ESTUDIO SOBRE CASOS DE CIBERCRIMEN EN ENTIDADES GUBERNAMENTALES DE COLOMBIA EN LOS ÚLTIMOS 5 AÑOS.

STEVEN TIGREROS MOJICA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PALMIRA
2019

ESTUDIO SOBRE CASOS DE CIBERCRIMEN EN ENTIDADES GUBERNAMENTALES DE COLOMBIA EN LOS ÚLTIMOS 5 AÑOS.

STEVEN TIGREROS MOJICA

Trabajo de monografía, para optar el título de especialista en Seguridad en Informática

Asesor
Ing. Hernando Jose Peña Hidalgo

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PALMIRA
2019

NOTA DE ACEPTACIÓN

Presidente del Jurado

Jurado

Jurado (En caso de ser solo uno, borrar este o agregar de ser necesario).

Ciudad y Fecha (Dia, Mes y Año)

DEDICATORIA

La presente investigación es dedicada a mi familia por permitirme contar con las herramientas necesarias para adelantar mi proceso académico, a mi madre por estar siempre apoyándome en el avance de mis estudios, a mi novia por apoyarme moralmente en cada reto tanto profesional como personal, a mi padre por su constante apoyo para superarme cada día más, a mis hermanos por ser una fuente de admiración para llegar cada vez más lejos y a todas las personas que de alguna manera están involucradas en mi entorno.

AGRADECIMIENTOS

Agradezco a cada uno de los tutores que dirigieron y asesoraron mi camino profesional para obtener los mejores resultados, al tutor del curso Proyecto de Seguridad Informática y al asesor Hernando Jose Peña quien profesionalmente hizo cada una de las observaciones requeridas para desarrollar un producto de alta calidad, a la Universidad Nacional Abierta y a Distancia por permitir llevar a cabo un proceso de calidad y la dirección hacia un título de postrado como lo es la Especialización en Seguridad Informática.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

RESUMEN

El cibercrimen se ha expandido en niveles exponenciales, afectando a todas las instancias de la cotidianidad, con el uso cada vez más consolidado de las tecnologías de la información, los cibercriminales han encontrado una oportunidad importante en la era de las tecnologías, el uso del internet y dispositivos que facilitan el acceso, hoy en día la información personal está más expuesta que hace unos años atrás, los gobiernos han dado grandes pasos en el uso e implementación de nuevas tecnologías, con el objetivo de automatizar sus procesos, de tal manera que, ofrezcan a los ciudadanos servicios mucho más agiles y eficientes, el gobierno de Colombia acompañado por los ministerios, entre ellos, el Ministerio de Tecnologías MinTIC, ha desarrollado proyectos que impulsan el uso de las tecnologías en todas las regiones del país, para agilizar trámites y procedimientos a los ciudadanos, sin embargo, se ha identificado que la carencia de seguridad de la información es una gran falencia en sus proyectos, omitiendo el soporte en materia de seguridad a los demás departamentos administrativos que componen al gobierno, es por ello que este estudio se enfoca en los casos que el cibercrimen ha afectado el sector gubernamental en Colombia entre los años 2015 al 2019.

ABSTRACT

Cybercrime has expanded exponentially, affecting all instances of everyday life, with the increasingly consolidated use of information technologies, cybercriminals have found an important opportunity in the era of technologies, the use of the internet and devices that facilitate access, personal information is more exposed than a few years ago, governments have made great strides in the use and implementation of new technologies, with the aim of automating their processes, in such a way that they offer citizens much more agile and efficient services, the government of Colombia accompanied by the ministries, among them, the Ministry of Technology MinTIC, has developed projects that promote the use of technologies in all regions of the country, to streamline procedures and procedures to the citizens, however, it has been identified that the lack of security of information is a great failure in us projects, omitting the support in security matters to the other administrative departments that make up the government, this is why this study focuses on the cases that cybercrime has affected the governmental sector in Colombia between 2015 to 2019.

2 INTRODUCCIÓN

La información es el eslabón más importante de todo sistema, es el activo más preciado el cual debe tener una capa robusta de protección, En los últimos años se han evidenciado diferentes delitos informáticos dirigidos al sector gubernamental, es importante conocer el contexto de estos ataques, pues al dirigirse a los departamentos gubernamentales, tienen un significado mucho mayor al que significa un ataque, ya que este en la mayoría de los casos se trata de una manifestación y forma de expresión en contra, ante decisiones y actos legislativos asimilados por parte del gobierno, esto ha venido sucediendo desde que la era digital llego a Colombia, recientemente se han conocido casos que han generado un impacto en la sociedad.

Con el auge de las tecnologías, las nuevas tendencias, las redes sociales y los nuevos dispositivos que interactúan cada vez más con el contorno y el ecosistema, ha habido un interés muy alto de las personas por aprender sobre temas relacionados con las TIC, y la seguridad de la información es un tema de mucho interés tanto para estudiantes activos como para empleados y entusiastas, esto también ha conllevado a que los ciudadanos aprendan sobre técnicas de ataques informáticos, faltando al código ético al realizar pruebas sobre ambientes no autorizados, lo que ha generado ataques al sector gubernamental en Colombia.

La tecnología juega un papel indispensable en todos los aspectos de nuestras vidas, llevando consigo cambios cada vez más sorprendentes, al permitir la estructuración del entorno a niveles que se puede sintetizar una acción a través de una sistematización redundante de información, el nivel de dependencia de la tecnología es tal que un ciberataque puede poner en jaque la economía de un país en cuestión de minutos.

3 DEFINICIÓN DEL PROBLEMA

3.1 ANTECEDENTES

El cibercrimen en Colombia es un tema que aún no está completamente definido ni estudiado por parte de las organizaciones de defensa de delitos informáticos, tampoco existen leyes contundentes que penalicen de manera categórica actividades ilegales promovidas por herramientas tecnológicas o servicios administrados por las nuevas tecnologías, actualmente existen leyes en Colombia que exponen de manera provisional sanciones a individuos que practiquen la ciberdelincuencia con el objetivo de beneficiarse o apropiarse de recursos de otro individuo u organización, como lo es la Ley 1273 de 2009, esta ley no está completamente definida, y carece de grandes consideraciones para formalizar y estandarizar procedimientos que permitan penalizar actividades consideradas como un delito informático, en los últimos años se han registrado varios casos de cibercrimen ante entidades gubernamentales debido a la poca importancia que se le da a la seguridad de la información, y los pocos controles, mecanismos prevención y planes de contingencia ante este tema.

La ley 1273 de Enero de 2009 busca ofrecer un nivel mayor de protección en cuanto al uso y manipulación de los datos de los usuarios, y también prevenir y estar bien preparados ante futuros ataques tanto al sector gubernamental como al sector privado y de las organizaciones, sin embargo, esta ley debe ser fortalecida, pues no está en constante actualización y no penaliza nuevos tipos de delitos hallados recientemente, por lo tanto es importante llevarlo a un debate para el fortalecimiento y creación de nuevos artículos que complementen la penalización de delitos informáticos en Colombia.

Sin embargo, la ley 1273 de 2009 no es la única ley que busca reglamentar las acciones por medio de dispositivos informáticos y electrónicos, mucho antes, para agosto de 1999 se oficializó el 21 de agosto del mismo año, la ley 527 de 1999 la cual expresa por escrito que custodia y vigila acciones como son, mensajes de datos por medios electrónicos, comercio electrónico, firma digital, intercambio electrónico de datos y sistemas informáticos.

Mas tarde, el estatuto nacional regido por los magistrados expone la ley 1341 de 2009, la cual es una ley que basa en definir conceptos sobre la sociedad de la información en las TICs, esta ley se promulgada en junio de 2009 desde el congreso de la república.

La Ley estatutaria 1581 de 2012 por la cual se dictan disposiciones para la protección de datos personales presentada en el Congreso de la república, dispone el uso y tratamiento de datos personales para la protección de la privacidad de los cibernautas, el almacenamiento y no divulgación ni distribución de datos con fines lucrativos ni económicos.

A lo largo de los años han sido muchas los trabajos de investigación que se han realizado alrededor de los delitos informáticos en Colombia, el impacto de los delitos a nivel económico ha sido crucial en la economía del país, afectando así el progreso del sector empresarial, educativo y político, las universidades han hecho aportes importantes en este aspecto, contribuciones que permiten indagar y destacar la importancia de generar más profesionales en la seguridad de la información.

