CIBERSEGURIDAD EN COLOMBIA, AVANCES Y RETOS.

Ensayo Académico presentado por:

LAURA DANIELA BUENO MUNAR

Ensayo académico para optar por el título de Profesional en Relaciones Internacionales y Estudios Políticos.

Coronel ra.Jorge Isaza, MBA-PhD

Tutor

FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD.

PROGRAMA DE RELACIONES INTERNACIONALES Y ESTUDIOS POLITICOS.

2022

Resumen

La nueva era informática y de digitalización han sido importantes para los sectores económicos, sociales e industriales, ya que se han visto permeados por los avances tecnológicos que van de la mano con procesos de desarrollo y crecimiento, aunque este fenómeno tiene grandes ventajas globales, también es necesario recalcar las amenazas que se pueden presentar al manipular estas herramientas digitales. Colombia ha tenido un gran progreso desde la implementación de estos instrumentos tecnológicos, pero a pesar del intento del Estado y las instituciones por preservar la seguridad cibernética, son notables los retos y desafíos que tiene Colombia en temas de ciberseguridad, si bien se han presentado avances sustanciales, aún persisten los casos de cibercrimen.

Palabras clave: amenazas, avances, cibercrimen, ciberseguridad, digitalización, retos, tecnología.

Abstract

The new computer and digitization era has been important for the economic, social and industrial sectors, since they have been permeated by technological advances that go hand in hand with development and growth processes, although this phenomenon has great global advantages, too. It is necessary to emphasize the threats that can arise when manipulating these digital tools. Colombia has made great progress since the implementation of these technological instruments, but despite the attempt of the State and the institutions to preserve cyber security, the challenges that Colombia has in cyber security issues are notable, although progress has been made substantial, cases of cybercrime still persist.

Keywords: threats, advances, cybercrime, cybersecurity, digitization, challenges, technology.

Introducción

Debido a la inmersión de las personas y las empresas en temas digitales y tecnológicos, se han generado grandes avances, pero también las amenazas están presentes esperando cualquier vulnerabilidad o punto débil para atacar, a pesar de que Colombia es un país en términos tecnológicos preparado, según la Asociación Colombiana de Ingenieros de Sistemas, Colombia ocupa el puesto número 7 en toda Latinoamérica, esto no es suficiente para contrarrestar los ataques que a diario se reciben en el ciberespacio (ACIS,2018). Desde el año 2009, Colombia ha dado gran valor a los temas tecnológicos mediante la promulgación una Ley exclusiva para sancionar los delitos cibernéticos y también para la creación de instituciones para velar por la ciberseguridad de los ciudadanos.

En el desarrollo de este ensayo, se analizará a grandes rasgos el avance tecnológico que ha tenido Colombia en los últimos dos años en comparación con los años anteriores, desde la sanción de la Ley 1273 del 2009, dado que antes de esta no existía una normativa o regulación que penalizara los delitos cibernéticos que atentan contra la ciberseguridad de personas y entidades a diario, ya sean del sector público o privado, dado que este fenómeno ha tenido un gran incremento contemporáneo por causa del amplio desarrollo digital y tecnológico global, y también por la accesibilidad colectiva del crimen organizado con respecto a los dispositivos tecnológicos, de esta manera aumenta la cantidad de riesgos y amenazas que existen por esta interacción digital. La importancia de conocer los avances y las amenazas tecnológicas en Colombia surge a partir de los problemas de seguridad que se generan, tanto para las personas como para las empresas que a diario reciben todo tipo de ataques cibernéticos, irrumpiendo la confidencialidad de los datos privados de empresas, y personas, ocasionando problemas financieros, de suplantación y también el robo de información, siendo esta última la más común, dado que para el ciberdelincuente es importante tener acceso a todos los datos personales de su víctima y así poder atacar, mantener secuestrada su información y lucrarse económicamente.

Objetivo general.

Conocer los avances y retos que tiene Colombia en temas de ciberseguridad, destacando cuáles han sido los beneficios y cuáles son las amenazas al ciberespacio.

Objetivos específicos.

- Identificar los avances que ha tenido Colombia en temas de ciberseguridad en los últimos dos años.
- Conocer las consecuencias de los ataques cibernéticos en el país.
- Determinar si las políticas de seguridad cibernética han sido efectivas para contrarrestar el cibercrimen.

Desarrollo

El avance tecnológico desde hace unas cuantas décadas ha venido evolucionando de manera rápida, para nadie es un secreto que se puede estar informado en tiempo real de cualquier novedad que ocurra al otro lado del mundo con tan solo un clic. Esto ha sido una gran ventaja para absolutamente todas las personas en todos los sectores de la economía, de este modo, se puede hablar de una "*revolución digital";* este fenómeno social, se percibe desde aproximadamente la mitad del siglo XX, cuando se empezaron a incorporar las nuevas herramientas digitales a todo tipo de procesos industriales y económicos. (Economipedia, 2020). De esta manera el mundo y las personas han tenido que familiarizarse con nuevos conceptos basados en la digitalización y la tecnología.

