentos, sosteniendo las estrategias de ciberseguridad como tema principal durante la evolución comercial y tecnológica a lo largo de la historia.

La característica más distintiva del enfoque cualitativo es la utilización de un método de recolección de datos no estandarizados ni predeterminados. Por lo tanto, el enfoque a utilizar en la presente investigación es el cualitativo, pues se pretende examinar y describir el problema que generan el crimen dentro del ciberespacio en su propio contexto para luego generar una perspectiva teórica analizando la coyuntura comercial, política y económica que este problema por defecto deriva y concatenarlo con las implicaciones de su trascendencia en el sector exportador, las estrategias utilizadas y en la imagen del país.

Con los instrumentos se analiza las respuestas de cada individuo y las medidas adoptadas por los diferentes actores, temas y conceptos como: ciberseguridad, comercio, exportaciones, estrategias, cooperación internacional e implicaciones que esto trae para el sistema internacional; sobre todo las consecuencias en las relaciones bilaterales de estos Estados. Todo esto ayuda a entrelazar cada temática y la importancia que tiene para el tema, pues va permitir hacer una serie de preguntas durante el proceso para reflexionar sobre algunos temas, dada la complejidad de la investigación. Con las informaciones recolectadas con estos métodos se busca profundizar y alcanzar el resultado deseado.

### 3.2. Diseño de la investigación

El diseño de la investigación seleccionado para este trabajo de investigación corresponde al descriptivo, pues pretende esclarecer y describir las propiedades destacadas del objeto investigado en su entorno. Con este método se analiza tanto las estrategias de ciberseguridad implementadas, como el principal punto de discusión dentro de las exportaciones comerciales para comprender mejor la investigación, por lo que es importante relacionar estas dos partes con el fin entender esos puntos de vista y llegar a conclusiones sobre las causas y efectos de este tema. Se investigará lo importante que se ha vuelto este tema para los Estados, para resguardar su seguridad y recursos estratégicos en el Sistema Internacional.

Hernández *et al* (2014), caracterizan al diseño descriptivo por buscar especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Es decir, únicamente pretenden medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren.

El diseño descriptivo permitirá tener una visión más amplia para entender mejor todo el tema que se desarrolla dentro de esta investigación. Además permite indagar más a fondo el punto de vista de las personas encuestadas sobre el fenómeno en estudio, ayudando así a entender y a llegar a las posibles conclusiones y recomendaciones que se desarrollen.

El diseño descriptivo busca descubrir algunas características fundamentales. Hernández, Fernández, Baptista (2014, p.89), "consideran al fenómeno estudiado y sus componentes" agregan miden conceptos y Definen variables. Los autores indican que se busca considerar distintos tipos de fenómenos abarcando los puntos más importantes en el objeto de estudio, además se miden diferentes conceptos en torno a las variables para buscar una mejor interpretación a la hora de buscar información donde las variables y sus componentes pueden analizar distintos conceptos.

Con la recopilación de información y las características particulares se determinará los tipos de investigación que se utilizarán para una mejor comprensión de la problemática actual, mediante la realización de preguntas abiertas, analizando cada una de las respuestas para una mejor percepción del objeto de estudio y así entender las actitudes u opiniones de los encuestados con respecto al tema de ciberseguridad. Además, se analiza la información del fenómeno de interés extrayendo datos de importancia que permita tener un análisis más efectivo y exitoso.

### 3.3. Fuentes de información

En este apartado se selecciona la información y los elementos de utilidad que conducen a la resolución del problema de investigación. Para esto, es necesario realizar una revisión literaria en donde se logre hacer una discriminación prudente de la información útil y la que no lo es. Este proceso es sumamente importante puesto que los datos seleccionados deben servir para alcanzar los objetivos propuestos (Barrantes, 2013).

Al realizar este ejercicio, se determinaron las fuentes primarias y las fuentes secundarias recopiladas para la elaboración de este trabajo, lo cual ayuda a establecer y generar nuevas visiones para desarrollar dentro del proceso de la investigación. Es por esto que son tan importantes ya que hacen una retroalimentación del conocimiento, además crean nuevas perspectivas a la hora del desarrollo del tema como tal.

Las fuentes sirven para analizar cada uno de los acontecimientos más importantes y mejorar los resultados en la investigación. La entrevista es la principal fuente primaria pues permite analizar los diferentes puntos de vista de cada persona, su conocimiento sobre el tema, si existe diferencia con el resto de los entrevistados. Las preguntas serán abiertas para

conocer los diferentes resultados y si existen propuestas para mejorar las relaciones bilaterales. La complejidad nos hace indagar y recolectar información para conocer la evolución en las relaciones económicas dentro del sistema internacional.

Gallego (2009) indica que esta fuente busca identificar el origen de la información a lo largo de la historia y establece su concepción sobre las fuentes al decir que. Las fuentes de información son toda huella o vestigio, testimonio y conocimiento legado por el discurrir de los hombres y mujeres a lo largo de la historia. De ello se desprende que la fuente de información es todo lo que contiene información para ser transmitida o comunicada y que permite identificarse con el origen de la información.

Con las fuentes se busca una mejor interpretación y exploración de los diferentes procesos con mayor profundidad para llegar a comprender cada situación y evaluar cada aspecto de interés mejorando el análisis de la información. A partir de tales aspectos con las fuentes de información obtenidas se relaciona un conjunto de puntos significativos sobre las estrategias de ciberseguridad aplicadas en las exportaciones comerciales. Esto permite llevar un orden desarrollando la estructura de la investigación, explicando cada tema con mayor alcance indagando en las fuentes primarias y secundarias para una mayor recolección de datos resaltando todos aquellos puntos valiosos para un resultado efectivo.

### 3.3.1. Fuentes primarias.

Las fuentes primarias son a donde acude el investigador cuando conoce su localización de estudio, son las primeras fuentes de conocimiento donde se va por primera vez para desarrollar el tema de investigación ya que da un sustento clave para empezar y para continuar con el progreso del tema como tal. Estas fuentes son la base de referencias y datos de la información, por lo que se tomará como la principal fuente primaria las entrevistas con diferentes especialistas en los temas a desarrollar.

Hernández *et al* (2014) mencionan que las fuentes primarias o directas constituyen el objeto de la investigación bibliográfica y proporcionan datos de primera mano. En esta investigación, se determinan fuentes primarias como: libros, tesis, informes de organizaciones gubernamentales y testimonios de profesionales en las diferentes áreas a tratar y que proporcionan una visión integral ante el problema planteado.

El perfil de los profesionales a investigar es muy diverso debido a las variables que se pretenden analizar dentro de estas variables destaca: el papel logístico de Estados Unidos y su ubicación estratégica comercial, esto implica un análisis profundo de informes oficiales de instituciones del Estado. Otra variable consiste en los actores gubernamentales que cumplen una tarea importante en la fiscalización, quienes intervienen en el proceso de la exportación, el perfil del entrevistado debe conocer los procedimientos de la exportación y estar relacionado con los mecanismos que controlan las exportaciones.

El papel estratégico de Estados Unidos en el continente americano corresponde a otra variable importante a considerar, el entrevistado debe contar un amplio conocimiento en geopolítica para aportar consideraciones valiosas a esta investigación y que permita analizar la posición geográfica como una estrategia que implica este país dentro del mercado. El último objetivo analiza dos variables importantes, los efectos negativos del cibercrimen dentro del comercio y en la imagen del país.

La entrevista a profundidad permite revelar las repercusiones, para ello es vital la opinión y las consideraciones referentes al tema de un experto en el sector informático y ciberseguridad. El enfoque cualitativo dará un mejor desarrollo del tema, evaluando cada uno de los aspectos a estudiar. La entrevista es una forma de fortalecer la investigación que junto con la observación llevará a los resultados deseados, con un total de cinco preguntas a cada persona.

Los entrevistados conocen sobre el tema y eso dará una mejor visión y conocimiento sobre el tema, y cómo ha transcurrido, evolucionado y desarrollado en los últimos años, así como todas las opiniones de cada persona, entendiendo esto como un problema real que cada día es más complicado para la comunidad internacional. La complejidad con que se tratan los problemas del ciberespacio dificulta los planes o estrategias a utilizar para las efectivas regulaciones.

Con las complejidades de las respuestas, las posibles percepciones serán amplias, a partir de tales aspectos la investigación se enfoca en el análisis de cada respuesta estableciendo una relación con los diferentes problemas. El resultado final dará un mayor acercamiento con los objetivos a explicar reuniendo la información necesaria para una

mayor aclaración sobre la importancia que tiene el ciberespacio y con ello la importancia de la ciberseguridad, lo que será de gran ayuda para las investigaciones futuras.

### 3.3.2. Fuentes secundarias.

Las fuentes secundarias dan una mejor descripción de lo que se necesita saber. La exploración de estas fuentes sirve para captar información que se considera relevante en el desarrollo del tema de estudio. El resultado es que la investigación da una mayor recopilación de datos que vienen a profundizar el tema, aportando mejores resultados al buscar explicar los diferentes hechos que han marcado la historia en el marco de la ciberseguridad de la mano con el comercio.

Las fuentes secundarias corresponden a información previa que contiene datos relacionados con el problema a investigar. De acuerdo con Del Cid, Méndez, & Sandoval (2011), el consultar datos secundarios aporta una referencia de las dimensiones de lo que se desea estudiar y son muy útiles para contextualizar el tema.

Las fuentes secundarias básicamente interpretan y analizan las fuentes primarias las cuales se retroalimenta y son utilizadas dentro de la investigación. Además, permite dar sustento a la actividad de la investigación, por lo que en esta investigación se utilizarán fuentes secundarias como: artículos de revista, críticas y comentarios.

Este proceso, que en el norte global ha durado décadas, ha sido bastante más corto en otras regiones como América Latina, en donde, luego de la implementación (tardía) de leyes de delitos informáticos o la suscripción del Convenio de Budapest, se ha empezado inmediatamente a trabajar en Planes Nacionales de Ciberseguridad. Muchas veces esto responde no solo a las necesidades apremiantes que produce el crimen globalizado, sino también al hecho de que en muchos casos la organización institucional que soporta el plan se ha tenido que replantear porque la anterior no estaba centralizada, era obsoleta o inexistente Fueron creadas para facilitar el proceso de consulta, agilizando el acceso un mayor número de fuentes en un menor tiempo” (Hiperderecho, pf.9, 2018)

Las fuentes secundarias dan un aporte extra para entender sobre los procesos históricos y las repercusiones de las relaciones bilaterales dentro del sistema internacional. Los documentos fueron consultados con el fin obtener información para un mejor análisis, enfocándose en aquellos documentos de interés sobre el trabajo de investigación; de esta forma se entiende mejor cada objeto de estudio mediante la unión de todo se llega determinar la importancia estratégica, política, económica, comercial y de cooperación que tienen las estrategias de ciberseguridad y las consecuencias internacionales a causa de posibles ataques. Cada proceso de recolección ayuda a explicar mejor el tema de estudio en cada una de sus apartados.

### 3.4. Variables

Barrantes (2013), define variables como un hecho, característica o fenómeno que varía y toma diferentes valores. Estos valores van fielmente relacionados con los objetivos de la investigación y sirven como guía para la recopilación de información y su desarrollo. A su vez, Del Cid *et al* (2011), agregan que las variables son todos aquellos elementos centrales y que en torno a ellos, girará toda la investigación.

Según los autores anteriores dentro de las variables existen una serie de factores internos y externos que pueden afectar la medición, las características los hechos e intereses porque cada una dependerá de los objetos de análisis de la investigación, permitiendo analizar cada punto, en el siguiente cuadro se explica brevemente algunos como: el poder económico, comercial, y políticos países para resolver los posibles ciberataques. Las recomendaciones dictadas por organismos y especialistas en el tema a pesar de que estas aún siguen siendo un tema sumamente nuevo y complicado.

Según Hernández, et al. (2014, pág.105), “Es una propiedad que puede fluctuar y cuya variación es susceptible de medirse u observarse” los autores indican que en las variables existe un sin número de acontecimientos que pueden cambiar, estudiar los diferentes hechos que llevan a las variables a medirse u observarse. En estas propiedades se buscan analizar los cambios en el objeto de estudio, para realizar una investigación más exhaustiva tomando en cuenta cada una de las variables.

Por esta razón, se explican las variables y definiciones de la investigación relacionándolas con los objetivos que se desarrollan con el fin de abarcar las implicaciones de lo que sucede con las exportaciones comerciales y las estrategias de ciberseguridadadaptadas por los Estados, de modo que se podrá hacer un conteo de los sucesos que han cambiado a lo largo de la historia.

## VARIABLES DE LA INVESTIGACIÓN

| Objetivo | Variable | Definición Conceptual | Definición Operacional | Definición Instrumental |
|---|---|---|---|---|
| 1. Describir el concepto y la relevancia de los elementos históricos de ciberseguridad. | Ciberseguridad | De acuerdo con los expertos de InformationSystemsAudit and Control Association (ISACA), la ciberseguridad se define como "una capa de protección para los archivos de información". La ciberseguridad es el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos. | Estrategias de ciberseguridad aplicadas al comercio | Línea del tiempo. |
| | | | | |
| 2. Examinar las propuestas de cooperación internacional en temas de ciberseguridad | Principales acuerdos, posturas o tratados | **Cooperación en materia especial**: "El espacio ultraterrestre, junto con el espacio marítimo, el espacio aéreo y el ciberespacio, constituye un dominio clave de los bienes comunes mundiales: nadie lo posee exclusivamente, pero todos tienen una participación en él" (Obama, 2010).<br><br>**Cooperación en materia de seguridad cibernética: B**usca disminuir el espionaje económico entre los Estados, especialmente el robo de propiedad intelectual y secretos comerciales. | Respuesta Internacional sobre la ciberseguridad en materia de seguridad nacional | Entrevista profunda |
| 3. Determinar las regulaciones de las exportaciones en materia de seguridad nacional. | Estrategia Nacional para Asegurar el Ciberespacio 2003.<br><br>Estrategia Nacional de Seguridad 2010 | **Estrategia Nacional para Asegurar el Ciberespacio-2003**:responde a la necesidad de proteger la infraestructura de la información y los activos que la soportan, de la amenaza constante.<br><br>**Estrategia Nacional de Seguridad 2010**: Fomentar la conciencia sobre seguridad cibernética y la alfabetización digital es una prioridad en las dos estrategias, así como el trabajo conjunto del sector público y privado. | Garantía de la seguridad nacional mediante las restricciones comerciales vinculados a medios electrónicos | Entrevista profunda. |

| | | | | |
|---|---|---|---|---|
| 4. Analizar el impacto comercial de las estrategias de ciberseguridadestado unidense en el mercado global. | Papel estratégico de EE.UU. | Estados Unidos ha sido uno de los países más activos en el desarrollo e implementación de estrategias en el tema de seguridad cibernética. | Relacionar las medidas de ciberseguridad aplicadas por EEUU para asegurar integridad nacional dentro del comercio mundial | Matriz Documental. |
| | Mercado Global | Impacto de la ciberseguridad en el mercado mundial | | |

### 3.5. Instrumentos de la investigación

Los instrumentos de la investigación consisten en los recursos diseñados para el proceso de recolección de la información. Según Hernández, Fernández y Baptista (2014), un instrumento de medición adecuado es aquel que registra datos observables que representan verdaderamente a los conceptos o variables que el investigador tiene en mente. Los instrumentos designados para la recolección de los datos en esta investigación son la matriz documental y la entrevista a profundidad.

#### 3.5.1 Instrumento Línea del tiempo.

Objetivo: La selección de este instrumento permite entender la evolución y trascendencia de los elementos históricos de ciberseguridad. Se llega a desarrollar los hechos históricos que marcaron un antes y un después de cada acontecimiento que llegó a marcar la historia de la humanidad como las revoluciones industriales, las cuales fueron responsables de dar un gran paso a llegada de nuevas tecnologías, globalización, y acontecimientos sociales como el 09-11 que llegó a dar un giro relevante dentro del comportamiento social.

#### 3.5.2 Instrumento Entrevista profunda.

Objetivo: La entrevista profunda es seleccionada para recabar información precisa sobre la propuesta de las principales posturas internacionales en temas de ciberseguridad y en materia de seguridad nacional.

Profesión: Profesional en el área de cooperación internacional.

1. ¿Cuáles han sido los principales acuerdos sobre la ciberseguridad?
2. ¿Cuáles son los efectos de la aplicación de estas posturas?
3. ¿Cuáles elementos de ciberseguridad se han desarrollado para fomentar la cooperación internacional?
4. ¿En qué medida no atender la ciberseguridad adecuadamente tiene riesgo para la evolución económica de un país y su desarrollo industrial?
5. ¿Cuáles factores han posicionado a los Estados Unidos como principal estratega en temas de seguridad aplicada?

### 3.5.3 Instrumento de Entrevista profunda.

Objetivo: Esta entrevista permite conocer las regulaciones en materia de exportaciones y de este modo entender situaciones de seguridad nacional.

Profesión: Profesional en el área de comercio.

1. ¿Cuáles son los efectos de la aplicación de estas estrategias que repercuten en el comercio?
2. ¿Cuáles son las principales barreras para su implantación?
3. ¿Qué tendencias tecnológicas están surgiendo en torno a la ciberseguridad industrial?
4. ¿Qué sectores industriales se están viendo más afectados por las amenazas de ciberseguridad?
5. ¿Qué tendencias tecnológicas están surgiendo en torno a la ciberseguridad industrial?
6. ¿Qué riesgos no tradicionales pueden aparecer en sectores críticos como el comercio para un país?

### 3.5.4 Instrumento de Matriz Documental.

Objetivo: La aplicación de este instrumento permite comprender aspectos fundamentales en el proceso comercial en las estrategias de ciberseguridad estadounidense en el mercado global.

| Actores involucrados en el impacto comercial estadounidense | Área de trabajo |
|---|---|
| **Papel estratégico de EE.UU.** | |
| **Mercado Global:** | |
| **Seguridad Nacional:** | |

Elaboración propia.

### 3.6. Proceso para la recolección y análisis de datos

La recolección de los datos corresponde a la base de la investigación, pues la adecuada compilación de la información permite lograr alcanzar los objetivos trazados. Este proceso requiere una previa distinción entre los datos pertinentes y útiles y los que no lo son, ya que los datos utilizados deben servir para probar, rectificar y alcanzar los objetivos.

# CAPÍTULO IV. ANÁLISIS DE RESULTADOS

Este capítulo explica diferentes puntos de vista sobre la matriz documental y entrevistas, desarrollando y analizando cada pregunta sobre los diferentes acontecimientos históricos y así poder entender los hechos con mayor relevancia sobre la propuesta discutida y aceptada en las conversaciones, cómo han tenido aciertos y desaciertos obteniendo así los diferentes resultados entre las naciones que han implementado diferentes formas estratégicas de ciberseguridad.