El trabajo realizado por Zulay Nayiv Sánchez Castillo en 2017 titulado “Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos

en Colombia"[1] abarca factores importantes en el análisis de los delitos frente a lo que se expone en la ley 1273 tomando como referencia informes anuales de la empresa de seguridad informática Symantec Norton frente a ataques y amenazas informáticas, además de denuncias por estafas e infracciones cometidas desde dispositivos electrónicos, también se realiza la comparativa entre la ley 1273 de 2009 con otros países de la región como Argentina, Chile y Venezuela.

El trabajo titulado "Incidentes informáticos en Colombia en los últimos 10 años."[2] Por el Ingeniero Jair Guerrero en el 2018 en la Universidad Nacional Abierta y a Distancia, indica cual es la afectación de los ataques informáticos en Colombia en los años comprendidos entre el 2008 y 2018, este trabajo permite analizar de forma progresiva como el número de delitos informáticos ha crecido de manera exponencial en Colombia en los últimos años, siendo el fraude por estafa cibernética el delito informático más concurrente en asuntos cibernéticos, la compra y venta de productos por medios electrónicos representa un nivel de seguridad el cual ha venido mejorando en los últimos años.

El trabajo titulado "Análisis de los delitos informáticos en el actual sistema penal Colombia"[3] realizado por Andres Camilo Montañez Párraga en la Universidad Libre de Colombia en el año 2017, se aborda el análisis de cómo se genera el impacto de los casos de delitos informáticos en el país y su impacto en las entidades estatales y en las empresas a raíz de infecciones de software malicioso y su fácil distribución, además del crecimiento de ataques cibernéticos a través de redes sociales.

---

[1] Sanchez Castillo, N (2017). Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia, En Línea, https://repository.unad.edu.co/handle/10596/11943

2 Guerrero, J. A. (2018). Incidentes informáticos en Colombia en los últimos 10 años. Recuperado de: https://repository.unad.edu.co/handle/10596/31941.

[3] Montañez Parraga, A, (2017). Análisis de los delitos informáticos en el actual sistema penal Colombia, En Línea, https://repository.unilibre.edu.co/bitstream/handle/10901/11041

Rodrigo Cortes Borrero en su trabajo titulado “Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia”[4] realizado en el 2015 en la Universidad Santo Tomas, expone que seis millones de personas son víctimas mediante alguna modalidad delictiva de cibercrimen digital en Colombia cada año, tomando como referencia la firma digital Norton security.

El trabajo titulado “La práctica de delitos informáticos en Colombia”[5] realizados por Edinson Raúl Serrano Buitrago en la Universidad Militar Nueva Granada en el año 2015 se refiere a la evolución en los métodos de ataques y la personificación como individuos de los atacantes, también explica los controles existentes y medidas utilizadas a través de herramientas legales disponibles.

[4] Cortes Borrero, R. (2015). Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia, En Línea, https://repository.usta.edu.co/bitstream/handle/11634/14032/2015rodrigocortes.pdf?seque

[5] Serrano Buitrago, E (2015). Practica de delitos informáticos en Colombia, Repo Unimilitar Nueva granada, En línea, https://repository.unimilitar.edu.co/handle/10654/13452

3.2 FORMULACIÓN DEL PROBLEMA

¿Cuál ha sido el contexto de los ataques informáticos ante las entidades gubernamentales en Colombia entre los años 2015 al 2019?

4 OBJETIVOS

4.1 OBJETIVO GENERAL

Realizar un estudio monográfico sobre casos de cibercrimen en entidades gubernamentales de Colombia en los últimos 5 años.

4.2 OBJETIVOS ESPECÍFICOS

- Conocer el alcance de los delitos de cibercrimen más relevantes realizados al sector gubernamental en Colombia en los años 2015 al 2019
- Identificar el perfil ético y psicológico de los ciberdelincuentes que han generado ataques informáticos al gobierno de Colombia.
- Conocer los sistemas de defensas que el gobierno tiene como contingencia en caso de recibir ataques de tipo informático.
- Identificar las falencias de la Ley 1273 de 2009 mediante la penalización de delitos cometidos con anterioridad al sector gubernamental.

5 JUSTIFICACIÓN

Los casos de delitos informáticos en el sector gubernamental en Colombia han crecido con el paso del tiempo, en los últimos años se ha evidenciado un aumento progresivo en los ataques de tipo informático ante entidades gubernamentales, es por ello por lo que es necesario legislarlos para que tengan una penalización que pueda controlar su ejecución y crecimiento. Es importante iniciar un estudio exhaustivo de la rama judicial a través de la Ley 1273 de 2009, Se debe conocer el panorama de la legislación nacional e internacional en contra de los delitos informáticos para dimensionar la problemática que está afectando a Colombia y a países que se pueden encontrar en las mismas condiciones.

La falta de vigilancia y falta de rigurosidad en las penalizaciones de los delitos informáticos hace que las personas que tengan conocimientos técnicos avanzados en ciberdelincuencia y en las leyes con referencia a este tipo de actividad se permitan tener licencias para proceder con los ataques y de esta manera operar de manera libre y sin temor a ser penalizados, hemos visto en Colombia diversos ataques al sector gubernamental, sin embargo, los autores intelectuales de estos delitos en el mayor de los casos reciben penas mínimas o incluso la posibilidad de afrontar dichas penas desde sus domicilios, con una vigilancia menor sin tener en cuenta que estos pueden seguir realizando actividades ilícitas.

Entre los años 2015 al 2019 se han evidenciado diferentes delitos dirigidos al sector gubernamental, es importante conocer el contexto de estos ataques, pues al dirigirse a los departamentos gubernamentales, tienen un significado mucho mayor al que significa un ataque, ya que este en la mayoría de los casos se trata de una manifestación y forma de expresión en contra de las instituciones, ante decisiones y actos legislativos asimilados por parte del gobierno, esto ha venido sucediendo

desde que la era digital llegó con más auge a Colombia, recientemente se han conocido casos que han generado un impacto en la sociedad, ya que, esta nueva forma de expresión hace un eco grande tanto en medios de comunicación como en las redes sociales; la sociedad Colombiana ha enfrentado casos de suma delicadeza como lo fue durante las elecciones presidenciales del año 2014, donde uno de los candidatos contrató a un hacker para obtener información sensible de un proceso de paz que estaba en marcha, de esta manera faltando a sus valores éticos y morales de quien en su momento era una persona publica muy importante, por lo tanto la decisión de realizar un ataque va más allá del conocimiento, es un tema ético y moral en donde actualmente existen grupos distribuidos por muchas ciudades del país, haciendo conocer su inconformidad con la toma de decisiones y acciones de los gobernantes y de los diferentes departamento que lo componen.

6 MARCO REFERENCIAL

6.1 MARCO CONCEPTUAL

6.1.1 Generalidades

El marco conceptual es “un conjunto de definiciones, teorías, conceptos, sobre los temas que estructuran el desarrollo de la investigación y que sirven para interpretar los resultados que se obtengan del trabajo realizado en campo” (Aula fácil, 2014, p.1).

Para conocer y entrar en contexto sobre los delitos informáticos en Colombia y su incremento exponencial que ha tenido en los últimos años, es importante recalcar que la seguridad informática como campo ha crecido también de manera proporcional, sin embargo, los métodos cada vez más eficientes y los alcances de los atacantes han permitido culminar con éxito muchos de sus objetivos.

De acuerdo con un reporte entregado en el año 2017 por la Policía Nacional hubo in incremento del 28,3% en los delitos cometidos a través de un sistema informático, siendo la interceptación y venta de datos personales, una de las categorías con mayor número de incidencias, a su vez la compra y venta de elementos ilegales como armas, animales, drogas, entre otros[6], esto ha hecho encender las alarmas en todos los entes reguladores y responsables de la ciberseguridad en Colombia.

