COLOMBIA: ¿ES UN ESTADO EFECTIVO EN TÉRMINOS DE SEGURIDAD DIGITAL CON ÉNFASIS EN EL SECTOR PRIVADO?

PONTIFICIA UNIVERSIDAD JAVERIANA

FACULTAD DE CIENCIAS POLÍTICAS Y RELACIONES INTERNACIONALES

DEPARTAMENTO DE RELACIONES INTERNACIONALES

BOGOTÁ D.C

JUNIO, 2019

COLOMBIA: ¿ES UN ESTADO EFECTIVO EN TÉRMINOS DE SEGURIDAD DIGITAL CON ÉNFASIS EN EL SECTOR PRIVADO?

Presentado por:

Sthefanie Puentes León

TRABAJO DE GRADO

Presentado como requisito para optar al título de

INTERNACIONALISTA

Bajo la dirección de:

ALEJANDRO BOHORQUÉZ KEENEY

PONTIFICIA UNIVERSIDAD JAVERIANA

FACULTAD DE CIENCIAS POLÍTICAS Y RELACIONES INTERNACIONALES

DEPARTAMENTO DE RELACIONES INTERNACIONALES

BOGOTÁ D.C

JUNIO, 2019

Tabla de contenido

Introducción **4**

Metodología **14**

Capítulo 1. Identificar la presencia de amenazas a nivel cibernético del sector privado..... **15**

Capítulo 2. Detallar las medidas que ha efectuado el sector privado para afrontar ciberataques y preservar la seguridad informática **23**

Capítulo 3. Exponer la situación del sector privado en Colombia a nivel global, en términos de seguridad digital **31**

Conclusiones **37**

Bibliografía **41**

Anexos **50**

Entrevista 50

Figuras

Figura 1: *Número de casos reportados de nuevas amenazas presentadas en el 2017 en Colombia* 53

Figura 2: *Factores de riesgo en el ciberespacio* 54

Figura 3: *Sistema inmune de seguridad integrado e inteligente IBM* 55

Figura 4: *Enfoque prioritario entre las tecnologías IT y OT* 56

Figura 5: *Diferencias redes IT y OT* 56

Figura 6: *Posición de Colombia a nivel regional* 56

Figura 7: *Grado de compromiso nacional* 57

INTRODUCCIÓN

El vertiginoso uso y adopción de las comunicaciones y tecnologías como medio para cualquier actividad socioeconómica en Colombia y en todo el mundo, genera que el ciberespacio se convierta en un ambiente de incertidumbre. Expuesto a riesgos, amenazas, vulnerabilidades e incidentes de numerosos tipos, a los que se ven en peligro la población y las organizaciones, públicas y privadas (Superintendencia Financiera de Colombia, 2015) (CONPES, 2016). Ante estos hechos que vulneran las estructuras informáticas en el país, Colombia establece una política de seguridad digital mediante el documento CONPES 3854 de 2016; con el objetivo de favorecer un entorno digital confiable y seguro mediante la protección, prevención y reacción a delitos y ataques cibernéticos (Mayorga Delgado, s.f).

Ahora bien, para cimentar y salvaguardar la seguridad digital, el Gobierno Nacional en cabeza de la Cancillería y los Ministerios de Justicia, Defensa y Tecnologías de la Información y las Comunicaciones (TIC), radicaron al Congreso de la República el Proyecto de Ley para adherirse al Convenio de Budapest contra la ciberdelincuencia. Este tiene como objetivo enfrentar los delitos informáticos y en Internet por medio de una política mundial común, la armonización de leyes nacionales, la mejora de las técnicas de investigación, el aumento de la cooperación entre los Estados y su relación con el sector privado, con el objetivo de prevenir los delitos en la red. De esta manera, Colombia avanza hacia una Economía Digital y este tipo de convenios son clave para resguardar a la ciudadanía ante diferentes ataques cibernéticos (MinTic, s.f).

Dicho lo anterior, se toma en cuenta los convenios internacionales de Colombia en cuanto a la seguridad digital como lo es la Resolución OEA AG/RES 2004, la Comunidad Andina: Decisión 587, el convenio de Ciberseguridad-UIT, entre otros. Su propósito, se centra en ejecutar políticas de seguridad, prevención y erradicación de amenazas para la seguridad del territorio respecto a un ataque de carácter cibernético, que no solamente afecta el entorno digital, sino que todas las infraestructuras que componen la agenda de un Estado (Arias Torres & Celis Jutinico, 2015). Adicionalmente, “Colombia ha aprobado una legislación procesal penal integral y de efectiva penalización (Ley 1273 y Ley 906) para abordar los

delitos cibernéticos y reconoce los tratados internacionales con Interpol y Europol" (Observatorio de la Ciberseguridad en América Latina y el Caribe, 2019).

Añadido a esto, en el caso colombiano, se evidenció que en el 2015 el Departamento de Delitos Informáticos de la Policía Nacional recibió 7118 denuncias por parte de víctimas de delitos informáticos, demostrando un incremento del 40% respecto al 2014. Por tal motivo, delitos cibernéticos como estos, presentaron pérdidas económicas cerca del 0.14% (Banco Mundial, 2014) del PIB nacional (Manrique Horta, 2016). Por ende, es importante que empresas y organizaciones efectúen medidas regulatorias de seguridad que debiliten cualquier tipo de ataque informático, con el objetivo de eliminar daños a información sensible de cada organización, ya sea pública o privada. En este caso, haciendo énfasis en el sector privado, las empresas dejan expuesta la gran fragilidad que presentan en seguridad informática y son aprovechadas para realizar ataques cibernéticos (Vidal Londoño, 2016).

Como respuesta, las empresas privadas colombianas han efectuado mecanismos para proteger sus infraestructuras frente a cualquier tipo de agresión que quebranten su integridad, estabilidad económica y social; en un mundo globalizado donde la información privada es propensa a ser hurtada y tener un mal manejo por delincuentes cibernéticos (Vidal Londoño, 2016). Acometimientos como los que se mencionaron anteriormente, dieron paso a una mayor consolidación en la construcción de una Política de Seguridad Digital con la intervención de:

- Representantes del sector privado
- Representantes del gobierno
- La sociedad civil.
- La industria de la Tecnología de la Información.
- La academia.

Lo anterior, junto con recomendaciones realizadas por estructuras internacionales como la Organización para la Cooperación y el Desarrollo Económicos (OCDE[1]) y de la

[1] Organismo Internacional de carácter intergubernamental del que forman parte 37 países miembros. La OCDE fue creada en 1960 con sede en París, para dar continuidad y consolidar el trabajo realizado por la antigua Organización Europea de Cooperación Económica (OECE) que se había constituido para canalizar la

Organización de Estados Americanos (OEA[2]), las mesas de trabajo concertadas entre el Departamento Nacional de Planeación, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional y otras entidades relacionadas con la seguridad digital en Colombia (MinTic, 2016). Junto con organismos especializados como el Comando Conjunto Cibernético de las Fuerzas Militares y el Centro Cibernétco Policial y el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT[3]) (Cortés Borrero, 2015).

Respecto al sector privado, es necesario crear una estrategia de protección de la infraestructura crítica cibernética en el país, orientado hacia la gestión de riesgos de seguridad digital. Por ende, representantes del sector privado como:

- Asobancaria.
- Claro Colombia.
- Ecopetrol.
- B-Secure.
- IQ Information Quality.
- IBM.

Los cuales, participaron en la implementación imprescindible de seguridad digital, debido a sus procesos de apropiación de tecnologías de la información. Por tal motivo, este tipo de intervención involucra un alto nivel de confianza que les demuestra a sus clientes, proveedores y aliados estratégicos "que cuentan con las medidas de seguridad necesarias y pertinentes" (MinTic, 2018).

---

implementación del Plan Marshall. La OCDE sustituyó a ésta en la tarea de impulsar la reconstrucción y el desarrollo en el continente tras la Segunda Guerra Mundial. http://www.exteriores.gob.es/RepresentacionesPermanentes/OCDE/es/quees2/Paginas/default.aspx

[2] Organismo regional más antiguo del mundo, cuyo origen se remonta a la Primera Conferencia Internacional Americana. Fundada con el objetivo de lograr en sus Estados Miembros, como lo estipula el Artículo 1 de la Carta, "un orden de paz y de justicia, fomentar su solidaridad, robustecer su colaboración y defender su soberanía, su integridad territorial y su independencia". http://www.oas.org/es/acerca/quienes_somos.asp

[3] El Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT, tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional.

De esta manera, se observa que el perfil general de quienes participan de esta estrategia, son empresas, siendo la mayoría del sector de Servicios y son aquellas que tienden a asignar un presupuesto más grande a la seguridad digital. Sin embargo, los ataques cibernéticos "aumentan en sofisticación e impacto mientras que la actualización de los recursos humanos y tecnológicos para defenderse y las dotaciones presupuestarias enfocadas en la seguridad digital son aún pequeñas y crecen con lentitud" (BID, MinTic & OEA, 2017). Generando que la gravedad de las amenazas y el perjuicio que realizan, solicitan acciones urgentes en las cuales el sector público y el privado colaboren en conjunto (BID, MinTic & OEA, 2017).

Ante la situación planteada, surge el interrogante acerca de: ¿Cuál ha sido la efectividad de la seguridad digital respecto al sector privado para enfrentar ciberataques y garantizar la seguridad de Colombia a partir del CONPES de 2016 hasta el 2018?

Para lograr dar respuesta a la pregunta, la hipótesis a defender en este trabajo de investigación gira en torno a la eficacia y efectividad de las acciones regulatorias realizadas por parte del sector privado, para enfrentar ataques de tipo digital a sus infraestructuras críticas y su respectiva capacidad de respuesta. De esta manera, se expone una primera variable desarrollada respecto a la protección de las estructuras informáticas del Estado, con apoyo del sector privado mediante gestiones de seguridad y de este modo, dar paso a la segunda variable comprendida como la capacidad de respuesta a amenazas cibernéticas latentes en el país que a su vez identifique la existencia de las mismas, y deje en evidencia la situación de Colombia en temas de seguridad digital a nivel global.

Por lo tanto, el accionar se ejecutará mediante entidades y mecanismos de seguridad del sector privado, que brinden herramientas protejan las estructuras informáticas. Posteriormente, la existencia de amenazas se establecerá por medio de organismos privados encargados de temas informáticos, con antecedentes de posibles ataques en el país y su accionar en cada caso.

Dicho lo anterior, el trabajo se sustenta en torno al objetivo principal de: demostrar la efectividad de los mecanismos de seguridad digital del sector privado, en contra de amenazas

cibernéticas que afectan a Colombia. Posteriormente, de este objetivo de desarrollarán tres subtemas específicos como lo son: 1) Identificar la presencia de amenazas a nivel cibernético del sector privado, 2) Detallar las medidas que ha efectuado el sector privado para afrontar ciberataques y preservar la seguridad informática y 3) Exponer la situación del sector privado en Colombia a nivel global, en términos de seguridad digital.

Para dar respuesta a la pregunta de investigación con base a las Relaciones Internacionales, en términos del sistema teórico, que logre explicar la efectividad de los mecanismos de seguridad digital del sector privado en Colombia, se alude al enfoque estructural-funcionalista, derivado del enfoque funcionalista, el cual relacionado uno con el otro, se caracteriza por identificar cuáles son las funciones para que un sistema de gobierno se desempeñe de forma adecuada, qué estructuras deben cumplirlas y a través de cuáles procesos son llevadas a cabo para cumplir determinada función, frente a diferentes situaciones, como en este caso es de riesgo y vulnerabilidad que no solo afecta al territorio Colombiano sino que es una amenaza global (Merton 1964: 61). Por lo tanto, este enfoque es una variable que logra cimentar las definiciones más importantes, a partir de elementos académicos que sean adaptables en el caso de seguridad digital, que sobrepasa las fronteras y son aplicados en diferentes países como Estados Unidos, Estonia, Rusia, entre otros. Este enfoque, se ajusta en el contexto colombiano, en el ámbito político contemporáneo, complementando así, la aplicación conceptual y teórica directamente en el tema a tratar.

En este enfoque sobresale el concepto de función reguladora, que determina la difusión de normas sobre diferentes actividades políticas, sociales, económicas, culturales o en este caso privadas. Lo anterior, para asegurar su calidad y aplicabilidad en determinado contexto como lo es la seguridad digital en Colombia, las normas que platea y en el enfoque que se traduce en mecanismos aplicables en el contexto del ciberespacio. (Dryzek, Honig & Phillips, 2006). A partir de dicho enfoque, el autor Gabriel A. Almond, menciona en el texto "*Comparative politics today: A worldview" (2005),* la adecuada aplicación de una teoría a contextos contemporáneos determinados. Esto será clave para el desarrollo de los objetivos específicos asociados al uso de las tecnologías de la información, como lo es ciberataques, seguridad digital y ciberespacio (Almond, 2005).

En este caso, con base al tema de investigación uno de los objetivos es detallar las medidas que ha efectuado el sector privado en Colombia contra ciberataques. Es pertinente identificar funciones y estructuras que se deben ejecutar y aplicar en determinados casos; en este contexto se entendería como los mecanismos que se emplearían en el ciberespacio y su apropiada aplicación. Enfocado en una aplicación sistemática de la teoría en la situación de varios sistemas políticos actuales, con el objetivo de que funcione adecuadamente en el desempeño de políticas públicas (Merton 1964: 61).

En este orden de ideas, otro enfoque teórico importante que es de utilidad para el desarrollo del trabajo, es el de la teoría de la información y cibernética planteada por Karl W. Deutsch, quien afirma que una característica de la política y de los sistemas políticos de Occidente, es el hecho de haber desarrollado diversas técnicas cuya función es acelerar la innovación y el aprendizaje social. En este punto, se destaca la técnica para formular y llevar a la práctica las decisiones, la cual es "un instrumento esencial del aprendizaje social": un "instrumento de supervivencia y desarrollo" más que de destrucción (Deutsch, 2007, Pág. 138). Siendo así, la cibernética se presenta como la ciencia que estudia las comunicaciones y el autocontrol en los sistemas complejos, animales y máquinas y en los sistemas sociales. Al mismo tiempo, se expone que el origen de la cibernética se encuentra en la investigación sobre técnicas bélicas, debido a que se buscaba diseñar mecanismos para que un proyectil de autopropulsión diera en un blanco móvil, pero en este caso se utiliza para técnicas de seguridad frente a posibles amenazas cibernéticas (Deutsch, 2007).