Con la matriz documental se plantea analizar las aplicaciones fundamentales en el proceso comercial de las estrategias de ciberseguridad estadounidenses en el mercado global al relacionarla con la seguridad nacional. Convenios como el de Budapest se hacen presentes para establecer las primeras bases de la cooperación internacional en materia de ciberseguridad y seguridad nacional.

## 4.1 Regulaciones de las exportaciones en materia de seguridad nacional estadounidense.

Las Estrategias de Seguridad Nacional (ESN) propiamente de los Estados, básicamente son documentos del área administrativa del país desarrollador, en este caso Estados Unidos, en los cuales se abordan temas de política exterior, defensa nacional, las relaciones comerciales, la economía y la política. Por lo que, al realizarse estos documentos se llega a plasmar en ellos los objetivos primordiales que se pretenden alcanzar, estableciendo métodos de trabajos que busquen la eficacia, y el desarrollo de aspectos importantes que buscan contribuir a la seguridad nacional.

Para el mandato del señor ex presidente Donald Trump, se despertó gran interés por parte de los ciudadanos en conocer las estrategias de seguridad nacional que se iban a

desarrollar para ese mandato en especial. Cuando se presentaron estas estrategias fue de gran sorpresa para la sociedad, ya que, como dato curioso fue una de las estrategias más largas de la historia en Estados Unidos, y otra característica que presentaba es que se logró publicar antes de cumplir el año de mandato de la Administración

Un breve apartado en las primeras páginas de la Estrategia, sobre este "mundo competitivo" –en el que no se menciona a los aliados como compañeros en esta competición– se convierte así en el hilo conductor del documento. Un mundo en el que China y Rusia desafían el poder de EEUU y obligan a repensar las políticas de las últimas décadas, basadas en la asunción de que la colaboración con los rivales y su inclusión en las instituciones internacionales y el comercio global les han convertido erróneamente en supuestos países fiables. Según (ESN, pág.3, 2018).

En el desarrollo de las estrategias de seguridad nacional de la administración del señor expresidente Trump, se puede observar como las orienta hacia la competitividad por perseguir sus propios intereses, principalmente haciendo énfasis en el comercio global. Por otra parte, deja a la vista el que el país tiene una ventaja inigualable en áreas de gran importancia, principalmente en los ámbitos tradicionales como el militar, político, pero además hace hincapié en las ventajas en el ámbito económico y tecnológico.

Pero la competición no siempre significa hostilidad ni lleva inevitablemente al conflicto. Se argumenta que si se compite bien, es decir, con fortaleza y confianza, se evitará el conflicto y se promocionará la paz. Y dicha fortaleza se conseguirá con la protección de cuatro pilares o grupos de interés nacional: (1) proteger el territorio y la forma de vida de los estadounidenses; (2) favorecer la prosperidad del país; (3) preservar la paz mediante la fuerza; y (4) hacer avanzar la influencia estadounidense en el mundo. Según (García, pág.6, 2018).

Estados Unidos busca mediante estas estrategias mantener su consolidación como potencia mundial dentro de un mundo cada vez más competitivo, donde la dinámica de la misma ha evolucionado a escenarios cada vez más escurridizos para su dominio y con actores cada vez más consolidados y participativos. Estos cuatro pilares están ligados estrechamente entre la relación causa y efecto, por lo que, Estados Unidos busca utilizar las

herramientas necesarias según su visión para asegurarse de mantener su posicionamiento y liderazgo.

Se parte principalmente de la convicción de que para tener una América fuerte se tiene que comenzar por tener una fortaleza interna. Solo con una economía sólida, se puede pensar en preservar la paz mediante la fuerza y hacer avanzar la influencia estadounidense en el mundo, ofreciendo una perspectiva "basada en el realismo y guiada por los resultados y no por la ideología". (ESN, pág.17, 2018).

Estas estrategias estadounidenses plantean una visión de un orden global basado en reglas multilateralismo, siendo esto un elemento clave para el desarrollo nacional. Se tiene en cuenta que una de las amenazas se califica en términos de competencia económica, junto con la existencia de otras amenazas transnacionales como el terrorismo, el retorno a la competición militar, la importancia del dominio del espacio y el ciberespacio.

Por esta razón, esta administración deja ver como se seguirá defendiendo el actual orden de seguridad esto cuando se habla de grandes competidores y el papel de Estados Unidos en la seguridad global. Aunque estas estrategias de seguridad nacional reconoce los beneficios del mundo interconectado, condena a los actores estatales y no estatales que busquen sacar ventaja dentro del ciberespacio para realizar actos de ilegalidad en contra de Estados Unidos violentando sus intereses económicos, comerciales, políticos e incluso de seguridad.

El panorama económico que ofrece la Estrategia hace, por tanto, necesario "rejuvenecer" la economía y hacerla más competitiva. El énfasis que hizo en su momento Donald Trump durante las primarias y la campaña electoral en "hacer América grande otra vez" estaba entonces relacionado precisamente con hacer un país más competitivo, afirma Steinberg, (s.p, 2018)

Estados Unidos busca de este modo que se resalten los avances tecnológicos, y las reducciones de las barreras regulatorias, fomentando así el impulso de reformas fiscales para la mejora continua de la infraestructura digital y que busca además la reducción de las deudas públicas disminuyendo así el gasto federal.

Todo esto, con una reducción del impuesto sobre sociedades del 35% al 21% con la que se pretende atraer a multinacionales y grandes empresas extranjeras. Al mismo tiempo, dicha reducción debe suponer un incentivo para que las grandes empresas estadounidenses repatrien los beneficios obtenidos en el extranjero –IBM y Apple ya han anunciado la repatriación de los capitales generados fuera de EEUU– y evitar que desvían su actividad al exterior, ya que se endurecerán las reglas relacionadas con los pagos a subsidiarias extranjeras. García, (pág.11, 2018)

Lo dicho anteriormente refleja el interés de los Estados Unidos por atraer y aumentar las actividades económicas, buscando el incentivo en el crecimiento de las pequeñas empresas para su debido desarrollo, además de las inversiones en temas de fabricación que fomenten los productos nacionales para su consumo y exportación. Por lo que se ha procedido a la mejora e incluir un presupuesto para infraestructura, transporte, y el área de las comunicaciones trabajando de la mano con asociaciones público-privadas para incentivar programas y proyectos de obra pública.

De cara al exterior, para mejorar la prosperidad económica del país, EE.UU buscará relaciones económicas bilaterales justas y recíprocas para hacer frente a los desequilibrios comerciales, al tiempo que se subraya la oposición de Washington a los bloques comerciales. Por lo que, según Daniel R. Coats, en su comparecencia ante el Comité de Inteligencia del Senado el pasado febrero: "las incertidumbres entre los aliados y socios de EEUU sobre la voluntad y la capacidad de EEUU de mantener sus compromisos internacionales puede llevarles a considerar la reorientación de sus políticas, en particular las comerciales, lejos de EEUU". (The White House, 2018)

Para la administración, la competencia desigual ha detraído recursos del país que debilitaban su economía, y por esta razón la nuevas estrategias buscaban el fortalecimiento interno en esta área que equilibren el daño económico con los beneficios obtenidos. En un mundo hipercompetitivo en el que nos desenvolvemos diariamente, se busca enfatizar en la ejecución del comercio justo, y que planteen estrategias de reducción del déficit en el ámbito comercial.

Según las estadísticas que recopila la *US NationalScienceFoundation*, EE.UU sigue siendo el líder global en ciencia y tecnología, pero el mundo está cambiando y ante el

crecimiento de otros países la cuota relativa de EE.UU se está reduciendo. En I+D, EEUU lideró el gasto mundial en 2015 con 496.000 millones de dólares (el 26% del total mundial), mientras que China ocupó un segundo lugar decisivo, con un 21% (408.000 millones de dólares). (NationalScienceBoard, s.p, 2018)

Estados Unidos busca preservar el liderazgo en el ámbito tecnológico como: la investigación, innovación tecnológica, las nuevas tecnologías de la información y comunicación, además de las emergentes en temas de nanotecnología, inteligencia artificial, robótica. Mientras que a la misma vez, trabaja en temas de ciberseguridad, regulaciones en temas como propiedad intelectual, todo esto en busca de mantener una protección en la que se resguarden de posibles competidores que ejecuten comercio injusto, que busquen la competitividad ilícita o el robo de la información.

Según la propia NationalScienceFoundation, si la actual tendencia continúa, China sobrepasará a EE.UU en gastos de I+D a finales de este año.14 EE.UU también es el mayor productor de manufactura de alta tecnología (con un 31% de participación global). Esto incluye la producción aeroespacial, semiconductores, ordenadores, productos farmacéuticos e instrumentos de medición y control. China ocupa el segundo lugar, con un 24%, más que duplicando su participación en la última década. Por primera vez, China ha sobrepasado a EE.UU en el número total de publicaciones científicas, con 426.000 estudios frente a los 409.000 de EE.UU. Según (NationalScienceFoundation, s.p, 2018)

Con el auge de las potencias emergentes surge la inquietud de que Estados Unidos ha ido perdiendo la ventaja de líder en términos de ciencia, e innovación tecnológica. Por esta razón es que las Estrategias de seguridad nacional se enfocan también en el ámbito comercial buscando así el desarrollo económico del país, las normativas de seguridad informática se vuelve esencial principalmente cuando se tiene un precedente en temas de ciberataques.

Uno de los primeros precedentes se da en el 2013 donde el señor expresidente Barack Obama le expone al líder chino, Xi Jinping sobre algunos casos de robos de tecnología industrial, por parte de oriente, por lo que se llegó al acuerdo de que China no apoyaría los robos tecnológicos. A consecuencia de antecedentes como estos se crea la

como prevención y respaldo nuevas tendencias en directrices como las estrategias de seguridad nacional.

La Base de Innovación de la Seguridad Nacional (*National Security Innovation Base, NSIB*), que hace referencia a la "red americana de conocimiento, capacidades, y personas –incluidos la academia, los laboratorios nacionales y el sector privado– que transforman ideas en innovaciones, descubrimientos en exitosos productos comerciales y compañías, y protege y mejora el estilo de vida americano" (NSIB,p. 21, 2018).

En consecuencia esta base o red debe ser protegida, ya que, con el antecedente anteriormente mencionado aunque se llegó a ¨acuerdo¨ los intentos de robo, estos desarrollados en temas de robo de propiedad la intelectual en Estados Unidos siguen siendo una constante. Por tanto, además de ser parte de una violación comercial también hace que se vuelta un tema de seguridad nacional.

El Comité de Inversiones Extranjera (CFIUS, en sus siglas en inglés) es quien protege la propiedad intelectual en EEUU, quien inspecciona las inversiones externas, la creciente preocupación por la propiedad intelectual puede someter a inspecciones a nuevas industrias y tipos de transacciones que puedan afectar a la seguridad nacional. Trump bloqueó la compra de una empresa de semiconductores a un comprador chino el pasado mes de septiembre, la Casa Blanca citó "la potencial transferencia de propiedad intelectual al comprador extranjero" como la principal razón de la decisión. (Trump, s.p, 2018)

El robo de tecnologías e incluso los temas de ciberataques aunque Estados Unidos recibe gran cantidad de estos robos no significa que sea exclusivo ante estas tendencias de robos. Sino que es una red a nivel globalizada donde todas las naciones e incluso actores de la comunidad internacional se vuelven blanco de estas situaciones. La necesidad de fortalecimiento de las estrategias de seguridad nacional y las normativas en términos de ciberseguridad se vuelve fundamentales para el resguardo y la prevención.

Para la administración de Barack Obama la producción de petróleo se incrementó más de un 70% desde que Barack Obama llegó a la Casa Blanca y el gas natural más de un 30%. En términos de comercio energético, la prohibición de exportaciones de petróleo se

levantó en 2015 y la primera exportación de gas licuado ocurrió en 2016. (García, pág. 14, 2016)

Estados Unidos busca abrazar el dominio energético, por lo que se establece en las estrategias de seguridad el objetivo de posicionarse tanto en el ámbito productivo como en el de consumo e innovación, esto con el objetivo de estimular su economía interna, y de ese modo establecer independencia energética por lo que se le adjunta a la agenda el deterioro en temas de seguridad económica y energética.

Bob Gates, aseguraba que era necesario entre un 3% y un 5% de crecimiento real anual sólo para mantener la estructura de defensa, teniendo en cuenta que el incremento de los costes de las operaciones y del personal solía ser mayor que la inflación. Si ese crecimiento real no se lograba, inevitablemente debía haber un recorte de los programas. Con la nueva Administración, todo apunta hacia un crecimiento en los gastos de defensa entorno al 3% pero incluida la inflación, por lo que el incremento real se quedaría alrededor del 2%. Según (García, pág.18, 2018)

Al presentarse un presupuesto tan limitado, se debe elegir dónde se implementará la inyección de este capital, por lo que se optan por implementarlo dentro de la capacidades el cual consta en la inversión de la preparación para la disponibilidad de incrementar en temas de ciber capacidades y guerra electrónica, además de la preparación de los especialistas.

La presentación de la Estrategia de Defensa Nacional publicada poco después de la ESN, el secretario Mattis hizo más énfasis en el desarrollo de nuevas capacidadesy disposición inmediata de las fuerzas, es decir, que probablemente se invertirá en innovación, modernización y adquisiciones más que en priorizar aumentar el tamaño de la fuerza. Algunos de los planes de modernización e innovaciones como: el B-21, la Inteligencia Artificial y la robótica, nuevos vehículos no tripulados, sistemas espaciales y sistemas electrónicos contra ciberataques. Según (US Department of Defense, 2018)

En la actualidad la carrera del espacio, el ciberespacio y de forma más amplia la ciberseguridad, también se posiciona como un elemento clave para el establecimiento de estrategias de seguridad nacional, principalmente ahora que la tecnología forma parte importante del desarrollo social. Todavía no existe un dominio único dentro del

ciberespacio, sin embargo, el uso de herramientas permite que los diferentes actores internacionales participen en la disputa por el dominio de este terreno.

Dentro del primer pilar hay también un apartado propio sobre cómo "mantener América segura en la era ciber" El segundo pilar de la Estrategia recoge la predecible lucha contra el robo de la propiedad intelectual concepto de la "Base de Innovación de la Seguridad Nacional" antes mencionado y donde se califica las acciones cyber-enabledeconomicwarfare.Es un lenguaje más asertivo que el utilizado en estrategias anteriores aunque no hay ningún principio sobre cómo prevalecer en este tipo de guerra. Según (García, pág.22, 2018)

La ciberseguridad, a nivel mundial se ha posicionado como un lugar destacado. Por lo que se busca ser implementado en todas las estrategias de seguridad dentro de todos los actores participantes de la comunidad internacional. Ya que, hay una relación estrecha entre ciberseguridad y prosperidad; en la era cibernética esto puede presentarse como un sinónimo de un futuro crecimiento y seguridad de la nación.

En el tercer pilar de la Estrategia, se subraya la necesidad de invertir en capacidades para responder de forma rápida a los ciberataques. Hubiera sido deseable una referencia a una ciber-fuerza dentro de la sección sobre la preparación para la disposición inmediata de las fuerzas (*readiness*) La Inteligencia Artificial es también crítica en el futuro de la ciberseguridad, tanto para evaluar y monitorizar las vulnerabilidades de los sistemas computarizados. (ESN, s.p, 2018)

El futuro pertenece a aquello países que logren posicionarse como líderes navegadores del ciberespacio y las nuevas tecnologías incluyendo el auge de la inteligencia artificial, por lo que ya se ha observado cómo los países empiezan a implementar las tentativas formas de implementación de este tema dentro de los planes nacionales donde incluyen la inteligencia artificial dentro de las estrategias de la mano con la ciberseguridad para el desarrollo de innovación tecnológica, comercial y crecimiento económico.

Estados Unidos debe defender también ahí su soberanía y avanzar en sus intereses y valores.Además, a Estados Unidos le piden un importante nivel de apoyo y esfuerzo en una institución, querrá un nivel de influencia proporcional justo y recíproco, al igual que en los

acuerdos comerciales. Para ello promoverá un nuevo modelo de desarrollo, modificando una asistencia a través de subvenciones por otra que atraiga el capital privado y que no promueva la dependencia, porque EE.UU quiere socios fuertes, no débiles. (García, pág.25, 2018)

Hay que recordar que aproximadamente a partir de la década de las novenas es donde se da la llegada del internet a la sociedad civil, y por ende como consecuencia surge una creciente conectividad y uso masivo del ciberespacio, por lo que los Estados empezaron a manejar los sistemas, principalmente a los que se les brindan soporte a los diferentes sectores de los servicios públicos, esto a través de las nuevas tecnologías. Por esta razón, los Estados se ven obligados a priorizar el tema de la seguridad cibernética.

Según Clay Wilson (s.p, 2008) Las relaciones comerciales entre los diferentes países han recorrido un largo camino en el pasar de la historia, desde el trueque hasta la difícil especialización y diversificación comercial:

> La mayoría de las infraestructuras básicas del mundo utilizan sistemas de supervisión, control y adquisición de datos para funcionar, se trata de sistemas informáticos especializados en su mayoría anticuados que controlan equipamiento físico con funciones tan dispares como hacer circular los trenes por las vías, distribuir la energía en una ciudad.

En un contexto económico global, rápidamente cambiante como el actual, donde la gestión empresarial está cada vez más influenciada por los avances tecnológicos y donde el talento es escaso, se hace necesario que las empresas sepan adaptarse, con flexibilidad, a un entorno de demanda cambiante, aprendiendo y actuando según su razón de ser, sabiendo a donde quieren llegar, contando con la disponibilidad de unos recursos y unas capacidades generadas por el personal de la empresa.

Ronda y Guerras (2012) realizaron un estudio cienciométrico sobre el concepto de estrategia a partir de 91 definiciones relevantes desde el año 1962 hasta el año 2008, que permitió elaborar una definición de consenso a partir de las palabras más repetidas en las distintas definiciones. Así, se consideró que la estrategia representaba “la dinámica de la

relación de la empresa con su entorno y las acciones que emprende, para conseguir sus objetivos y/o mejorar su rendimiento mediante el uso racional de recursos" (Navas y Guerras, s.p, 2012).

Por esta razón, el concepto de estrategia es introducido en el área de la economía bajo el ideal de competición, posteriormente es incorporado en el ámbito empresarial como parte de la recolección y manejo de la información de carácter cuantitativo o cualitativo, según sea conveniente para la toma de las decisiones de forma efectiva en situaciones de incertidumbre. Además, debemos recordar que es un término que se refleja y desarrolla en el ámbito político por y para las diferentes naciones.