Es por ello que la Policía Nacional en 2006 como estrategia de seguridad y atención rápida a incidentes crea un portal virtual conocido como CAI Virtual[7], este portal tiene como principal objetivo brindar la posibilidad a los colombianos a reportar incidentes y denuncias de ataques de tipo informáticos a través de internet de manera rápida y ágil, este proyecto es liderado por las oficinas de delitos informáticos la DIJIN, ahí un grupo especializado de policías debidamente

[6] Policia Nacional de Colombia, CAI VIRTUAL, 2017, [En Línea] Reporte de incidentes en Colombia 2017, https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

[7] EL CAI Virtual, 2006 [En Línea], https://www.semana.com/enfoque/articulo/el-cai-virtual/78640-3

preparados para reacción inmediata recibe las denuncias e incidentes para ser atendidos rápidamente y estos entren en investigación por parte de estas entidades.

Ataque: Se conoce como ataque a aquella acción que puede llevar a cabo una persona contra otra, un animal contra otro, o bien en un alcance mayor, la acción que un pueblo entabla contra otro, como consecuencia de la enemistad que los relaciona y que tiene la estricta finalidad de proferirle al otro un cierto daño que puede ser físico o moral.

Definición de conceptos, En el abordaje de este documento se utilizarán diferentes conceptos, entre los cuales están,

Ataque informático: Un ataque informático es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etcétera).

Cibercrimen: El cibercrimen se trata de delitos cometidos a través de internet por medio del uso de un computador o mecanismo análogo o por dispositivos electrónicos (por ejemplo: smartphone, pendrive, Tablet, etc.). También se han empleado términos tales como computer crime, computer related crime, digital/electronic/virtual, IT, high tech-crime, delitos informáticos, entre otros.

Ciberseguridad: Conjunto de acciones de carácter preventivo que tiene por objeto el uso de las redes propias y negarlo a terceros.

Confiabilidad: La confidencialidad se define como la capacidad que tiene un determinado elemento para desempeñar una función para la cual este existe en un tiempo determinado, por lo tanto, este siempre está a disposición en el momento y tiempo requerido.

Confidencialidad: La confidencialidad es una propiedad que ostenta algún tipo de información y mediante la cual se garantizará el acceso a la misma solamente a aquellas personas que estén autorizadas a conocerla, y por consiguiente no será revelada ante aquellos que no cuenten con la autorización de conocerla.

Delito informático: La policía nacional de Colombia como ente regulador de la nación define un delito informático como, conductas asumidas por un delincuente mediante el uso de programas o software informático para cometer delitos con objetivos personales a través de software ilegal[8].

Disponibilidad: La disponibilidad es una propiedad que tiene un elemento o servicio para ser usada o consultada en un momento determinado, Se denomina también disponibilidad a la posibilidad de una cosa o persona de estar presente cuando se la necesita.

Entidad gubernamental: Entidad u organismo gubernamental es una institución estatal cuya administración está a cargo del gobierno de turno. Su finalidad es brindar un servicio público que resulta necesario para la ciudadanía.

[8]CIBERSEGURIDAD, N. (2019). Revista NOISE- 4° Edición - noviembre 2017. [En Linea] Issuu. https://issuu.com/noiseciberseguridadla/docs/4.noviembre_202017

Hacker: Experto informático que tiene la posibilidad de hacer uso de los sistemas informáticos en un nivel superior al de los demás usuarios, por lo general el hacker aprende de manera autodidacta y adquiere conocimientos de manera más abstracta que el de muchos profesionales.

Información: Es la constitución de una serie de datos que tiene como objetivo representar un mensaje, está constituida a base del conocimiento, se representa a través de un lenguaje entendible por el individuo a quien está dirigido, este emite un mensaje con el objetivo de generar o aportar nuevo conocimiento.

Integridad: La integridad es la característica que tiene un elemento para conservar su estructura tal como fue diseñado, un elemento es íntegro cuando este siempre está completo y posee todas sus partes intactas.

Seguridad: La seguridad hace referencia a la ausencia del peligro, riesgo o miedo, la seguridad es un factor importante en las organizaciones y la información es el elemento en el cual se debe priorizar.

Seguridad Informática: Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante

Virus informático: Un virus informático es un programa malicioso o programa maligno que contamina el sistema operativo de los sistemas electrónicos como computadores o teléfonos inteligentes (smartphones).

Vulnerabilidad: Identificadas como aquellas debilidades existentes en el sistema de información y que comprometen la seguridad de los datos, pudiendo llegar a su perdida. Es un elemento de riesgo interno, que representa la factibilidad con que los activos o el sistema completo sean afectados por el fenómeno que caracteriza la amenaza

6.2 MARCO LEGAL

Se presenta de esta manera el marco de la legalidad en cuanto a delitos informáticos.

6.2.1 LEY 527 DE 1999 (agosto 21 de 1999)

"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones." [9]

Artículo 9o. INTEGRIDAD DE UN MENSAJE DE DATOS.

Para efectos del artículo anterior, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido, será

[9] Ley 527 de 1999. (1999), En Línea, http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

Artículo 11. CRITERIO PARA VALORAR PROBATORIAMENTE UN MENSAJE DE DATOS.

Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente, habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

Artículo 12. CONSERVACION DE LOS MENSAJES DE DATOS Y DOCUMENTOS.

Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones:

1. Que la información que contengan sea accesible para su posterior consulta.
2. Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y
3. Que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.

No estará sujeta a la obligación de conservación, la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos.

Los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta.

Artículo 28. ATRIBUTOS JURIDICOS DE UNA FIRMA DIGITAL.

Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido de este.

PARAGRAFO. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:

1. Es única a la persona que la usa.
2. Es susceptible de ser verificada.
3. Está bajo el control exclusivo de la persona que la usa.
4. Está ligada a la información o mensaje, de tal manera que, si éstos son cambiados, la firma digital es invalidada.
5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

6.2.2 LEY 1341 de 2009 (julio 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 –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones."[10]

Artículo 4o. INTERVENCIÓN DEL ESTADO EN EL SECTOR DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.

En desarrollo de los principios de intervención contenidos en la Constitución Política, el Estado intervendrá en el sector las Tecnologías de la Información y las Comunicaciones para lograr los siguientes fines:

1. Proteger los derechos de los usuarios, incluyendo a los niños, niñas y adolescentes, y a la familia velando por la calidad, eficiencia y adecuada

[10] Ley 1341 de 2009. (2009), En Linea, http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

provisión de los servicios, y la promoción de la digitalización de los trámites asociados a esta provisión.

…

7. Garantizar el uso adecuado y eficiente del espectro radioeléctrico, que maximice el bienestar social generado por el recurso escaso, así como la reorganización de este, respetando el principio de protección a la inversión, asociada al uso del espectro. Los proveedores de redes y servicios de telecomunicaciones responderán jurídica y económicamente por los daños causados a las infraestructuras.

…

9. Garantizar la interconexión y la interoperabilidad de las redes de telecomunicaciones, así como el acceso a los elementos de las redes e instalaciones esenciales de telecomunicaciones necesarios para promover la provisión y comercialización de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones.

Artículo 11. ACCESO AL USO DEL ESPECTRO RADIOELÉCTRICO.

El uso del espectro radioeléctrico requiere permiso previo, expreso y otorgado por el Ministerio de Tecnologías de la Información y las Comunicaciones.

El permiso de uso del espectro respetará la neutralidad en la tecnología siempre y cuando esté coordinado con las políticas del Ministerio de Tecnologías de la Información y las Comunicaciones, no generen interferencias sobre otros servicios, sean compatibles con las tendencias internacionales del mercado, no afecten la seguridad nacional, y contribuyan al desarrollo sostenible. El Ministerio de Tecnologías de la Información y las Comunicaciones adelantará mecanismos de selección objetiva, que fomenten la inversión en infraestructura y maximicen el bienestar social, previa convocatoria pública, para el otorgamiento del permiso para el uso del espectro radioeléctrico y exigirá las garantías correspondientes. En aquellos casos, en que prime la continuidad del servicio, el Ministerio de Tecnologías de la Información y las Comunicaciones podrá otorgar los permisos de

uso del espectro de manera directa, únicamente por el término estrictamente necesario para asignar los permisos de uso del espectro radioeléctrico mediante un proceso de selección objetiva.

En la asignación de las frecuencias necesarias para la defensa y seguridad nacional, el Ministerio de Tecnologías de la Información y las Comunicaciones tendrá en cuenta las necesidades de los organismos de seguridad del Estado. El trámite, resultado e información relativa a la asignación de este tipo de frecuencias tiene carácter reservado. El Gobierno nacional podrá establecer bandas de frecuencias de uso libre de acuerdo con las recomendaciones de la UIT. Así mismo, podrá establecer bandas exentas del pago de contraprestaciones para programas sociales del Estado que permitan la ampliación de cobertura en zonas rurales.