Por tal motivo, este enfoque teórico será clave para lograr el objetivo de identificar la presencia de amenazas cibernéticas y detallar las medidas ha efectuado el sector privado del Estado Colombiano, para preservar la seguridad informática. Esto es debido a que la cibernética, es un medio tanto de defensa como de ataque (bélicos como lo plantea la teoría) que permite tener mayor conocimiento de las medidas que se pueden tomar al enfrentar ataques de tipo informático. Ahora bien, se afirma que lo anteriormente mencionado, Deutsch lo menciona en su obra "Los Nervios del Gobierno" (1963), en el cual en muchos conceptos provenientes de la Cibernética y de la Teoría de la Información con base a las funciones del Estado y el Gobierno, se cuestiona el nivel de eficacia que tiene el Gobierno para prever

problemas y tomar medidas preventivas junto con los factores que influyen sobre el Gobierno al adoptar decisiones (Deutsch, 1963). De esta forma, expone que se debe articular elementos propios del sistema (agrupar sector público y privado) y abarcar varias dimensiones como los son los recursos humanos, el desarrollo económico, la disponibilidad de recursos materiales y humanos, la autodeterminación, la ciencia, la tecnología, entre otras. Es así, que se logra tener la capacidad de poner pautas de organización, comunicación seguridad y defensa, aplicadas en el trabajo mediante la seguridad digital y su eficacia en respuesta a un ataque (Deutsch, 1963).

Vale la pena mencionar para desarrollar las políticas de seguridad digital en Colombia y su accionar, un tercer enfoque teórico planteado por Shreyas Sundaram, profesor asistente en la Escuela de Ingeniería Eléctrica y Computación de Purdue. Es la teoría, denominada "teoría prospectiva", la cual describe cómo las personas toman decisiones cuando hay incertidumbre y riesgo; decisiones que a menudo son solo en parte racionales. Esto genera una comprensión más amplia de las vulnerabilidades que surgen en los sistemas interconectados a gran escala y da paso al diseño de sistemas más seguros, con los correspondientes beneficios sociales (Lima, 2011). Además, se aborda la complejidad de proteger los sistemas actuales a gran escala, en el cual se proporcionará nuevos conocimientos sobre los tipos de decisiones que se toman cuando se enfrentan amenazas de seguridad; a través de un enfoque integral que abarca la teoría y experimentos (Lima, 2011).

Es preciso, en este caso nombrar y relacionar la teoría prospectiva con la teoría de la turbulencia comprendida como una teoría del cambio, continuidad e incertidumbre (como la teoría prospectiva), planteada por el Profesor en Asuntos Internacionales de la Universidad de George Washington, James N. Rosenau. En su libro "Turbulence in World Politics: A Theory of Change and Continuity" lo esboza como una explicación de la continua agitación del mundo actual, junto con el impacto de la revolución microelectrónica, el orden postindustrial y los abundantes cambios políticos, económicos y sociales. De esta manera, se enfoca en el camino de la política global en la que un mundo autónomo multicéntrico se ha convertido en un competidor del mundo centrado en el estado, de larga data (Rosenau, 1990).

Así pues, la teoría prospectiva se aplicaría en las amenazas a la seguridad digital; de la mano a este enfoque conceptual relacionado al tema de seguridad y toma de decisiones, sobresale Daniel Kahneman, un psicólogo que de la mano con Tversky publicaron una serie de artículos seminales. Dichos artículos, se basan en el campo general del juicio y la toma de decisiones, que describe cómo las personas toman decisiones frente a situaciones en las cuales deben decidir entre alternativas que involucran riesgo (International Journal of Psychological Research, 2008). Por ejemplo, decisiones financieras, estratégicas que en este contexto se ejecutarían en el ciberespacio e involucran empresas privadas del sector financiero.

Complementario a lo anteriormente mencionado, la teoría de la turbulencia muestra la manera en que las estructuras macroeconómicas de la política global han sufrido transformaciones vinculadas con aquellas en el nivel micro. Son los fenómenos que van debilitando la autoridad de antiguas estructuras, la fragmentación de colectivos, la adquisición de mayor poder por parte de los subgrupos, los cambios en las lealtades nacionales o la recomposición temática de la agenda política mundial que forman parte de un agitado panorama globalizado. Esto enmarca simultáneamente tendencias centralizadoras y descentralizadoras que producen una división de las estructuras mundiales (Rosenau, 1990).

Así que, para una mayor comprensión y apropiación del tema, es importante la comprensión y entendimiento de conceptos básicos, pertenecientes al tema a tratar como lo es la seguridad digital, entendida según la Asociación para el Progreso de las Comunicaciones como:

> “el entender internet como un escenario real (como el hogar o la calle), donde se viven situaciones reales; en el que se debe procurar tener cuidado y evitar situaciones de riesgo, como, por ejemplo, la pérdida de información laboral al dañarse o extraviar el computador, el acceso de otras personas a las cuentas en redes sociales o a las transacciones bancarias que se encuentran registradas en el celular, entre otras” **(**Colnodo, 2016)

Complementario a lo anterior, en el documento CONPES 3854 de 2016, se define como:

> "la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante: 1) la gestión del riesgo de seguridad digital; 2) la implementación efectiva de medidas de ciberseguridad; y 3) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país"

Posteriormente, a esto y con base al desarrollo del trabajo se destaca el concepto de ciberespacio que para Alejando Piscitelli en su texto "ciberculturas 2.0. En la era de las máquinas inteligentes" (2002) lo define como:

> "Un nuevo universo en el que temporalmente tenemos conciencia de nosotros mismos como viviendo en él; este ciberespacio configura y estabiliza una red de relaciones sociales que modifican de modo latente nuestro trasfondo cognitivo para la interacción social y, por consiguiente, nuestra mente, nuestra sociedad y nuestra cultura"

De esta manera, se evidencia una clara influencia del ciberespacio en nuestras vidas en todos los ámbitos, siendo

> "un territorio factible de ser dominado, al igual que la tierra, el mar, el aire y la alta atmósfera en lo relativo a la guerra (…) El ciberespacio estará presente en cualquier guerra que se produzca en el futuro; se puede utilizar como arma militar, aunque normalmente limitado en el tiempo, pero también se puede emplear para el espionaje, en cuyo caso el tiempo pierde importancia." (Pérez Fernández, Pág. 81, 2013).

Acorde al desarrollo de conceptos, surge otro preponderante en el tema de seguridad digital como lo es el de infraestructuras críticas, definida por Manuel Sánchez Gómez-Merelo, vicepresidente de la Asociación para la Protección de Infraestructuras Críticas (APIC) y Consultor Internacional de Seguridad como:

> "Aquellas instalaciones, redes, servicios y equipos físicos, y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas" (Sánchez, 2011).

De acuerdo a esta definición, en el sector privado las infraestructuras críticas se observan en empresas en su mayoría del sector de servicios como lo son Claro Colombia, ETB, Ecopetrol, entre otros. Pero por otro lado también son empresas del sector financiero como Asobancaria.

En último lugar, otro término importante acorde al trabajo de investigación es el de ciberataque, que para el Vicealmirante Julio Albert Ferrero en la Revista General de Marina (2013), lo concibe como aquellas acciones que "pueden afectar a ciudadanos, empresas, administración, infraestructuras críticas, sector bancario, etcétera" representados mediante virus, troyanos, códigos dañinos, botnet[4] (robots informáticos), entre otros, en el cual su acción se pueden clasificar en que están patrocinados por el Estado, pueden ser usados en servicios de inteligencia y contrainteligencia, en acciones de terrorismo y extremismo político e ideológico, ataques de delincuencia organizada y ataques de perfil bajo; observando de esta manera los grandes daños que puede generar ataque informático en una población o en un Estado como tal.

Finalmente, se puede evidenciar que cuanto mayor es el índice de desarrollo de una sociedad, mayor dependencia se tiene de los sistemas de información y de las comunicaciones. Es así, que cualquier tipo de sabotaje, vulneración, interrupción o violación de estos sistemas, tienen una repercusión no solo en los sistemas informáticos sino a millones de personas a nivel global. Bajo este contexto, el ciberespacio es un medio sin fronteras geográficas, anónimo, asimétrico y puede ser considerado fácilmente clandestino. Por tal motivo, en el caso específico de Colombia, la seguridad digital es un ámbito de la Seguridad

[4] Es una red constituida por un gran número de equipos informáticos que han sido "secuestrados" por malware, de forma que quedan a disposición de un hacker. https://www.avast.com/es-es/c-botnet

Nacional en la cual, el gobierno debe establecer una estrategia elaborada y ejecutada en conjunto con los sectores público y privados, para localizar las diferentes amenazas, instaurar sistemas de respuesta y ataque, con ayuda y soporte de la cooperación internacional para lograr dichos objetivos (Leiva E, 2015).

METODOLOGÍA.

Para el desarrollo del trabajo de investigación en términos metodológicos, inicialmente con ayuda de profesionales (profesores) en el tema, mediante una entrevista o fuentes bibliográficas sugeridas que se consideren apropiadas para lograr consolidar y tener mayor profundidad acerca de conceptos fundamentales, los mecanismos de control, además de cómo operan estos, contra ataques informáticos en Colombia. Esto, para comprender todo lo que está vinculado con el almacenamiento, protección, procesamiento y transmisión de la información. Este concepto contiene todo lo relacionado con la informática, la electrónica y las telecomunicaciones, que han generado importantes cambios en el sistema económico y social, influyendo en las relaciones sociales. Es importante identificar y explicar el significado seguridad digital junto con las modalidades de seguridad y los diferentes conceptos que se abarque en el contexto del ciberespacio.

Como segunda medida, se buscará mediante entrevistas y el posible contacto de entidades encargadas de la seguridad digital en Colombia del sector privado como Asobancaria, Claro Colombia, Ecopetrol, DirecTV, B-Secure, IQ Information Quality, IBM, entre otros; que permitan tener mayor conocimiento respecto a posibles amenazas del ciberespacio en territorio Colombiano, para registrar si ya se han realizado ataques informáticos o por otra parte si se evidencian amenazas cercanas que vulneren el espacio virtual y su red informática o bien, lograr un mayor acercamiento referente a la presencia de amenazas, debido al grado de confidencialidad que contiene este tipo de información. Lo anterior, dirigido siempre hacia la protección de las infraestructuras críticas y la capacidad de respuesta.

Posteriormente, en el tercer lugar, se realizará una investigación con ayuda de artículos académicos, documentos, acuerdos, entre otros elementos escritos, que abarquen temas como los mecanismos e instrumentos de seguridad del sector privado que combatan las amenazas cibernéticas y las respectivas acciones que se han realizado para enfrentarlas o prevenirlas, aplicadas en Colombia, a partir del 2016, cuando Colombia creó una Política Integral de Ciberseguridad y Ciberdefensa (CONPES 3854), la cual se cimenta en tres pilares principales: 1. Implementar la institucionalidad apropiada. 2. Fomentar programas de capacitación especializada. 3. Fortalecer la legislación y cooperación internacional.

Por último, con el uso de fuentes bibliográficas y posibles entrevistas que se puedan realizar, se busca identificar la efectividad que tienen los mecanismos de ciberdefensa y ciberseguridad, plasmados por medio de convenios, tratados, leyes, entre otros, en el momento de presenciar una amenaza a la seguridad informática o una posible sospecha de esta misma y de esta manera, muestre un panorama general de las condiciones que presenta Colombia a nivel mundial respecto a la seguridad digital.

CAPÍTULO 1.

Identificar la presencia de amenazas a nivel cibernético del sector privado.

Para el desarrollo de estrategias precisas y efectivas frente a la seguridad cibernética de cualquier sector, es necesario tener un conocimiento amplio en el tema, en términos de capacidad de respuesta y protección de infraestructuras críticas. Contar con especialistas frente a temas de seguridad informática se convierte en una prioridad a la hora de identificar oportunamente amenazas cibernéticas. Expresado, mediante agentes amenazantes que han ido adaptando y tomando ventaja de todos los avances y vulnerabilidades de las redes y sistemas de información que son accesibles (Alfaro Calvo, y otros, 2013). Lo anterior, se realiza mediante actos delictivos realizados por el crimen organizado, que utilizan la red para extender su campo de acción, en el cual actualmente se generan enormes retos a las Grandes Corporaciones y los Estados, en torno a la ciberseguridad y su respectiva respuesta (Alfaro Calvo, y otros, 2013).

En Colombia, a pesar de que existen ciertas instituciones de educación superior que brindan especializaciones de seguridad y derecho informático; tales como La Universidad Sergio Arboleda, la Universidad Externado, la Universidad Piloto, La Pontificia Universidad Javeriana, entre otras; se ha evidenciado la gran debilidad que se tiene en métodos de defensa y seguridad informática, tanto en términos de su aplicación como en el ámbito de educación (Cárdenas Moreno, 2015).

Agregado a esto, el conocimiento sobre seguridad digital y defensa es deficiente en el sector público y privado; y se demuestra que no existen instituciones u organismos a nivel nacional que logren coordinar y desarrollar operaciones de ciberseguridad. Razón por la cual, es difícil establecer mecanismos adecuados y efectivos que neutralicen, debiliten y afronten ataques cibernéticos contra las infraestructuras críticas y protejan los intereses del Estado (Cárdenas Moreno, 2015).