En resumen, se puede decir que es un conjunto de actividades, objetivos y recursos que se analizan, se organizan y se desarrollan las actividades estructuradas, de acuerdo a su estructura, recursos y capacidades de la mano del área o mercado donde se emplee, con el fin de cumplir con los objetivos planteados inicialmente. Por lo que se convierte en un tema esencial para desarrollar en época de evolución tecnológica en la que nos encontramos.

El poderío tecnológico va cada vez en mayor aumento, al igual que los datos masivos, sus riesgos masivos y por supuesto que los efectos secundarios y riesgos potenciales son cada vez más elevados. Por lo cual se llega a destacar una visión futurista hacia la implementación de diferentes habilidades para la sociedad en la búsqueda de adaptación a las nuevas tecnologías.

Incluye, además a toda la industria en general, así como a las organizaciones internacionales, quienes se vieron en la obligación de brindarle mayor prioridad al tema de la ciberseguridad, buscando de esta forma desarrollar las estrategias en este ámbito, con el fin de tener mayor estabilidad en sus industrias. De este modo establecieron instituciones que les brinden procesos y estrategias, así como habilidades en temas de ciberseguridad para resguardarse de los ciberataques.

Según John Brennan, el asistente del presidente para la Seguridad Nacional y Contraterrorismo : "la seguridad de nuestra nación y la prosperidad económica depende de la seguridad, la estabilidad y la integridad de las comunicaciones y la infraestructura de

información que son en gran parte privados que operan a nivel mundial" y habla de la respuesta del país a un "ciber - Katrina".), en la que se debe aumentar la conciencia pública sobre las cuestiones de seguridad cibernética, y fomentar la investigación y la ciberseguridad fondo. (Ferro Veiga, pf.315, 2020).

Esta es una de las razones más importantes, por la cual los Estados soberanos comienzan a disponer de diferentes estrategias que puedan abordar áreas de ciberseguridad de forma integral para hacerle frente, y así evitar impactos imprevistos de amenazas cibernéticas, buscando de esta forma, un respaldo híbrido entre lo jurídico y lo técnico, donde además se pudiera también desenvolver en el entorno empresarial.

Por esta razón, el l 1 de julio de 2009, el senador Jay Rockefeller (D -WV) introdujo la "Ley de Seguridad Cibernética de 2009 - S. 773 "en el Senado, el proyecto de ley, escrito con los senadores EvanBayh (D- IL), BarbaraMikulski (D -MD), Bill Nelson (D -FL) y Olympia Snowe (R -ME), se remitió a la Comisión de Comercio, Ciencia y Transporte, que aprobó una versión revisada del mismo proyecto de ley "Ley de ciberseguridad de 2010 " el 24 de marzo de 2010. (Ley de ciberseguridad, s.p, 2010)

Básicamente, lo que busca este proyecto de ley es mantener y fomentar gradualmente la colaboración entre los sectores público-privado en todas las áreas tecnológicas, específicamente la búsqueda del fortalecimiento en el ámbito de la ciberseguridad, en especial en las entidades privadas que poseen infraestructuras primordiales para la seguridad nacional.

Por otro lado, en la estrategia de ciberseguridad podemos encontrar como sus principales objetivos de la ciberseguridad de los Estados Unidos se pueden resumir en los siguientes puntos:

1. La actuación conjunta de los sectores públicos y privados con el propósito de proteger las infraestructuras críticas del país.

2. Elaborar planes y tácticas con el propósito de desarrollar esta capacidad de actuar en conjunto entre los sectores públicos y privados, fomentar y apoyar al sector privado para

que pueda llevar a cabo su labor en el ámbito del espacio cibernético y el desarrollo de un sistema federal que sirva a estos objetivos.

3. Aumentar la conciencia de la sociedad y las empresas ante los ciberataques y dar importancia a las actividades de enseñanza y orientación a nivel federal.

4. Desarrollar planes con el objetivo de eliminar la amenaza que supone el creciente poder cibernético de Rusia para la ciberseguridad de Estados Unidos.

5. Tomar las medidas necesarias para proteger las innovaciones tecnológicas de Estados Unidos y los intereses comerciales del sector privado ante las actividades de espionaje cibernético de China.

6. Definir como infraestructura crítica nacional los ordenadores, *software* y tecnologías en red de los sectores agricultores, alimenticios, agua potable, sanitarios, seguridad social, informativos y de telecomunicaciones, energéticos, transporte, financieros, mensajería y marítimos y protegerlos de los posibles ataques cibernéticos.

7. Tomar las medidas necesarias para garantizar la libertad y seguridad del espacio cibernético y luchar, a nivel global, contra las medidas técnicas y administrativas de Rusia y China para fragmentar el internet.

8. Apoyar a los aliados contra los ciberataques que tengan como objetivo desestabilizarlos. (BurakDaricili, pf.4-13, 2020)

Por consiguiente, el ciberespacio al crear un nuevo entorno masivo y dinámico en las nuevas tecnologías entorno a la conectividad, se tiene la necesidad de fijar una base común en la cual se pueda hacer frente a las diferentes vulnerabilidades en las que se puedan desarrollar ataques o una acción delictiva sobre los ciudadanos, empresas o el mismo estado. En este sentido se comprende bajo el mandato del expresidente de los Estados Unidos Donald Trump, que los Estados Unidos a partir del 2017 empezaron a trabajar de lleno en las estrategias de seguridad nacional que llegaron actualizar las establecidas en el 2015.

Lo que se pretende con esta actualización de estrategias es involucrarse activamente en la dura competencia global, donde en este caso los Estados Unidos busca la mantenerse a la delantera en el ámbito de las nuevas tecnologías y la innovación, e incursionar en la competencia activa por el ciberespacio, ya que esta es la nueva carrera a la que se enfrentan las naciones por mantener el dominio.

El panorama económico que ofrece la Estrategia hace, por tanto, necesario "rejuvenecer" la economía y hacerla más competitiva. El énfasis que hizo en su momento Donald Trump durante las primarias y la campaña electoral en "hacer América grande otra vez" estaba entonces relacionado precisamente con hacer un país más competitivo. Su insistencia en ser firmes con China y renegociar muchos de los acuerdos bilaterales era una reflexión de su interés por incrementar la competitividad de EE.UU, con el riesgo de que esa atención se transformara en proteccionismo y aislacionismo, como está ocurriendo ahora. Según (Steinberg, s.p. 2018)

Cuando sale a la luz la creación de estas estrategias se llega a dar el reconocimiento adecuado hacia el tema estratégico que tiene el ciberespacio para las naciones que se desenvuelven en el nuevo entorno virtual. Por lo que se vuelve un tema prioritario dentro de las agendas de las naciones mantener cierto liderazgo en temas de ciberseguridad, con esto lograr establecer la coordinación de sus acciones, y los actores internacionales involucrados tracen su lucha contra el cibercriminal enfatizado en dimensiones sociales, económico, comercial y político.

A pesar de la apuesta de Trump por el fortalecimiento interno para hacer frente al mundo hipercompetitivo en el que vivimos, es en este apartado económico donde aparece la idea de trabajar con "socios afines" like-mindedpartners, con el objetivo de enfatizar en el comercio justo, pero será difícil encontrar países que busquen exclusivamente una estrategia de negociación bilateral que además ayude a EEUU a obtener su objetivo de reducir su déficit comercial. Según (García Encina, 2018)

El poderío tecnológico va cada vez en mayor aumento, al igual que los datos masivos, por ende sus riegos aumentan drásticamente, por lo que también se tendrán efectos secundarios y los riesgos potenciales son cada vez más elevados, por lo cual se llega

a destacar una visión futurista hacia la implementación de diferentes habilidades para la sociedad en la búsqueda de adaptación a las nuevas tecnologías.

Según el director nacional de inteligencia de EE.UU, Daniel R. Coats, en su comparecencia ante el Comité de Inteligencia del Senado el pasado febrero: "las incertidumbres entre los aliados y socios de EEUU sobre la voluntad y la capacidad de EEUU de mantener sus compromisos internacionales puede llevarles a considerar la reorientación de sus políticas, en particular las comerciales, lejos de EEUU" (R.Coats, pág.12, 2020).

En las últimas décadas, la llegada de las nuevas tecnologías, la evolución de los servicios electrónicos, así como el desarrollo de las redes de comunicación se ha incorporado cada vez más a nuestra vida diaria. Por lo que, a medida de que la sociedad se empezó a volver cada vez más dependiente es cuando se volvió un tema de interés primeramente nacional y después se desplaza a nivel global, esto cuando todos los Estados empiezan a enfrentar los diferentes cambios tecnológicos dentro de sus propias naciones, y con ello se prevé una evolución en las estrategias comerciales y sus actores para su debida adaptación que permita su sobrevivencia.

En la actualidad, las tecnologías permiten la automatización de la actividad realizada por muchas de las máquinas de producción e incluso de procesos enteros. Esta automatización viene a significar que las máquinas puedan trabajar sin intervención humana pero sometida a unas reglas muy estrictas. El reto consiste en dotar de cierta inteligencia a las máquinas de forma que puedan interaccionar con el entorno de manera más autónoma y sean capaces de adaptarse a las situaciones y a los cambios directamente, sin que sea necesaria la intervención manual. (Ariel, pág.55, 2016)

El área del ciberespacio llego adentrarse en cada ámbito existente y como vemos anteriormente, el comercio internacional no se queda atrás por lo que los estados buscan mantener una protección adecuada en lo que se pueda realizar incluso de la mano del sector industrial. Aunque Estados Unidos ha tratado de trabajar fuertemente en este ámbito y si bien es cierto, ha establecido estrategia de protección como el robo de propiedad intelectual, y entre otros ejemplos donde se ha marcado de forma efectiva su protección hay otros ámbitos en los cuales se deben seguir trabajando.

Siguiendo a Díaz y Orueta, G (2013) en su obra: “Procesos y herramientas para la seguridad de redes”:

> Internet, es un sumatorio complejo de redes y sistemas que ha modificado desde años todas las formas habituales de comunicación, cambiando radicalmente los hábitos de vida y formas de trabajar de todos los sectores de la sociedad, ha provocado cambios organizacionales a todos los niveles, robotización de las cadenas de producción, etc..

De acuerdo con el autor anterior, los sistemas gozan de una serie de propiedades complejas y capaces de interactuar, este tipo de propiedades con vacíos llamados bugs son una clase de fallos que pueden ocurrir en el sistemas que no se encuentran previstas, esto significa que el sistema no llegue a funcionar correctamente. Se ha atribuido el hecho que entre mayor sea el nivel de sofisticación tenga el sistema, es mayor la posibilidad el número de bugs que puede contener.

Es importante mencionar esto ya que, gran parte de estos fallos llamados bugs se puedan transformar en problemas de seguridad informática para los diversos sistemas y sus debidos protocolos. Por lo que este tipo de *bugs* de seguridad se vuelven en vulnerabilidades dentro del sistema, provocado en las aplicaciones de los software en general y que pueden ser aprovechados por personas mal intencionadas, provocando a los sistemas y a las redes a que sufran ataques a su seguridad en infraestructura tanto del sector público como el privado.

Esto se llega a vincular, ya que, existen ocasiones donde infraestructuras automatizadas se han visto afectadas por temas de cibercrimen y aunque son casos específicos y muy pocos; esto no significa que se encuentren exentos a este tipo de situaciones. Por lo general, se ha llegado a visualizar grandes cantidades de ciberataques especializados en la obtención de información principalmente en temas como de: contraseñas, aplicaciones, espionaje, entre otros. Por lo que se ha intentado realizar algunos acuerdos en temas de regulación.

Conviene apuntar que en este pilar hay una conexión explícita entre ciberseguridad y prosperidad. Por un lado, porque la respuesta de EE.UU a los retos y oportunidades de la

ciber-era determinarán el futuro crecimiento del país y su seguridad. Por otro, se afirma que "las transacciones económicas y personales dependen del mundo '.com', y la creación de la riqueza depende de un Internet seguro y fiable" Éstas son palabras importantes para empresarios, universidades y otras instituciones, no sólo por la creación de riqueza sino porque la ciberseguridad es un peligro claro y presente para la economía del país. (García, pág.22, 2018)

La seguridad informática debe tener muy en cuenta la prevención, ya que las tecnologías están evolucionando en cuanto al tema de detección y respuesta. Se utilizan cada vez más herramientas de detección como los sistemas de intrusiones, herramientas, procedimientos y sistemas de análisis, gestión de riesgos y auditorias de vulnerabilidades.
Se debe tratar las preguntas que se hacen para definir mejor el sistema que se quiere asegurar, explorando alguna solución realista, basada en lo que se llama política de seguridad del sistema, así como herramientas básicas para la seguridad.

Actualmente, se puede decir que es relativamente accesible encontrar herramientas en internet que permitan realizar pruebas en redes para encontrar algunos fallos y vulnerabilidades en los sistemas como se mencionó anteriormente, los llamados "bugs", para ser reportados. Todas estas herramientas pueden ser utilizadas con mala intención lo que conlleva nuevos riesgos por lo que es fundamental para los gobierno la creación de diferentes estrategias o planes en las que se contemplen el tema de ciberseguridad como parte esencial para la seguridad nacional.

Sin embargo una de las mayores barreras es la complejidad que rodea este tema y es que, los factores diversos que influyen en un ataque se presentan principalmente en que muchos de los objetivos propensos a los ataques son las empresas privadas, por lo que su seguridad depende únicamente de sus medidas preventivas y protocolo de enfrentamiento. Otro factor importante a tener en cuenta según el experto Alonso Castro Arias es ¨el tema de la falta de conciencia y educación social en temas de prevención¨. Lo que dificulta la toma de medidas y de coordinaciones eficaces en la lucha contra la disminución de estos crímenes.

La influencia y el uso de las TIC en la sociedad se llegan a intensificar con los compromisos adquiridos en la Cumbre Mundial de la Sociedad de la Información y el Conocimiento. Esta cumbre fue organizada por la Unión Internacional de Telecomunicaciones (UIT), con origen en el años 2003 y 2005, y se llegó a convertir en un eje importante dentro de la comunidad internacional y que además representa los grandes cambios a los que nos hemos enfrentado con la llegada de la era digital, dando así inicio a nuevas formas de organización mundial.

La Resolución 130 (Rev. Guadalajara, 2010) hace numerosas referencias a decisiones recientes de otros órganos de la UIT, así como a iniciativas más recientes tales como la Agenda sobre Ciberseguridad Global. Resuelve que la UIT siga atribuyendo una elevada prioridad a esta actividad, teniendo en cuenta su competencia y conocimientos técnicos.

Las naciones buscan definir estrategias que se puedan ejecutar en coordinación entre los entes del sector público y privado, siendo compatibles con los derechos, libertades individuales para coordinar con otras acciones tanto para detectar amenazas como establecer sistemas de respuestas ante eventuales ciberataques. Sin dejar por fuera el fomento de cooperación internacional como punto clave para lograr acuerdos de colaboración internacional.

Según la Nueva Resolución 174, La utilización ilícita de las TIC puede tener repercusiones indeseables en la infraestructura, la seguridad nacional y el desarrollo económico. Esta nueva Resolución denominada "Función de la UIT respecto a los problemas de política pública internacional asociados al riesgo de utilización ilícita de las tecnologías de la Información y la comunicación", llama a la acción para detener dicha utilización. (Rev. Guadalajara, 2010)

Esta resolución básicamente busca mantener el papel de la UIT en la cooperación internacional, incluyendo órganos como las Naciones Unidas en la búsqueda de utilización indebida de las Tecnologías de la Información y Comunicación. Además de destacar la

importancia de mantener lazos como el de la Cumbre Mundial sobre la Sociedad de la Información.

Según la Cumbre Mundial sobre la Sociedad de la Información (2010), en la línea de acción C5 establece que:

> Los Gobiernos, en cooperación con el sector privado, deben prevenir la ciberdelincuencia y la utilización indebida de las TIC, detectarlas y responder a las mismas: elaborando directrices que tengan en cuenta el trabajo que se hace actualmente en estos ámbitos; introduciendo normativas que permitan investigar y castigar efectivamente la utilización indebida; propiciando una colaboración eficaz; reforzando el apoyo institucional a nivel internacional para evitar y detectar estos incidentes y reaccionar de forma adecuada; propiciando la enseñanza y la sensibilización.

Este tipo se resolución busca la cooperación entre los diferentes Estados miembros, pero además fomenta que las naciones se interesen en que se realicen diálogos nacionales e incluso regionales para que se vele por el bien común en la búsqueda de soluciones ante posibles riesgos a los que actualmente se ven afectadas la comunidad internacional con el uso indebido de las TIC.

En este punto se hace referencia a la presencia comercial y económica en el ciberespacio, donde surge la implementación de la tecnología de la información y la comunicación con las nuevas tecnologías donde principalmente se desarrollan en el ámbito de la automatización, por lo que todo este ámbito llega a evolucionar sus operaciones incluso las formas de organizar el intercambio de bienes y servicios como por ejemplo: empresa-empresa, cliente-empresa, entre otros. Todos estos procesos se llegan a implementar sin importar la ubicación geográfica, ni las diferencias de tiempos, por lo que llegamos a observar que una de las actividades más desarrolladas son e-commerce, y e-business.

Durante el desarrollo investigativo hemos visto cómo muchas de las reformas propuestas durante los años propuestos en estudio, en los Estados Unidos han coincidido al

desarrollo de la Administración del señor Donald Trump, expresidente de los Estados Unidos de América. Durante su administración una de las estrategias reguladoras del comercio principalmente en el tema de las exportaciones, decidió incluir algunos apartados donde impone algunas limitaciones para las exportaciones de servicios cibernéticos.

El Departamento de Comercio de Estados Unidos**,** actuando bajo el mandato de una ley de 2018 (Export Control ReformAct, o ECRA) ordena a la agencia la escritura de normas para impulsar la supervisión de la exportación de tecnología sensible a adversarios,tanto por razones económicas como de seguridad. También requiere que el Gobierno examine cómo puede restringir la exportación de tecnologías emergentes y esenciales para la seguridad. Entre ellas está la Inteligencia Artificial. Según (Valdeolmillo, pf.3, 2020)

Durante la administración del señor expresidente Donald Trump, se interpusieron regulaciones dentro del comercio internacional esto en temas de exportaciones de bienes y servicios tecnológicos. Pero además, incluyo dentro de estas regulaciones temas de exportaciones de programas cibernéticos como software, todo esto con el fin de que sus adversarios no puedan obtener tan fácilmente sus recursos tecnológicos y tratando de evitar posibles amenazas que puedan surgir a futuro.