6.2.3 LEY 1273 DE 2009 (enero 5 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'[11] y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.

El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

[11] Ley 1273 de 2009. (2009) [En línea], https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Artículo 269C. INTERCEPTACION DE DATOS INFORMATICOS.

El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

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, envié, compre, intercepte, divulgue, modifique, emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

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 envié páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

Artículo 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 la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Artículo 269I. 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, incurrirá en las penas señaladas en el artículo 240 de este Código.

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, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre

que la conducta no constituya delito sancionado con pena más grave. la pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado victimas en la cadena del delito.

6.2.4 LEY ESTATUTARIA 1581 de 2012 (octubre de 2012).

"Por la cual se dictan disposiciones generales para la protección de datos personales."[12]

Artículo 4o. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES. En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:

a) **Principio de legalidad en materia de Tratamiento de datos**: El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen;

b) **Principio de finalidad**: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular;

c) **Principio de libertad**: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento;

d) **Principio de veracidad o calidad**: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error;

e) **Principio de transparencia**: En el Tratamiento debe garantizarse el derecho del Titular a obtener del responsable del Tratamiento o del Encargado del

[12] Ley estatutaria 1581 de 2012, En Línea, http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan;

f) **Principio de acceso y circulación restringida**: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley;

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;

g) **Principio de seguridad**: La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

h) **Principio de confidencialidad**: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de esta.

Artículo 5o. DATOS SENSIBLES.

Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Artículo 6o. TRATAMIENTO DE DATOS SENSIBLES.

Se prohíbe el Tratamiento de datos sensibles, excepto cuando:

a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;
b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular;
d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;
e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

Artículo 19. AUTORIDAD DE PROTECCIÓN DE DATOS.

La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

6.3 MARCO CONTEXTUAL

El cibercrimen se refiere a un término que está vinculado a la delincuencia cibernética, se entiende que se conoce como delitos realizados por medio de internet, con el uso de un ordenador o dispositivo similar a la Unidad de almacenamiento de datos, Smartphone, Tablet, entre otros, lo cual consiente en hacer usos de medios informáticos para comete ciberdelitos.

Con la afluencia de los sitios web y las redes sociales, los cibercriminales, han conseguido la ocasión de poder ingresar y sabotear datos personales sin escrúpulos. Por la falta de conocimiento e ignorancia les han puesto a sus pies todas las herramientas que ellos necesitan para cometer fácilmente delitos informáticos mediante métodos que se hacen pasar como legítimos, técnica conocida como ingeniería social. Además, está comprobado que los cibercriminales han aprendido a usar la psicología para este fin, que valiéndose de artes llegan hasta compañías que tienen información de gran relevancia y muy útil para sus propósitos criminales

Son acciones por medio del cual un delincuente por medio de mecanismos lo usa como herramienta con el fin de cometer una actuación delictiva, siendo actos delincuenciales que van al deterioro de la reserva, integridad y disponibilidad de los datos, relacionando formas de vías a causar perjuicios a un sistema informático. Estos influyen en la sociedad de manera negativa, porque en la actualidad donde haya acceso a un medio virtual que permite cambiar información, el riesgo y la

vulnerabilidad este a la orden del día afectando la intimidad de una persona y/o empresa.

6.4 MARCO TEÓRICO

6.4.1 Historia del Internet

Es importante conocer y tener un contexto un poco más amplio de los delitos informático, su evolución y sus alcances, el internet es el factor común, por lo tanto, conocer su historia conlleva a comprender los factores que han generado esté presente.

Lo que se conoce como internet hoy en día no está muy relacionado a lo que en algún momento Licklider J.C imagino allá en los años 60s en los laboratorios del Instituto de Massachussets MIT; Licklider concebía el internet de hoy como una red global o "red galáctica"[13] como en alguna ocasión llego a nombrar, el imagino un conjunto de redes que conectarían múltiples computadores a nivel global, con la posibilidad de compartir información desde cualquier parte del mundo, Licklider fue director del programa de investigación de DARPA para ese entonces, cuando comenzó con este visionario y revolucionario proyecto, pues fue ahí en donde se conoció un primer concepto sin mucho contexto de lo que hoy es la gran red de redes.

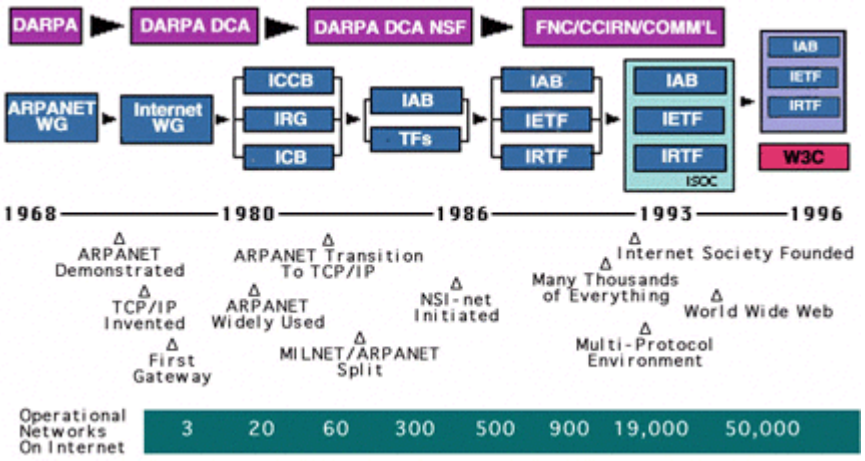
En 1962 Licklider público un libro en donde habla sobre la posibilidad de comunicación de información a través de paquetes en vez de circuitos, fue entonces para el año 1965 cuando se logró uno de los pasos más importantes en la historia de la computación, realizar de manera satisfactoria que 2 máquinas se hablasen entre sí, de esa manera se creó la primera red local de 2 máquinas, posteriormente

[13] Breve historia de Internet, *Los primeros conceptos de Internet*, Recuperado de, https://www.internetsociety.org/es/internet/history-internet/brief-history-internet

se realizaron diferentes investigaciones por parte de científicos del MIT y de la universidad de Utah, realizaron avances en la investigación hasta crear el proyecto ARPANET, el cual es el punto considerado como el inicio del Internet.

Con ARPANET se emitieron los primeros mensajes a diferentes nodos, entre ellos Utah, MIT, UCLA, el proyecto tuvo mucho éxito y rápidamente se empezaron a desarrollar proyectos para complementar él envió y transferencia de información a través de la red, 1972 se introdujo por primera vez el concepto de correo electrónico, para ese entonces Estados Unidos estaba en medio de una guerra con países del medio oriente y Asia, el proyecto ARPANET fue financiado por el gobierno de EEUU para que se aplicara en el sistema de defensa como un método de compartir información de manera secreta y segura.

Figura 1 Historia de Internet



Fuente. https://www.internetsociety.org/

Los desarrollos y las investigaciones avanzaron a medida que el computador personal fue también avanzando, así mismo, tecnologías de redes como el protocolo TCP/IP y el ethernet, de tal manera que se desarrolló para conectar a más computadores y a distancias más largas, para los años 80 el proyecto estaba bastante avanzado, ya era posible conectar miles de computadoras a nivel global,

las investigaciones continuaron e Internet se generalizo y se expandió a nivel mundial, con el nacimiento del World Wide Web “WWW” y de navegadores web, el internet creció exponencialmente.

6.4.2 Delito Informático.

El internet nace a mediados de la década del 60 por medio de múltiples investigaciones por parte de científicos de diferentes universidades de EEUU entre las que están, El Instituto Tecnológico de Massachussets (MIT), La Universidad de California de Los Ángeles (UCLA), la Universidad de Utah, entre otras, también se vieron involucradas empresas como la Stanford Reserch Institute (SRI)[14], estos proyectos fueron financiados por el gobierno y respaldados por las fuerzas militares estadounidenses debido a la necesidad de compartir información entre sus bases militares, este proyecto es conocido como ARPA (Advance Research Project Agency)[15] con el objetivo de mantener una comunicación segura en caso de un eventual ataque nuclear, más tarde, a inicios de la década de los 70, la investigación avanzó de manera rápida gracias a la contribución de varios científicos de estas Universidades lo que llevó a la obtención de una red avanzada que lograba comunicar varios computadores en diferentes regiones en los Estados Unidos, ahí nace lo que hoy en día conocemos como internet.