Siguiendo en este razonamiento, en términos teóricos de las Relaciones Internacionales se observa de manera directa, una falla estructural de aquellos sistemas que hacen posible el desarrollo integral de un Estado, obstaculizando la obtención de suficientes recursos, oportunidades y capacidades para la presencia y eficacia del derecho dentro del territorio colombiano, que en este caso se aplica en la seguridad digital y es característico del enfoque estructural-funcionalista (Betancourt Higareda, s.f). Esta "falla" estructural genera "trampas de seguridad", en las cuales actores sociales corporativos como bancos, medios de comunicación masiva, oligopolios, elites partidistas, carteles de drogas, organizaciones criminales, entre otros; así como son afectados también destruyen progresivamente el funcionamiento estructural adecuado de los sistemas internos de un Estado y su correcta aplicación del derecho en cuanto a entes regulatorios y normas (Betancourt Higareda, s.f). En este aspecto, aplicado a la capacidad de respuesta frente a un ataque cibernético, traducida por leyes, tratados, normas, etc.

En este orden de ideas, el número de resultados que un ciberataque puede generar en la infraestructura crítica de un Estado, afecta la sociedad y por ende al adecuado funcionamiento de un Estado. En este tipo de ataques el factor común es la tecnología y la dependencia a esta herramienta hace que las consecuencias tengan un efecto dominó (Lozano

Quintero, 2015). En el momento que la infraestructura crítica, reciba un ciberataque no solo causará un perjuicio fundamental en este sector, si no que paralelamente afectará otros sistemas importantes; tanto en lo privado, como el sector petroquímico (ej. Ecopetrol), el energético, de transporte (ej. Aviatur), defensa, química, alimentos y minero; como en sectores que incluyen tanto lo público como lo privado, tales como el sector de la salud, medio ambiente, gobierno, hídrico, financiero (ej. Asobancaria. Privado), tributario y educación. Entorpeciendo, obstaculizando y colapsando el adecuado funcionamiento del Estado (Lozano Quintero, 2015).

Por tal motivo, al existir un flujo de información de carácter digital y la popularización del uso de internet surge la proliferación desmedida de riegos contra personas y empresas (en este caso privadas), por el motivo de que la mayoría de actividades se vienen automatizando y requieren una conexión constante a Internet (Baldomero Contreras, 2019). Razón por la cual, las empresas deben evolucionar, conocer los entornos en los que se desenvuelve y el "nuevo" medio digital que puede afectar directamente a la empresa y a terceros. Este entorno se caracteriza y se define fundamentalmente por ser volátil, incierto, complejo y ambiguo.

De esta manera, sobresale en las Relaciones Internacionales y la Ciencia Política la teoría cibernética planteada por Karl Deutsch, quien plantea con relación a la seguridad digital, que los canales de comunicación se articulan con la toma de decisiones. Todo esto, debido a que los canales de comunicación son transcendentales para la formación de decisiones gubernamentales (en este caso decisiones del gobierno para proteger las infraestructuras críticas) y para cualquier organización social, en la cual las comunicaciones constituyen los nervios del gobierno, es decir, todo aquello que impulsa al gobierno a su accionar a nivel de seguridad, en este caso de estudio (Sánchez, 2011).

A pesar de que empresas privadas destinen a la seguridad digital menos del 1% (como lo indica el informe de la OEA y el BID) de las ventas o inversiones, es importante e imperativo analizar las amenazas y el daño que generan en el sector público y privado. Por ende, es necesario actualizar el marco de riesgos por uno que sea dinámico y que comprenda

el entorno, dando paso al surgimiento de la ventana de AREM[5] (riesgo emergente, riesgo latente) (Cano J, 2017).

Es así, como Colombia ha estimado en planes de desarrollo el fortalecimiento y ampliación de la red e infraestructura tecnológica del país. Con su ejecución se ha aumentado el comercio electrónico entre los ciudadanos en un 59% y entre las empresas en un 79%. Y ha implementado una serie de leyes en pro a combatir los delitos informáticos. Una de ellas es la Ley 1273 del 2009, la cual promulga por la protección de la información y los datos, por lo tanto, esta ley condena como delitos ciertas conductas que tienen que ver con el manejo de los datos personales y el esparcimiento de softwares maliciosos (Cuervo, 2014). Y más recientemente, en 2018, el Congreso de Colombia firmó la Ley en la cual se aprueba el Convenio sobre la Ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest, el cual se habla de la necesidad de aplicar una política penal común para combatir la ciberdelincuencia y anota cada caso de ciberdelincuencia en los que se puede incurrir y medidas legislativas que se pueden emplear (Cuervo, 2018).

Sin embargo, estos esfuerzos no han sido suficientes para combatir y reducir los ataques cibernéticos, que "para el año 2014 cobró 6 millones de víctimas, representado en pérdidas económicas de 464 millones de dólares por año (Certicámara, 2014), debido a los vacíos existentes en la normatividad y en el tratamiento" lo cual permitió acciones de cibercriminalidad (Cárdenas Rodríguez & Vásquez Zárate, 2016). Complementario a lo anterior, se une la gran debilidad la regulación y legislación de la protección de la información y los datos, debido a la falta de comprensión de este contexto para que se ejecuten de la manera más adecuada en las leyes colombianas, haciendo énfasis en la problemática de la penalización en ciberdefensa y seguridad digital (Quintero Agudelo, s.f).

Cabe destacar esta clase de acciones criminales de tipo cibernético, ya que empresas del sector público y privado han migrado paulatinamente sus negocios hacia el "ciberespacio" (Ministerio de Defensa Nacional, 2009). Estableciendo enlaces fundados en

[5] Estrategia para anticipar los riesgos y amenazas en ciberseguridad empresarial. https://www.isaca.org/Journal/archives/2017/Volume-5/Pages/the-arem-window-spanish.aspx

tecnología e implementado en el control de sus operaciones, sistemas informáticos complejos; que a su vez abren caminos para hechos delictivos como: hackeo, crackeo, denegación de servicios, falsificación de documentos electrónicos, robos en cajeros automáticos y tarjetas de crédito, robos de identidad, phreaking, fraudes electrónicos e incluso sabotaje informático (Cárdenas Rodríguez & Vásquez Zárate, 2016). Siendo este, uno de los crímenes económicos que más afectan a las compañías colombianas.

En Colombia, el sector financiero es el más atacado por delincuentes informáticos, un hecho atribuible a los recursos y la información que maneja. “El sector registra cerca de 214.000 ataques por día, el 39,6% del total de ataques cibernéticos, lo que representa pérdidas cercanas a los $411 millones de pesos diarios. Según cálculos de Asobancaria, el fraude a través de canales electrónicos ha crecido cerca de 60,6% de 2015 a 2017, pasando de $93.452 millones a $150.060 millones” (Asobancaria, 2018). Por otra parte, según el Centro Cibernético Policial de la DIJIN, en 2017, en el país se registró un aumento del 28,3% de delitos cibernéticos respecto al 2016. En dicha información sobresalen nuevas amenazas como la estafa por suplantación de simcard y el engaño por teléfono (Asobancaria, 2018). (Figura 1: Número de casos reportados de nuevas amenazas presentadas en el 2017 en Colombia)

En este mismo orden de ideas, para la compañía de seguridad y data centers: Cyxtera Technologies, los ataques más sofisticados y recientes que vulneran a empresas, instituciones financieras y consumidores se realizan mediante amenazas como:

- **Phishing:** El 90% de los ejecutivos de ciberseguridad mencionan que sus compañías fueron blanco de ataques entre 2017 y 2018.
- **Ransomware:** Hubo un incremento del 229% en el número de ataques de ransomware entre 2017 y 2018.
- **Troyanos Bancarios:** En promedio, más de 200 instituciones alrededor del mundo han sido afectadas por cada una de las iteraciones del troyano Trickbot.
- **Redes Sociales:** Cerca del 15% de todas las cuentas de Twitter son cuentas falsas manejadas por robots.

- **Brechas de datos:** Los incidentes que son mitigados durante los primeros 30 días les cuestan las organizaciones US$4.56 millones de dólares en promedio anualmente. Si la mitigación toma más de 90 días, el costo puede ascender a los US$12.07 millones. Así mismo, el 48% de las empresas sufrieron al menos dos brechas de datos en el 2017.
- **Afectación de emails corporativos:** Globalmente se vio un incremento del 136% en las pérdidas financieras originadas por ataques BEC entre diciembre de 2016 y mayo de 2018
- **Inteligencia Artificial**: Al enfrentare a sistemas de detección de fraude basados en IA, los ataques de phishing estándar tienen una tasa de éxito de solo 0.24%
- **Hackeo de elecciones:** Las elecciones de mitad de periodo de 2018 en Estados Unidos han sido el más reciente blanco de la interferencia cibercriminal (COMPUTERWORLD, 2018).

Por tal motivo, la progresiva consideración del ciberespacio e internet como un bien público, obliga al Estado a desplegar acciones necesarias que garanticen condiciones mínimas de seguridad para que toda la población pueda usarla en forma confiable. Sin embargo, sigue siendo blanco de ataques que dan origen a factores de riesgo para el gobierno y el sector privado. (Figura 2: Factores de riesgo en el ciberespacio)

Es así, como hechos mencionados anteriormente vulneran las infraestructuras críticas de un Estado y al Estado como tal, obligando a reconocer la importancia de la seguridad en el ciberespacio y aceptando su complejidad, ya que las amenazas en el ciberespacio pueden tener numerosos orígenes (estatal o no estatal), afectar a las personas, dañar a las organizaciones y entorpecer el normal funcionamiento de instituciones (Sancho Hirare, 2017). Esto se da mediante múltiples acciones como el acceso fraudulento de información personal a través del engaño, el “ransomware” o secuestro de datos en el ciberespacio, robo de información en formato electrónico, “malware” que se han incrementado por mutación o por la aparición de nuevos softwares maliciosos.

Con lo anteriormente mencionado, para el caso específico de Colombia, se han evidenciado dos ciberataques recientes: El primero, es el caso de Anonymous[6] y su ataque a las páginas web de las entidades colombianas, en el cual estos "hacker/activistas" desde twitter invitaron a las personas a efectuar un ingreso masivo a la página del Ministerio de Educación, con la finalidad de colapsarla, ya que no estaban de acuerdo en que esta entidad buscara atraer capitales privados a las universidades. Luego, el ataque se extendió a otras entidades como el Ministerio de Defensa, El Senado y la Presidencia, generando que éstas fueran suspendidas temporalmente (Lozano Quintero, 2015).

El segundo, se dio a raíz de los diálogos de paz realizado en la Habana, en el 2014, en el cual se revelaron graves acusaciones en contra del "Hacker" Andrés Sepúlveda, por efectuar movimientos de ciberespionaje, acceso abusivo a un sistema informático, uso de software malicioso y la violación a datos personales. También, se encontró culpable por realizar interceptaciones a miembros del equipo negociador de la Habana, en donde se especula que fue contratado por grupos políticos interesados en asuntos de Seguridad Nacional, mediante operaciones ilegales de espionaje como interceptación telefónica y hackeo de correos electrónicos (Lozano Quintero, 2015).

Teniendo en cuenta lo expuesto anteriormente, se pueden evidenciar las teorías como la estructural funcionalista y la prospectiva. La primera se relaciona porque el Estado es un gran sistema complejo en donde interactúan muchos subsistemas, si uno falla, el todo colapsa de la misma forma; existe una interdependencia (Rodríguez, 2009). Desde lo privado, es necesario comprender las normas establecidas tanto en Colombia como en el mundo para prevenir ataques cibernéticos, establecer estructuras adecuadas para la aplicación de dichas normas y plantear qué estrategias son las más apropiadas para aplicar desde el sector específico que no solo ayudarán a la identificación de amenazas en dicho sector, sino a la prevención de las mismas amenazas en el sistema Estado en general. Asimismo, es importante destacar que la teoría estructural funcionalista contempla concepciones como

[6] Autodenominado 'hacktivistas', es el seudónimo de un grupo de hackers que no tiene una jerarquía ni ideología definida. Esto debido a lo poco que se conoce sobre ellos y la gran cantidad de miembros que tienen alrededor del mundo. https://capital.pe/tendencias/anonymous-quienes-son-y-que-han-hecho-hasta-el-momento-noticia-842990

estructuras, mecanismos, funciones, equilibrio y supervivencia o adaptación articulados con conceptos como rol de normas, la noción de integración, entre otros (Oquist & Oszlak, 1970). Dichos elementos, dan paso a la identificación de amenazas latentes que vulneren la seguridad digital de un Estado y de esta manera lograr proteger las infraestructuras (ya sean públicas o privadas) y tener una capacidad de respuesta óptima en cuanto al contexto estructural funcionalista que abarca mecanismos, adaptación, rol de normas, estructuras, entre otros; mencionados anteriormente.

Por otro lado, los ataques cibernéticos que han venido en aumento han creado una sensación de incertidumbre entre las compañías tanto privadas como públicas, y gracias a esto, ha crecido el interés por la seguridad informática. Teniendo en cuenta lo que se plantea en la teoría prospectiva que habla sobre la aversión a las pérdidas, que quiere decir que, en situaciones de incertidumbre, le damos mayor peso a aquellas decisiones que nos genere menos pérdidas (Figueroba, s.f).

Por lo tanto, el incremento en toma de acciones frente al tema de seguridad informática, puede estar ligado a la aversión a las pérdidas que analizan las empresas frente a una amenaza cibernética que pueda implicar grandes pérdidas. Además, cabe destacar que la prospectiva en el ámbito tecnológico es una de los instrumentos más utilizados en los métodos de planeación estratégica para la innovación que abarca sectores como el empresarial, académico, gubernamental entre otros. Lo anterior, vinculado con sectores de investigación y la planeación estratégica, que ocupan un elemento central en los mecanismos de esferas gubernamentales, empresariales y últimamente académicas para impulsar el desarrollo científico-tecnológico y la innovación, que contribuyen a la identificación y ataques de amenazas digitales, que bajo el lente prospectivo se de en un contexto de incertidumbre (Guarneros Navarrete, 2017).