Para entender esta evolución tecnológica, es necesario tener en cuenta el término *"ciberespacio",* este se define como el espacio artificial creado por el conjunto de sistemas de la información y telecomunicaciones que utilizan las TIC, es decir de redes de ordenadores, mucho más que Internet, más que los mismos sistemas y equipos (Sánchez, M. 2019). Básicamente, éste es el espacio o ambiente que existe dentro de los computadores y las redes digitales, por ello todos son parte desde el momento en el cual ingresan a alguna página web, o red social (ciberespacio), y se les denomina, cibernautas. En este campo digital existe gran cantidad de información que se puede obtener con tan solo un clic, y se interactúa con esta a diario, por eso es normal que en varios sitios web se almacenen algunos datos personales de las personas que ingresan, como relación reciproca entre el ciberespacio y el cibernauta (Sánchez, 2019).

El progreso ha sido histórico, todas las actividades sociales, económicas y culturales se ven permeadas por este fenómeno, que si bien tiene bastantes beneficios para quien lo sabe utilizar, también se encuentran significativas desventajas en seguridad, o ciberseguridad. Uno

de los beneficios que tiene este gran avance tecnológico es la conexión con el mundo, y con las personas, cada vez se está más cerca de "todo" virtualmente, este fenómeno aumentó en el 2020 con el inicio de la propagación del virus COVID-19, pues esto imposibilitaba el contacto físico o acercamiento con personas, de este modo todo tipo de encuentros o reuniones fueron realizadas mediante sitios web y plataformas digitales, compartiendo documentos, archivos e ideas ya sean de negocios, ciencias o simplemente culturales. Este suceso cambió la perspectiva de todas las áreas educativas y laborales, pues se observa un incremento en el uso de redes móviles y conexiones durante la pandemia y actualmente.

Figura 1.

Figura 1. *Crecimiento digital en Colombia en el año 2021, desde el uso de herramientas digitales, y el incremento de los cibernautas, en comparación con el año 2020. Alvino Clay, 2021, "Estadísticas de la situación digital de Colombia en el 2020-2021". We are Social & Hootsuite. Traducción por Branch. Recuperado de: https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-colombia-en-el-2020-021/#:~:text=El%20crecimiento%20digital%3A%20enero%202020,%2C%20espec%C3%ADficamente%20en%20un%201.9%25*.

En Colombia ha aumentado el porcentaje de usuarios aproximadamente un 4% de el 2020 al 2021, donde se unieron alrededor de 1.3 millones de ciberusuarios en todo el territorio nacional. (Branch, 2021). Esto deja ver el amplio crecimiento al que se han enfrentado los ciudadanos colombianos en el campo tecnológico y también se hizo necesario que las empresas buscaran como lograr fortalecer sus páginas web y sistemas informáticos, para evitar las amenazas de los ciberdelincuentes.

Este gran crecimiento tecnológico también tiene consecuencias, pues de algún modo se crea una dependencia muy fuerte hacia el internet, lo que deja expuestos a muchos

gobiernos y compañías, quienes reciben diariamente ataques por parte de *"hackers"*. "Los hackers de sombrero negro tienen fines ilícitos y buscan dañar o beneficiarse económicamente en base a terceros e intentan penetrar en las redes para extraer información, plantar virus, hackear mails, etc." (Saín, 2015, p. 1).

De este modo los hackers tienen muchas maneras de entrar a los sistemas privados de las páginas privadas, buscando información confidencial o intentando dañar los sistemas operativos que, si bien tienen algún tipo de seguridad, estos ciberdelincuentes logran burlar por ciertas fallas en el sistema, o la falta de aplicación de un sistema fuerte de seguridad digital, que cuide la información y los datos.

Avances de la ciberseguridad en Colombia.

Según la Asociación de Auditoría y Control sobre los Sistemas de Información (en inglés; ISACA) la ciberseguridad se puede definir como: "La protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados" (Esic Business & Marketing School, 2020, párr. 1).

A pesar de que Colombia es un país en vías de desarrollo, ha tenido que enfrentar los nuevos retos frente a la evolución digital, es así como ha tenido que desarrollar alternativas para la prevención de los delitos cibernéticos e informáticos, esto con el fin de evitar casos posibles como fraudes financieros, robo de información, clonación de tarjetas, implantación de virus dentro de los sistemas de cómputo, pornografía infantil, y otros delitos que pueden realizarse desde el ciberespacio y que afectan de manera negativa a los ciberusuarios, por esto, en el 2009, con el mandato presidencial de Álvaro Uribe Vélez, se reforma el nombre del Ministerio de las Comunicaciones, para darle paso al Ministerio de Tecnologías de la Información y Comunicaciones, (MinTIC) donde se promueve el control de las nuevas tecnologías y la información, mediante la Ley 1273 del 2009; en esta "se crea un nuevo bien jurídico tutelado sobre la protección de la información y de los datos, de este modo se busca preservar integralmente a los sistemas que utilicen las tecnologías de la información y las comunicaciones" (Ojeda et al. 2010).