Internet al ser el medio por el cual se transmite información, este desde sus inicios ha enfrentado diversos desafíos, entre los que están la seguridad de la información, desde que es posible conectar dos o más computadores para transmitir datos, la integridad, confidencialidad y la disponibilidad de ha sido los pilares para tener en cuenta para la protección de los datos.

---

[14] Breve historia de Internet, *Origines de Internet,* Recuperado de, https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/#f3

[15] 45 años de ARPANET, *el origen del Internet,* Recuperado de, https://hipertextual.com/2014/11/arpanet-45-anos

6.4.3 Tipos de Delitos Informáticos

Los delitos informáticos son una representación de la necesidad de obtención de la propiedad que no pertenece al individuo a través de mecanismos electrónicos que afectan la privacidad de las personas desde sus datos personales como del abuso intelectual, para definir los tipos de delitos informáticos es importante hacer referencia al Convenio sobre la Ciberdelincuencia el cual fue presentado en Noviembre de 2001[16], este tuvo lugar en el marco tecnológico en la Unión Europea, el cual fue firmado en Budapest, por lo cual se definen los siguientes grupos.

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

- Acceso ilícito a sistemas informáticos.
- Interceptación ilícita de datos informáticos.
- Interferencia en el funcionamiento de un sistema informático.
- Abuso de dispositivos que faciliten la comisión de delitos.

Este tipo de delitos usualmente son cometidos a través de usos de mecanismos como, el robo de identidades, conexión a redes no permitidas, y la utilización de software ilegal como son keyloggers y software espía.

Delitos informáticos, los delitos informáticos cometidos dentro de este grupo son aquellos cuando de manera no autorizada se borra información o se corrompen ficheros para beneficio propio, ellos son,

- Falsificación informática mediante la introducción, borrado o supresión de datos informáticos[17].

[16] Tipos de delitos informáticos, *Clasificación según el "Convenio sobre la Ciberdelincuencia" de 1 de noviembre de 2001,* Disponible en, https://delitosinformaticos.info/delitos_informaticos/tipos_delitos.html

[17] Tipos de delitos informáticos, *delitos informáticos,* disponible en, https://delitosinformaticos.info/delitos_informaticos/tipos_delitos.html

- Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.
- Delito relacionado con contenido,

Toda aquella propagación, creación, edición, difusión, producción de contenido pornográfico infantil, a través de sistemas electrónicos.

7 ALCANCE DE LOS DELITOS INFORMÁTICOS EN COLOMBIA

Durante el abordaje de este documento se realiza el análisis y colección de datos con respecto a los delitos informáticos que han tenido lugar en Colombia a través de dispositivos electrónicos e internet, se estudia las causales y consecuencias de dichos delitos y se hace un análisis a las normas y leyes actuales en Colombia, como lo son la Ley 527 de 1999, la Ley 1341 de 2009, la Ley 1273 de 2009, y la Ley 1581 de 2012, las cuales serán usadas como base para el análisis de dichos delitos y las consecuencias legales que este conlleva.

De acuerdo con esto, se utilizarán fuentes de información mayormente electrónicos, como son revistas electrónicas, diarios, noticias y fuentes complementarias donde se realiza el reportaje de las noticias sobre delitos informáticos, además también el estudio de trabajos de grado, proyectos de investigación y tesis, permitiendo de esta manera realizar un estudio que permita abordar de manera completa la evolución de los delitos informáticos y las leyes en Colombia.

Para llevar a cabo esta investigación se requirió de la siguiente metodología:

- Determinar los lineamientos necesarios que competen los diferentes sectores gubernamentales en Colombia.
- Identificar cada una de las entidades responsables, las cuales están relacionadas con la prevención de los delitos informáticos.
- Identificar el estado del arte, eso se llevó a cabo a través de la búsqueda de información y documentos alojados en internet, el buscador más usado fue Google, se consultó múltiples fuentes para obtener la mayor cantidad de información posible
- Se realizo una búsqueda de los diferentes delitos informáticos cometidos dentro del territorio nacional, cuyos objetivos fueron especialmente las entidades gubernamentales.

- Se investigó por la ley vigente que contempla judicialmente las competencias con respecto a los delitos informáticos, la ley 1273 de 2009.

7.1 ALCANCE DE LOS DELITOS INFORMÁTICOS MÁS RELEVANTES AL SECTOR GUBERNAMENTAL EN LOS ÚLTIMOS 5 AÑOS

El cibercrimen en Colombia ha crecido a pasos agigantados en los últimos años, según datos reportados por la revista Dinero, Colombia representa el 8,05% del total de los ataques informáticos en Latinoamérica, y tan solo en el año 2017[18] se registraron más de 198 millones de ataques cibernéticos en el país, siendo los ataques tipo phishing los más comunes, el sector más afectado por el cibercrimen fue el financiero, representando más de 215.000 ataques por día, seguido del sector de Telecomunicaciones, posteriormente el sector gubernamental recibe más de 83 mil ataques por día, cerca del 15,45% del total de los ataques registrados en Colombia tanto a nivel privado como del estado.

Una persona es usuario activo del ciberespacio cuando realiza una consulta de información, se envían correos electrónicos, realiza transacciones en línea, hace uso de los medios audiovisuales y telemáticos, o navega en las redes sociales, cada actividad que un usuario realiza en internet es registrada en un sistema de logs tanto local como remota, la mayoría de sitios web están diseñados para que un usuario se registre o cree una cuenta, lo que permite crear perfiles personalizados para cada usuario, esto permite a los programadores realizar un seguimiento individual y más preciso de los usuarios, Internet cuenta con múltiples formas de identificar las actividades realizadas por los usuarios, a esto se le conoce como ‘tracking’, una de las formas más comunes de realizar ‘tracking’ es mediante las ‘cookies’ estos son archivos diseñados para almacenar información relevante durante la navegación de

[18] Los sectores económicos más impactados por el cibercrimen en Colombia (2017), [En Línea] https://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321

los usuarios en un sitio web, sin embargo, también existen otros métodos más avanzados de almacenamiento de información, esta es una práctica legal que favorece a los propósitos publicitarios y de seguridad, sin embargo, también se convierte en un factor que puede comprometer la seguridad de los usuarios, los atacantes puede robar remotamente las 'cookies' con motivos dañinos, ya que estos almacenan información sensible como sesiones activas, identificación de usuarios, credenciales, entre otros.

El gobierno nacional desde el Ministerio de Defensa a través del Consejo Nacional de Política Económica y Social CONPES[19], en su documento 3701 de 2011 otorgo la defensa y seguridad Nacional en el Ciberespacio a esta entidad, estos esfuerzos están articulados con entidades como coICERT (Grupo de respuestas a emergencias en Colombia) el cual coordina aspectos como ciberseguridad y ciberdefensa, también hace parte de este grupo de defensa el Comando Conjunto Cibernético CCOC de las fuerzas militares proporciona estrategias que permiten prevenir o contrarrestar amenazas que afecten los intereses nacionales, al igual que el CCP Centro Cibernético Policial el cual ofrece información, apoyo y protección ante delitos cibernéticos, este implemento a su vez un CAIV (Comando de Atención Inmediata Virtual) el cual recibe reportes de delitos informáticos, por lo tanto las entidades responsables de la seguridad ante delitos informáticos son,

- CONPES (Consejo Nacional de Política Económica y Social)
- coICERT (Grupo de respuestas a emergencias en Colombia)
- CCOC (Comando Conjunto Cibernético)
- CCP (Centro Cibernético Policial)
- CAIV (Comando de Atención Inmediata Virtual)

Colombia fue el primer país en Latinoamérica en incorporar mejores prácticas en gestión de riesgos de seguridad digital mediante el CONPES, el cual a través del

[19] Ciberseguridad entorno colombiano [En Línea], https://www.oas.org/juridico/spanish/cyber/cyb8_col.pdf

MinTIC[20] busca detener el crecimiento del cibercrimen tanto en entidades privadas como en el sector público, por este motivo se implementaron 5 factores específicos:

- Establecer un marco institucional claro en torno a la seguridad digital, basado en la gestión de riesgos.
- Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.
- Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos.
- Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.
- Impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional.