Para finalizar este capítulo, es pertinente comprender, mencionar y explicar, los tipos de amenazas que ha presenciado el Estado colombiano y sus respectivas consecuencias que han generado contra las infraestructuras críticas comprendidas como instalaciones, redes, servicios y equipos físicos del sector privado. Dichos ataques, generan que cada empresa privada o pública, ya sea del sector financiero, de las telecomunicaciones, del Gobierno, entre

otros; se vean en la necesidad de tomar medidas regulatorias al respecto, con base a la protección de infraestructuras críticas y una capacidad de respuesta óptima. De tal manera, se da paso al segundo capítulo que abarca las medidas efectuadas del sector privado para dar frente a ataques que vulneran la seguridad digital de Colombia.

CAPÍTULO 2

Detallar las medidas que ha efectuado el sector privado para afrontar ciberataques y preservar la seguridad informática

Para hablar de medidas efectuadas por el sector privado en Colombia, cabe destacar que los ataques a la infraestructura crítica en Colombia y en el mundo, se ha convertido en una importante preocupación para los gobiernos y proveedores privados, ya sean ataques perpetrados por criminales cibernéticos que buscan beneficiarse con ganancias financieras o por hackers mediante actos políticos que buscan quebrantar la credibilidad de los gobiernos y las compañías (Organization of American States, 2015). Dichos ataques, generan en el sector privado la gran preocupación proteger sus infraestructuras y mejorar su capacidad de respuesta frente a delitos cibernéticos, en las cuales empresas como IBM, Claro Colombia, Ecopetrol, entre otros; se destacan de diferentes maneras, en el desarrollo de mecanismos que resguarden la seguridad digital en el país. Estos ataques se han vuelto más comunes y sofisticados y seguirán creciendo en el futuro próximo, por tal motivo es imperativo crear y efectuar medidas de seguridad digital que tengan una capacidad de respuesta efectiva a ataques cibernéticos.

Llegados a este punto, surge una estrategia nacional en el CONPES 3854, el cual debe ser consistente con el conjunto de principios formulados, debe crear los escenarios para que las múltiples partes interesadas puedan gestionar la seguridad digital de sus actividades económicas y sociales, debe impulsar la confianza en el entorno digital (OCDE, 2015) y, además, debe:

1. Estar apoyada desde el más alto nivel de gobierno.

2. Afirmar claramente que su objetivo es aprovechar el entorno digital abierto para la prosperidad económica y social.
3. Estar dirigida a todas las partes interesadas.
4. Ser el resultado de un enfoque intragubernamental, coordinado, abierto y transparente, donde participen las múltiples partes interesadas.

Con base en esto, el enfoque estructural-funcionalista de Robert Merton[7] brinda un concepto importante en este caso el cual es el de función reguladora, comprendida con relación al tema como una de las formas de intervención del Estado en múltiples ámbitos (políticos, económicos, sociales). Lo anterior, con la finalidad de corregir las fallas del Estado, en este caso sus fallas operacionales respecto a las medidas efectuadas en la seguridad digital del país, para garantizar su adecuada aplicación (Giraldo Saavedra, 2012). Llegado a esto, el Estado recurre al derecho con el objetivo de regular las acciones entre los diferentes actores que componen el Estado, que en temas de seguridad digital se comprenden como el Internet, las tecnologías de la información, entre otros (Giraldo Saavedra, 2012).

Ahora veamos, que la función reguladora es un fenómeno el cual presenta las grandes transformaciones a las que han sido expuestas las instituciones, desde el momento en cual el rol del Estado es el de garantizar las reglas del juego. Esto, surge como resultado de las relaciones entre agentes económicos, políticos y sociales como respuesta y posible solución a los problemas surgidos en el llamado Estado de bienestar (Giraldo Saavedra, 2012). En este caso, aplicado en un Estado digitalizado, que se mueve mediante las redes o el ciberespacio bajo el lente público, privado o mixto. Bajo este contexto, se designa tanto la presencia de reglas de derecho sobre una cuestión determinada (en este caso reglas sobre la seguridad digital), como la actividad y el proceso de producción de las mismas y su adecuada aplicación y capacidad de respuesta (Giraldo Saavedra, 2012).

[7] Sociólogo estadounidense. Sus investigaciones se enfocaron en la sociología del conocimiento y la teoría sociológica y sus análisis fueron basados en un método funcional-estructural, según el cual los hechos sociales y sus funciones deben ser considerados como subsistemas del conjunto social, lo convirtieron en una de las figuras más relevantes de la sociología anglosajona.
https://www.biografiasyvidas.com/biografia/m/merton_robert.htm

De la mano a lo anteriormente mencionado, mediante los ministerios a cargo se requirió la realización de mesas de trabajo durante los años 2014 y 2015 con expertos nacionales e internacionales junto con la participación de miembros de los ministerios que conforman la comisión, del colCERT, del CCOC, del CCP, de las unidades cibernéticas de las Fuerzas Militares, y del sector público y privado (OEA, 2014). Estos actores platearon medidas regulatorias regidas por cinco dimensiones:

1. Gobernabilidad y coordinación efectiva.
2. Preparación y prevención.
3. Conocimiento de la situación actual.
4. Resiliencia, recuperación y respuesta.
5. Efectiva cooperación e intercambio de información.

Avanzando en nuestro razonamiento, cabe destacar el concepto PPP *"Public Private Partnership"* comprendido como asociaciones de carácter público-privadas, en las cuales se realizan formas de cooperación entre las autoridades públicas (mencionadas anteriormente como el colCERT) y el sector privado (como IBM, Ecopetrol, Asobancaria, entre otros). Estas asociaciones tienen como objetivo garantizar el financiamiento, la construcción, la renovación, la gestión, el mantenimiento de las infraestructuras y la prestación de servicios (Partnerstva Kosovo & Ministry of Economy and Finance, s.f). A nivel global, las asociaciones público-privadas crecen notablemente en cuando a la contratación pública en todo el mundo, demostrado en los últimos 10 años en el que los gobiernos y autoridades públicas acuden cada vez más a las PPP, como una herramienta de entrega de infraestructura en diferentes sectores que ocupan la agenda global (Singer & Friedman, 2014). Observando así, un rol determinante del sector privado en temas de seguridad digital y defensa a nivel regional y global.

Por otra parte, según Espinoza (2015), una Estrategia Nacional de Ciberseguridad por parte del sector privado que permita la disminución o erradicación total de ataques cibernéticos, debe tener cinco ejes claves:

1. La definición de un marco jurídico robusto.

2. La difusión de información y culturización a la población sobre temas de ciberseguridad y protección de datos.
3. La capacitación de personal en la temática.
4. El trabajo conjunto entre gobierno y sector privado.
5. El fortalecimiento de la ciberdefensa.

Estos ejes mencionados, ya han sido ejecutados por varios países a nivel mundial con mayor o menor desarrollo entre los que se pueden mencionar a Estados Unidos, Alemania y Reino Unidos; y de manera más reciente: Corea del Sur, Argentina, Francia, Colombia, Suiza, Bélgica, Panamá, Noruega, España, Kenia, entre otros (Olmedo & Gavilanez, 2018)

Gremios del sector privado, han analizado cómo abordar la seguridad digital bajo una orientación de política que se ajuste a los cambios del mercado, y permita que las organizaciones y los ciudadanos entiendan, evalúen y tomen las medidas apropiadas para afrontar las incertidumbres y los riesgos en el entorno digital (OCDE, 2015). Las medidas para gestionar los riesgos en el entorno digital deben tener en cuenta la protección de los derechos humanos y de los valores nacionales, las cuales deben intervenir de manera positiva al desarrollo de actividades socioeconómicas en el medio digital.

Para la empresa del sector privado IBM, en cuanto a amenazas de ciberseguridad, nadie es inmune y se enfoca en "si eres atacado" a "lo rápido que puedes responder" comprendido como la capacidad de respuesta. Por esto, IBM está ayudando a que los usuarios desarrollen un sistema inmune integrado e inteligente, en el que las soluciones de seguridad empresarial trabajan para prevenir y subsanar los daños que los ciberataques pueden provocar a su compañía (IBM, s.f). Por tal motivo, crean un sistema inmune de seguridad integrado e inteligente, explicado de la siguiente manera:
(Figura 3: Sistema inmune de seguridad integrado e inteligente IBM)

Por otra parte, en Claro la empresa de servicios de comunicaciones mediante su Centro de Operaciones de Ciberseguridad, trabaja en la importancia de gestionar mejor el riesgo de un ataque cibernético con el apoyo de proveedores, usuarios, individuos y

organizaciones. Es así, que, en el 2018, más de 2 millones de eventos de seguridad se realizaron al día que protegieran rápidamente y de manera efectiva los servicios propios como los que les prestan a otras compañías junto con la confidencialidad de la información y datos de carácter personal de sus usuarios (Claro Colombia, s.f). De esta manera, Claro Colombia propone ciertas recomendaciones que se deben aplicar como:

1. Tener un modelo de seguridad que se anticipe y responda inmediatamente a cualquier tipo de peligro cibernético en tiempo real.
2. Proteger toda la infraestructura de nube, sistemas físicos y dispositivos móviles de su empresa con un backup para resguardar la información sensitiva de su empresa.
3. Tener siempre un respaldo en línea de los archivos, para sincronizarlos y acceder a ellos desde cualquier sitio.
4. El uso del Big Data Analytics para la monitorización, prevención y detección de fraude en tiempo real y de las tecnologías Blockchain integradas a la generación de nuevos desarrollos en la prestación de servicios, como parte de las soluciones de seguridad.
5. Evitar errores humanos de manejo inadecuado de la información de los clientes, por esto se recomienda capacitar a los empleados en ciberseguridad para empresas y así están alertas e implementan protocolos de seguridad.

En cuanto a ECOPETROL, la finalidad de los sistemas de control e instrumentación en términos ciberdefensivos, es garantizar la operación confiable y segura de los procesos productivos y por tanto su gerenciamiento debe realizarse como cualquier equipo del ámbito industrial basados en la gestión de activos. En este punto, las tecnologías de la información y las tecnologías de la operación, pueden comprenderse en el espacio industrial mediante: las tecnologías de IT, comprendidas en el tratamiento de volúmenes de datos a través de infraestructura de telecomunicaciones. Y las tecnologías de OT, entendidas como el monitoreo, control y seguridad de los procesos industriales, con el fin de proteger todo tipo de información que manejan (Velásquez Lombana & Pusey Mitchell, s.f). (Figura 4: Enfoque prioritario entre las tecnologías IT y OT) (Figura 5: Diferencias redes IT y OT)

Con base a lo anterior, se entiende la confidencialidad como "la Información disponible exclusivamente a personas autorizadas; la integridad como el mantenimiento de la exactitud y validez de la información, protegiéndola de manipulaciones o alteraciones y la disponibilidad como el acceso y utilización, al momento de ser solicitada por una persona autorizada" (Velásquez Lombana & Pusey Mitchell, s.f).

En consonancia con el sistema internacional, se observa que los Estados Miembros de la OEA aprobaron la Estrategia Interamericana Integral para Combatir las Amenazas a la seguridad cibernética en la resolución AG/RES. 2004 (XXXIV-O/04) (OEA, 2018). Esta estrategia, tiene la finalidad de buscar la construcción de capacidades de seguridad cibernética entre los Estados Miembros, aprobando que la responsabilidad nacional y regional para la seguridad digital recae en entidades tanto del sector público como el privado, tomando aspectos políticos y técnicos (OEA, 2018).

Por su parte, Asobancaria se asoció con la OEA para fortalecer la ciberseguridad en el sector financiero tanto en lo público, en lo empresarial y en la sociedad en general. Esta iniciativa nace como respuesta al crecimiento de nuevas tecnologías que pone como prioridad crear mejores salvaguardas en el sector financiero. De esta forma, se crea el primer centro de respuesta de seguridad cibernética en el sector financiero en América Latina (OEA, 2018).

De igual forma, uno de los objetivos del acuerdo era establecer vínculos de cooperación entre las entidades privadas, lo cual se ve evidenciado en el CSIRT[8] de Asobancaria. El último, es un equipo de apoyo para dar respuesta a incidentes cibernéticos, el cual tiene un enfoque colaborativo. Por lo tanto, uno de sus objetivos es la sensibilización de entidades sobre la importancia de la ciberseguridad y la protección de las infraestructuras

[8] Definición de CSIRT (Computer Incident Response Team): Organización responsable de recibir reportes de incidentes de seguridad, analizarlos y responderlos. En Colombia, es el equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL, un grupo creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones. Tomado de: https://cc-csirt.policia.gov.co/Publicaciones/quienes_somos.

tecnológicas con el fin de prevenir perjuicios y mitigar el impacto ocasionado por la materialización de riesgos (Asobancaria, 2018).

De esta manera, empresas pertenecientes al sector privado al verse bajo cierto nivel de riesgo e incertidumbre frente a posibles ataques de carácter digital, a nivel teórico es viable aplicar y comprender la teoría prospectiva expuesto como un modelo normativo de elección racional (Kahneman & Tversky, 1987). En este contexto, se toman en cuenta al tomar una decisión las pérdidas y ganancias de esta, que en términos de seguridad se entendería como los beneficios y perjuicios que pueda ocasionarle, generando una mayor eficiencia al momento de plantear mecanismos regulatorios en el ciberespacio que protejan las infraestructuras críticas y tengan una capacidad de respuesta óptima, disminuyendo pérdidas o perjuicios que afecten al Estado y la sociedad en general.

Por otro lado, B-secure sostiene que la única forma de estar seguro frente a las amenazas que provienen de múltiples lugares está en "análisis integral capaz de detectar comportamientos sospechosos, generar alertas en tiempo real y determinar con el comportamiento global de los sistemas que un compromiso se ha producido". De ahí nace el Centro de Operaciones de Seguridad (B-secure, s.f.), con el cual reducen y eventualmente eliminan riesgos para los negocios, contando también con la capacidad de automatización y orquestación de seguridad que agiliza la capacidad de respuesta frente a los incidentes.

IQ Information Quality, está regido por la norma PCI DSS, la cual es un conjunto de prácticas óptimas en la industria con respecto a la protección de la información de tarjeta habiente, ayudando con esto a la protección de los pagos electrónicos. De esta manera, realizan un análisis de riesgos, un escaneo de vulnerabilidades a nivel interno y externo, capacitación en el manejo de la norma ya mencionada y desarrollo seguro del software, entre otros servicios (Guía soluciones TIC, s.f).