Por lo que implementó el uso de licencias especiales para las exportaciones de software a los países que quieran adquirir estos recursos como medida de regulación con la excepción de Canadá**,** país al que se podrá exportar sin mayores restricciones que las que se aplican al software de IA exportado a dicho país. Esta medidaes la primera en entrar en vigor de una serie de normas que se están desarrollando con el objetivo de limitar exportaciones de elementos de este tipo, pensadas para beneficiar a la industria estadounidense. (Valdeolmillo, párr.2, 2020)

La administración estadounidense libra una batalla comercial, en la que ha incorporado restricciones para las exportaciones comerciales que ha afectado el flujo de componentes y servicios tecnológicos. Aunque estas medidas se proyectan y se rigen actualmente para las exportaciones en los Estados Unidos, es probable que en algún momento se adquieran por los organismos internacionales, con el fin de crear un escenario de normativas igualitaria para toda la comunidad internacional.

### 4.1.1 Resumen de instrumento utilizado.

En este apartado se procedió a utilizar el instrumento de entrevista profunda, con variedad de profesionales en diferentes ramas de estudios, así como sus experiencias, esto con el fin de captar toda la información necesaria para el desarrollo de esta investigación.

**Entrevista 1.**

Edgar Oviedo Blanco.

Puesto: Dueño, director de negocios y relaciones corporativas.

Empresa: Grupo Babel

1. **¿Qué sectores industriales se están viendo más afectados por las amenazas de ciberseguridad?**

Respuesta: No es un tema discriminatorio, por el contrario, esto va para todas las áreas de todos los sectores existentes. Sin duda los ciberataques son actos ilícitos

principalmente vinculados a negocios ilegales que buscan la rentabilidad de las grandes empresas de mayor valor.

Por lo que, por lo general buscan las vulnerabilidades para realizar sus fechorías a grandes empresas, y de mayor valor adquisitivo como sistemas bancarios y grandes corporaciones esto con el fin de asegurar obtener un capital sustentable.

Por otro lado, como dije anteriormente, no es un tema discriminatorio, y aunque sus objetivos comunes sean basados en las ganancias que puedan obtener esto no quiere decir que los demás entes, o sectores que tienen menor porcentaje de ser atacados no sean a un cien por ciento, incluso entidades gubernamentales o naciones enteras se pueden y se han visto afectadas de forma de alguna forma.

Análisis: Se concuerda con el experto y su posición, cuando indica que este es un tema sumamente amplio donde no hay discriminación en los crímenes, para tener datos exactos se tendría que acceder a cierta información que no se pueden acceder. Por otro lado, el tema del cibercrimen siempre buscará una vulnerabilidad existente en todos los ámbitos para buscar penetrar y almacenarse bajo algún vacío y que este le proporcione la facilidad de realizar sus fechorías.

A lo que sí se puede hacer referencia son los datos y números estadísticos donde reflejan de forma cuantitativa los incidentes reportados, estos los envía a los "ComputerEmergency Response Team" (CERT), y como es de conocimiento Estados Unidos es quien más tiempo lleva realizando estas notificaciones y estas mismas dejan reflejado que una de las mayores áreas que reportan este tipo de eventos son los sistemas de operaciones, y sistemas de automatización industrial donde casi siempre se identifican en el área de energía, transportes como: vehículos, aviones, trenes, estos son solo algunos ejemplos que podemos mencionar.

2. **¿En qué medida no atender la ciberseguridad adecuadamente tiene riesgo para la evolución económica de un país y su desarrollo industrial?**

Respuesta: Es un tema transversal, esto quiere decir que la ciberseguridad conlleva gran conectividad con todas las áreas, por lo que también va de la mano de la analítica de datos. De este modo, entre más datos mayores servidores, usuarios.

Por lo que en la actualidad la ciberseguridad no debe de ser un tema aislado a un solo sector, ni tampoco debe ser tratado como una adquisición por gusto de si quiero implementarlo o no, simplemente es un ámbito el cual debe ser desarrollado sí o sí.

Análisis: Al tratarse de un tema tecnológico tenemos en cuenta que uno de los factores que amplifica este tema es el hecho de la conectividad o interdisciplinariedad que conlleva este tema de ciberseguridad, y el efecto que presenta con cada uno de los temas en los que se vea desarrollado.

Teniendo en cuenta que la ciberseguridad es el área especializada en mantener seguro el ciberespacio, se puede entender su magnitud e importancia que el mismo implica. Por esta razón el hecho de no darle la prioridad que merece o no atender algún riesgo que esté presente se puede convertir en un tema con desenlaces desfavorables que se pueden presentar tanto en lo micro como a nivel macro.

3. **¿Qué riesgos no tradicionales pueden aparecer en sectores críticos como el comercio para un país?**

Respuesta: considero que un riesgo no tradicional sería el robo de los datos e información, con mi experiencia en la empresa hemos visto cualquier cantidad de robos de información utilizados para extorsión hacia una entidad.

Donde en la actualidad lo que secuestran es la información empresarial y lo que literalmente se utiliza como rehén ya no solo son personas, sino que esto ha escalado a un concepto donde el que los datos que procesa una empresa pasaron a ser rehenes, en lo personal considero que estos son los nuevos riesgos no tradicionales a los que se enfrentan las industrias actualmente.

Análisis: en concordancia con el experto uno de los riesgos no tradicionales que llegaron a relucir como efecto de la ciberseguridad es el robo de datos, lo que casi siempre se piensa a la hora de hablar de ciberseguridad es que se tiene el pensamiento que únicamente es que este tema hace referencia únicamente a la seguridad nacional y aunque si

bien es cierto, es una de sus tantas ramas, no podemos dejar de lado a todos los demás actores que se encuentran dentro de la comunidad internacional.

En cuanto a la industria, la ciberseguridad al conectarse con todas las áreas y al volverse las industrias uno de los actores más apetecibles por el cibercrimen, lo vuelve un factor importante ya que, en un robo de información puede traer daños colaterales a la economía y comercio de un país además de afectar su reputación.

**4. ¿Cuáles son las principales barreras para su implantación?**

Respuesta: Primero la alfabetización digital para la sociedad civil, los usuarios conocen el tema de prevención, pero todavía no interiorizan la importancia de estos temas. Un ejemplo claro: como empresario puedo llegar a tener un cliente al cual le brinde mis mejores servicios de protección, con los mejores especialistas, le puedo brindar el mejor sistema, incluso el más robusto.

Pero ¿Qué se logra con eso si al final del día el usuario no cumple con los criterios básicos de prevención? Así como este ejemplo existen otros que se viven en la cotidianidad que resultan ser barreras para la implementación efectiva de un proceso de seguridad.

Considero que una segunda barrera es la voluntad gerencial: Este es un caso que vivimos a diario como proveedores de servicios, aquí lo dividimos en dos casos 1- cuando la gerencia de una empresa desconoce la importancia del tema de ciberseguridad, o lo conoce muy superficialmente y se crea la idea de que son temas aislados a su realidad. La famosa frase: ¨a mí no me va a pasar¨, o ¨eso solo le pasa a empresas grandes¨

2- Empresas que cuenta con personal consciente de manejar un tema de ciberseguridad que les permita desarrollarse de forma segura, sin embargo cuentan con poca voluntad gerencial, este es el más común por lo general en este ejemplo las gerencias brindan un presupuesto muy limitado para el desarrollo adecuado de protección o del todo prefieren omitir las consecuencias y no destinan del todo un presupuesto para cubrir esta necesidad.

Análisis: Todos los expertos entrevistados concuerdan en la importancia de tener conocimientos básicos digitales para la sociedad, y se considera que es uno de los puntos

más importantes ya que, la falta de este conocimiento por lo menos de forma básica se vuelve una barrera importante para mantener una seguridad en términos sociales en general.

En el ámbito empresarial, podemos compararlo o visualizar la ciberseguridad como un peaje o como consecuencia que se debe desarrollar para lograr obtener la introducción de las nuevas tecnologías de la Información y comunicación. Cuando el experto hace mención de la importancia que le debe prestar las altas gerencias en la prevención y el desarrollo adecuado de la ciberseguridad, es sustancial agregar que toda compañía debería trabajar en la realización de protocolos adecuados para posibles eventualidades que denotan riesgos.

4. **¿Qué tendencias tecnológicas están surgiendo en torno a la ciberseguridad industrial?**

Respuesta: Una de las mayores tendencias que estamos viviendo es la transformación tecnológica, principalmente lo podemos observar en la transición digital en la que nos encontramos. Yo le agregaría que gracias a estas tendencias el sector el sector informático se ha visto bastante beneficiado, las ventas de servicios ha tenido gran auge además que los especialistas en tecnología en general ha tenido mayor reconocimiento en la industrial, que quizás antes no se nos daba tanto como ahora.

Es importante mencionar que considero que esta transformación tecnológica se da bajo tres principales necesidades: 1- Aspecto social: como hablamos anteriormente la importancia de la alfabetización digital y todo lo que esto conlleva, 2- Los procesos, las buenas prácticas, y 3- La implementación de la tecnología. Estos tres puntos han sido fundamentales para la creación de las tendencias tecnológicas.

Análisis: El análisis de triángulo de trabajo como lo plantea el experto, nos deja ver como estos tres puntos son esenciales para un buen funcionamiento del trabajo en pro de la seguridad cibernética. Además, como deja ver la estructura o pautas a seguir para tener una armonía en el desarrollo de la prevención.

Cuando se habla del orden asegurar para un funcionamiento eficaz dentro de la industria se menciona como primer punto el tema de la necesidad social en la importancia de la alfabetización tecnológica y digital, esto le permite a la sociedad tener una primera

conexión con las nuevas tecnologías y entender cómo éstas operan, cómo evolucionar con ellas y cómo adaptarnos a su existencia. Seguidamente, de una primera interacción tenemos que pasar al plano práctico donde se ejecuta lo aprendido anteriormente. Como ciudadanos, debemos de mantener las buenas prácticas desde el primer momento en que llegamos a tener la formación y conocimiento.

Si realizamos praxis de lo aprendido desde el primer momento, como consecuencia estas buenas prácticas las tendríamos tan adheridas que las aplicaremos de forma natural en el desarrollo de otras actividades como en el ámbito laboral. Lo que nos convertiría en profesionales conscientes del implemento y desarrollo de las buenas prácticas y por ende transmitiremos este conocimiento a quienes nos rodean.

Una vez teniendo estos dos puntos de equilibrio se armoniza con una dotación de buenos implementos tecnológico, ¿cuál es la importancia que conlleva implementar este orden expresado por el experto? Simple, si se cumple este orden sugerido la probabilidad de que se realice un trabajo de forma eficiente es cada vez mayor. Puesto a que si se rompe como se ha reflejado en muchas compañías el desgaste y el gasto es mucho mayor para lograr llegar a brindar un servicio de calidad y eficaz.

5. **¿Cuál ha sido el registro de Costa Rica en temas de comercio de servicios, y su desarrollo en temas de ciberseguridad en comparación con otros países?**

Respuesta: Nosotros somos una de las empresas nacionales que exporta servicios tecnológicos, por lo que podemos tener una visión amplia de cómo se comporta gran parte del comercio que brinda servicios tecnológicos desde el área de seguridad preventiva hasta la solución de problemas informáticos.

Nuestra empresa tiene presencia en toda América Latina, si se usa esta información para hacer una comparación del comportamiento considero que Costa Rica se encuentra muy bien en temas de adaptabilidad tecnológica, creo que es uno de los país en América Latina que se ha destacado en el desarrollo de tecnológico, y continúa liderando en la implementación de la nuevas tecnologías y su seguridad. Si busco un punto de

comparación, podría decir que Colombia es uno de los países que mantiene un comportamiento similar al nacional.

Ahora si ponemos a Costa Rica, frente a un escenario global considero que sí nos encontramos bastante rezagados o como decimos popularmente: ¨a nivel mundial si nos dejaron ¨botados¨, sin embargo todo es un proceso y nos falta camino por recorrer mientras mantengamos un buen ritmo en la evolución y adaptabilidad tecnológica estaremos avanzando de la mejor manera como lo hacemos hasta ahora.

Análisis: desde una perspectiva diversa a la que tiene el experto, a simple vista desde la óptica meramente de observación, se podría pensar que nos encontramos mal en términos de estructura informática y ciberseguridad. Sin embargo, dejando el pensamiento pesimista debemos resaltar las buenas labores y es que, Costa Rica aunque no tenga una calificación de nota excelente por así decirlo sí que ha buscado la forma de trabajar en la búsqueda de una mejora continua.

Esfuerzos en la alfabetización digital, y la disminución de brechas digitales e infraestructura tecnológicas, es algo que se debe resaltar. Costa Rica aunque si bien es cierto tiene muchas carencias en las que debe empezar a trabajar, al igual que otros países también deben de buscar la puesta en marcha en temas de vacíos meramente legales para su adecuada regulación.

**6. ¿Qué recomendaciones como experto en este tema nos puede brindar?**

Respuesta: A nivel país continuar trabajando en esta transformación tecnológica, y por otro lado sigo insistiendo en fomentar e impulsar a las altas gerencias en la importancia de resguardarse en el tema de ciberseguridad.

**Entrevista 2.**

**Roberto LemaÎtre Picado.**

Puesto: MSc. ingeniero informático, Abogado: Especialista en delitos informáticos, testigo pericial, profesor y conferencista.

Empresa: Organismo de Investigación Judicial (dep. ciberseguridad y crímenes informáticos), Universidad Cenfotec.

1. **¿Qué se está haciendo en materia de legislación?**

Respuesta: varias cosas, no solo qué se está haciendo sino que existe también, nivel internacional Costa Rica en lo que mejor sale calificado en todos los índices es en materia de legislación en ciberseguridad es en lo que mejor estamos en el país. Todo esto incluye varios elementos de tanta legislación penal en materia de delitos informáticos con las reformas que se hicieron ya hace un tiempo pero que están bastante bien en comparación con las normativas existentes a nivel internacionales, e incluso las regionales.

En el 2013, se reformó el Código Penal incluyendo los nuevos delitos informáticos. Contamos con leyes de protección de datos que últimamente han salido muchas observaciones al respecto pues tenemos un marco jurídico en materia de protección de datos con la ley de protección de datos, un reglamento de protección datos y además una gerencia de protección de datos que regula el buen uso de las bases de datos personales y su correcta administración.

Además esta misma normativa establece un procedimiento para los temas de cómo gestionar adecuadamente los temas de protección de datos. Los otros elementos podemos mencionar que tenemos una ley de firma digital certificada que regula la normativa de firma digital, permite tener un elemento técnico que brinde un respaldo jurídico.

Por lo que, la construcción técnica que tiene la firma digital certificada, y en conjunto con la ley permite tener un nivel de certeza totalmente alto y que a la hora de presentar alguna firma digital certificada se tiene un respaldo y credibilidad. Esto permite que se realicen múltiples actividades como firmas de

contratos, convenios que garantizan un nivel de certeza alto y que está respaldado por la ley por lo que se le reconoce los efectos que se tiene.

Leyes de protección de la niñez en materia cibernética, por esto también el código penal sufrió reformas relativas relacionadas con la protección de menores en materia de pornografía infantil, y mantienen regulaciones de protección en materia de violación de datos personales, entre otros muchos artículos de los que se compone esta ley.

Análisis: Es común que muchos de los ciudadanos solo disfruten del uso de la tecnología, evolucionan y se adaptan a ella como a sus cambios. Sin embargo, gran porcentaje de la población costarricense no tienen conciencia de la variada gama normativa con la que se cuenta en temas de tecnologías de información y comunicación incluso en términos de ciberseguridad.

Es muy poco porcentaje de la población que conoce sobre este tema y sus respaldos, y el otro por ciento de la población tiene muy poca conciencia de todo lo que abarca a profundidad todas estas regulaciones.

2. **¿Cuáles son las barreras para su implementación?**

Respuesta: Siempre van a existir vacíos legales y esto se da porque las leyes nacen a partir del surgimiento de una situación, es decir hasta que nazca un precedente se crea una contraparte. Hasta que no haya una necesidad de regulación, no se crea esta regulación frente a esas problemáticas.

La aplicación en la tecnología es diferente, porque la tecnología avanza mucho más rápido. Entonces el reto normativo es mucho mayor ya que, pueden darse cambios muy acelerados y que la normativa no se dé al mismo tiempo e incluso se dure más en los procesos.

Otra barrera sería que falta del desarrollo de normativas específicas, esto porque si existe un delito específico en un ámbito donde no se regula específicamente ese crimen se procede aplicar la norma general y esto sirve de variante en para las condenas que se lleguen a establecer.

Análisis: como menciona el especialista el indica que existe déficit en desarrollo de normativas específicas en temas de ciberseguridad para situaciones especiales; y esto se correlaciona con las opiniones de los demás especialistas donde ellos hacen énfasis en la necesidad de educación, y esto porque hay una faltante a nivel internacional de especialistas en temas específicos como el de ciberseguridad.

Incluso en temas de alfabetización digital, hay que tener conciencia de la importancia de mantenerse actualizados la mayoría de las tecnologías. Que permita conocer sus derechos y deberes en este campo tan cambiante y dinámico constante.

**4. ¿Está la Justicia preparada para abordar los conflictos que puedan surgir incluyendo la transnacionalidad?**

Respuesta: Considero que sí, como hemos venido conversando tenemos un marco jurídico bastante robusto que nos permite desarrollarnos bien para los conflictos en las diferentes situaciones. La utilización de las herramientas de cooperación, el pedir ayuda y brindar la misma están funcionando de la mejor manera para el desarrollo de las investigaciones.

Análisis: Tenemos que darnos cuenta de que hay una evolución de esos delincuentes independientemente de que tengamos un marco regulatorio que garantice la privacidad de nuestra información, independientemente de que las empresas tengan que funcionar.Cuando hablamos de seguridad, estamos hablando de implantar medidas que nos protejan frente a los delincuentes. Podemos tener todo el marco legal que queramos, pero cuando planteamos una evaluación de ciberseguridad, es implantar medidas, mecanismos, políticas que van a levantar una barrera que nos protege frente a las posibles amenazas.

5. **¿Conoce de algún tratado, o algún tipo de cooperación que se de en el tema de ciberseguridad?**

Respuesta: Costa Rica se integró a la Convención de Ciberdelincuencia Internacional, conocida como la Convención de Budapest. Esta convenció crea una red de colaboración 24/7 que permite mejorar los procedimientos de investigación a nivel internacional, ya que, muchos de estos delitos deben de investigarse y la información no se encuentra en el país, o en caso contrario que alguien ocupe la información y esta solo se encuentre en un lugar específico. Por lo que esta convención llega a crear un marco común de delitos en todos los países miembros, y además permite la colaboración para mantener pruebas digitales y que de esa forma las investigaciones se puedan desarrollar.

Este elemento se vuelve fundamental, ya que los procesos tradicionales no son tan rápidos para los temas de investigación de delitos informáticos, lo que permite ante alguna eventualidad pedirle al país miembro que mantenga la información para realizar un debido proceso.