Por su parte, el Ministro de Defensa, Luis Carlos Villegas[21], destacó que con estos nuevos lineamientos de política el Sector Defensa y Seguridad continuará fortaleciendo las capacidades en materia de ciberseguridad y ciberdefensa, "esto posiciona la experticia de nuestras Fuerzas Militares y de la Policía Nacional a nivel internacional, garantizando la defensa y seguridad en el entorno digital para todos los colombianos" afirmó.

El MinTIC[22] mediante el documento CONPES del 2011 expresa lo siguiente *"La problemática central se fundamenta en que la capacidad actual del Estado para*

[20] Colombia cuenta con una Política Nacional de Seguridad Digital (2016) [En Línea] http://www.mintic.gov.co/portal/604/w3-article-15033.html

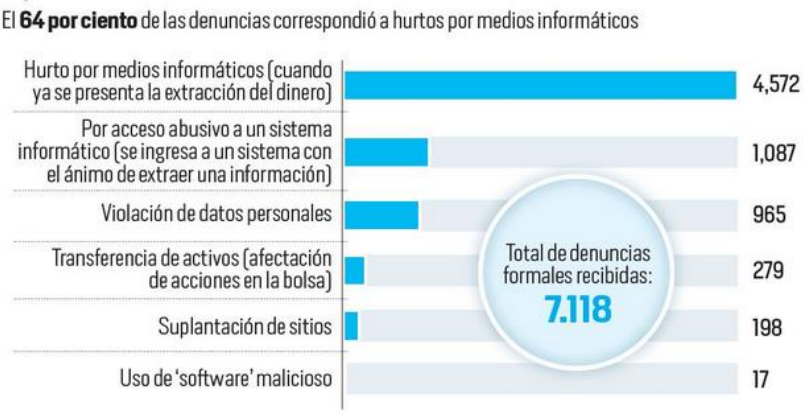
[21] Colombia cuenta con una Política Nacional de Seguridad Digital, MinTIC, (2016), [En Línea], https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/15033:Colombia-cuenta-con-una-Politica-Nacional-de-Seguridad-Digital

[22] Lineamientos de política para ciberseguridad y ciberdefensa [En Linea] http://enticconfio.gov.co/images/stories/normatividad/Conpes_3701.pdf

enfrentar las amenazas cibernéticas presenta debilidades y no existe una estrategia nacional al respecto. A partir de ello se establecen las causas y efectos que permitirán desarrollar políticas de prevención y control, ante el incremento de amenazas informáticas. Para la aplicabilidad de la estrategia se definen recomendaciones específicas a desarrollar por entidades involucradas directa e indirectamente en esta materia. Así lo ha entendido el Gobierno Nacional al incluir este tema en el Plan Nacional de Desarrollo 2010-2014 "Prosperidad para Todos", como parte del Plan Vive Digital".

Las noticias sobre ataques informáticos frente a organizaciones, ciudadanos, empresas y sectores del gobierno son cada vez más habituales tanto en medios de comunicación como en el mundo de la información a través de internet.

Figura 2 Denuncias por delitos informático

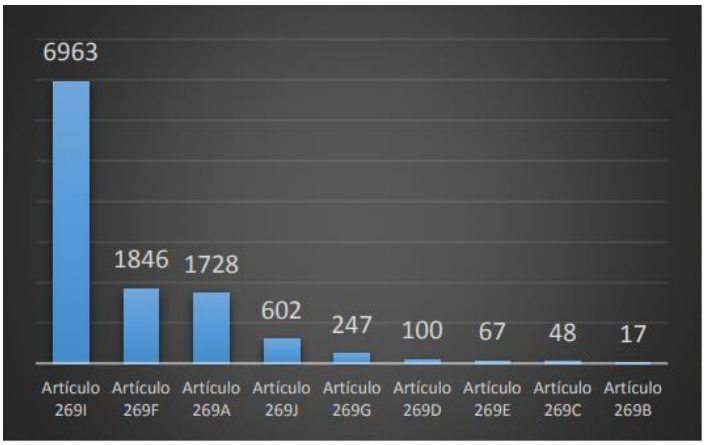


Fuente: Unidad de delitos informáticos de la Dijin.

El hurto electrónico es el causal principal de delitos los cuales han sido denunciados directamente representando así un 60% de las denuncias, este tipo de delitos está contemplado en el artículo 269I, "Hurto por medios informáticos y semejantes", este es seguido por el articulo 269F "Violación de datos personales" el cual representa el 16% de los delitos denunciados.

La siguiente figura ilustra los delitos denunciados por los ciudadanos durante el año 2017 representados de la siguiente manera,

Figura 3. Distribución de denuncias por artículo.



Fuente, CAI Virtual, disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_201217_1_1_0.pdf

7.1.1 Voto electrónico en Colombia y sus riesgos

El pasado 27 de Mayo de 2018 los colombianos tuvieron la posibilidad de elegir el que sería el próximo apoderado de la casa de Nariño durante 4 años, Colombia como un estado demócrata lleva a las personas la posibilidad de escoger al próximo presidente por medio de la consulta popular quienes solo personas mayores de 18 años nacidos en Colombia pueden ejercer el derecho del voto, desde sus inicios hasta la actualidad la manera de elegir a un presidente es mediante las urnas, toda la logística que conlleva a las elecciones tanto de concejales, alcaldes, gobernadores y presidenciales son organizadas por la Registraduría Nacional de Colombia, es la entidad que se encarga de realizar todo el trámite logístico para llevar a cabo de la manera más transparente posible este proceso, actualmente las personas con más de 2 meses de anticipación son informadas para conocer el punto de votación al cual corresponde cada Colombiano para ejercer su derecho, este se hace de manera presencial y estrictamente personal, cumpliendo con unos

requisitos impuestos por la Registraduría y por la legislación Colombiana; las tecnologías cumplen un papel fundamental en este proceso, hasta este momento las tecnologías son usadas para facilitar a los sufragantes conocer cuál es el puesto de votación, entre otra información importante, sin embargo, desde hace varios años se ha llevado a cabo un debate para dar un paso más allá al proceso electoral en Colombia, este es, hacer uso de las Tecnologías de Información TIC's para el proceso electoral, este es un debate que ha traído muchas opiniones por parte de expertos en la informática como lo expone un artículo de la Registraduría,

> *"Votar con computadoras es abrir una*
> *puerta grande al fraude, no podemos*
> *dar por supuesto que el fabricante es*
> *honesto, ni que la autoridad electoral*
> *es honesta ni que los dos no conspiran juntos"*
> Richard M. Stallman

La seguridad de la información y la transparencia en el proceso electoral es el factor crucial en cuanto a la decisión de implementar el voto electrónico en Colombia, garantizar que el voto electrónico es transparente es el principal reto para el gobierno colombiano, pues el uso de las tecnologías para este fin tiene varias ventajas, entre las que se encuentran.

7.1.2 Ventajas

- El voto a distancia a través del uso de Internet incrementaría en gran medida el número de sufragantes y participación en las elecciones a niveles históricos.
- La contabilización inmediata del escrutinio y resultados de la votación.
- La reducción exponencial en el uso del papel y costos logísticos por organización.

- Solución a la problemática de uso de papel excesivo en las urnas y a su vez la posibilidad de que estos se agoten durante el proceso electoral.

7.1.3 Desventajas

- La falta de transparencia durante el proceso electoral
- La dificulta en el ejercicio del voto de los adultos mayores durante el proceso
- La alta posibilidad de sabotaje en cuanto a la red eléctrica y la alteración del resultado del proceso electoral.

Sin embargo en Colombia existe un estigma y bajo nivel de aceptación ante la propuesta del voto en blanco, sumado a eso se debe tener en cuenta las ocasiones en que las elecciones han quedado en evidencia con videos de supuesto fraude, al igual que múltiples denuncias e informes al respecto, uno de los casos más recientes es el de la funcionaria Aida Merlano quien en las pasadas elecciones del 11 de Marzo aspiraba a ser Senadora de la Republica, una vez escrutado más del 99% de los votos se dio a conocer que la funcionaria obtuvo el número de votos para ganar la curul, posteriormente en las redes sociales circulaba un video donde se evidencio que la funcionaria recurrió a factores extra legales[23] para ganar la curul, después de investigaciones por parte de la Fiscalía se concluyó que la funcionaria compró votos durante la campaña, varias personas fueron capturadas.