Esta Ley, es la más importante relacionada con la ciberseguridad en Colombia, pues conceptualiza los delitos cibernéticos que tienen lugar dentro del territorio colombiano, y desde allí se busca tomar las medidas necesarias para el control y prevención de los mismos, a continuación, podemos ver los principales delitos.

Ley 1273 del 2009.

Ley 1273 del 2009. "Por medio de la cual se modifica el código penal, y se crea un nuevo bien jurídico tutelado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". 05 de enero del 2009. D.O. No. 47223. Esta Ley colombiana sanciona los siguientes delitos cibernéticos:

Artículo 269A. Acceso abusivo a un sistema informático. En el que sin autorización acceda a un sistema informático protegido o no.

Artículo 269B. Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático.

Articulo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático.

Artículo 269D. Daño informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.

Artículo 269E. Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

Artículo 269F. Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.

Articulo 269G. Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.

Articulo 269H. Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si se continua con su divulgación.

Artículo 2691. Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero. (Ley 1273, 2009, Art. 1)

También existen otros decretos y actos administrativos que regulan diferentes actividades relacionadas con el entorno digital, por ejemplo; la Ley 1341 de 2009 “por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones” (Ley 1341, 2009). También el decreto 1377 de 2013, “por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales” (Decreto 1377, 2013). Estas son solo algunas de las normas jurídicas que en Colombia regulan los delitos cibernéticos y la protección de los datos personales.

En Colombia la ley es clara, se deben sancionar estos delitos cibernéticos dentro del territorio nacional, sin embargo, es muy común que se sigan realizando este tipo de crímenes, sin ningún tipo de pena o judicialización, ahí es donde se puede observar grandes desaciertos en las instituciones encargadas de la regulación de las tecnologías, aunque se han realizado varios intentos para controlar esto, por ejemplo en el año 2011 el Gobierno Nacional expidió el Documento Conpes 3701, donde se establecen los Lineamientos de Política para Ciberseguridad y Ciberdefensa, ya que a pesar de conocer las amenazas que existen en el

ciberespacio, quedaban grandes vacíos que impedían navegar seguramente por la web, es así como el Gobierno Nacional decide implementar el desarrollo de una estrategia nacional que ayude a contrarrestar el incremento de las amenazas informáticas. Debido al incremento de la participación de los ciudadanos en temas digitales e informáticos, es normal que se desarrollen nuevas y diferentes amenazas, por algunos vacíos en su fundamentación, posteriormente, el Gobierno Nacional expide el Conpes 3854, donde se establece una nueva política nacional de seguridad digital, que tiene como objetivo: "Fortalecer las capacidades de las partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia" (Conpes 3854, 2016).

Estos dos documentos se dedicaron a desarrollar el fortalecimiento del Gobierno Nacional, basados en un enfoque de gestión de riesgos, cuyo objetivo principal era la prevención del delito mediante diferentes alternativas adoptadas por sectores privado y públicos. Posteriormente en el 2020, el Gobierno Nacional publica el nuevo Conpes 3995, éste busca desarrollar una política nacional cuyo fin es establecer medidas concretas para aumentar la confianza digital y así lograr mejoras continuas en el ámbito de seguridad digital (Conpes 3995, 2020).

Con la aplicación de estos planes de desarrollo, el Gobierno Nacional ha buscado el fortalecimiento de la red y de la infraestructura tecnológica del país, desde la legislación. Como la tecnología siempre está un paso adelante, será necesaria la verificación de las antiguas políticas de seguridad informática, para estar a la vanguardia e ir avanzando de la mano en la implementación de nuevos proyectos que ayuden a contrarrestar las amenazas digitales en Colombia.

Figura 2.