Hay temas de cooperación a nivel interno entre los ministerios del país, en materia de ciberseguridad para mejorar las capacidades técnicas, de aprendizaje y de logística para implementar las mejoras. Incluso entre los ministerios se ve la cooperación internacional técnica ya que, también es importante reforzar en materia de conocimientos ya que permite mejorar las capacidades y experiencia con cursos, información, entre otros.

Análisis: Es interesante abordar en este espacio, el tema de la importancia de la cooperación técnica que se desarrolla en el ámbito de la ciberseguridad. Naturalmente cuando se habla de cooperación internacional pensamos automáticamente en la modalidad financiera, sin embargo, dejamos de lado la cooperación técnica.

Y analizando podemos entender la importancia que aporta la cooperación técnica en este ámbito. Pues, como cita el experto es fundamental que los profesionales en el ámbito de la tecnología siempre mantengan sus conocimientos continuamente actualizados, esto para estar a la vanguardia y poder resolver cualquier eventualidad.

Recordando que la evolución tecnológica siempre se encuentra en una evolución constante, que nos obliga a llevar su propio ritmo. Por lo que este tipo de cooperación se vuelve fundamental en el ámbito laboral y profesional.

**6. ¿Disponemos de suficientes mecanismos de protección? ¿Qué hace falta?**

Respuesta: Considero que sí mantenemos un marco legal bastante robusto, puesto a que existen normativas en variación de diversas áreas como: derechos de autor, propiedad intelectual, normativas en tecnologías, redes, e incluso en telecomunicaciones. Entonces, el marco en temas de tecnología se encuentra bien estructurado.

Claro está, en que se debe promover la actualización continua como los proyectos de actualización de datos, actualización de datos en delitos informáticos, proyectos en temas de porno venganza, proyectos en temas de comercio electrónico, una ley especial para comercio electrónico donde no se basen con una ley general que se tiene en el código de comercio, pero que no se tiene una ley especializada en comercio electrónico.

Aunque si bien es cierto se la han jugado con la implementación de la ley general, se está trabajando en la creación de en esta área en específico.

Lo que nos puede hacer falta es seguir trabajando y mejorando en los temas de coordinación, trabajo en equipo, cooperación internacional, ya que son áreas donde los informes internacionales han reflejado este tipo de problemas. Sin embargo, en temas jurídicos siempre tenemos buenas calificaciones.

Importante que se vea bajo una premisa de inversión más que un gasto para las empresas no solo para las empresas sino que para todas las organizaciones.

Análisis: A nivel nacional, a la hora que se realiza investigación a profundidad podemos encontrar que Costa Rica se mantiene sobre un camino bastante próspero en el sentido de que se está realizando labores importantes para mantener el ritmo de evolución tecnológica. Esto quiere decir que el nivel de adaptación a estos cambios el país lo han hecho muy bien.

Por lo que, se puede considerar que a nivel nacional no es una faltante sino que se debe alentar a seguir trabajando de este modo como se ha venido implementando. La observación a nivel país como faltante es importante que se tomen en consideración realizar las mejoras que se le brinda por parte de las calificadoras, organizaciones como la OCDE, incluso de comentarios realizados por profesionales que se desenvuelven en el ámbito laboral.

A nivel internacional es importante que se empiecen a realizar cambios curriculares donde se los profesionales tengan la oportunidad de especializaciones que permitan una integración de conocimientos. Ya que de este modo direccionara de la forma adecuada de los nuevos mercados.

7. **¿Qué implicación tiene la ciberseguridad en el desarrollo de nuevos servicios?**

Respuesta: Un punto bastante importante e interesante es que un país ciberseguro se vuelve un país más influyente e incluso atrae más inversión, es un país que se vuelve atractivo para la inversión comercial.

Un país que cuenta con seguridad cibernética por consecuente es un país desarrollado en infraestructura cibernética, que cuenta con un marco normativos equipos a nivel judicial, tiene una sección especializada en esta área, tiene un Centro de Respuesta a Incidentes Informáticos (CSIRT) que coordina con las demás instituciones para la persecución y compartimiento de la información.

Si se tiene esas políticas que respalden, al contar con grandes probabilidades de respaldo en seguridad, gracias a los índices que nos permite mantener porcentajes positivos no solo a nivel nacional sino que también a nivel internacional. Ya que, comercialmente se vuelve un país atractivo para las empresas.

Costa Rica se encuentra en una estrategia de transformación digital donde se plantean todos los cambios del sector público en temas de digitación, por lo que el tema de la ciberseguridad se vuelve un pilar fundamental para brindar seguridad en el respaldo a los posibles riesgos.

Análisis: Actualmente con la evolución tecnológica, el mundo cada vez más digital, y sobre todo la llegada del virus COVID-19 hizo que la aceleración

tecnológica el desarrollo tecnológico, se dice que aproximadamente entre 3 a 5 veces más rápido de lo esperado.

Por lo que, a consecuencia se implementó como tendencia a nivel mundial fue el teletrabajo, y con ello la creación de los nómadas digitales. Este es uno de los nuevos servicios que surgen a la evolución tecnológica pero gracias también a la ciberseguridad la cual hace posible este servicio y fomenta el atractivo turístico, y tecnológico de un país preparado en este ámbito.

8. **¿Cómo cree que puede ser la evolucionar del ecosistema de empresas dedicadas a la ciberseguridad?**

Respuesta: Costa Rica ya cuenta con varias empresas que brindan servicios de ciberseguridad, donde las empresas privadas ofrecen servicios tanto nacional como internacional que les permite el crecimiento. Empresas como pymes especialistas en el tema de ciberseguridad, que a nivel país se vuelven importantes ya que su crecimiento a la falta de profesionales en este ámbito a nivel internacional, lo vuelve un nicho importante para el comercio, lo cual nos brinda ventajas, por motivo de que al ser este un servicio que va en aumento las pymes en este ámbito crecen, e incluso con ese desarrollo brinda mayores probabilidades de nuevos empleos incrementando así la economía del país.

Análisis: Para hablar del ecosistema que se emplea con la ciberseguridad entendemos que se vuelve sumamente amplio, porque básicamente abarca todas las aristas existentes. Sin embargo, si buscamos intentar hacer un tipo resumen podemos decir que se basa principalmente en uno de los muchísimos entornos que están dentro del Internet of Things, como es el caso de las smartcitiesu otro tipo de ámbitos abiertos, donde muchos de esos dispositivos tienen una amplísima exposición. Nos referimos a unos sensores dispersos por una ciudad que van a interactuar directamente con los usuarios.

Se puede mencionar el desarrollo de la interconectividad, en temas industriales se verán donde la ejecución de máquinas se encontrará de forma interconectada, por lo que la forma de hacerle frente a las amenazas se debe hacer en ese contexto, incluyendo así la

ciberseguridad en la búsqueda de garantizar que ese espacios de interconectividad sean cada vez más seguros, sin perjudicar el rendimiento global del sistema.

De este modo, en concordancia con lo expresado por el experto, la creación y el auge de pymes especializadas en brindar servicios de ciberseguridad, es una de las tendencias que va ganando terreno, sin dejar de lado que esto trae consigo impactos, en todos los ámbitos tanto en lo económico, como incluso en lo comercial. Porque aunque parezca que son ámbitos totalmente distintos impactan indirectamente uno con el otro, en la actualidad esta tendencia se asienta incluso en temas comerciales como en el ámbito de las exportaciones e importaciones.

Esto lo presenciamos con empresas que se dedican  a exportar servicios, incluyendo servicios de ciberseguridad. Este tipo de exportación sin duda alguna es una de las tendencias emergentes pero también uno de los ámbitos con mayor expansión a nivel global.

**Entrevista 3.**

**Alonso Castro Arias.**

Puesto: Lic. Ing. en Sistemas, docente informático e instructor de Cisco:(Dep. Iot, TIC, Ciberseguridad).

Empresa: Cisco Academy, y Colegios Técnicos.

1. **¿Disponemos de suficientes mecanismos de protección? ¿Qué hace falta?**

Respuesta: Considero que hasta el momento tenemos buenos y variados mecanismos de protección en el ámbito de la sociedad civil y la industria. Sin embargo, como docente me doy cuenta de la necesidad en el cambio cultural, de pensamiento y acción por parte de la sociedad en general.

Para explicarme mejor, durante todos los años de educación que recibe un joven se empieza a trabajar diferentes temas informáticos, el contenido que prevalece de principio a fin es el tema preventivo esto quiere decir que se busca concientizar desde jóvenes todo lo

relacionado con la prevención de las tecnologías de la información. Se trabaja con ellos temas de cuidados básicos.

Aunque este tipo de temas también se comparten con la población en general, aún seguimos sufriendo lastimosamente de situaciones que se pudieron prevenir fácilmente con la implementación de buenas prácticas de educación preventiva básica. Lo que nos deja a reflexionar, que la información está llegando a todos o a gran cantidad de ciudadanos, pero todavía son muchos los que prefieren hacer caso omiso de lo que se le educa.

Análisis: En esta respuesta se deja en evidencia cómo el trabajar en la concientización es uno de los puntos importantes, pero además se debe buscar innovación no solo en temas teóricos de concientización, sino que también en las formas de fomentar las buenas prácticas de prevención básicas a las que la ciudadanía tiene acceso para lograr tener mayor efectividad.

2. **¿Qué implicación tiene la ciberseguridad en el desarrollo de nuevos servicios?**

Respuesta: Todos los servicios tecnológicos deben de integrar la ciberseguridad, como ya se ha mencionado es importante este tema porque ningún sector tiene garantizado su seguridad más que la prevención misma y la actualización continúa en este tema.

Análisis: el tema de la ciberseguridad se ve impregnada en todos los ámbitos de servicios tecnológicos. Por lo que las consecuencias dentro del desarrollo de nuevos si no se toma en cuenta la importancia de desarrollar este ámbito puede tener implicaciones fatales. Sin embargo, la implicación de la ciberseguridad en ámbitos de bienes y servicios cada vez va a estar más presentes conforme se desarrolle en el tiempo.

3. **¿Qué tendencias tecnológicas están surgiendo en torno a la ciberseguridad industrial?**

Respuesta: Considero que nuevas tendencias tecnológicas no hay, quizás lo veo bajo una perspectiva diferente. Me explico, considero que son tecnologías ya existentes que han

estado ahí desde hace mucho tiempo pero que hasta ahora se ha logrado tener la adaptación masiva de la sociedad y que por ende se ha logrado implementar dentro del diario vivir incluyendo la industria.

Análisis: Según el alcance que se ha logrado de conocimiento, gracias al desarrollo de esta investigación un dato importante a tener en consideración para las tendencias que surgen a raíz de las nuevas tecnologías, es que cada vez más se crean simuladores que nos permiten identificar las amenazas; por ejemplo: en los dispositivos inteligentes, en los smartmetering, podemos encontrar herramientas existentes que te permiten colocar en una arquitectura una serie de dispositivos inteligentes.

Por otro lado, encontramos simuladores que tienen la capacidad de detectar una serie de amenazas y obtener las medidas que deberías aplicar, porque al no poder aplicar las medidas en el entorno de producción, los simuladores son una de las tendencias que llegan a prestar un espacio para la creación de nuevos instrumentos de seguridad.

4. **¿Qué riesgos no tradicionalespueden aparecer en sectores críticos de un país?**

Respuesta: Esta pregunta me hace transportar mi memoria a diferentes sucesos, que usándolos de ejemplos podemos darle una respuesta a esta cuestionante. Si hablamos de la actualidad podemos recordar lo que pasó hace unos días con el Banco de Costa Rica, donde se filtraron datos personales de los usuarios, para ese caso me tocó realizar una investigación del suceso como estudioso del tema, como profesor aprovechando de lo sucedido se le dio cobertura de lo sucedido para un tema propiamente de aprendizaje.

En esta ocasión uno de los riesgos más claros que se pueden observar al realizarle un análisis a lo sucedido es la importancia y relevancia que tiene la manipulación de datos. Lo que deja en reflexión la importancia del cuidar nuestra información, casos como estos son los que se están volviendo cada día más comunes y esto lo podemos observar en organismos estatales como en el sector privado.

Otro riesgo no tradicional es la minería, que si se plantea de forma escueta puede que no sea inofensiva, pero si hacemos memoria podremos recordar que una de los

diferentes sucesos que ha dado paso a la creación de lo que hoy llamamos ciberseguridad se basa en acciones delictivas detectadas por la minería. El caso expuesto anteriormente también nos puede ayudar como referencia, esto porque a la hora que vulneraron la seguridad del banco se filtró información que si es manipulada inadecuadamente puede resultar con inconvenientes ya que, se mostraban datos como ingresos y flujo de capital de los usuarios.

Estos dos ejemplos de riegos no tradicionales mencionados anteriormente, condicionan a las instituciones la búsqueda de mejoras en la implementación de políticas preventivas. A nivel comercial, una entidad se puede ver afectada de forma directa como se dejó ver anteriormente, pero además de forma colateral se le dan pésimas calificaciones en términos de credibilidad y reputación con sus usuarios.

Análisis: El hecho de que la sociedad se ha vuelto cada vez más informada, hace que tenga cierto nivel de conciencia y por ende mayor responsabilidad de lo que puede pasar con sus datos. Cuando se presentan situaciones como la ejemplificada anteriormente, hace que las personas se pongan automáticamente en alerta y presenten cierto desconforme con la entidad que sufra una violación de vulnerabilidad.

Los Estados y las industrias deben trabajar de la mano para garantizar que los datos personales y sensibles de sus usuarios prevalezcan de forma segura dentro de sus bases de datos. ¿Por qué se sugiere esto? Es simple en la era de la información sabemos que los enfoques del uso de datos debe visualizarse un enfoque innovador para la prevención del posible abuso y mal manejo de datos, ya que, los usuarios al ver que entidades que tienen su información sufren algún cibercrimen va a perder la confianza, y esto puede traer complicaciones para la industria al verse no sólo atacado bajo un crimen sino que además tener que trabajar extra para recuperar la confianza de sus usuarios y la reputación a nivel competitivo dentro del comercio.

**Entrevista 4.**

Jazmín Esquivel Vega.

Puesto: Licenciada en Relaciones Internacionales con énfasis en Comercio Exterior.

1. **¿Qué consecuencias económico-financieras tienen los problemas de ciberseguridad?**

Respuesta: Este es un tema sumamente amplio, tanto que no solo hablamos de servicios y tecnologías, sino que se entrelazan muchísimas áreas, estamos hablando de toda la infraestructura de los países, de la sociedad en general, que estaba acostumbrada y sabía cómo proteger su infraestructura física. Ahora la sociedad y su economía se mueven en esa infraestructura lógica donde hay que dar respuesta y protección a todos los niveles incluyendo el económico y financiera de un país, de una industria, e incluso de toda una sociedad.

Análisis: la tecnología al ser un instrumento que se desarrolla en todos los ámbitos y sectores hace que se vuelva un tema sumamente amplio. Sin embargo, existen antecedentes de sucesos que se han presentado cuando no se han establecido las medidas de seguridad necesarias dentro de estos ámbitos.

Un claro ejemplo fue el caso de niños que han vulnerado la seguridad fácilmente de instituciones bancarias, incluso el caso del niño que ingresó con las instrucciones de un manual a un cajero automático. O bien el caso del niño que en base a una comisión minúscula de centavo por retiro de dinero, logró desviarlo a la cuenta de su madre obteniendo en segundos cantidades desorbitadas de dinero.

Todos estos ejemplos dejan en evidencia los peligros a los que se enfrentan en el ámbito económico, financiero de una institución y las vulnerabilidades en las que se deben trabajar para fomentar el fortalecimiento de las infraestructuras actuales en las que la era digital predomina.

2. **¿Cuáles son los efectos de la aplicación de estas posturas?**

Respuesta: Pienso que en este ámbito se llega a centrar más en el aspecto de la seguridad nacional, y se deja de lado el ámbito comercial. Principalmente dentro de este enfoque de seguridad nacional podemos ver como la recopilación de datos en especial los datos sensibles son los más buscados por los ciberdelincuentes.

Considero que hay grandes vacíos legales en materia de seguridad nacional y comercio en general. Ya que, todavía vemos como no existen pautas claras en seguridad cibernética y protección de datos. Claro está, que cuando se implementen todas estas estrategias, y se busque rellenar todos estos vacíos legales debe coexistir con el principio de legalidad, esto quiere decir que el Estado debe asegurar la información y proteger los datos, pero no puede hacer uso de ellos, por el mismo principio que lo resguarda.

Análisis: en este apartado existe una discordancia con la experta, ya que, por el contrario, se considera que en las diferentes posturas que brinda las aplicaciones de la ciberseguridad entran dentro del ámbito de seguridad nacional, pero además en gran medida se evidencia la presencia en el comercio. Ya que es uno los lugares con más frecuencia de la industria que presentan acceso ilegal por parte de criminales cibernéticos.

Sin duda alguna, aún existen muchos vacíos legales en temas de seguridad nacional, pero también en la seguridad de entes público/privado en igualdad de medida.

3. **¿Disponemos de suficientes mecanismos de protección? ¿Qué hace falta?**

Respuesta: En el tema propiamente de los Estados se debe seguir trabajando en buscar sus mejoras, en el tema de comercio como las aduanas, o empresas algunas de ellas no cuentan con mecanismos suficientes por tener un tema de confianza, y hasta que no se dé un ataque a lo macro, es muy probable que se siga omitiendo estos puntos.

Análisis: el tema legislativo sigue presentando déficit en las políticas de desarrollo de seguridad en el ciberespacio y en cada uno de sus posibles alcances. En el sector comercial y empresarial deben de tener en cuenta que son focos importantes para el cibercrimen, por lo cual tienen una razón y peso extra para implementar sus protocolos de prevención posibles para evitar ser vulnerados.

4. **¿En qué medida no atender la ciberseguridad adecuadamente tiene riesgo para la evolución económica de un país y su desarrollo industrial?**

Respuesta: Si las industrias y los Estados no toman las medidas necesarias para su protección otros sectores pueden sufrir daños colaterales, por ejemplo el comercio naranja.

Si no se atienden los vacíos legales podemos ver afectados sectores comerciales en áreas como las exportaciones, logística de envíos.

Ya se han presenciado diferentes ciberataques que se le han realizado a grandes corporaciones como redes sociales donde se logró visualizar que un ataque puede lograr paralizar las comunicaciones a nivel global. Un claro ejemplo de afectación en el comercio lo pudimos vivir con el tema de la pandemia actual del COVID-19. Ahora bien si este mismo ejemplo lo situamos a un ataque cibernético en una empresa de logística y envíos podríamos experimentar un parálisis en el comercio casi igual al que hemos presenciado en estos tiempos.