Adicional a este caso en Colombia existen muchas denuncias con respecto a los proceso electorales, por tal motivo muchas personas no están de acuerdo con el uso de las TICs en el proceso electoral, expertos en la materia exponen que el mal uso de las TICs facilita en gran medida la alteración de los resultados, advierten que el uso de software privativo no es recomendado ya que el fabricante podría diseñarlo a beneficio de algún candidato, sin embargo, también defienden y recomiendan el

[23] En sede de la senadora Aida Merlano se movería compra de votos [En línea], disponible en: http://www.eltiempo.com/colombia/barranquilla/en-la-sede-de-la-senadora-aida-merlano-se-movia-la-compra-de-votos-193432

uso del software libre como alternativa para implementar el voto electrónico ya que este asegura una elección honesta, debido a su posibilidad de ser intervenido libremente y permitir contribuciones a su desarrollo de manera controlada, el problema radica cuando la información queda en manos de las entidades que ofrecen los resultados, ya que estos pueden ser alterados.

Sin embargo, se han realizado diferentes estudios y propuestas para presentar la posibilidad de implementar el voto electrónico como alternativa y solución a los diferentes problemas que existen actualmente, mediante la promulgación de la ley 892 de 2004, articulo 258, en la cual se emite el mecanismo electrónico de votación como alternativa a las urnas tradicionales, es por ello que este articulo expone en su parágrafo uno lo siguiente, "*Se entenderá por mecanismo de votación electrónico aquel que sustituye las tarjetas electorales, por terminales electrónicos, que permitan identificar con claridad y precisión, en condiciones iguales a todos los partidos y movimientos políticos y a sus candidatos.*"[24] Esta ley sigue en vigencia, pero hasta ahora no se ha implementado como mecanismo valido y consolidado de votación, a pesar de diversos intentos de aplicación, pues en 2009 se solicitaron recursos por valor de $100.000 millones de pesos para la implementación de esta tecnología con el fin de implementarse en las votaciones del 2010, sin embargo, no hubo una respuesta positiva por parte del gobierno, posteriormente, se solicitaron recursos por valor de $30.000 millones de pesos para la aplicación de mecanismos robustos de seguridad en los controles biométricos en las zonas de mayor riesgo.

Para el año 2018 se realizó una propuesta de auditoría independiente por parte de Karisma, una fundación que busca responder a amenazas y oportunidades que plantea la tecnología para el desarrollo de derechos humanos, esta organización expone que en Holanda se introdujo el voto electrónico en los años 90, pero luego de que en el año 2006 un grupo de hackers probara que era fácil cambiar los

[24] Sistema único de información normativa, Ley 892 de 2004, articulo 1, parágrafo 1, (2004), [En Linea], http://www.suin.gov.co/viewDocument.asp?ruta=Leyes/1670113

resultados de las votaciones, regresaron al proceso manual, en Brasil se hace uso del voto electrónico, pero en 2012 se comprobó que es posible identificar la identidad del ciudadano que emitió el voto, sin embargo, el mecanismo sigue en vigencia, en Alemania hubo un intento de migrar el voto por urnas al voto electrónico pero luego de que en Holanda se evidenciara la posibilidad de fraude, estos declinaron la posibilidad.

En Colombia hay diferentes partidos que están a favor de la implementación del sistema electrónico como una solución al fraude en Colombia, el partido MIRA es uno de los más interesados en promover la reforma, después de que en 2014 perdieron 3 curules a senador por supuestos actos de corrupción en las urnas electorales, también hay senadores como Jorge Robledo y Antonio Navarro que están a favor de esta propuesta

7.1.4 Casos de ciberataques en Colombia

Uno de los casos más conocidos fue en el 2014 durante los procesos de paz realizados en la Habana, Cuba, cuando a través de las noticias se dio a conocer que un experto en informática, Andrés Sepúlveda, fue señalado de cometer actos de ciberespionaje, acceso abusivo a sistemas informáticos, uso de software malicioso y violación de datos personales, quien fue contactado para favorecer de manera directa la campaña del aspirante a presidencia en ese entonces el señor Oscar Ivan Zuluaga, quien fue destituido de la posibilidad de ser aspirante a presidencia.

7.1.5 El “hacker político” que incomodó a varios Gobiernos en América Latina

Figura 3 ‘Hacker’ Andres Sepulveda capturado por hombre del CTI

https://www.publico.es/uploads/2016/04/01/56fe2147b9fbb.jpg

Andrés Sepúlveda, logró filtrar información y documentos de inteligencia sobre el proceso de paz con las FARC y el gobierno de Santos del cual se pretendía que iba a sabotear, documentos de la fuerza pública, listados de desmovilizados y lo que llamó aún la atención, los reportes de campañas políticas.

Dentro de la evidencia recolectada, se detectó también documentos de la mesa de diálogos, fotografías y correos desde y hacia las FARC, como pruebas suficientes para que pagara una condena de 10 años en la cárcel en el estado colombiano por espiar e interceptar conversaciones de manera ilegal, y al que también se le atribuyó actos de concierto para delinquir, violación de datos personales, acceso abusivo informático y uso de software malicioso.

También se conoce que Andrés Sepúlveda, estuvo involucrado en escándalos de campañas electorales en otros países como Nicaragua, Panamá, México y

Venezuela.

7.1.6 ‘Oroburuo’ el paisa con más de 3000 ataques a dominios del gobierno

Figura 4 ‘Hacker’ Oroboruo, capturado por la Policía Nacional, octubre 2016

Fuente: https://www.elcolombiano.com/colombia/images/article-26548/image

‘Oroboruo’ como era conocido en el mundo cibernético, esta persona se dedicaba a atacar páginas del gobierno, especialmente a la registraduría, uno de sus ataques más comunes fue cuando atacó al sitio web de la registraduría antes de las votaciones del plebiscito, vulnero en más de 3000 ocasiones a casi 1400 dominios, la mayoría de ellos del gobierno, su intención era inyectar código malicioso para infectar a los usuarios visitantes y también modificar el comportamiento de la página web.

Este hacker perteneció al grupo de hackers colombiano ‘Colombian Hackers’ dejo diferentes registros de ataques a páginas del gobierno en el foro ‘Zone-H’ entre los que dejo el ataque que realizo a la Registraduría el 26 de septiembre, uno de sus primeros ataques fue cuando vulnero la seguridad de la página de la alcaldía de Ibagué en el año 2015, posteriormente continuo con sus ataques a empresas locales, a radios, páginas de televisión, emisoras entre otras.

Este hacker colombiano de origen paisa fue capturado en su lugar de residencial, el barrio buenos aires, Medellín, quien fue sorprendido cuando se preparaba para realizar más ataques a páginas del gobierno, ahora es un recluso en una cárcel en Itagüí.

7.1.7 "Ataque del grupo Anonymous a las páginas webs del Ministerio de Educación"[25]

Este caso catalogado como ciberactivismo, dado que son personas dedicas a cuestiones sociopolíticas que emplean las redes sociales para atraer seguidores e informar cada una de sus acciones, para este ejemplo se utiliza YouTube (hacer lobby) y Twitter. Adicionalmente se clasificó también como hacktivismo, pues sus prácticas persiguen el control de ordenadores o sitios web para promover su causa, como sucedió en el caso de Colombia, en donde estos a través de su cuenta de twitter invitaron a las personas a realizar un ingreso masivo a la página del Ministerio de Educación, con el objetivo de colapsarla pues no estaban de acuerdo en que dicha entidad buscara atraer capitales privados a las universidades, posteriormente el ataque se extendió a otras entidades como el Ministerio de Defensa, El Senado y La Presidencia conllevando a que estas fueran suspendidas temporalmente.

7.1.8 Rafael alias 'R4lph'

Ingreso a la página de la procuraduría y coloco una imagen del alcalde Gustavo Petro, con la frase "Petro no se va" e ingreso a la página web del Ministerio Publico cerca de 4 horas. En este lapso ingreso a una base de datos reservada. La firma de este era 'R4lph_is here', la cual contaba con tres años, el inició actividades en las comunidades de hacktivismo, desde los 14 años.