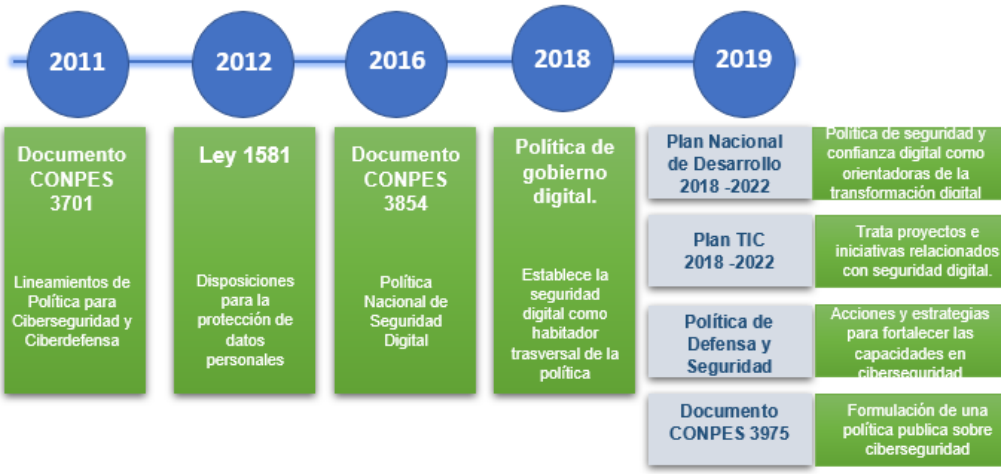

Figura 2. Breve línea del tiempo relacionada con las políticas y estrategias que ha desarrollado el Gobierno Nacional en pro de la Ciberseguridad. Departamento Nacional de Planeación, 2020, Documento CONPES 3995. Pag, 10.

El Gobierno Nacional ha tratado de estar a la vanguardia en temas de ciberseguridad y ciberdefensa, pero esto no es suficiente, a pesar de que en el 2016 se publicó el documento Conpes 3854 para prevenir este tipo de riesgos, en 2017 más de 12 empresas colombianas se vieron afectadas por el ciberataque mundial de un "*ramsomware",* éste se trata de un tipo de malware que consigue tomar el control del dispositivo para cifrar el acceso al mismo a cambio de recuperar esta información, es un tipo de secuestro de información, que busca generar ganancias económicas, generando pérdidas económicas en las empresas y poniendo en riesgo su seguridad (El Tiempo, 2017).

Además de la legislación, el gobierno colombiano, mediante el sector defensa y seguridad, tiene varias dependencias que se encargan netamente del direccionamiento estratégico de las Tecnologías de la Información, de proponer capacitaciones tecnológicas en el sector, e implementar las políticas que emita el Gobierno Nacional. (Plan estratégico de Tecnologías de la Información y las Comunicaciones del Sector Defensa y Seguridad, 2018)

Figura 3.

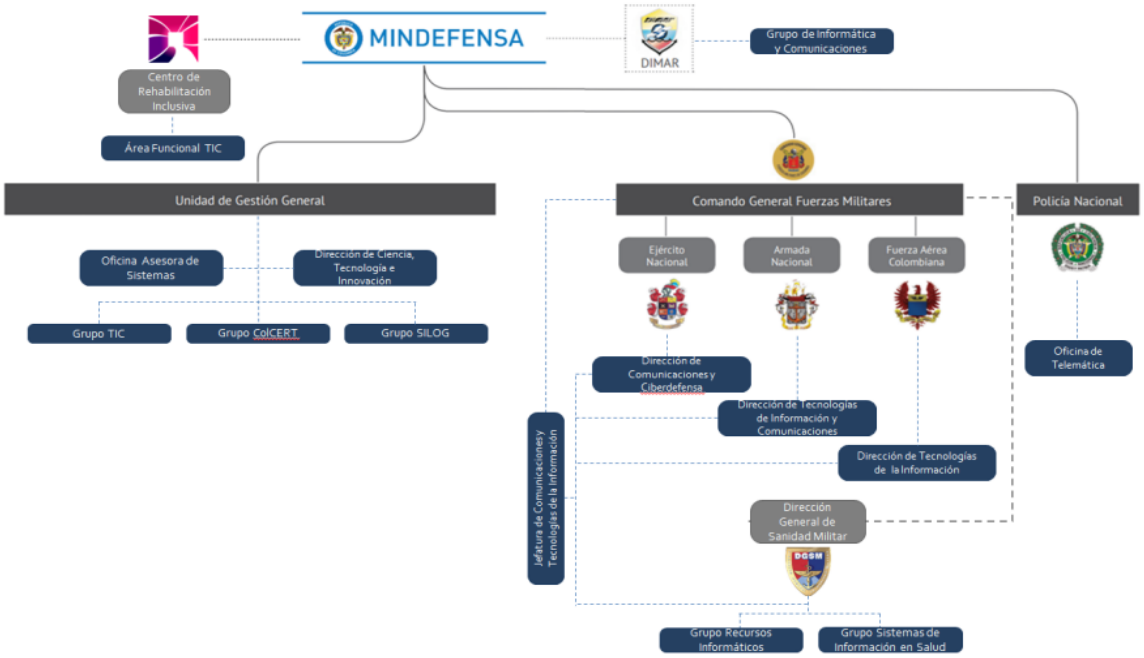

Figura 3. Sectores que desde el Ministerio de Defensa apoyan la protección de los ciudadanos en temas de ciberseguridad. Ministerio de Defensa, 2018. Plan estratégico de Tecnologías de la Información y las Comunicaciones del Sector Defensa y Seguridad, pág. 14.