Teniendo en cuenta que las empresas mencionadas anteriormente corresponden a un sector económico distinto, se puede evidenciar la teoría estructural funcionalista. Cada uno de los sectores económicos representa una parte de una gran estructura, de acuerdo con la teoría, dicha estructura sólo puede sobrevivir por medio de la cooperación y que la

cooperación depende de un consenso, de unas reglas de conducta (Gallardo, s.f). Es así como cada empresa, por medio de los esfuerzos que realizan individualmente, están aportando para la que la seguridad cibernética del país en general avance cada vez más, y las reglas de conducta, en este caso, son los estándares y normas internacionales que están adoptando muchas empresas para el mejoramiento de la ciberseguridad.

En términos de la teoría de la turbulencia y el caos con base al contexto digital, se hace referencia a un sistema dinámico fuertemente sensible, que genera cambios impredecibles de otro sistema (Ramz, s.f). En las relaciones internacionales y bajo el lente de seguridad digital es concebido como el inicio de nuevos fenómenos internacionales, originados a partir de movimientos y decisiones entre diferentes Estados y actores de orden privado y social como empresas y OIG's (Ramz, s.f). De esta manera, en cuanto a las medidas efectuadas por el Estado para enfrentar ataques cibernéticos, su aplicación se evidencia en el estudio de realidades internacionales (en este caso la realidad cibernética), actores, fuerzas de orden privado y en la manera como generan nuevas estructuras de poder político y su adecuada reglamentación, aplicada en la seguridad digital mediante medidas y acciones de carácter normativo (Arrighi & Silver, 2001).

En definitiva, se evidencia el accionar de empresas pertenecientes al sector privado en Colombia con énfasis en la protección de las infraestructuras críticas y la capacidad de respuesta. Dichas maniobras, generan que el Estado cuente con una asociación entre lo privado y lo público que logre responder efectiva y eficazmente problemas de carácter digital que presenta el Estado y vulnera su adecuado funcionamiento a nivel doméstico y en la agenda global. De esta manera, varias empresas de carácter multinacional presentes en Colombia, que soportan y apoyan temas de ciberseguridad y ciberdefensa, generen que el país esté más presente a nivel internacional en temas de seguridad digital y busque posicionase de manera positiva en la arena internacional junto con Tratados, Cooperación y relaciones con otros Estados, como se expondrá en el siguiente capítulo.

CAPÍTULO 3

Exponer la situación del sector privado en Colombia a nivel global, en términos de seguridad digital.

En este capítulo, para exponer la situación de Colombia a nivel mundial cabe destacar que la importancia del valor de la información digital a nivel global y el aumento progresivo de la desconfianza en cuanto a la utilización del Internet (Linares Lizarazo, 2018). Por ende, ha ocasionado que grandes Organizaciones Internacionales como la ISO[9], NIST[10], ISACA[11], entre otras: a realizar proyectos de investigación enfocados a disminuir la incertidumbre, mediante operaciones de gestión de seguridad de la información, amparado a la normatividad internacional, las leyes y las buenas prácticas para disponer de la mejor capacidad para realizar acciones que protejan las infraestructuras críticas en un Estado y su respectiva capacidad de respuesta (Linares Lizarazo, 2018).

Hecha esta salvedad, Colombia fue unos de los países que mayor progreso demostró en el campo digital durante la última década, ubicándose en la cuarta posición frente a sus pares de la región. Aunque este progreso trae importantes beneficios, se genera mayor dependencia a la tecnología, y expone un alto riesgo de incidente cibernético que atente contra los sectores de la sociedad nacional, ya sean mixtos o privados (CCIT & Centro de Investigación Económica y Social, 2014). (Figura 6: Posición de Colombia a nivel regional)

Llegados a este punto, el tema de seguridad en las Relaciones Internacionales se toma como un objeto de estudio, que busca interpretar varios problemas y estructurar el debate acerca de elementos que se estudian cada uno por su cuenta, como lo es el este caso la seguridad digital. Adicionalmente, abarca fenómenos como la industria, el comercio, la

[9] ISO (International Organization for Standardization)*:* Es la Organización Internacional de Normalización**,** cuya principal actividad es la elaboración de normas técnicas internacionales.
[10] NIST (National Institute of Standards and Technology): Es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.
[11] ISACA (Information Systems Audit and Control Association): Asociación que ayuda a los profesionales globales a liderar, adaptar y asegurar la confianza en un mundo digital en evolución ofreciendo conocimiento, estándares, relaciones, acreditación y desarrollo de carrera innovadores y de primera clase.

inversión internacional, la elaboración de la política exterior, la dinámica del sistema y la soberanía, los cuales se desenvuelven dentro de un amplio marco a nivel global (Orozco, 2006). De esta manera, se observa que el objeto de estudio del concepto de seguridad con base a los fenómenos que se desenvuelven en el Sistema Internacional, son elementos que posicionan a un Estado (ya sea a nivel global o regional) en términos de seguridad digital. El motivo está, en las diferentes variables que se estudian, como lo es la política exterior de un país, la cual enmarca diversas dimensiones (de ciberseguridad, en el caso específico) y ejecuta acciones regulatorias o normativas que sistematicen temas específicos, los cuales poseen un nivel de afectación a nivel global. De esta manera, expone las habilidades que tiene un Estado a nivel mundial como lo es su capacidad de respuesta y su protección a las infraestructuras críticas.

No obstante, Colombia sobrelleva problemas significativos en temas de ciberseguridad, pero esas fallas no son tan críticas si se comparan con las de otros países de la región, e incluso del mundo desarrollado en general (Comparitech, 2019). Este balance se realizó entre 60 países estudiados, donde Argelia, ocupó el primer puesto, respecto a los peores índices de ciberseguridad, y Japón, por el contrario, en el último puesto, lo que significa que tiene los mejores índices en términos de ciberseguridad (Semana, 2019). Colombia quedó en el puesto 39, lo que significa que el país está en el rango medio de la seguridad en la red (Semana, 2019).

Con base a esta información, se evidencia la aplicabilidad de la teoría de la información, respecto a que esta, se enfrenta a la necesidad de mutarse, en cuanto a sus categorías, para lograr su objetivo de cartografiar todo conocimiento y todo fenómeno de carácter comunicativo e informativo que suceda en el mundo (Aladro Vico, 2011). Que, bajo el lente del ciberespacio, esta teoría se adaptaría a los múltiples enfoques y cambios de contexto que han ido surgiendo en la vida social informativa (Aladro Vico, 2011). Teniendo en cuenta esta explicación, se evidencia que países vulnerables en términos de ciberseguridad como Argelia, presentan poca adaptabilidad a los cambios dinámicos que presenta el mundo en general, en temas de carácter informático o cibernético (así como lo expone la teoría de la información). En el caso de Colombia, su nivel de adaptación y mutación respecto a la

seguridad digital no es la mejor, pero tampoco la peor a nivel mundial; es un Estado que avanza progresivamente y se va posicionando poco a poco.

No obstante, al país no le fue muy bien en la calificación de su legislación, la cual evalúa qué tan actualizada está para ofrecer garantías que resguarde la seguridad digital. El puntaje fue de 4 sobre 10, aunque ningún país pasó de 7, ni China ni Francia (Semana, 2019). En este estudio, se logra articular lo que propone Talcott Parsons y Robert K. Merton, en su teoría estructural funcionalista, al plantear la importancia de las normas (acciones regulatorias) para el orden social, en el cual los cambios que experimenta una parte producen cambios en todo el sistema y mantiene un equilibrio (UNIR, 2006). Es así, como se observa la búsqueda de regular y resguardar el entorno digital, mediante actos legislativos y normativos, que logren buscar un equilibrio favorable para el Estado y lo ubique en una posición que lo beneficie y no transgreda su seguridad a nivel informático.

Respecto a qué tan competente está el país para resistir un ciberataque, el puntaje que se lleva es de 0,56, cuando 1 es el tope. Por otro lado, Colombia no esta tan mal, respecto a la cantidad de ataques cibernéticos y en los ataques con software que infecta dispositivos para la minería de criptomonedas[12] sin autorización (Semana, 2019). Según dicho análisis, en Colombia se producen el 0,5% de los ataques al software financiero con el que se pretende robar a los usuarios. En este aspecto, los datos giran en torno a la capacidad de respuesta de Colombia ante un ciberataque y se evidencia que no es la más óptima, que aún requiere de mucho trabajo para que sus acciones sean eficaces y eficientes, para lograr crear condiciones que gestionen el riesgo de la Seguridad Digital en las actividades socioeconómicas y de esa manera, genere mayor confianza en el uso del entorno digital (Contreras, 2019).

Por otra parte, un estudio realizado por la compañía McAfee[13] y la Organización de Estados Americanos (OEA), Colombia se posicionó como el sexto país en generar una mayor actividad maliciosa en línea para el año 2013. Estos ataques han estado encaminados a todas

[12] Son monedas virtuales. Pueden ser intercambiadas y operadas como cualquier otra divisa tradicional, pero están fuera del control de los gobiernos e instituciones financieras. https://www.ig.com/es/invertir-en-criptomonedas/que-son-las-criptomonedas

[13] Compañía de software especializada en seguridad informática

las esferas de la economía, los delincuentes digitales se han enfocado especialmente contra los ciudadanos, el sector bancario, la fuerza pública y el Gobierno Nacional según el balance del Centro Cibernético Policial (CCP) (Linares Lizarazo, s.f). Se demostró que al menos tres de cinco empresas en la región, sufrieron por lo menos un incidente de seguridad mediante códigos maliciosos. Complementario a esto, una de cada cinco empresas encuestadas en Latinoamérica fueron víctimas del secuestro de información, según ESET[14] Latinoamérica (2018) (Contreras, 2019).

A nivel internacional, mediante diferentes organizaciones, como la Unión Internacional de Telecomunicaciones (ITU, 2015), se desarrolló el Índice Mundial de Ciberseguridad (IMC) por medio de un trabajo conjunto con la ABI Research[15], que pretende medir el nivel de compromiso de Estados soberanos en cuanto a la ciberseguridad (Serna Patiño, 2018). Esto permite clasificar cada Estado en un ranking mundial en términos de preparación, para responder asuntos relacionados con la seguridad digital, y así se logre medir la existencia de estructuras nacionales para implementar y promover la ciberseguridad (ITU, 2015 p 11). (Figura 7: Grado de compromiso nacional)

Acorde con lo anterior, Colombia tiene un índice de 0.588, ocupando la posición número 9 a nivel mundial, lugar que comparte con países como Dinamarca, Egipto, Francia y España (Serna Patiño, 2018). El ranking se encuentra liderado por Estados Unidos con una puntuación de 0.824, seguido por Canadá y Australia. Hay que mencionar, además su relación con la propuesta estructural funcionalista de Merton, quien habla acerca de los sistemas de acción de la sociedad, la cual se encuentra dividida en cuatro subsistemas: (1) Una comunidad Societaria con un componente estructural basado en las normas, un desarrollo basado en la inclusión y con la función de integrar. (2) Un fiduciario o de mantenimiento de patrones con un componente estructural enfocado hacia los valores, un desarrollo orientado en la generalización de los valores y con la función primeria de mantener

[14] Empresa pionera en protección antivirus, nació con la creación de un multipremiado software para la detección de amenazas. https://www.eset.com/co/acerca-de-eset/
[15] Firma de asesoría de mercado, que ofrece orientación estratégica sobre las tecnologías transformadoras más convincentes.

los patrones. (3) Una constitución política con un componente estructural basado en las colectividades, un desarrollo cimentado en la diferenciación y con la función de alcanzar metas. (4) Una economía con un componente estructural enfocado en los papeles (roles), un desarrollo orientado en el ascenso de adaptación y con la función primaria de adaptarse (Sánchez Pinilla, 2006).

Es por esto que, los resultados mencionados anteriormente con base a la teoría, demuestran que es imperativo buscar una adaptación en el medio para tener resultados favorables que paralelamente correspondan a una puntuación favorable para cada Estado. Dicha adaptación va de la mano con normas que reglamenten el entorno informático y se alcancen metas beneficiosas a nivel regional e internacional para Colombia, que le permita superar y ascender la posición en la que se encuentra (novena) mundialmente y supere las falencias que tiene a nivel sistemático, educativo, legal, económico, entre otros.

Ahora bien, de acuerdo con la UIT[16], países que no cuentan con una estrategia de seguridad obtienen una buena calificación en sus informes, como por ejemplo Brasil, Japón, Omán o Colombia, que superan o igualan la clasificación de España (que ya tiene publicada la estrategia o están en proceso de su elaboración) (Instituto Español de Estudios Estratégicos, 2015). Lo anterior evidencia una posición relativamente sobresaliente de Colombia bajo esta medición, exponiendo a nivel mundial la necesidad de fortalecer algunos elementos asociados a la ciberseguridad para enfrentar los riesgos que trae consigo la tecnología de manera eficiente, eficaz y oportuna, como se plantea en los objetivos que rige el trabajo de investigación.

De esta manera, en términos teóricos se aplicaría la teoría estructural funcionalista, en el ámbito de que esta toma una perspectiva dinámica de la sociedad internacional privilegiando algunos tipos de procesos o relaciones que se dan en la arena internacional (Calduch, 1991). Estas poseen una visión común de la sociedad internacional, en la cual se dan métodos de reajuste y mutación, como una realidad social en constante dinamismo

[16] Organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación – Tic. https://www.itu.int/es/about/Pages/default.aspx

(Calduch, 1991). Es así, que con una visión global que tome en cuenta variables como iniciativas políticas y económicas para establecer o desarrollar organizaciones y/o procesos de integración supranacional, se da paso a un análisis más consensuado en términos globales respecto a la posición de Colombia en el mundo, frente a la seguridad digital. El motivo está, en el amplio espectro que toma la teoría y las múltiples variables que comprende para su comprensión y respectiva aplicabilidad.