Análisis: Los diferentes ciberataques que se han presentado a lo largo del tiempo, ha demostrado que el hecho de no atender temas de ciberseguridad puede traer consigo consecuencias primeramente de inestabilidad estructural en un país, el robo de datos, el bloqueo económico dentro de la industria, o incluso temas de jurisprudencia es el desenlace que puede tener una nación.

Tenemos que tener en cuenta que un Estado tendrá implicaciones tanto nacionales donde sus ciudadanos pueden recibir daños colaterales como el ejemplo de Estambul cuando un ataque cibernético dejó al país desconectado por días dando problemas en diferentes actividades en la que las ciudades se vieron afectados.

En las implicaciones internacionales se puede experimentar desconfianza, y la inversión extranjera no realizará inversiones comerciales, provocando así déficit en el desarrollo económico y financiero del país.

5. **¿Cuáles factores han posicionado a los Estados Unidos como principal estratega en temas de seguridad aplicada?**

Respuesta: Estados Unidos ha desarrollado tecnologías industriales innovadoras ya que se ha posicionado específicamente en el estado de California como cuna de la innovación, otro elemento importante es que esta nación permite fomentar la innovación principalmente en los jóvenes para el desarrollo de sus ideas innovadoras.

Análisis: Todo lo que vamos a exponer a continuación se fundamenta en el importante auge de la digitalización de cualquier ámbito o sector de actividad y todo este

auge implica mayor grado de exposición de la información y de los datos. Por consiguiente, van a existir numerosas oportunidades de negocios en ciberseguridad.

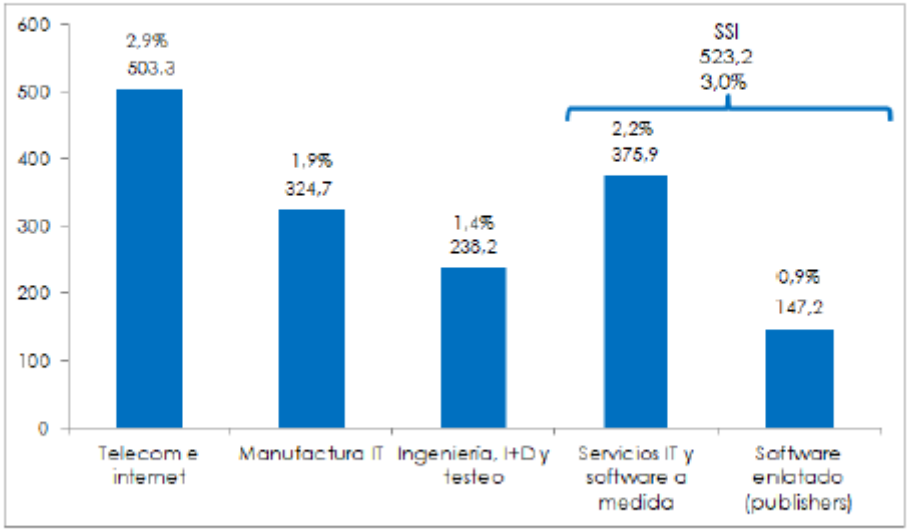
### 4.2. Analizar el impacto comercial de las estrategias de ciberseguridad estadounidense en el mercado global.

Para nadie es un secreto que los Estados Unidos están posicionados como la mayor economía del mundo, y es uno de los actores más relevantes a nivel internacional. Además, posee un Producto Interno Bruto (PIB) global de 24,3% y contiene una población de 326 millones de habitantes con ingreso per cápita de aproximadamente $60 mil anuales. Además es uno de los líderes en el ranking del comercio internacional de servicios.

Al igual que en la mayoría de los países desarrollados, en EEUU los servicios son el sector más relevante en la producción y el empleo representan aproximadamente 80% del PIB, el empleo y las inversiones directas en el exterior, casi 60% de las exportaciones medidas en valor agregado y la inversión extranjera directa y 45% del valor agregado importado (OECD, 2017).

Gráfico #1.

**Gráfico 1. EEUU: Producto bruto del sector tecnológico**
Valor en miles de millones de USD y contribución al PIB estadounidense en porcentaje, 2017




Fuente: Elaboración propia con datos de CompTIA (2018).

Fuente: Software y servicios de informática Estados Unidos (2018).

Por esta misma razón Estados Unidos es uno de los países que impulsa la innovación tecnológica, y fomenta en los jóvenes la creación creativa de ideas innovadoras en el tema tecnológico, lo que volvió a este país líder en esta industria. Uno de los sectores más grandes dentro de la industria tecnológica es la tecnología de la información (IT) y por lo que el Departamento de Comercio de Estados Unidos indica que este país se posiciona en el cuarto nivel del mercado mundial de IT.

La economía de la seguridad informática estudia los aspectos económicos de la privacidad y la seguridad en cómputo e información. La economía de seguridad informática busca comprender las decisiones y comportamientos individuales u organizacionales con respecto a la seguridad y la privacidad como decisiones de mercado. El reto es asignar estratégicamente los recursos para cada equipo de seguridad y bienes que intervengan, basándose en el impacto potencial para el negocio, respecto a los diversos incidentes que se deben resolver. (Sánchez Montañés, pág.105, s.f)

Por esta razón, Estados Unidos se ha sabido posicionar como uno de los países con mejores estrategias de ciberseguridad cubriendo la mayoría de los sectores. Esto hace que Estados Unidos sea una industria líder no solo en la implementación de estrategias, sino, que también en la industria de las tecnologías de la información esto tanto por el tamaño del sector como sus desarrollos tecnológicos, observemos la tabla a continuación.

Tabla # 1

*D. Comparación de Estrategias Nacionales de Ciberseguridad*

| | BLOQUE GEOPOLITICO | ANGLOSAJON | | | UNION EUROPEA | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PAIS | CAN | ENG | USA | ALE | FRA | ESP | EST | JPN | RUS |
| PROTECCIÓN | Infraestructuras criticas | X | X | X | X | X | X | X | X | X |
| | Economía | | X | X | X | | X | | X | |
| | Seguridad Nacional | X | X | X | X | X | X | | X | |
| | Bienestar social | X | X | X | X | | | X | X | X |
| ENFOQUE | Concientización | X | X | X | | | | X | | |
| | Conocimiento | | X | X | | | | | | X |
| | Educación | | X | X | | | | X | | |
| | Capacidades cibernéticas militares | | X | X | X | X | | | | X |
| SECTOR PUBLICO | Liderazgo | X | X | X | X | X | X | X | X | |
| | Marco jurídico | | X | X | X | X | | | X | X |
| SECTOR PRIVADO | Participación en la estrategia | X | X | X | | X | X | X | X | X |
| COOPERACION INTERNACIONAL | Cooperación en su grupo | X | | X | X | X | X | | | |
| | Cooperación con otros países | X | X | X | X | X | X | X | X | X |

Fuente: Leiva E. (2015).

Este cuadro permite analizar de forma comparativa el registro de cada uno de los países en el desarrollo de las estrategias implementadas en cada una de las diferentes áreas. Por tanto la primera impresión que se puede observar es que, los Estados Unidos, Inglaterra, e incluso Alemania tiene las estrategias nacionales de ciberseguridad más completas de la tabla.

Otro punto importante a observar es que Estados Unidos e Inglaterra disponen de un importante papel dentro del sector privado como parte de sus estrategias, mientras que en

comparación con Alemania este último pone mayor énfasis en el sector público, además de ocupar desarrollo en el marco legislativo regulatorio.

Y por último pero no menos importante, podemos observar un comportamiento usual de alineación, y dentro del ciberespacio no es la excepción que adopte esta misma característica de alineación de acuerdo a sus bloques geopolíticos.

Por esta razón, a lo largo de las implementaciones de las Estrategias Nacionales de Ciberseguridad (ENCS) de EE.UU se describen un conjunto de actividades basadas en un modelo de colaboración entre el Gobierno, los socios internacionales y el sector privado:

> • Economía: promover las normas internacionales y la innovación (los mercados abiertos).
> • La protección de la infraestructura crítica: fortalecimiento de la seguridad, la confiabilidad y flexibilidad.
> • Marco legal: extender la colaboración y el Estado de derecho.
> • Capacidades cibernéticas militares: preparación para los retos de seguridad.
> • Desarrollo internacional: creación de capacidad, seguridad y prosperidad.
> • Bienestar social: apoyo de las libertades fundamentales y de la privacidad.
> (Leiva E. pág.4, 2015)

Debe ser primordial establecer normas internacionales que velen no solo por el desarrollo económico, sino que además vaya de la mano con la seguridad nacional. Y el resguardo en todos sus ámbitos comercial, económico, social y gubernamental.

Para determinar el establecimiento de prioridades, el sistema de gestión de incidentes necesita saber el valor de los sistemas de información que pueden ser potencialmente afectados por incidentes de seguridad. Esto puede implicar que alguien dentro de la organización asigne un valor monetario a cada equipo y un archivo en la red o asignar un valor relativo a cada sistema y la información sobre ella.

Dentro de los valores para el sistema se pueden distinguir: confidencialidad de la información, la integridad (aplicaciones e información) y finalmente la disponibilidad del sistema. Cada uno de estos valores es un sistema independiente del negocio, supongamos el

siguiente ejemplo, un servidor web público puede poseer la característica de confidencialidad baja (ya que toda la información es pública) pero necesita alta disponibilidad e integridad, para poder ser confiable. (Sánchez Montañés, pág.105, s.f).

Dada esta circunstancia, los Estados deben plantearse en sus estrategias de seguridad el desarrollo de la confiabilidad y ciberseguridad, que permita al Estado tener un respaldo para él y para las organizaciones participantes de su economía, así como a su sociedad civil.

### 4.2.1. Dónde poner énfasis.

Como se ha mencionado anteriormente, como es de conocimiento el tema de la tecnología llegó para quedarse y aún mejor para expandirse, evolucionar y generar nuevas tendencias en el mercado global con las nuevas tecnologías. Por esta razón se ha puesto énfasis en el tema de la exportación de bienes y servicios tecnológicos y se centra la vista en Estados Unidos ya que es una potencia que se mantiene con bastante movimiento en este tema.

Una agrupación de empresas y ONG estadounidenses ha presentado sus observaciones al Departamento de Comercio de Estados Unidos, con respecto de una propuesta que busca limitar las ventas internacionales de productos y tecnologías de seguridad cibernética a todos los países del mundo, a excepción de Canadá. La intención de Washington es reducir la propagación de software que pueda ser utilizado con fines hostiles contra Estados Unidos. Sin embargo, Cisco aduce que la misma tecnología es utilizada en investigación científica de ciberseguridad, con el fin de prevenir ataques. Según (Cisco, pf.2, 2021)

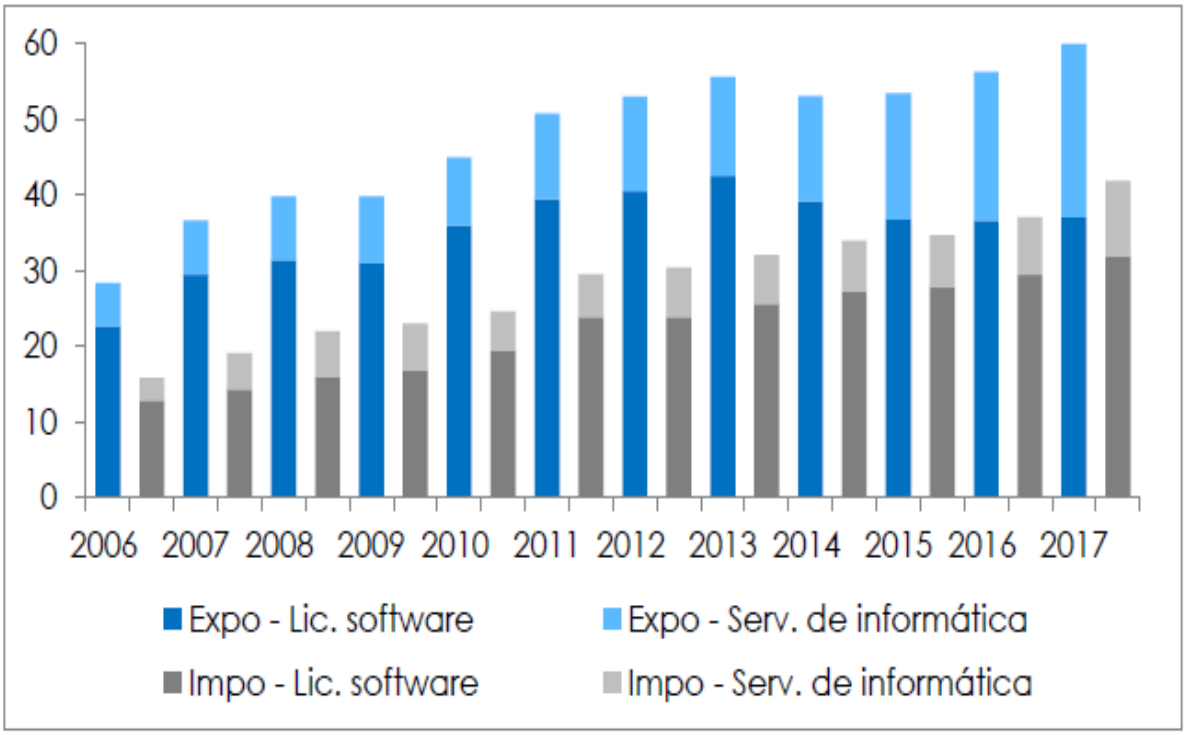
Dentro de la administración del señor expresidente Barack Obama, se planteó la necesidad de realizar protección de la privacidad, restringiendo así las exportaciones de alta tecnología diseñada para la detección y sabotaje informático. Sin embargo muchas de las oposiciones que se presenta remarcan la importancia que tiene este tipo de tecnologías tanto en modo de estudio así como su forma de mantener al alcance las herramientas necesarias e

igualdad de condiciones ante un posible ataque, por esta razón se deja ver por medio del siguiente gráfico la importancia que representan las exportaciones comerciales en servicios de ciberseguridad dentro del comercio internacional Estadounidense.

Gráfico #2

**Gráfico 14. EEUU: Comercio internacional de SSI**

Miles de millones de USD




Fuente: Elaboración propia con datos de BEA.

Fuente: Comercio de bienes y servicios entre la Unión Europea y Estados Unidos, con datos de la Oficina de Análisis Económicos de EEUU (BEA).

Según el grafico anterior de Bureau of EconomicAnalysis (BEA), y según investigaciones de la Organización Mundial del Comercio (OMC), nos indica que Estados Unidos tiene un 29% de las exportaciones estadounidenses corresponden a licencias y distribución de *software* al exterior. Además se tienen registros de los servicios

informáticos donde Estados Unidos es el segundo exportador en esta área después de la India.

Por consiguiente, las exportaciones estadounidenses se expandieron el 64% durante la última década, impulsada principalmente por las ventas de servicios informática que según el gráfico anterior, lograron alcanzar los $23 mil millones USD en el 2017. Lo que provocó realizar una facturación al exterior que llegó a sumar aproximadamente $37 mil millones USD. Por otro lado, en el área de servicios rondan aproximadamente los $10 mil millones, como se muestra en el gráfico 1.

De acuerdo con toda la información brindada por BEA, los principales socios comerciales de los Estados Unidos son: La Unión Europea (UE), y los países Asiáticos Asia-Pacífico para ser más exactos. Una tabla Elaborada con los datos de la BEA, nos deja mostrar los principales países socios y además nos brinda información del valor y porcentaje de participación.

Tabla #2

**Cuadro 3. EEUU: Exportaciones de software y servicios de informática, principales destinos**

Valores en millones de USD y participaciones en porcentaje – Datos de 2017

| Origen | Serv. informática | | Licencias software | | Total | |
|---|---|---|---|---|---|---|
| | Valor | Particip. | Valor | Particip. | Valor | Particip. |
| **Total** | **22.941** | **100,0%** | **37.081** | **100,0%** | **60.022** | **100,0%** |
| **Unión Europea** | **7.313** | **31,9%** | **16.239** | **43,8%** | **23.552** | **39,2%** |
| Irlanda | 426 | 1,9% | 8.747 | 23,6% | 9.173 | 15,3% |
| R. Unido | 3.086 | 13,5% | 1.818 | 4,9% | 4.904 | 8,2% |
| Alemania | 1.036 | 4,5% | 2.494 | 6,7% | 3.530 | 5,9% |
| Resto UE | 2.765 | 12,1% | 3.180 | 8,6% | 5.945 | 9,9% |
| **Asia Pacífico** | **6.919** | **30,2%** | **12.058** | **32,5%** | **18.977** | **31,6%** |
| Japón | 1.764 | 7,7% | 2.135 | 5,8% | 3.899 | 6,5% |
| Corea | 710 | 3,1% | 1.960 | 5,3% | 2.670 | 4,4% |
| Resto Asia Pacífico | 4.445 | 19,4% | 7.963 | 21,5% | 12.408 | 20,7% |
| América Latina y Caribe | 2.957 | 12,9% | 4.788 | 12,9% | 7.745 | 12,9% |
| Canadá | 2.807 | 12,2% | 2.084 | 5,6% | 4.891 | 8,1% |
| Resto del mundo | 2.945 | 12,8% | 1.912 | 5,2% | 4.857 | 8,1% |

Fuente: Elaboración propia con datos de BEA.

Fuente: Comercio de bienes y servicios en la Unión Europea, Asia Pacifico, Canadá, América Latina y Caribe, con datos de la oficina de análisis económicos de EEUU (BEA).

Una de las curiosidades que nos brinda esta recolección de información es que, este país cuenta con un esquema tributario que se vuelve favorable para el sector. Aquí vemos como los servicios de informática y las ventas se llegan a diversificar entre los diferentes destinos.

En los últimos datos se podrá observar que América Latina y el Caribe absorben el 12,9% de las exportaciones y proveen apenas el 3,5% de las importaciones. Un dato importante que resaltar es que, dentro de los proveedores más importantes son México y

Brasil. Una curiosidad en este tema es que seguido de estos países con un poco inferior se encuentran los países de Argentina, Costa Rica, y Colombia.

Hay que tener en cuenta que al tratarse de datos reportados por Bureau of EconomicAnalysis, contienen limitaciones en comparación con las fuentes privadas de las economías de la región informan como exportaciones al mercado estadounidense; principalmente estas limitaciones se encuentran en la información detallada por país. Continuando con el análisis, el mercado estadounidense mantiene una dinámica abierta en comparación con otros países, sus servicios de informática tienen gran acceso al mercado global.

Tal como sucede en otros sectores, las principales barreras corresponden a la provisión de servicios por modo 4 (cuando las personas físicas viajan para prestar el servicio *in situ* de manera temporal). Existen limitaciones a la cantidad de proveedores contractuales e independientes que pueden ingresar anualmente y se requiere paridad salarial con los empleados locales. El período de permanencia puede ser de hasta 36 meses, superior al de otros países desarrollados. (OECD, 2017).