Dentro de estas unidades del Ministerio de Defensa, se encuentra el Grupo de Respuestas a Emergencias Cibernéticas de Colombia (colCERT) que tiene como objetivo inicial coordinar la Ciberseguridad y Ciberdefensa del territorio nacional, también lo hace en entidades públicas y privadas, y es el delegado para atender en primera instancia los incidentes cibernéticos y preservar la infraestructura crítica cibernética en Colombia (Observatorio de Ciberseguridad, 2020). También se encuentra el Sistema de Información Logística del Sector Defensa y Seguridad (SILOG): sistema de información tipo ERP donde se gestionan en una misma plataforma, todos los procesos logísticos y financieros, convirtiéndose en una herramienta de soporte para la planeación, el control y fiscalización del sector (Plan Estratégico de Tecnologías de la Información y las Comunicaciones del Sector Defensa y Seguridad, 2018). Estas unidades, son las encargadas de los lineamientos y políticas de las Tecnologías de la Información.

Aparte de estos avances paulatinos, también debe tenerse en cuenta que en el transcurso de todo el año 2021, el Ministerio TIC, se empeñó en capacitar gratuitamente a PyMES (Pequeñas y Medianas Empresas) en materia de ciberseguridad, esto con el fin implementar acciones para proteger la información y para lograrlo era necesario que sus

equipos de trabajo estuvieran en capacidad de enfrentar este reto y dar respuesta inmediata a cualquier tipo de amenaza, según dijo Karen Abudinen, ex ministra TIC. (MinTic, 2021)

Consecuencias de los ciberataques en Colombia para el año 2021.

Según las denuncias instauradas al finalizar el mes de noviembre del 2021, se registraron aproximadamente 46.500 denuncias por múltiples delitos cibernéticos, esto equivale a un incremento del 21% con respecto al año 2020 (CCIT, 2021). En los últimos tres años, los ciberataques han mostrado ser aún más persistentes que en otros años, un acelerador de este fenómeno fue el inicio de la pandemia, pues en este lapso las personas se vieron obligadas a compartir información importante mediante la web, y realizar varias actividades virtuales tales como el comercio electrónico, algo que generalmente se realizaba en tiendas o almacenes, actualmente lo realizan con una tarjeta y mediante un monitor, esto permitió a los delincuentes acaparar un área específica criminal, que tiene múltiples vacíos y desventajas, los delitos cibernéticos.

Figura 4.

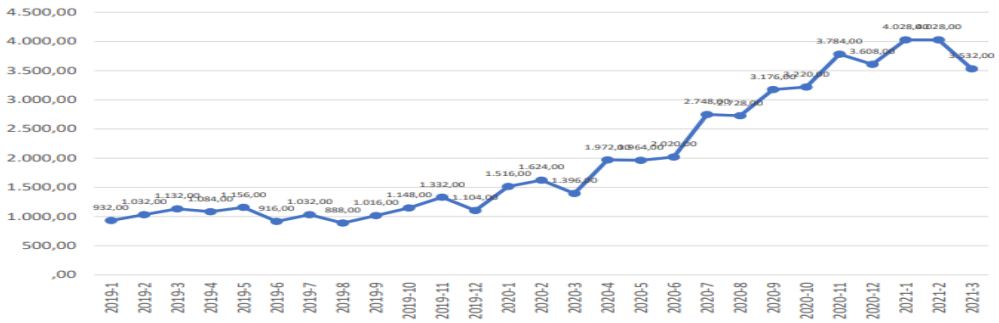

Figura 4. Estadística del incremento de las denuncias por violación de los datos personales, en Colombia, en el 2021. Fiscalía General de la Nación, 2021. Recuperado de: https://www.fiscalia.gov.co/colombia/gestion/estadisticas/delitos/

El delito con mayor crecimiento en el 2021, fue la violación de los datos personales, con un crecimiento de aproximadamente el 45% con respecto al 2020, mediante la modalidad llamada *"phishing"* donde los cibercriminales realizan envíos masivos de emails adjuntado enlaces a páginas webs fraudulentas, así pueden llegar a infectar el dispositivo con un archivo adjunto malicioso o *"malware"* y de esta manera roban la información que necesitan. (INCIBE, 2010). Este tipo de delito en Colombia se estipula en el Artículo 269D y 269E de la Ley 1273 del 2009, mencionada anteriormente. Los ciberdelincuentes con este tipo de ataques lo que buscan es poder robar o secuestrar información confidencial de personas,

empresas, o instituciones públicas, pero así mismo es común que al implantar el archivo dañado, se pueda perder información, o se genere un daño en los equipos, la mayoría de las veces lo hacen con fines económicos, donde en otras palabras “secuestran” esta información y a cambio de no hacerla pública, piden una suma de dinero, dependiendo la víctima, si es una empresa privada, o si es algún tipo de institución pública.