Según CEPAL[17] (2014), se ha solidificado una economía basada en tecnologías comprendida como 'economía digital', la cual es un facilitador cuyo desarrollo y despliegue se produce en un ecosistema internacional caracterizado por la creciente y acelerada correlación entre diversas tecnologías. Estas se rigen por tres componentes principales: (1) la infraestructura de redes de banda ancha, (2) la industria de aplicaciones TIC y (3) los usuarios finales (CONPES, 2018). Lo anterior, se menciona con el fin de demostrar que, en el aspecto regional, Colombia se ha posicionado como uno de los países que más ha avanzado en la región en aspectos relacionados con Ciberseguridad y Ciberdefensa, lo cual se refleja en estadísticas formales, tales como el Índice Mundial de Ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT). Así, el país se ubica actualmente en el quinto lugar del ranking a nivel regional, siendo superado por Estados Unidos, Canadá, Brasil y Uruguay (como se mencionó anteriormente, pero haciendo énfasis en la posición regional) (CONPES, 2018).

Conforme a lo mencionado, se vincula la teoría de la turbulencia o caos, debido a que se esboza ámbitos de la vida y la naturaleza, que son altamente impredecibles pero que no se puede afirmar que presenten comportamientos sin ley, dado que existen pautas que determinan el comportamiento (Lizcano, 2000). Dicha incertidumbre se desarrolla en el avance o progreso que tenga cada país, respecto a sus puntajes a nivel mundial en termino de seguridad digital, ya que no se sabe que otras variables puedan surgir con el tiempo que hagan

[17] Comisión Económica para América Latina: Es una de las cinco comisiones regionales de las Naciones Unidas y su sede está en Santiago de Chile. Se fundó para contribuir al desarrollo económico de América Latina, coordinar las acciones encaminadas a su promoción y reforzar las relaciones económicas de los países entre sí y con las demás naciones del mundo. Posteriormente, su labor se amplió a los países del Caribe y se incorporó el objetivo de promover el desarrollo social. https://www.cepal.org/es/acerca

que mejore o empeore la seguridad informática en un país, no se tiene certeza que medidas o acciones realice un Estado para salvaguardar sus infraestructuras críticas y, por ende, siempre existirá incertidumbre. Por otra parte, también se relaciona en el ámbito de la existencia de pautas de comportamiento (conocidas en este caso como medidas o normas), las cuales, a pesar de existir siempre incertidumbre, deben existir elementos que normalicen la conducta de un Estado y, asimismo, sean un camino para que corrijan sus falencias y les abran posibilidades para mejorar en puntuaciones y posiciones mundialmente, con base a su capacidad de respuesta y la protección de sus infraestructuras críticas.

Como resultado, toda la información compilada en este capítulo, expone un panorama general respecto a la posición de Colombia en el mundo y a nivel regional, en temas de ciberseguridad. Así, se evidencia que a pesar de ser un país "débil" en varios factores que derivan del ciberespacio, no es el peor de todos y ha demostrado desde el primer CONPES 3701 de 2011, el CONPES 3854 de 2016 (contemplado en este trabajo de grado) hasta la actualidad, que Colombia junto con el sector privado y mixto, han presentado propuestas, leyes, documentos, entre otros; que buscan erradicar el cibercrimen o los ciberataques que atentan contra las infraestructuras del Estado y entorpecen su capacidad de respuesta. Adicionalmente, su vinculación a Tratados Internacionales, su búsqueda de cooperación y vinculación con organismos internacionales como la OEA, la OCDE, entre otros; genera que se encuentre más presente en la arena internacional y ascienda su posición regional e internacional en temas se ciberseguridad y ciberdefensa.

CONCLUSIONES

El sector privado y mixto, tiene grandes retos respecto a la consolidación de la seguridad digital que abarca temas de privacidad y/o secretos empresariales, para lograr proteger sus infraestructuras críticas, conocer y reconocer las amenazas cibernéticas generadas a través de la web y así, lograr tener una capacidad de respuesta efectiva (Contreras, 2019). Para esto, no solamente es necesario el uso y manejo de tecnologías de la

información, también es apropiado hablar e involucrar de una gestión de riesgos apropiada, capacitación y concientización, acceso a herramientas que permitan una mayor dinámica en términos de actualización y disminuyan el elevado número de vulnerabilidades que aumentan paralelamente con el crecimiento del uso del Internet de las cosas[18] "Internet of Things", dispositivos electrónicos, entre otros. Así se beneficiaría las dos variables que rigen este trabajo de investigación que son la protección a las infraestructuras críticas y la capacidad de respuesta.

Primero, con base a la identificación de amenazas cibernéticas del sector privado, se demostró que, si se han ejecutado estrategias que busquen dar respuesta a ataques de tipo informáticos por parte de empresas privadas y logren identificar la presencia de amenazas latentes, sin embargo, no han sido suficientemente efectivas. El motivo está, en que las empresas día a día son más vulnerables, debido a que la gran mayoría de actividades que se realizan en la actualidad se han automatizado y demandan de una conexión continua a la red que buscan el crecimiento del sector productivo, pero los exponen más a ser atacados. El aumento del uso de las Tecnologías de la Información y las comunicaciones, aumenta y da paso a nuevos riesgos asociados con la confidencialidad y protección de la información.

Bajo este enfoque, en el caso colombiano, se estima que con el Convenio del Congreso de Colombia y su firma en la Ley que aprueba el Convenio sobre la Ciberdelincuencia, realizado en Budapest en 2001, se logre disminuir los ataques cibernéticos, pero antes de ello se logren identificar a tiempo y se actúen de la mejor manera, tomando siempre en cuenta que, acciones delictivas como estas de tipo informático, tendrán consecuencias penales. Por ende, en este contexto es importante mencionar la teoría cibernética, ya que propone que los canales de comunicación se relacionan con la toma de decisiones del gobierno, en este caso las decisiones para lograr identificar amenazas. También sobresale la teoría estructural funcionalista para comprender las normas

[18] Refiere a la interconexión digital de objetos cotidianos con Internet.

establecidas tanto en Colombia para prevenir ataques que vulneran la seguridad digital del país.

En segundo lugar, respecto a las medidas que ha efectuado el sector privado para enfrentar ataques cibernéticos, cabe destacar que, a pesar de la poca participación del sector privado para preservar la seguridad digital en Colombia, les preocupa proteger sus infraestructuras y mejorar su capacidad de respuesta. Por ende, empresas como del sector financiero como Asobancaria, del sector de servicios como Claro Colombia y Direct TV, y de otros sectores como IQ Information Quality, B-secure, Ecopetrol, entre otros; pertenecientes al sector privado buscan evaluar y tomar medidas apropiadas para afrontar incertidumbres y riesgos en el entorno digital (Teoría de la turbulencia) basadas en la protección de infraestructuras críticas y su respectiva capacidad de respuesta. Cada empresa, de carácter privado tienen una manera diferente de desarrollar dichas variables.

Por ejemplo, la capacidad de respuesta por parte Claro Colombia se enfoca en una adecuada gestión de riesgos y su protección a las infraestructuras se basa en un modelo de seguridad que se anticipe y responda rápidamente ataques cibernéticos, junto con un backup para proteger la información, el uso del Big Data Analytics, entre otros. Empresas como Asobancaria centran su capacidad de respuesta en constituir relaciones de cooperación entre las entidades privadas, como el CSIRT, para tener un equipo de apoyo para dar pronta respuesta a ciberataques; en cuanto a la protección de infraestructuras se encamina hacia la sensibilización de entidades sobre la importancia de la ciberseguridad y la protección de las infraestructuras tecnológicas. Destacando siempre las pérdidas y ganancias (Teoría Prospectiva).

En tercer lugar, al exteriorizar la situación de Colombia en términos de seguridad digital a nivel mundial, es claro que Colombia a pesar de no tener medidas efectivas y eficaces, fue unos de los países que mayor avance demostró en el campo digital durante la última década a nivel regional. Sin embargo, se debe mencionar que el país posee problemas importantes en temas de ciberseguridad y su respectiva legislación, pero no son tan graves si se realiza una comparación con otros países de la región como El Salvador o a nivel mundial

como Argelia. A nivel regional según el Índice Mundial de Ciberseguridad de la Unión Internacional de Telecomunicaciones, Colombia se posiciona en el quinto lugar, siendo superado por Estados Unidos, Canadá, Brasil y Uruguay. A nivel global, Colombia ocupa la novena posición, lugar que comparte con países como Dinamarca, Egipto, Francia y España, en cuanto al nivel de compromiso respecto a la ciberseguridad.

De esta manera, en términos teóricos se habla de la teoría de la turbulencia, respecto al desarrollo y ascenso que tenga cada Estado, con base a su posicionamiento a nivel regional o global, ya que se da en un contexto de poca certeza e incertidumbre. En cuanto a la teoría estructural funcionalista y la teoría de la información, se evidencia en términos de mutación a los constantes cambios que tiene el mundo, así que se busca una adaptabilidad a cada contexto que abarca temas de la agenda global como lo es la política exterior, economía, tecnologías, entre otros (regidos por normas); los cuales son elementos claves para posicionar a un Estado en el Sistema Internacional.

Para concluir, es imperativo realizar una advertencia al sector privado y público, de aportar más e involucrarse más en temas de seguridad digital y defensa, ya que, así como se utiliza la tecnología para beneficiarse de múltiples maneras, también "ciberdelincuentes" utilizan este mismo para realizar ataques que afectan la producción y distribución de grandes empresas, como el sector petrolero, de gas y energía. En el caso de Colombia y América Latina en general, se evidencia un gran interés por investigar más del tema cibernético y sus respectivas implicaciones (positivas y negativas), pero el nivel presupuestal, a comparación de países europeos y de Estados Unidos, es mucho menor y, por ende, obstaculiza este interés de progresar en el entorno digital. Se espera, que en un futuro próximo Colombia siga mejorando como lo ha hecho en la última década y alcance los más altos estándares de ciberseguridad y ciberdefensa para lograr cumplir correctamente con las dos variables que rigen este trabajo de investigación, como lo es la protección de las infraestructuras críticas y la capacidad de respuesta.

BIBLIOGRAFÍA

¿Qué es ISO?. Retrieved from https://www.fundibeq.org/informacion/infoiso/que-es-iso

¿Qué es la OCDE?. (2018). Retrieved from http://www.exteriores.gob.es/RepresentacionesPermanentes/OCDE/es/quees2/Paginas/default.aspx

¿Qué es un CSIRT? | CSIRT-ANTEL. Retrieved from https://www.csirt-antel.com.uy/node/3

¿Qué son las criptomonedas y qué es el trading de criptomonedas?. Retrieved from https://www.ig.com/es/invertir-en-criptomonedas/que-son-las-criptomonedas

"La seguridad de la información es un ejercicio de construcción conjunta" Jeimy Cano. (2016). Retrieved from https://www.ecopetrol.com.co/wps/portal/es/ecopetrol-web/contratistas/informacion-general/noticias/2016/contenido/seguridad-informacion-responsabilidad

Acerca de ESET. Retrieved from https://www.eset.com/co/acerca-de-eset/

Acerca de ISACA. Retrieved from http://www.isaca.org/spanish/Pages/default.aspx

Acerca de la CEPAL | Comisión Económica para América Latina y el Caribe. Retrieved from https://www.cepal.org/es/acerca

ALADRO VICO, E. (2011). La Teoría de la Información ante las nuevas tecnologías de la comunicación. Retrieved from https://webcache.googleusercontent.com/search?q=cache:86tIQhiUWIYJ:https://revistas.ucm.es/index.php/CIYC/article/download/36988/35797+&cd=2&hl=es-419&ct=clnk&gl=co

Alfaro Calvo, P., Díaz Tejera, A., García García, E., & Sánchez Benítez, S. (2013). RIESGOS Y AMENAZAS EN EL CIBERESPACIO. SITUACIÓN ACTUAL. Retrieved from

https://www.researchgate.net/publication/301754465_RIESGOS_Y_AMENAZAS_EN_EL_CIBERESPACIO_SITUACION_ACTUAL

Amenazas del Cibercrimen en Colombia 2016-2017. (2016). Retrieved from https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Anonymous: ¿Quiénes son y qué han hecho hasta el momento? | Radio Capital. (2015). Retrieved from https://capital.pe/tendencias/anonymous-quienes-son-y-que-han-hecho-hasta-el-momento-noticia-842990

Arrighi, G., & Silver, B. (2001). Caos y orden en el sistema-mundo moderno. Retrieved from https://books.google.com.co/books?id=jXQgFWbFLZwC&printsec=frontcover#v=onepage&q&f=false

Así está Colombia en el ranking de ciberseguridad mundial. (2019). Retrieved from https://www.semana.com/nacion/articulo/asi-esta-colombia-en-el-ranking-de-ciberseguridad-mundial/601118

Avances y retos de la defensa digital en Colombia. (2014). Retrieved from https://www.ccit.org.co/wp-content/uploads/Avances-y-retos-de-la-defensa-digital-en-Colombia-Noviembre-de-2014-Fedesarrollo.pdf

Betancourt Higareda, F. (2017). Una perspectiva estructural funcionalista del Estado de derecho y la seguridad Pública en México. Retrieved from https://archivos.juridicas.unam.mx/www/bjv/libros/9/4443/15.pdf

Biografia de Robert King Merton. Retrieved from https://www.biografiasyvidas.com/biografia/m/merton_robert.htm

Calduch, R. (1991). La sociedad internacional. Retrieved from https://www.ucm.es/data/cont/media/www/pag-55159/lib1cap3.pdf

Cano, J. (2017). La ventana de AREM. Una estrategia para anticipar los riesgos y amenazas en ciberseguridad empresarial. Retrieved from https://www.isaca.org/Journal/archives/2017/Volume-5/Pages/the-arem-window-spanish.aspx

Cano, J. Colombia no está preparada ante un ciberataque. Retrieved from http://www.urosario.edu.co/UCD/Colombia-no-esta-preparada-ante-un-ciberataque/

Cárdenas Moreno, W. (2015). CIBERDEFENSA Y CIBERSEGURIDAD EN EL SECTOR DEFENSA DE COLOMBIA. Retrieved from http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2849/00002590.pdf?sequence=1

Cárdenas Rodriguez, P., & Vásquez Zarate, A. (2016). Propuesta de buenas prácticas para fortalecer los controles de prevención y detección temprana del cibercrimen en las empresas colombianas. Retrieved from https://repository.javeriana.edu.co/bitstream/handle/10554/18900/VasquezZarateKatyAlejandra2015.pdf?sequence=1&isAllowed=y

Ciberseguridad para empresas. (2019). Retrieved from https://www.claro.com.co/institucional/ciberseguridad-para-empresas/

Colombia. Retrieved from http://observatoriociberseguridad.org/country/co

Contreras, A. B. (2019). *La Seguridad en el Ciberespacio. Un desafio para Colombia.* Bogotá.