Estados Unidos maneja un rubro de compromiso establecido en el Acuerdo General sobre Comercio de Servicios (GATS, siglas en inglés) de la Organización Mundial del Comercio, específicamente para los servicios de informática. En este acuerdo Estados Unidos debe asumir algunos compromisos establecidos en el acuerdo, entre ellos las limitaciones, transacciones, proveedores de servicios y la participación capital del extranjero, entre otros puntos.

La provisión de servicios al Gobierno está limitada a los oferentes de países que integran el Acuerdo sobre Contratación Pública (ACP) de la OMC y a los de aquellas economías con las cuales Estados Unidos cuenta con acuerdos comerciales con provisiones de compras gubernamentales (OECD, 2017). Si bien no todos estos acuerdos tienen el mismo alcance, hay compromisos que permiten la provisión de algún tipo de servicio de informática y/o software a distintas entidades gubernamentales con Australia, Brunei, Canadá, Chile, Colombia, Corea del Sur, Costa Rica, El Salvador, Guatemala, Honduras,

Israel, Marruecos, México, Nicaragua, Omán, Panamá, Perú, República Dominicana y Singapur.

En las últimas décadas, la evolución continúa de las nuevas tecnologías, así como servicios electrónicos y las redes de comunicación se han implementado cada vez más en nuestra vida diaria, por los cual es difícil visualizarse sin ella, convirtiéndose indispensable en la actualidad. Por esta razón, es que los países buscan no quedar rezagados y han logrado integrar el desarrollo e implementación en el ámbito comercial, la exportación de servicios tecnológicos. Por esto, es que se vuelve un tema influyente dentro de la sociedad para identificar y darle seguimiento a este tipo de información brindando así un mayor desarrollo y diversificación comercial.

El acceso a las nuevas tecnologías es una herramienta fundamental, que es necesaria para el avance en la disminución de la brecha digital. Todo esto demuestra que ha trabajado arduamente en el abordaje de esta problemática, con el objetivo de disponer cada día de información que sea confiable, y actualizada en la disminución de los desafíos que presenta la brecha tecnológica dentro del desarrollo de un país.

Una de las principales relaciones que se dan con la brecha digital, se le atribuye a la ubicación geográfica ya que, este elemento es determinante para el acceso que pueda tener las Tecnologías de la Información y Comunicación. Por lo tanto, es común ver que las TIC se lleguen a concentrar principalmente, e incluso zonas centrales y este mismo acceso disminuye en las zonas rurales.

Se debe tener en cuenta que la centralización de la población en zonas centrales genera mayor acceso a la actividad económica, y además a un mejor acceso de la mano de obra profesional y técnica, lo que permite a su vez mayor oferta de servicios y productos incluyendo las TIC. Además, las instituciones públicas, privadas, y la calidad del servicio resultan ser mejores que en los territorios rurales.

Todos estos aspectos logran atraer más la centralización de servicios como la parte tecnológica, productiva, educativa y económica del país.

Entre 2016 y 2020 los puntajes de madurez para la "legislación sobre delitos cibernéticos sustantivos" no progresaron, posiblemente porque ese aspecto ya tiene el puntaje promedio más alto de toda la región. Este avance en la legislación sustantiva se ha complementado cada vez más con el progreso en la "legislación procesal del delito cibernético", que es el aspecto legal que ha registrado la mayor actividad en el período desde 2015. (Oxford, pág. 22, 2020)

Es importante mencionar que si bien es cierto, se debe poner énfasis principalmente en el auge que se está presentando en las exportaciones comerciales de servicio, por lo que no se puede dejar de lado el tema de la seguridad y la implementación de estrategias propias para su resguardo. Por esta razón, es importante darle un vistazo en esta área ya que, va de la mano con el desarrollo de las nuevas tecnologías y la innovación.

La ciberseguridad es crítica para nuestra prosperidad y seguridad. Las actividades cibernéticas maliciosas no solo amenazan las economías, sino también el funcionamiento mismo de nuestras democracias, libertades y valores. Nuestra seguridad futura depende de que sepamos transformar la capacidad para protegernos contra las amenazas cibernéticas: tanto la infraestructura civil como la capacidad militar dependen de sistemas digitales seguros. (PawelHerczynski, pág.24)

Se dice que las estrategias nacionales de ciberseguridad llegan a definir una estructura en términos de sistemas de la información y redes, esto se da porque en caso de fallos dentro de unos sistemas informáticos puede presentar impactos en áreas sensibles como la salud, la economía y el bienestar ciudadano civil, la industria en general, y Gobierno. Por esta misma razón, se debe trabajar en generar políticas que respalden la mayoría de los sectores.

Para realizar evaluaciones de manera efectivas, se debe mostrar la postura del país en materia de ciberseguridad. De manera que donde se pueda realizar un análisis detallado y comparativo de datos esenciales que permita mostrar la evolución en la que se ha desarrollado un país en los últimos años. Esta recolección de datos para su consulta deben ser materiales oficiales, así como documentos de entidades en colaboración del sector público, privado y la sociedad civil, esto para tener un enfoque integral.

Primeramente, hay que indicar que un país con seguridad cibernética permite la creación y generación de confianza a sus usuarios, el fomento de confianza en el ecosistema de la transformación digital a nivel nacional, de manera que llega a tener respaldo legal en materia de derechos e intereses de los usuarios y que además garantiza la seguridad de sus datos en el desarrollo de los sistemas, se vuelve un tema fundamental que abre paso al aprovechamiento potencial de las oportunidades que se llegan a brindar en temas sociales, políticos y económicos que ofrecen gracias a la implementación de regulaciones que le brindan respaldo a las tecnologías de información y comunicación.

Posteriormente, gracias al fomento y desarrollo de regulaciones los Estados contarán con mayor desarrollo tecnológicos y por ende el país obtendrá buena calificación a nivel internacional en las evaluaciones, y esto le genera buena reputación a nivel internacional. Esto le permite obtener mayor atracción en la inversión comercial y la economía digital se fomenta de forma efectiva. Por lo que mantener este progreso es fundamental para el país, ya que al existir mayor atracción de la inversión comercial, esto contribuye a la creación de nuevos empleos, dato importante para el desarrollo interno de un país.

Sin dejar de lado las regulaciones en materia de gobierno electrónico y firma digital, todos estos esfuerzos brindan mayor transparencia, seguridad y respaldo para el desarrollo de actividades y su debida legitimidad. Temas como la adhesión al Convenio de Budapest, e incluso de otros convenios que desarrollan estrategias nacionales contra la lucha del ciberdelito hace que logremos tener la posición líder en la que nos encontramos a nivel global.

En el tema de tecnologías y estandarización, se observa que se ha mantenido durante el tiempo la misma cantidad en el desarrollo de estos temas. Sin embargo, se refleja cómo se ha implementado la creación en temas específicos donde no existían precedentes. Mientras que en otros se ha mantenido al margen no hay ni avance ni retrocesos. Estos son los temas en los que se deben buscar las mejoras para equilibrar el desarrollo de forma uniforme y continua.

Es importante mejorar el desarrollo de la formación profesional, ya que al tener buena legislación nos da estabilidad en el desarrollo comercial y económico del país por lo que, este ámbito debe de ser explotado de la mejor manera para la atracción de nuevas inversiones.Además, si se trabaja en la mejora de estos índices, adicionalmente, se podría brindar mayores servicios de mano de obra especializada que permita atraer mayor posicionamiento del mercado, apertura de la innovación y la creación de nuevas tendencias tecnológicas.

Dentro de la cultura cibernética en este tema no se ha quedado atrás, ha obtenido un avance significativo a lo largo del tiempo. Se ha logrado avanzar en términos de ciberseguridad y adaptación que ha tenido los diferentes sectores que se integran dentro de la sociedad.

La adopción de políticas, procesos y medidas a escala nacional que aporten seguridad a los servicios esenciales que se prestan al ciudadano como el gobierno electrónico, el comercio electrónico y las transacciones financieras digitales, entre otros) basados en las tecnologías de la información y la comunicación. Este tipo de acciones instauró el principio de confianza no solo entre la población en general, sino también dentro de las organizaciones públicas y privadas que ofrecen sus servicios basados en las TIC a los ciudadanos.

**Ciberseguridad en los tratados internacionales de EEUU**

El internet ha llegado a revolucionar todos los aspectos de desarrollo humano. Por lo que, las regulaciones del comercio internacional para llegar a establecer una forma de ordenamiento general y específico dentro del desarrollo de las exportaciones comerciales principalmente de los Estados Unidos en términos de ciberseguridad.

Pasando ahora al contexto específico, si se considera que la mayoría de las economías desarrolladas y en desarrollo tienen leyes y regulaciones que restringen la inversión extranjera directa, sobre la base de preocupaciones relacionadas con la seguridad nacional o la pérdida de los recursos naturales de los países, ¿cuál sería el equivalente para desarrollar protecciones en el ciberespacio? Según (Anahiby Becerril, pág.20, 2019)

Las preocupaciones en torno a la ciberseguridad y las políticas comerciales se han hecho presente en los últimos años. Dado su carácter transnacional en las transacciones comerciales, este se ha posicionado dentro de las TICs.

La seguridad económica trata el comercio, la producción y las finanzas (Albert y Buzan, 2011). Hay que tener en cuenta que los Estados desarrollados como Estados Unidos, y los que se encuentran en proceso de desarrollo, su mayor preocupación se basa en la posibilidades de robo de IP que puedan ser utilizados para el espionaje económico. Ya que, se puede volver un peligro para su desarrollo económico y comercial.

**Comercio electrónico.**

El comercio electrónico es definido como la compra y venta de productos o servicios, exclusivamente a través de canales electrónicos. Existen tres ramas principales del comercio electrónico, la forma más conocida es la compra en línea, también conocida como negocio a consumidor (B2C). Aquí, los individuos pueden ordenar diversos productos y pagar por su compra en internet. Según (Karen Sigmond, pág.3 ,2018)

El comercio electrónico es la nueva economía global, y digital que se va realizando en tiempo real, sin la necesidad de sobre pasar ningún tipo de fronteras geopolíticas del comercio tradicional. El desarrollo del comercio dentro de la interacción del ciberespacio

Para la Organización Mundial del Comercio (OMC), el Ecommerce o comercio electrónico constituye «la producción, distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos». Mientras que para la OCDE esta modalidad de comercio constituye «la venta o compra de bienes o servicios, realizada por computadora redes por métodos diseñados específicamente para recibir o colocar pedidos» (2013).

Según las definiciones anteriores se logra visualizar la importancia que llega a posicionar el comercio electrónico en todas las aristas incluyendo así las transacciones electrónicas, las transferencias de pagos y movilidad de fondos que puedan existir. Conforme avanzan los años, la economía mundial se conecta y digitaliza por lo que se busca de este modo la implementación responsable del comercio electrónico.

En 1996, para cumplir con su labor de establecer relaciones económicas internacionales amistosas, la Comisión de Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), publicó la Ley Modelo sobre Comercio Electrónico, con la Guía para su Incorporación en el Derecho Interno. Según (Anahiby Becerril, pág.10, 2019)

Bajo esta primicia, se destaca que el comercio electrónico amplía su visión más allá de lo tradicional y los pago en papel trasladándose así hacia un ámbito cada vez más amplio. Incluyendo así todo método de pago bajo transacciones comerciales realizadas por medios electrónicos o digitales que surgen a través de un mundo cada vez más globalizado, donde el comercio de bienes, productos y servicios tiene una gran variación de su misma exposición a través de mercados cada vez más virtuales.

La economía que se lleva a cabo dentro del ciberespacio agrupa a las empresas en grandes redes de relaciones de interdependencia, en cuyo seno comparten actividades e intereses (Rifkin, s.p, 2013). La industria se ha desarrollado principalmente dentro de las empresas de carácter técnico-científica y las famosas transnacionales. Que en la actualidad no solo se han llegado a posicionar sino que también se han tenido que ir adaptando a las diferentes circunstancias y a sus entornos cada vez más digitales.

El comercio electrónico es cada vez más relevante para la economía y la seguridad nacional de los Estados Unidos por la relación tan estrecha que tiene con la ciberseguridad y las barreras que estas representan para el comercio internacional y las inversiones.

Una barrera relacionada con la ciberseguridad para el comercio internacional y la inversión se define como «cualquier problema relacionado con los riesgos de seguridad reales y percibidos en el entorno cibernético que obstaculiza directa o indirectamente el crecimiento del comercio internacional y la inversión» (Kshetri, s.p. 2016).

Por lo que, con la finalidad de lograr establecer las bases de crecimiento comercial y económico se llega a establecer Tratados de Libre Comercio de América del Norte

(TLCAN), buscando así la prosperidad entre los países firmantes. Buscando así salvaguarda el ciberespacio, el cual es de carácter común y global. Por esta razón, se propuso el añadir el capítulo 19 dentro de este tratado, donde básicamente lo que busca es integrar temas digitales como lo es el comercio digital, principios de acceso, ciberseguridad, el uso del internet, protección de datos personales, e información por medios electrónicos. Por otro lado, todo lo referente al tema de ciberseguridad se está desarrollando bajo el enfoque de la cooperación internacional.

En el T-MEC:

Según En el artículo 19.15 referente a la ciberseguridad, el compromiso entre los tres países se enfocará también al desarrollo de capacidades de las entidades responsables de la respuesta a incidentes de ciberseguridad.Las partes contratantes se comprometen al desarrollo de capacidades de las entidades nacionales responsables de la respuesta a incidentes de seguridad informática, así como a emplear los mecanismos de colaboración para la identificación y mitigación de intrusiones maliciosas o la diseminación de códigos maliciosos que afecten las redes electrónicas de las partes (artículo 14.16).

Con estos artículos se busca establecer y además fortalecer toda el área de cooperación entre los países involucrados esto para brindar el desarrollo y las capacidades necesarias para conformar entidades que sean responsables dentro del ciberespacio y el respaldo de la ciberseguridad.

Respecto del comercio electrónico, se debe buscar que una estrategia de ciberseguridad no se convierta en obstáculo o barrera para estas transacciones electrónicas. Es decir, así como existen barreras comerciales, las cuales constituyen restricciones impuestas al libre flujo de comercio e inversión, una barrera relacionada con la ciberseguridad para el comercio internacional y la inversión se define como «cualquier problema relacionado con los riesgos de seguridad reales y percibidos en el entorno cibernético que obstaculiza directa o indirectamente el crecimiento del comercio internacional y la inversión» (Kshetri, pag.16, 2016).

Para los países miembros de TLCAN es importante el desarrollo e implementación de estas buenas practicas ya que, garantizan que los gobiernos y las organizaciones tengan una alta conciencia en la prevención de los ciberataques. Estableciendo así la prioridad e importancia que representan la ciberseguridad como método de protección y prevención dentro de sus agendas.

La industria TI de Estados Unidos también ve con optimismo este proceso. En un posicionamiento enviado a El Economista**,** el director de la Asociación de Tecnología de Consumo (CTA), Gary Shapiro, comentó: La renegociación del TLCAN ofrecen a la Administración Trump una oportunidad notable: la oportunidad de construir un acuerdo comercial modernizado que promueva las tecnologías y los empleos del futuro y ayude a asegurar el liderazgo global de Estados Unidos en las próximas décadas. Según (Sánchez Onofre, paf.4 ,2017)

En el caso de los Estados Unidos, las estructuras y capacidades que este país ha lgrado a través de los años en los temas propiamente de ciberseguridad han sido incomparables con los demás países, ya que, este país ha modernizado sus tratados en virtud de mejorar el auge de sus nuevas tecnologías y ha demás ha brindado la importancia debida al ciberespacio. Del mismo modo que ha incluido las diferentes propuestas en la elaboración y desarrollo gubernamental que llegaron a marcar sus políticas en la aprobación de estrategias en temas de seguridad nacional en el ciberespacio.

La Asociación de la Industria de la Tecnología Informática de Estados Unidos (CompTIA), que agrupa a 2,000 empresas, considera que la modernización del acuerdo comercial de 23 años de antigüedad debe mejorar las relaciones comerciales clave de Estados Unidos con dos de los principales socios comerciales de la industria, México y Canadá. Cuando se negoció el TLCAN, las empresas de tecnología de los Estados Unidos se beneficiaron de reducciones arancelarias, fuertes derechos de propiedad intelectual, normas de concesión de licencias, protecciones de patentes y normas preferenciales de origen. Según (Sánchez Onofre, paf.6 ,2017)

Además de los pilares básicos comunes que se presentan dentro de un Tratado de Libre Comercio, El TLCAN, los países miembros designaron como un objetivo de gran relevancia para sus agendas la implementación, el desarrollo de la mano con la modernización de disponer de normas comerciales que busquen la mejora de las relaciones comerciales entre los países de Norte América.

Brindando así beneficios de carácter mutuo, y que a su vez logren permitir brindar un antecedente que sirva de ejemplo para los demás Estados en la preparación adecuada de estrategias que abarquen el impacto de las nuevas tecnologías en las relaciones comerciales como un aliado más en temas de cooperación internacional en todos sus ámbitos, siendo así una esfera de trabajo integrado que permita el avance continuo de las naciones en su avance y crecimiento de forma eficaz y armónico.

# CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

En este apartado se desarrolla la conclusión de cada objetivo y las recomendaciones de la investigación, sobre las estrategias de ciberseguridad, empezando desde sus orígenes de la creación de la ciberseguridad como necesidad de seguridad nacional. Además de las consecuencias de las aplicaciones de estas estrategias, así como la importancia de la participación de los organismos internacionales y los diferentes actores involucrados.

## 5.1.CONCLUSIONES

La presente investigación se ha centrado en el análisis de la implementación y desarrollo de estrategias de ciberseguridad y el impacto que estas muestran en el ámbito comercial como el caso de las exportaciones. La globalización de las nuevas tecnologías y el alcance que estas tienen dentro de los diferentes sectores se vuelve un tema dinámico y apetecible para muchos fines no siempre de carácter innovador y lícito.

A nivel global se puede decir que cada nación aborda de manera específica el tema de la ciberseguridad, dependiendo de las variantes a las que se enfrenta su país, algunas de estas variantes se encuentran en sectores como la economía, política y cultura en la que se desarrollen.

La tercera e incluso cuarta revolución tecnológica, llegó para quedarse y para evolucionar abriendo así un sinfín de oportunidades sin precedentes para la humanidad. Este nuevo escenario que brinda miles de propuestas conceptuales, llegan a modificar los elementos tradicionalmente conocidos dentro de la historia, brinda un auge de las innovaciones tecnológicas.