Por otro lado, el sector público no es ajeno a este tipo de ataques, a pesar de que el esfuerzo que se ha hecho, durante los meses de abril y mayo del 2021, se presentaron ataques a algunas páginas del gobierno como al Ministerio de Defensa, la Policía Nacional y la Presidencia de la República (SAFE, 2021). Estos hechos se registraron mediante ataques de denegación del servicio o “Ataques DDoS”, el objetivo de este tipo de ataques es bloquear o saturar el servicio de esta página dejándola inhabilitada para todos los usuarios, y que se colapse es sistema (INCIBE, 2010).

En noviembre del 2021 la página oficial del Departamento Administrativo Nacional de Estadística de Colombia (DANE) fue víctima de un ataque cibernético, de este crimen se sabe que secuestraron información a cambio de dinero, para poder liberarla, además el hacker logró acceder al sistema de las bases de datos, y en cuestión de minutos pudo borrar aproximadamente 200 terabytes (medidas de almacenamiento digital) del sistema y para entender cuan grande fue la perdida, se puede decir que 1 terabyte equivale a la información que se puede almacenar en 4 computadores portátiles (El Colombiano, 2021). Como se mencionó, la irrupción fue en cuestión de minutos, pero sus consecuencias fueron bastante graves, además el DANE advirtió a los ciudadanos que hicieran caso omiso a los posibles mensajes de texto o emails que les llegaran haciéndose pasar por funcionarios, cometiendo el delito de suplantación de identidad, delito que también es sancionable en el artículo 269G de la Ley 1273 del 2009. Este hecho crítico para el Estado dejó inhabilitada la página web oficial del DANE por aproximadamente ocho días, mientras que el equipo de ingenieros encargados, intentaban controlar la situación.

Este caso de nivel nacional, deja como secuela el temor colectivo de los todos ciudadanos, que de alguna u otra manera tienen información personal registrada en el DANE, y aunque se logró recuperar cierta parte de la información, no es suficiente para estar seguros de que la información este en buenas manos. Pues como ya se ha visto, el robo de estas bases de datos, pueden ser utilizados para estafas, suplantación de identidades y otros delitos, para los ciudadanos es difícil comprender que una entidad del estado, no cuente con sistemas de

protección robustos y más cuando se trata de la información personal de todos los ciudadanos colombianos.

La segunda modalidad más alta de cibercrimen en Colombia, es el acceso abusivo a sistemas informáticos, pues representa un incremento del 18% con respecto al 2020, un ejemplo reciente que se registró durante el 2021, fue el ataque hacia los servidores internos de la Aeronáutica Civil de Colombia, este hecho generó que los servicios internos como el correo y la página web de la aeronáutica civil, quedaran completamente suspendidos por unas horas. Aunque este ciberataque no causó mayor repercusión, si logró el cese de las actividades normales de las pagina web (El Tiempo, 2021).

Estos ataques que se han presentado en los últimos meses, son el abrebocas de lo que puede pasar si se pone en riesgo la información de las empresas, ya sean públicas o privadas, y si no se toman las medidas adecuadas para evitar estos ataques, aunque según lo investigado, el cibercrimen va creciendo conforme la era digital va evolucionando. El efecto al que están expuestas las empresas colombianas, después de un ciberataque abarca desde costos económicos por las pérdidas de sus activos financieros hasta las afectaciones a la productividad, y algo sumamente importante, que afecta a todas las empresas son los “daños reputacionales e incluso implicaciones de carácter legal por fuga de información privilegiada y datos privados” (CCIT, 2019).

Efectividad de las medidas de ciberseguridad en Colombia.

Dentro de todas las medidas de ciberseguridad que el gobierno colombiano ha desarrollado, es imposible concretar que estas han sido efectivas debido a que el ciberdelincuente siempre encontrará la manera de ir un paso adelante mediante las nuevas tecnologías y nuevos sectores que generalmente van a estar permeados por ambigüedades jurídicas, según Jeimy José Cano, Director de la Revista “SISTEMAS” de la Asociación Colombiana de Ingenieros de Sistemas, es inevitable no tener fallas dentro de una empresa, y menos dentro del ámbito de ciberseguridad, pues si se tiene información sensible, es necesario fortalecer el sistema de gestión de incidentes, esto se traduce a que *siempre* se presentaran amenazas en ciberseguridad, ya sean leves o graves en el escenario digital, y más cuando se ha aumentado la interacción digital en los últimos años, lo que realmente es importante y debería ser el as bajo la manga de todas las empresas, es la rapidez y efectividad con que la empresa reaccione ante esta amenaza o incidente.