Cortada de Kohan, N. (2008). LOS SESGOS COGNITIVOS EN LA TOMA DE DECISIONES. Retrieved from http://www.redalyc.org/pdf/2990/299023503010.pdf

CSIRT - Asobancaria. Retrieved from https://www.asobancaria.com/csirt/

Cuervo, J. (2014). Convenio del Consejo de Europa sobre la cybercriminalidad, Budapest 23 noviembre 2001 - Informática Jurídica. Retrieved from http://www.informatica-

juridica.com/anexos/convenio-del-consejo-de-europa-sobre-la-cybercriminalidad-budapest-23-noviembre-2001/

Cuervo, J. (2014). Legislación de Colombia. Ley 1273 de 5 de enero de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas q - Informática Jurídica. Retrieved from http://www.informatica-juridica.com/anexos/legislacion-de-colombia-ley-1273-de-5-de-enero-de-2009-por-medio-de-la-cual-se-modifica-el-codigo-penal-se-crea-un-nuevo-bien-juridico-tutelado-denominado-quot-de-la-proteccion-de-la-informacion-y-de-los-datos-quot-y-se-preservan-integralmente-los-sistemas-q/

Documento CONPES 3854. (2016). Retrieved from https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Gallardo, S. ENSAYO EL FUNCIONALISMO Y ESTRUCTURAL FUNCIONALISMO. Retrieved from https://www.academia.edu/36356081/ENSAYO_EL_FUNCIONALISMO_Y_ESTRUCTURAL_FUNCIONALISMO

Giraldo Saavedra, A. (2012). La función reguladora del Estado y el Derecho. Retrieved from https://www.researchgate.net/publication/318354197_La_funcion_reguladora_del_Estado_y_el_Derecho

Giraldo Saavedra, A. (2012). La función reguladora del Estado y el Derecho The regulatory role of the State and Law. Retrieved from http://webcache.googleusercontent.com/search?q=cache:w3P-FdpTzH8J:hemeroteca.unad.edu.co/index.php/revista-de-investigaciones-unad/article/download/783/1420+&cd=5&hl=es&ct=clnk&gl=co

Gobierno radicó Proyecto de Ley para adherirse al Convenio de Budapest contra la ciberdelincuencia. Retrieved from https://www.mintic.gov.co/portal/604/w3-article-56315.html

GUARNEROS NAVARRETE, A. (2017). “EL EXPERTO EN PROSPECTIVA TECNOLÓGICA PARA LA PLANEACIÓN ESTRATÉGICA DE LA INNOVACIÓN. ENRIQUECIMIENTO DEL CONCEPTO Y SU CLASIFICACIÓN SEGÚN LAS METODOLOGÍAS MÁS UTILIZADAS”. Retrieved from http://www.uam.mx/altec2017/pdfs/ALTEC_2017_paper_164.pdf

Hoyos Buiron, V. (2015). ¿Que tal esta Colombia en cuestion de ciberseguridad?. Retrieved from https://repository.unimilitar.edu.co/handle/10654/7794

IMPACTO DE LOS INCIDENTES DE SEGURIDAD DIGITAL EN COLOMBIA 2017. (2017). Retrieved from http://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf

IQ Information Quality | Servicios TIC - Seguridad en Pagos Electrónicos, Servicios de Verificación de Cumplimiento. Retrieved from https://www.guiadesolucionestic.com/seguridad/2014-07-20-19-08-35/938-iq-information-quality-

Kahneman, D., & Tversky, A. (1987). Teoría prospectiva: un análisis de la decisión bajo riesgo. Retrieved from https://dialnet.unirioja.es/descarga/articulo/65981.pdf

Leiva, E. Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local | Revista Latinoamericana de Ingenieria de Software. Retrieved from http://revistas.unla.edu.ar/software/article/view/775

Lima, L., Daboín, Á., Hernández, L., León, E., Poletto, J., & Vides, F. (2011). INCERTIDUMBRE Y DECISIÓN. Retrieved from http://lilianalima.blogspot.com/2011/02/incertidumbre-y-decision.html

Linares Lizarazo, Y. ¿CÓMO ESTAMOS EN CIBERSEGURIDAD NACIONAL E INTERNACIONAL, SU GESTIÓN DE RIESGOS Y TENDENCIAS?. Retrieved from http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4653/00004875.pdf?sequence=1&isAllowed=y

Lizcano, J. LAS TEORÍAS DEL CAOS Y LOS SISTEMAS COMPLEJOS: Proyecciones físicas, biológicas, sociales y económicas. Retrieved from http://www.encuentros-multidisciplinares.org/Revistan%C2%BA7/Seminario%20Teor%C3%ADa%20del%20Caos%201.pdf

Lo que usted debe saber del Conpes de Seguridad Digital - Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Retrieved from https://www.mintic.gov.co/portal/604/w3-article-15410.html

Los ataques cibernéticos se incrementaron este año. (2018). Retrieved from https://www.dinero.com/internacional/articulo/incremento-de-ataques-ciberneticos-en-el-2018/264180

Los ataques de ciberfraude del 2018 | Computerworld Colombia. (2018). Retrieved from https://computerworld.co/los-ataques-de-ciberfraude-del-2018/

LOZANO QUINTERO, L. (2015). AMENAZAS A LA INFRAESTRUCTURA DEL SECTOR DE TELECOMUNICACIONES (TIC) EN COLOMBIA. Retrieved from https://repository.unimilitar.edu.co/bitstream/handle/10654/7161/Ensayo%20para%20optar%20al%20titulo%20de%20Internacionalista%20y%20Polit%C3%B3loga.%20Lady%20Carolina%20Lozano%20Quintero%20.pdf?sequence=1&isAllowed=y

Mayorga Delgado, A. Lineamientos, Tendencias y Estrategias sobre Ciberseguridad y Ciberdefensa en Colombia. Retrieved from http://polux.unipiloto.edu.co:8080/00001904.pdf

MinTIC realizó mesas de trabajo para enriquecer el Modelo de Riesgos de Seguridad Digital con los sectores público y privado. (2018). Retrieved from https://www.mintic.gov.co/portal/604/w3-article-63911.html

OEA :: Fotonoticia :: OEA y ASOBANCARIA firman acuerdo en ciberseguridad para blindar a sector financiero en Colombia. (2018). Retrieved from http://www.oas.org/es/centro_noticias/fotonoticia.asp?sCodigo=FNC-95085

Oquist, P., & Oszlak, O. (1970). ESTRUCTURAL-FUNCIONALISMO: UN ANÁLISIS CRÍTICO DE SU ESTRUCTURA Y FUNCIÓN. Retrieved from http://oscaroszlak.org.ar/images/articulos-espanol/Estruct%20func%20un%20anal%20critico%20de%20su%20estruct.pdf

Orozco, G. EL CONCEPTO DE LA SEGURIDAD EN LA TEORÍA DE LAS RELACIONES INTERNACIONALES. Retrieved from https://core.ac.uk/download/pdf/39008156.pdf

Política general de seguridad de la información. Retrieved from http://www.banrep.gov.co/es/politicas-de-seguridad-de-la-informacion

POLITICA NACIONAL DE SEGURIDAD DIGITAL. (2016). Retrieved from https://www.mintic.gov.co/portal/604/articles-14481_recurso_1.pdf

Primer Foro de Seguridad de la Información: “El impacto de la seguridad en la estrategia de las compañías” | colCERT. Retrieved from http://www.colcert.gov.co/?q=blog/primer-foro-de-seguridad-de-la-informaci%C3%B3n-%E2%80%9Cel-impacto-de-la-seguridad-en-la-estrategia-de-las

PUBLIC-PRIVATE PARTNERSHIPS. Retrieved from http://www.pppkosova.org/repository/docs/public_private_partnerships.pdf

Qué es NIST - INGEMED. Retrieved from http://www.ingemed.cl/documentos/que-es-nist/

Qué es una botnet y cómo defenderse contra ella | Avast. Retrieved from https://www.avast.com/es-es/c-botnet

Quintero Agudelo, Y. La seguridad y la ciberdefensa en Colombia. Retrieved from http://polux.unipiloto.edu.co:8080/00001596.pdf

Ramírez Morán, D. (2015). LA VISIÓN INTERNACIONAL DE LA CIBERSEGURIDAD. Retrieved from http://www.ieee.es/Galerias/fichero/docs_informativos/2015/DIEEEI02-2015_VisionInternacional_Ciberseguridad_DRM.pdf

Ramz, A. Teoría del Caos y Relaciones Internacionales. Retrieved from https://geopolmundial.wordpress.com/2017/04/24/teoria-del-caos-y-relaciones-internacionales/

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR) y FLACSO Sede Ecuador. (2017). Retrieved from https://repositorio.flacsoandes.edu.ec/xmlui/bitstream/handle/10469/12197/RFLACSO-01-Sancho.pdf?sequence=1&isAllowed=y

Retos de Colombia en ciberseguridad a propósito de la adhesión al “Convenio de Budapest”. (2018). Retrieved from https://www.asobancaria.com/wp-content/uploads/1148.pdf

Retrieved from https://repository.upb.edu.co/bitstream/handle/20.500.11912/4152/AN%C3%81LISIS%20DE%20LA%20CAPACIDAD%20DE%20CIBERSEGURIDAD%20PARA.pdf?sequence=1&isAllowed=y

Retrieved from https://repository.upb.edu.co/bitstream/handle/20.500.11912/4152/AN%C3%81LISIS%20DE%20LA%20CAPACIDAD%20DE%20CIBERSEGURIDAD%20PARA.pdf?sequence=1&isAllowed=y

Retrieved from https://trabajosocialunam.files.wordpress.com/2014/02/la-teorc3ada-de-parsons-y-merton.pdf

Rodríguez, M. (2009). La “estructura” en las ciencias del hombre: Estructuralismo y Estructural-Funcionalismo. Retrieved from https://revistas.ort.edu.uy/letras-internacionales/article/view/1669

Sánchez, R. (2011). Karl Deutsch y su contribución al estudio de las Relaciones Internacionales. Retrieved from http://webcache.googleusercontent.com/search?q=cache:ITRQlL8MfQ8J:www.revistas.una.ac.cr/index.php/ri/article/view/111+&cd=1&hl=es-419&ct=clnk&gl=co

SÁNCHEZ-PINILLA, M. (2006). *LECTURAS TEORÍA SOCIOLÓGICA CONTEMPORÁNEA*[Ebook]. Retrieved from https://www.um.es/tic/LIBROS%20FCI-I/Clasicos%20T%20Com.pdf

Security for today’s world: integrated and intelligent. (2017). Retrieved from https://www.ibm.com/downloads/cas/BP8RKLOW

Seguridad Cibernética :: Inicio. (2018). Retrieved from https://www.sites.oas.org/cyber/Es/Paginas/default.aspx

Seguridad de la información para compañías | Claro Empresas. Retrieved from https://www.claro.com.co/empresas/soluciones/seguridad/

Singer, P. F. (2014). *Cybersecurity and Cyberwar. What everyone needs to know.* United States of America: Oxford University Press.

Sobre la Unión Internacional de Telecomunicaciones (UIT). Retrieved from https://www.itu.int/es/about/Pages/default.aspx

Velásquez Lombana, M., & Pusey Mitchell, A. Gestión de activos de tecnología de la operación. Caso estudio: Refinería de Barrancabermeja. Retrieved from https://educacion.aciem.org/CIMGA/2019/Trabajos/19090_TRA_COL_M_VELASQUEZ_CIMGA2019.pdf

Vidal Londoño, J. (2016). Una nueva experiencia en seguridad hacking ético. Retrieved from https://repository.unimilitar.edu.co/handle/10654/15838

ANEXOS.

1.1.Entrevista

NOMBRE: Diego Barbosa Molina

CARGO: Profesor de Cátedra

ESTUDIOS REALIZADOS: Politólogo, Especialista en Gestión del Desarrollo, Maestría en Estudios Interdisciplinarios sobre Desarrollo.

1. ¿Considera que los aportes realizados por el sector privado en temas de seguridad digital, han funcionado para identificar amenazas latentes en Colombia? Argumente.

   Creo que el sector privado ha tenido un papel importante en el ecosistema de ciber seguridad del país. Dentro del sector privado se destaca, por ejemplo, la labor del sector académico creando oferta académica e investigativa en torno a asuntos de ciber seguridad. El Estado ha promovido estrategias como los *Centros de Excelencia* en ciber seguridad que combinan acciones públicas y privadas para promover la investigación y la innovación en el desarrollo de productos y portafolios dirigidos a la demanda de servicios de seguridad digital. También se debe resaltar la labor del sistema financiero, pues este segmento de la economía es pionero en la implementación de tecnologías de la información, y hace transferencia a otros sectores de la economía; este sector, además, es paso obligado para activar el comercio electrónico, y en esa medida, las fortalezas que tiene el sector financiero son fortalezas que gana en su conjunto el país.