Naturalmente, el precedente histórico de la creación de la ciberseguridad se basa en sucesos de vulnerabilidades propiamente filtradas, hechos que llevaron a que se produjera una resistencia a esta invasión, una contraparte que se enfocará en mantener la seguridad aun cuando se hable en un ámbito intangible como lo es el ciberespacio, y como consecuencia la búsqueda de implementar medidas necesarias para la prevención y el abordaje de situaciones próximas de carácter similar.

Estos sucesos de cibercrímenes han brindado nuevas oportunidades a los diferentes actores del sistema internacional, para posicionar su vista en la ejecución de estrategias regulatorias que busquen de esta forma hacer frente a los próximos desafíos que traigan consigo las nuevas tendencias tecnológicas. Es importante recordar que uno de los mayores desafíos actuales es la regulación del ciberespacio, por su carácter natural de intangibilidad lo convierte, sin lugar a dudas, en un elemento que a futuro puede traer consigo conflictos dentro del sistema.

Un buen ejemplo y apreciación que permite el ciberespacio, es el sigilo que logra mantener en la ejecución de las acciones maliciosas, lo escurridizo que puede ser a través del manejo de la red. Todo esto pone en manifiesto la capacidad real de lo que se puede enfrentar ante ataques cibernéticos y la dificultad para controlar este espacio.

Ya que, históricamente el poderío militar y económico fue pieza fundamental para ejercer poder e influencia dentro de los Estados, pero se debe echar un vistazo a la actualidad que nos rodea y es que, el escenario ha cambiado drásticamente, aunque si bien es cierto se mantiene esta forma en la que se regía el poder, esta misma además ha evolucionado y se ha incorporado dentro del ciberespacio donde basta con un dispositivo inteligente para producir algún tipo de daño a quien considere su oponente.

Por otro lado, dentro del panorama digital en el que vivimos en temas del internet de las cosas, la robotización, de las cadenas de producción entre otras y ante las problemáticas de ciberseguridad, se vuelvecada vez más importante la implementación de una estrategia que abogue por la seguridad del ciberespacio y sus usuarios.

Por consiguiente, se llega a la conclusión de que los diferentes actores de la comunidad internacional deben trabajar arduamente en la consolidación de estrategias que trabajen de la mano en la implementación de cooperación entre sectores para reforzar y fomentar la prevención de posibles ataques cibernéticos que los puedan perjudicar; sin dejar de lado la importancia que surge para las naciones fortalecer los lazos en la lucha contra el cibercrimen.

Tratados como los de Budapest permiten la recolección de información necesaria para la implementación de regulaciones estandarizadas para un mejor manejo de posibles situaciones, y los nuevos retos que surjan gracias a la evolución tecnológica. El desarrollo de la era del conocimiento que nos posiciona en un mundo interconectado, los datos y su tratamiento es imprescindible para el crecimiento y competitividad tanto para las naciones como para las empresas.

Ante estos nuevos panoramas es importante la búsqueda de formas de implementación de las regulaciones, así como los métodos a emplear en los diferentes modelos de cooperación, que permitan mantener el desarrollo de la ciberseguridad. Es fundamental que se siga ahondando en la investigación de la ciberseguridad y toda cooperación que se puedan realizar por parte de los diferentes sectores es fundamental para la búsqueda de una seguridad común.

En materia de seguridad nacional, se vuelve fundamental la aplicación de la ciberseguridad ante todos los eventos posibles que se puedan realizar en este ámbito. Al tratarse de un tema sumamente amplio hace que el mismo contenga un carácter que se impregna en todos los ámbitos de la sociedad, desde las tendencias se contemplan el ámbito comercial, social, económico.

La era digital ha traído consigo serias implicaciones en temas de seguridad nacional, Aunque las naciones han sido y seguirán siendo uno de los actores de mayor relevancia y dominio a nivel mundial. Hay nuevos retos debido al aumento de actores no gubernamentales que se han establecido dentro de la comunidad internacional. Además del acceso que ellos mismos tienen al poder que les brinda el acceso y manipulación de la información; por lo que los retos actuales son mucho más desafiantes que antes.

Así mismo podemos mencionar las nuevas oportunidades que brinda el ciberespacio para los Estados, que les permiten establecerse en la entrada de nuevos jugadores dentro de la comunidad internacional que además traen consigo gran peso debido a la influencia y amplio dominio. Estados Unidos por sí solo ha tenido una presencia y es un peso clave en el ámbito de la ciberseguridad; el auge de la innovación hace que sea un país fundamental para la exportación en temas tecnológicos, pero además los posiciona como un actor atractivo para escenarios de amenazas de delitos y vulnerabilidades constantes.

El ciberespacio ha generado un impacto en la política mundial debido a los cambios y trasformaciones que afectan al ejercicio y actividades de la política internacional. Todas las naciones por el simple hecho de estar interconectadas hacen que sean vulnerables, por lo que la necesidad de brindar seguridad en las redes crece y se vuelve fundamental.

Las naciones a medida que se llegan a enfrentar amenazas cada vez más sofisticadas, requieren adoptar medidas y realizar los ajustes necesarios para las estrategias nacionales e internacionales que permitan solidificar. Tenemos que tener en cuenta que al tratarse de un espacio intangible que no conoce de fronteras muchas veces las estrategias nacionales no son suficientes para abordar algunas de las problemáticas.

Cuando se menciona el desarrollo de las TIC, es un mundo tan amplio que va más de lo que podemos creer a simple vista, estamos abordando temas de innovación, empoderamiento de los usuarios ante ella, para lograr un mayor beneficio y que de manera colateral impacte en el colectivo social de la mejor manera.

En cuestión de tratados internacionales, el Convenio de Budapest es hasta ahora el único tratado que atiende la problemática de los delitos informáticos y entre los cuales se contemplan los delitos relacionados con infracciones de propiedad intelectual y de los derechos afines.

La adhesión al Convenio supone una mejor cooperación entre los Estados Parte, ya que se tipifican de forma común las actividades delictivas por medios electrónicos, se permite el intercambio de información entre jurisdicciones para localizar a los delincuentes informáticos y se implementan procedimientos para penalizar los delitos cometidos por medios electrónicos.

Por lo que la cooperación internacional se vuelve fundamental para la buena administración y control de este dominio. Aunque la ciberseguridad por ser un tema tan amplio en temas de cooperación puede parecer un poco insuficiente. Sin embargo, es una de las áreas en las que mayormente se viene trabajando y existen muchísimos órganos que han dedicado espacios para este abordaje.

El Acuerdo sobre Seguridad Cibernética que se firmó el 2015, es un avance significativo y gracias a este avance surge una esperanza, no solo para las naciones sino para la comunidad internacional. También se puede mencionar los acuerdos por parte del

expresidente el señor Barack Obama y los más recientes por parte del expresidente el señor Donald Trump, estos acuerdos forman parte y base como precedentes para futuras administraciones que busquen abordar y ampliar temas en el ámbito de la ciberseguridad, las estrategias a nivel comercial.

Dentro de las estrategias establecidas, aunque la cooperación en el campo de la ciberseguridad sea compleja, es importante que los países encuentren incentivos para crear estrategias comunes para el tratamiento, donde se pueda desarrollar la gestión y prevención de las actividades maliciosas que podemos encontrar en el ciberespacio. En las relaciones bilaterales es importante que los países busquen la adaptabilidad a las nuevas tendencias tecnológicas, principalmente ahora donde el virus del Covid-19 ha traído consigo la aceleración en la implementación de estas tecnologías.

No se puede dejar de lado el tema económico y comercial, puesto que es una de las áreas claves para el desarrollo de un país. Esta investigación muestra un poco lo que abarca este gran mundo digital, da un panorama en lo que refiere las estrategias de ciberseguridad, es solo una pequeña parte de lo que puede abarcar la ciberseguridad. Dejando a futuro que se pueda desarrollar más contenido que surja a partir de las nuevas tendencias tecnológicas a raíz de la ciberseguridad.

Dentro del TLCAN, se ha implementado esfuerzos necesarios para el desarrollo social, educacional y económico que le han permitido tener ventajas competitivas ante las economías emergentes del sector TIC, por lo que ha tenido la oportunidad de posicionarse en esta nueva corriente y además formar parte de la era de la sociedad de la información y era digital.

La negociación del TLCAN da una oportunidad para incorporar el tema del comercio electrónico Estados Unidos, México y Canadá tienen la oportunidad de establecer un modelo para abordar el comercio electrónico en futuros acuerdos comerciales. Adicionalmente, esto dará un empuje para que se modernice estas legislaciones en este tema y, finalmente, se regule en una sola ley que esté armonizada con lo que será el TLCAN 2.0.

## 5.2 RECOMENDACIONES

En este apartado se exponen las recomendaciones a considerar para la elaboración de futuras investigaciones relacionadas con los nuevos retos que afrontan las exportaciones y nuevas tendencias en material tecnológicas.

La primera recomendación es la concientización de las vulnerabilidades y de las consecuencias que conlleva un ciberataque a un sistema, por lo que los Estados deben seguir trabajando en la educación digital, la concientización a la sociedad civil, principalmente en la educación para que los ciudadanos realicen praxis preventivas, y que les permitan tener una sociedad cada vez más segura.

Es importantísimo medir los impactos negativos de las ciberamenazas y profundizar en la docencia en este ámbito, para fomentar el crecimiento y formación de profesionales de élite especializados en ciberseguridad para la atracción de las industrias tecnológicas. Es fundamental para el desarrollo, fomentar el aprendizaje continuo y eficaz.

En el ámbito jurídico es importante que se trabaje para involucrar todas las partes, actores como organizaciones públicas y privadas, sin dejar de lado el trabajo de la mano con la sociedad civil, para la construcción de herramientas e instrumentos en el área de defensa basada en pilares como la responsabilidad política y ciudadana.

En el ámbito industrial, se debe seguir trabajando en la calidad de los procesos y los tratamientos de la información, afinar los puntos necesarios para aumentar la credibilidad, mejorar la gestión de riesgos empresariales y brindar el abordaje necesario para la prevención en este tema.

Es importante mantener una actualización adecuada en el tema de ciberseguridad ya que, esto permite que el tener buena reputación en este tema, y beneficie en la atracción de mayor inversiones económica. Lo cual es importante seguir las recomendaciones que se obtengan para que se establezcan objetivos en común para el desarrollo del país.

Fomentar la investigación básica y aplicada en materia de ciberseguridad en todos los sectores y en diversos grupos de interesados. Los países deben tratar de establecer, en el marco de la estrategia, vínculos con la comunidad internacional de investigación en los ámbitos científicos relacionados con la ciberseguridad, como la informática, la ingeniería eléctrica, las matemáticas aplicadas y la criptografía, pero también en ámbitos no técnicos

como las ciencias sociales y políticas, los estudios empresariales y de gestión y la psicología, por citar algunos.

Como recomendación final, se insta a los futuros investigadores a desarrollar y dar un abordaje al tema de la ciberseguridad aplicada en las nuevas tecnologías, así como el análisis de la aplicación que se le da en las diferentes áreas del comercio exterior.

**Bibliografía**

Barrantes, R. (2013). *Métodos de estudio a distancia e investigación: A la búsqueda del conocimiento científico*. San José: EUNED.

Carlos A. Ledesma & Cristina L. Zapata (1995) *Negocios y Comercialización Internacional, Comercio Exterior*. Editorial: Buenos Aires : Ediciones Macchi, 1995 ISBN/ISSN/DL: 950-537-255-8.

Carlota García Encima (2018) La estrategia de Seguridad Nacional de la Administración Trump; Real Instituto El Cano, Royal Institute. Príncipe de Vergara 51.28006 Madrid, España.

Carmen Sánchez Montañés. Valoración de intangibles para la ciberseguridad en la nueva economía, Universidad de Sevilla.

Centro Nacional Criptónimo de España (2017) Principios y recomendaciones básicas de Ciberseguridad. CCN-CERT BP/01.

Cecilia Bembibre (2008)

Cecilia Pastorino (2017) Convenio de Budapest: Beneficios e implicaciones para la seguridad informática. (Welivesecuritybyeset) recuperado de: https://www.welivesecurity.com/la-es/2017/12/06/convenio-budapest-beneficios-implicaciones-seguridad-informatica/

Celia Valdeolmillos (2020) Estados Unidos pone límites a la exportación de software de Inteligencia Artificial, Noticias McPro. Recuperado de: https://www.muycomputerpro.com/2020/01/06/estados-unidos-limites-exportacion-inteligencia-artificial

Daniel R. Coats, "Wordlwide Threat Assessment of the US Intelligence Community", Office of the Director of National Intelligence, 13/II/2019, Recuperado de: https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf. (cont.)

Daniels y Radebaugh (2004) Plan de negocios de exportación.

Data BreachInvestigations (2017) Repor-Verizon Enterprise Solutions, Recuperado de: www.verizonenterprise.com>dbir

David Reinares Lara (2020) *Origen e importancia de la ciberseguridad*. CW: OpenWebinar Recuperado de: https://openwebinars.net/blog/origen-e-importancia-de-la-ciberseguridad/

Del Cid, A., Méndez, R., & Sandoval, F. (2011). *Investigación*. Fundamentos y metodología. (2ª ed.) México D.F. Pearson.

Donald Trump. Order Regarding the Proposed Acquisition of Lattice Semiconductor Corporation by China Venture Capital Fund Corporation Limited, Executive Order, White House, 13/IX/2018. Recuperado de: https://www.whitehouse.gov/presidential-actions/order-regarding-proposed-acquisition-lattice-semiconductor-corporation-china-venture-capital-fund-corporation-limited/.

Federico Steinberg (2018), "Lo que hay que saber sobre la guerra comercial iniciada por Trump", *Comentario Elcano nº 19/2018,* Real Instituto Elcano, Recuperado: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/comentario-steinberg-guerra-comercial-iniciada-por-trump.

Dr. AliBurakDaricili (2020). Política, Análisis; ¿Cuáles son los objetivos e las estrategias de ciberseguridad de los países con más poder del mundo?, Recopilado de: Anadolu Agency.

Eliana Rodríguez Zubieta (2018). Ciberseguridad: los acuerdos de cooperación para el tratamiento de las amenazas en el ciberespacio. El caso de Estados Unidos y China.

Federico Steinberg (2018), "Lo que hay que saber sobre la guerra comercial iniciada por Trump", *Comentario Elcano nº 19/2018,* Real Instituto Elcano, Recopilado de: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/comentario-steinberg-guerra-comercial-iniciada-por-trump.

Gartner (2019) Procomer: Principales Tendencias en Tecnologías estratégicas para 2020, Implicaciones para Costa Rica. Recuperado de:

https://www.procomer.com/alertas_comerciales/exportador-alerta/principales-tendencias-en-tecnologias-estrategicas-para-2020/

Gallego, L. (2009). Fuente de información y manejo de informacióndifusa. Obtenido de

https://www.google.com/amp/s/www.gestiopolis.com/fuentes-informacion-manejoinformacion-difusa/amp/

Graham Wright (2009) "DefenceTechnologyStrategy": Diseñado y producido por el Ministerio de Defensa de Reino Unido. Octubre de 2006. Fuente: http://www.science.mod.uk).

Hernández, R., Fernández, C., Bap

tista, P. (2014). *Metodología de la investigación*. (6ª ed.) México D.F.: McGraw Hill.

Hiperderecho (2018) El convenio de Budapest llega al Perú: Una breve historia de la ciberseguridad importada, Derechos Digitales América Latina, Recuperado de: https://www.derechosdigitales.org/12329/una-breve-historia-de-la-ciberseguridad-importada/

José Manuel Ferro Veiga (2020) Asesor/Gestor en seguridad privada integral: Curso superior en dirección de seguridad privada, Recuperado de: https://books.google.co.cr

Juan Carlos Vásquez Pesina (2021) Ciberseguridad: Una guía completa del concepto, tipos, amenazas y estrategias. Infosecurity, México. Recopilado de: https://www.infosecuritymexico.com/es/ciberseguridad.html

Koremenos, Barbara; Lipson, Charles and Snidal, Duncan, .The rational design of international institutions, *International Organization*, 55, 2001, pp.
761-800.

Kshetri, N. (2014). Cybersecurity and International Relations: The US Engagement with China and Russia. In Proc. FLACO-ISA Joint Conf.

Leiva E. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo basado en un enfoque Top-Down desde una visión global a una visión local. Revista Latinoamericana de Ingeniería de Software, 3(4): 161-176, ISSN 2314-2642.

Muñoz, C. I. (2015). *Metodología de la investigación*. México D.F.: Oxford UniversityPress.

National Science Board (2018), Science & Engineering Indicators 2018, National Science Foundation, 2018, Recuperado de: https://www.nsf.gov/statistics/2018/nsb20181/assets/nsb20181.pdf.

Navas Lopez, J.E.; Guerras Martin, L.A. (2012): Fundamentos de la Dirección estratégica de la Empresa. CIVITAS-THOMPSON REUTERS. NAVARRA.

National Science Foundation, "National Science Board Statement on Global Research and Development (R&D) Investments NSB-2018-9", News Release, National Science Foundation, 7/II/2018, Recuperado de: https://www.nsf.gov/nsb/news/news_summ.jsp?cntn_id=244465.

Óscar Pastor Acosta (2009). Seguridad Nacional y Ciberdefensa. Cátedra ISDEFE-UPM 6.

PawelHerczynski, (2020) Director Gerente de PCSD y Respuesta a Crisis, Servicio Europeo de Acción Exterior. Reporte de Ciberseguridad 2020, Inter American Development Bank , Organization of American States.

RAE. (s.f.). Diccionario de la Real Academia Española. Obtenido de Definición comercio: https://dle.rae.es/

Repplinger. (2017). *Fuentes secundarias.* Obtenido de https://www.google.com/amp/s/www.lifeder.com/fuentes-primarias secundarias/amp/

Ronda, G.A.; Guerras, L.A. (2012): Dynamics of the evolution of the strategy concept 1962–2008: a co-word analysis; Strategic Management Journal 33; 162-188

SadieCreese Directora (2020) Centro global de capacidad en Seguridad Cibernética, Universidad de Oxford.

Sergio López (2019). Nuevas Tendencias: La breve historia de la ciberseguridad. SofisticCybersegurity. Fuente:https://www.sofistic.com/blog-ciberseguridad/la-breve-historia-de-la-ciberseguridad/

The White House (2018), "Legislative Outline for Rebuilding Infrastructure in America", The White House, Febrero 2018, Recuperado de: https://www.whitehouse.gov/wp-content/uploads/2018/02/INFRASTRUCTURE-211.pdf.

Thomas Mun(1664): *La riqueza de Inglaterra por el comercio exterior*; versión en español del Fondo de Cultura Económica, México, 1978.

US Department of Defense (2018) , "Summary of the 2018 National Defense Strategy of the United States of America", US Department of Defense, Enero 2018. Recuperado de:https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Waltz, Kenneth N., .The stability of bipolar World, *Daedalus*, 93 (3), 881-909, 1965.