Las empresas invierten una parte de su presupuesto en seguridad cibernética, pero esta siempre resulta ser un 1 o 2 % del presupuesto total de la empresa, y está bien, porque sería un despropósito invertir más de lo que se puede. La diferencia se puede ver en la focalización del presupuesto, saber exactamente las necesidades de la empresa y los puntos débiles de la misma. Por ejemplo, el presupuesto puede estar destinado a softwares actualizados que ayuden a contrarrestar los ataques a sistemas privados, en sistemas de gestión de riesgos más amplios y robustos, y en un excelente equipo de ingeniería informática que este siempre al tanto de los movimientos digitales de la empresa.

Aunque como evidentemente se ha mencionado, Colombia cuenta con varias dependencias en el sector defensa cuyo objetivo principal es ayudar a contrarrestar este tipo de delitos que ponen en riesgo la ciberseguridad de los ciudadanos y del país, estas medidas no han sido suficientes, de acuerdo a las cifras que anteriormente se han presentado, no es justo decir que Colombia no está preparada para hacerle frente a este tipo de delitos, pero sí que se debe continuar con el apoyo de las instituciones encargadas, de la mano con capacitaciones en todos los sectores, y que cada empresa conozca las amenazas que tiene en sus áreas, y así poder invertir en la protección de su información y sus activos. El Cibercrimen seguirá perfeccionando sus actos delictivos y utilizará todas las capacidades tecnológicas disponibles a su favor, (CCIT, 2019) ya que los ciberdelincuentes actúan bajo una serie de premisas que le permiten cometer sus delitos bajo la sombra del anonimato.

- *Ataques de mayor efectividad con el mínimo esfuerzo*; esto habla de la comodidad con la que un atacante puede robar información, o dinero, sin preocuparse por los daños físicos que este pueda tener.

- *Anonimato, sin dejar evidencia*; nadie sabe quién va a entrar al sistema de información de una empresa, usa seudónimos, apodos y cualquier tipo de palabras, con el fin de que nunca nadie sepa quien los hackeo.

- *Actuar en sectores nuevos, donde hay ambigüedad jurídica;* siempre van un paso adelante explorando las nuevas áreas tecnológicas, y buscando vacíos jurídicos para finalmente no tener asuntos legales pendientes con la ley, en caso de ser descubiertos.

- *Uso de las plataformas digitales públicas;* esto lo hacen con el fin de encontrar información personal de quien ellos quieran, para poder efectuar estafas, o robos de identidad.

Estas cuatro premisas son las que principalmente se encuentran, cuando de riesgos y amenazas cibernéticas se habla, no obstante, es difícil intentar contrarrestar los ataques digitales y tecnológicos, y lo único que se puede hacer es fortalecer el conocimiento en el área, porque muchas veces se espera a que suceda el crimen, para poder tomar medidas de acción. Y muchas veces, las PyMES, no se vuelven a recuperar de un ataque cibernético, porque su capacidad financiera no se lo permite (Cano, 2020).

Conclusiones

La alta dependencia a la tecnología actualmente genera todo tipo de incertidumbre, debido a las nuevas y variadas amenazas a las que se están expuestos todos los sectores económicos y sociales, los avances y el esfuerzo del gobierno colombiano para intentar contrarrestar los ciberataques han estado presentes, pero es necesario una transformación desde el eje central de las entidades del gobierno nacional que están involucradas en el apoyo a la ciudadanía, dado que la tendencia del cibercrimen sigue en aumento y no hay manera de evitarlo, por ello es necesario adoptar nuevas medidas jurídicas, que castiguen estos hechos de manera fuerte y contundente, para que así se disminuya este tipo de ataques que ponen en riesgo financiero y económico a muchas personas y entidades públicas y privadas.

Por otro lado, las consecuencias de los ciberataques han sido muy graves y han puesto en jaque el poder del Estado, ya que se ha robado información clasificada que afecta al sector público y privado. Las pérdidas aparte de ser económicas, también son perdidas de información de alto impacto, como es bien sabido en todo el mundo la era de la digitalización está presente en todos los ámbitos y para una empresa es bastante peligroso que estén manipulando su información, con el fin de secuestrarla y lucrarse económicamente. Debido a estos casos de ataques al gobierno nacional y a empresas privadas, se disminuye la confianza del ciudadano ante el estado, pues lo denota como débil, al no tener medidas completamente fuertes para contra atacar el cibercrimen.

Actualmente, el Gobierno Nacional de la mano con el Ministerio de Tecnologías de la Información y Comunicaciones, (MinTic) adelantan proyectos para fortalecer

estructuralmente y legislativamente las entidades encargadas de la protección de la ciberseguridad, tales como los grupos de respuesta a emergencias cibernéticas, anteriormente mencionados. El gobierno nacional busca ampliar la participación ciudadana en los temas de protección informática y así esperar que los ciudadanos amplíen la confianza digital en todos los sectores, ya que el avance digital es imprescindible.