   Colombia está experimentando la entrada de grandes jugadores de la industria tecnológica (ej: Accenture, Amazon, etc.), lo que permite que los estándares de seguridad desarrollados por estos agentes estén disponibles a través de los productos y los servicios que comercializan tanto para individuos como para organizaciones. En general se podría decir que el sector privado está teniendo un rol positivo; no obstante,

no se podría esperar que la responsabilidad de acción frente a las amenazas recaiga mayoritariamente en el sector, pues en este aspecto es imperativa la coordinación estatal y la regulación del sector administrativo de las TIC, como ya sucede con el Comando Conjunto Cibernético del sector defensa y las iniciativas de promoción de la ciber seguridad en el Estado a través del Ministerio de las Tecnologías de la Información y las Comunicaciones.

2. ¿Las medidas ejecutadas por parte del sector privado o mixto para enfrontar ciberataques, has sido las adecuadas, eficaces y efectivas? De lo contrario, explique brevemente las falencias y cómo se puede mejorar

   El país ha adoptado medidas efectivas y pertinentes para afrontar ciber ataques, esto es evidente a través de lo que comúnmente se conoce como los CSIRTs o CERTs. Colombia tempranamente se ha unido a estas estrategias colaborativas de monitoreo y respuesta a los ataques cibernéticos provenientes de cualquier parte del mundo, y tiene un reconocimiento a nivel regional por su rol en tareas conjuntas y coordinación para la respuesta a incidentes de ciberseguridad.

   Hemos avanzando, sobre todo a través del sector público en la participación en los foros internacionales sobre ciber seguridad, especialmente en el marco de la OEA Y su grupo de ciber seguridad, lo que se ha capitalizado en transferencia de conocimiento.

   Como aspectos de mejora, se puede señalar la necesidad de profundizar la adopción de estándares y lineamientos (Ej: controles de la ISO 27001) para unificar el modelo de seguridad y privacidad la información, especialmente por parte de organizaciones que administran activos de información relevantes e infraestructura crítica (sector energético, servicios públicos, salud, educación, transporte, y abastecimiento).

3. A nivel global y regional, ¿considera que Colombia se destaca en temas de seguridad digital? ¿Ha presentado mejoras desde el CONPES 3854 de 2016?

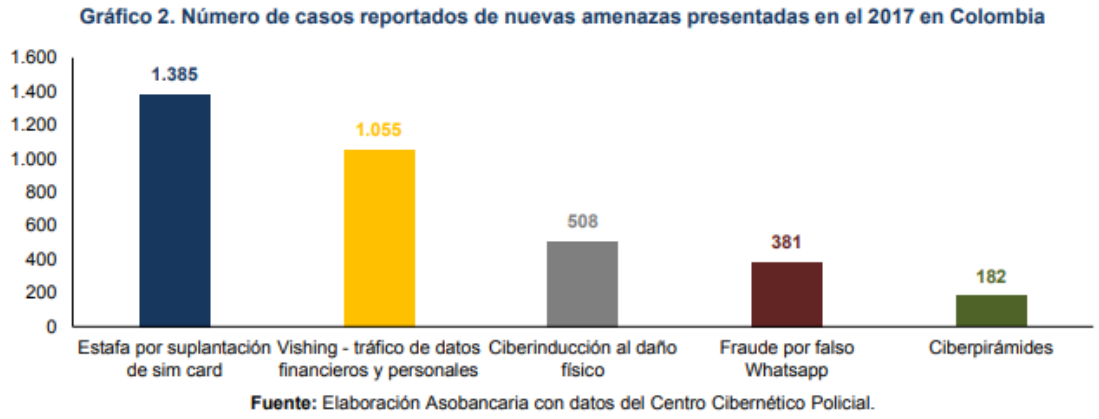
Colombia ocupa un lugar relevante a nivel regional temas de ciber seguridad. Esto es evidente cuando se analiza la decidida incorporación del país del Convenio de Budapest y la participación constante en los foros de discusión sobre ciber seguridad en el sistema internacional, especialmente en el contexto regional de la OEA. Si bien estos avances son anteriores a la expedición del CONPES, este documento de política ha promovido la perspectiva de la cooperación internacional para afrontar las amenazas en el ecosistema digital y ha hecho explícita la obligación de los agentes públicos y privados en Colombia de colaborar para hacer permanente una estrategia de prevención y reacción efectiva frente a las amenazas del ciber seguridad.

4. ¿Desde su perspectiva como ve a Colombia en términos generales, respecto a su seguridad digital? ¿Cómo la ve en un futuro próximo?

   Colombia presenta un nivel de rezago controlable en términos de sus estrategias de seguridad. No obstante, hacia el futuro es pronosticable un aumento de las amenazas relacionadas con el aumento de la penetración de la conectividad y del consumo de servicios provistos a través de Internet. En la medida en la que el ecosistema de usuarios y servicios mundo digital vaya creciendo en el país, las amenazas también lo harán; por esta razón, es necesario que los mecanismos de cooperación y coordinación de agentes públicos y privados profundicen y proyecten una agenda preventiva en la que se pueda reaccionar con pertinencia a los nuevos escenarios.

1.2. Figuras.

(Figura 1: Número de casos reportados de nuevas amenazas presentadas en el 2017 en Colombia)



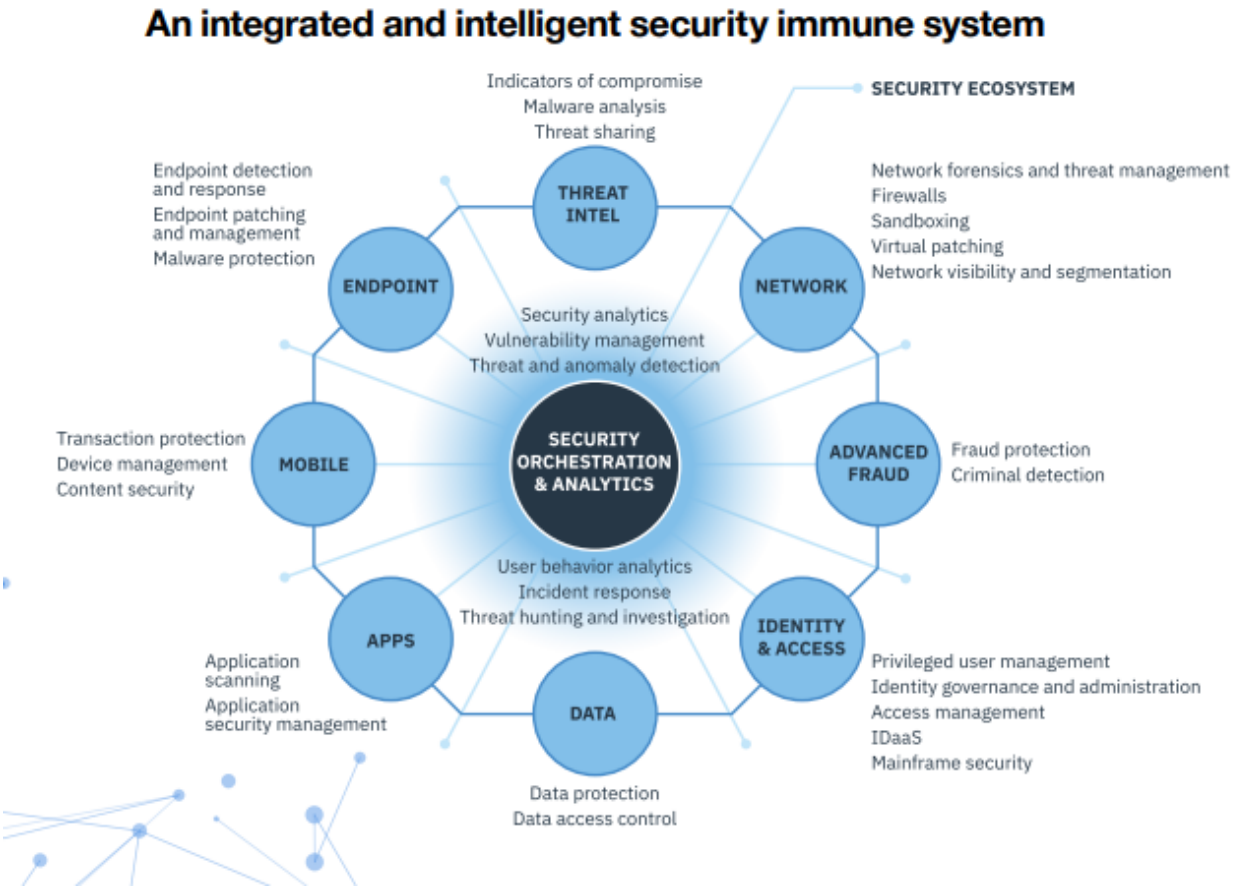
(Figura 2: Factores de riesgo en el ciberespacio)

Figura 1. Factores de riesgo en el Ciberespacio

Autoría	Objetivos	
	Gobierno	Sector Privado
Ataques patrocinados por otros Estados	Espionaje, ataques contra infraestructuras críticas, amenazas persistentes avanzadas (APT, por sus siglas en inglés)	Espionaje, ataques contra infraestructuras críticas, APT
Ataques patrocinados por privados	Espionaje	Espionaje
Terroristas, extremismo político e ideológico	Ataques contra redes y sistemas; contra servicios de Internet; infección con *malware*; contra redes, sistemas o servicios de terceros	Ataques contra redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros
Hacktivistas	Robo y publicación de información clasificada o sensible, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros	Robo y publicación de información clasificada o sensible, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros
Crimen organizado	Espionaje	Robo de identidad digital y fraude
Ataques de bajo perfil	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros
Ataques de personal con accesos privilegiados (*Insiders*)	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros, robo y publicación de información clasificada o sensible, APT	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros, robo y publicación de información clasificada o sensible, APT
Impacto	**Alto**	
	Medio	
	Bajo	

Fuente: Instituto de Ciberseguridad de España (2012).

(Figura 3: Sistema inmune de seguridad integrado e inteligente IBM)



(Figura 4: Enfoque prioritario entre las tecnologías IT y OT)

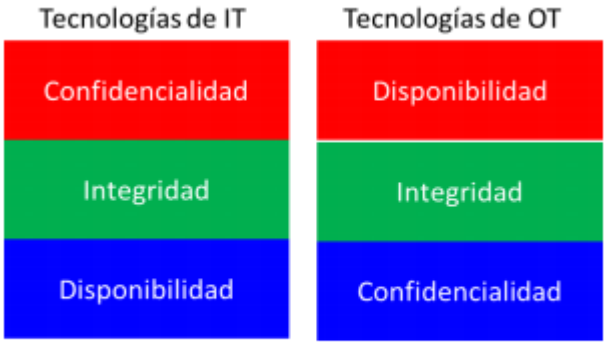


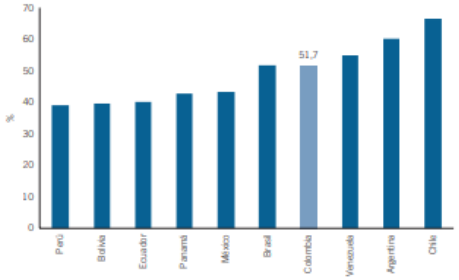
Figura 2. Enfoque prioritario ente las tecnologías de IT y OT. Fuente: los autores. 2019

(Figura 5: Diferencias redes IT y OT)

Tabla 1 Diferencias redes IT y OT. Adaptada de PEREZ, 2018

Prioridades REDES IT	**Prioridades REDES OT**
1. Confidencialidad 2. Integridad 3. Disponibilidad	1. Disponibilidad 2. Integridad 3. Confidencialidad
Parches Sistema Operativo y software: Actualizaciones con políticas bien definidas.	*Parches Sistema Operativo y software:* Complejo de desplegar y actualizaciones por periodos de fabricación.

(Figura 6: Posición de Colombia a nivel regional)



(Figura 7: Grado de compromiso nacional)

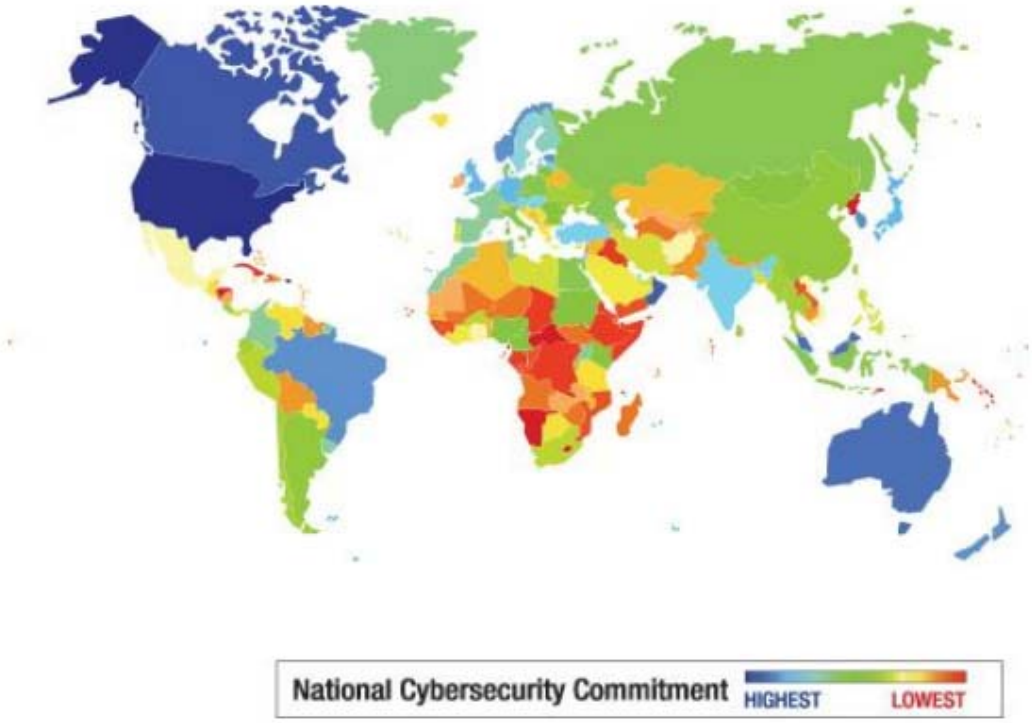


Figura 1. Grado de compromiso nacional (Fuente: ITU y ABI Research)