Recomendaciones

El Gobierno Nacional deberá continuar con el fortalecimiento de las principales instituciones cuyo objetivo principal es controlar los delitos cibernéticos, ampliando los recursos destinados para esta área y así mismo facilitar la puesta en marcha de todos los proyectos y estrategias que se presenten.

Las instituciones delegadas por el Gobierno Nacional deberán fortalecer a todos los empresarios y PyMES, realizando continuas capacitaciones cuyo objetivo principal sea conocer los nuevos métodos de cibercrimen y las acciones de prevención que se pueden aplicar.

Establecer un área de concientización para los ciudadanos desde el ámbito escolar para proteger sus datos personales en plataformas digitales y así evitar el robo de información, y suplantación de identidad. Porque es ineludible que la era de la digitalización llegará a todas las generaciones.

Referencias.

Asociación Colombiana de Ingenieros de Sistemas. 2018. *Cisco presenta estudio global sobre la preparación digital por países.* Recuperado de: https://acis.org.co/portal/content/NoticiaDelSector/cisco-presenta-estudio-global-sobre-la-preparacion-digital-por-paises

Banco Interamericano de Desarrollo. 2020. *Ciberseguridad riesgos, avances y el camino a seguir en américa latina y el caribe.* Recuperado de: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Becerra, J. et al. 2019. *La seguridad en el ciberespacio. Un desafío para Colombia.* Escuela Superior de Guerra. Recuperado de: https://esdeguelibros.edu.co/index.php/editorial/catalog/download/42/48/741?inline=1

Cámara Colombiana de Informática y Telecomunicaciones. 2021. *El rol de la ciberseguridad en el actual contexto nacional.* Recuperado de: https://www.ccit.org.co/estudios/el-rol-de-la-ciberseguridad-en-el-actual-contexto-nacional/

Cámara Colombiana de Informática y Telecomunicaciones. 2021. *Tendencias del cibercrimen 2021-2022.* Recuperado de: https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf

Clay, A. 2021. *Estadísticas de la situación digital de Colombia en el 2020-202.* Recuperado de: https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-colombia-en-el-2020-2021/

Coll, F. 2020 *Revolución Digital*. Recuperado de https://economipedia.com/definiciones/revolucion-digital.html

Departamento Nacional de Planeación. 2016. *Documento CONPES 3854. Política Nacional de Seguridad Digital. Recuperado de:* https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Departamento Nacional de Planeación. 2020. *Documento CONPES 3995. Política Nacional de Confianza y Seguridad Digital. Recuperado de:* https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

El Tiempo. 2021. *Aeronáutica Civil recibió ataque cibernético.* Recuperado de: https://www.elcolombiano.com/colombia/secuestro-a-informacion-del-dane-en-colombia-IE16031966

El Tiempo.2017. *En Colombia hay 12 empresas afectadas por ciberataque mundial.* Recuperado de: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/numero-de-empresas-afectadas-en-colombia-por-ciberataque-mundial-103550

Esic Bussiness and Marketing School. 2020. Definición de la ciberseguridad y su riesgo. Recuperado de: https://www.esic.edu/rethink/tecnologia/definicion-ciberseguridad-riesgo.

Instituto Nacional de Ciberseguridad. 2020. *Guía de ciberataques, todo lo que debe saber a nivel usuario*. Recuperado de: https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

Ministerio de Defensa. 2018. *Plan estratégico de Tecnologías de la Información y las Comunicaciones del Sector Defensa y Seguridad 2018-2022.* Recuperado de: https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/Documentos_Descargables/espanol/PETI2018-2022.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. 2021. *Equipos de trabajo de 110 empresas recibirán capacitación gratuita en ciberseguridad con el Ministerio TIC*. Recuperado de: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/176180:Equipos-de-trabajo-de-110-empresas-recibiran-capacitacion-gratuita-en-ciberseguridad-con-el-Ministerio-TIC-Karen-AbudinenSaín, G. 2015. Que es un hacker. Revista Pensamiento penal. Recuperado de: https://www.pensamientopenal.com.ar/system/files/2015/04/doctrina40977.pdf

Ojeda. J, Rincón. F, Arias. M y Daza. L. (2010). *Delitos informáticos y entorno jurídico vigente en Colombia*. Recuperado de: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

Superintendencia de Industria y Comercio. 2009. *Ley 1273 del 2009.* Recuperado de: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Universidad del Rosario. *Colombia no está preparada ante un ciberataque***.** Recuperado de: https://www.urosario.edu.co/UCD/Colombia-no-esta-preparada-ante-un-ciberataque/