[25] Casos de Ciberataques en Colombia, [En Linea] disponible en, http://repository.unimilitar.edu.co/bitstream/10654/7161/1/Ensayo%20para%20optar%20al%20titulo%20de%20Internacionalista%20y%20Politóloga.%20Lady%20Carolina%20Lozano%20Quintero%20.pdf

El hacker era un joven de 17 años, oriundo de la ciudad de Barranquilla. De acuerdo con las investigaciones realizadas entre el 2011 y 2015 logro violar la seguridad de 170 páginas del estado, este era muy cuidadoso y borrada las huellas, sin embargo, la Dijin lo identificó. R4lph_is_here', hace parte de la organización '*Colombian hackers'*

Figura 5 'Pagina web de la Procuraduría alterada'

https://www.elespectador.com/noticias/judicial/hackearon-pagina-de-procuraduria-decision-contra-petro-articulo-463244

El ministerio de las TIC plantea una visión que consolide las bases del documento CONPES 3701, con el objetivo de generar lineamientos ante la Ciberseguridad que permita crear estrategias para contrarrestar el inminente incremento de las amenazas y riesgos que afectan el sector gubernamental, el Ministerio de Tecnologías presenta unos vectores de desarrollo que corresponden a directrices dentro del marco de seguridad en cuanto a la información y el manejo de esta, cada uno de estos vectores está compuesto por líneas temáticas, las que detallan los temas específicos en los cuales se debe enfocar los esfuerzos de innovación en el país.

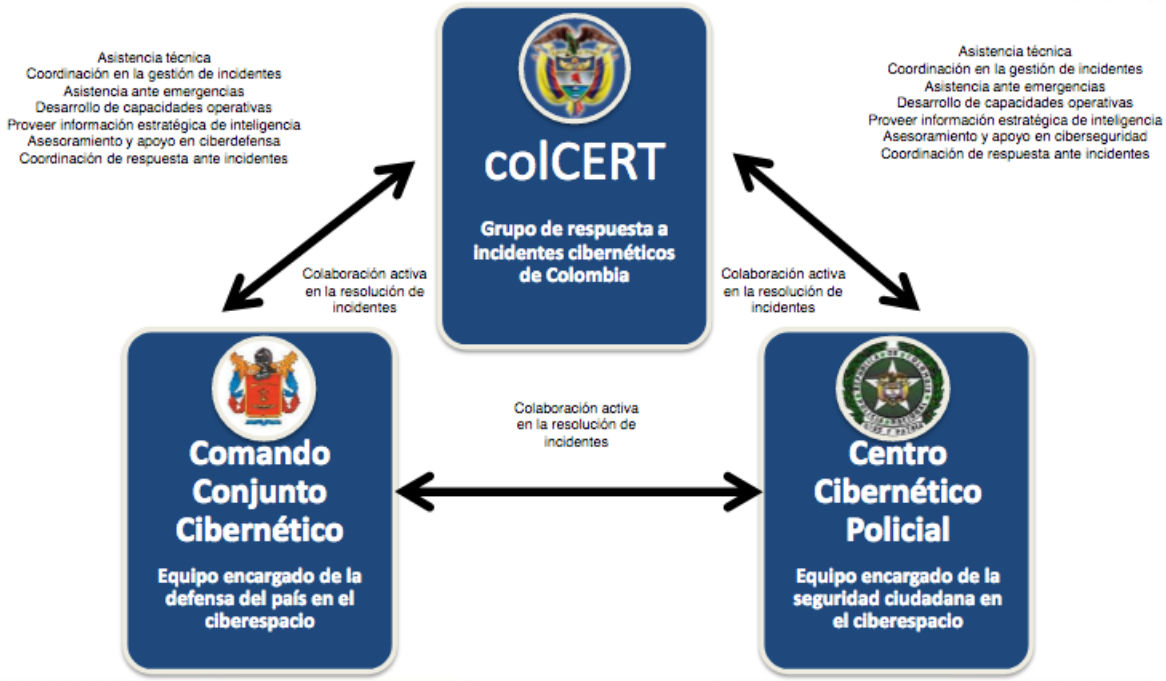
El nodo de seguridad se ajusta al documento CONPES 3701 con el fin de minimizar el nivel del riesgo al que la información está expuesta para,

- Fortalecer la posición estratégica en el ciberespacio
- Asegurar la infraestructura del estado y la protección de los servicios que provee a los ciudadanos
- Enfrentar de formar adecuada los riesgos en ciberseguridad

El nodo busca,

- Adaptar las tecnologías existentes
- Generar nuevas tecnologías
- Permitir la apropiación y el uso de las tecnologías
- Minimizar y contrarrestar los riesgos e incidentes de naturaleza cibernética en el estado.

Figura 6 Concejo Nacional de Política Económica y Social



Fuente: https://oas.org

En Colombia uno de los casos más conocidos es el caso del hacker ‘Sepúlveda’ con él en ese entonces aspirante a Presidencia ‘Oscar Iván Zuluaga’ podemos determinar que este es una actividad con objetivos propiamente políticos, este tipo de casos afectan directamente la ética de los involucrados, pues sabemos que el hacker fue dispuesto a las autoridades y ahora cumple una pena de 10 años en prisión, sin embargo, también debió ser procesado el contratista quien adquirió un servicio y fue autor intelectual de estos hechos, pero este y muchos casos similares, son casos comunes; no yendo tan lejos, debemos recordar el caso de Jaime Lozano, quien fue reconocido como el ladrón de millas a famosos; también objetivos sociales, como es el caso del grupo Anonymous, quienes anónimamente luchan contra la corrupción y casos de denigración humana a nivel mundial, en Colombia también conocemos un ataque muy sonante el cual fue el del hacker ‘Oroboruo’ quien realizo más de 3000 ataques a entidades gubernamentales, con el objetivo de obtener información reservada, modificación del funcionamiento de sitios web, y entre el más conocido el sabotaje a la votación por el plebiscito en el año 2016, este tipo de ataques son por orden psicológicos, es relevante destacar que los ataques realizados para llamar la atención, no son los más importantes, pues provienen de personas que no tienen mucha experiencia en este campo, y que están aprendiendo, un caso muy conocido, pero no menos importante es el de un chico de 17 años que se hace llamar en el mundo cibernético como ‘R4lph_is_here’ este chico hizo un ataque a la página de la procuraduría cuando se disputaba el tema de la inhabilitación del entonces alcalde de Bogotá Gustavo Petro de su carrera política y de su cargo, este joven puso una imagen, este ataque hace parte de un tipo de llamada de atención y a su vez un ataque social.

De los delitos cometidos el 64% se relaciona con el hurto de medios informáticos, el 16% por el acceso abusivo a sistemas informáticos, 12% por violación de datos personales, 4% por transferencias de activos, 3% por suplantación de sitios y 1% por la creación y uso de software malicioso.

Entre los actos más apetitosos por los criminales informáticos son el de acceder a bases de datos de entidades bancarias, la clonación de tarjetas bancarias y el ingreso abusivo a las redes sociales y correos electrónicos.

Según el diario el tiempo, en 2015 el cibercrimen genero pérdidas por más de $600 millones de dólares en Colombia, con el crecimiento exponencial de los dispositivos tecnológicos y la aplicación de la tecnología en cada aspecto de la cotidianidad, tanto académico, laboral, personal, de negocios, de ocio, entretenimiento y demás, el uso de dispositivos conectados a internet cada vez es mayor, pues según Caracol 7 de cada 10 colombianos está conectado a internet, es decir casi 33 millones de colombianos tiene al menos un dispositivo conectado a internet, lo que representa un enorme número de personas que desde el punto de vista de seguridad están expuestos a posibles ataques informáticos, es de opinión publica saber que las personas no tienen cultura para hacer uso de estos dispositivos (sean, Teléfonos inteligentes, Smart TV, portátiles, equipos de mesa, otros) la seguridad es el factor menos importante a la hora de hacer uso de un dispositivo, pero también debemos conocer cuáles son los factores para que la proliferación de dispositivos a internet sea aún mayor, conocemos algunos proyectos del gobierno que buscan alcanzar la mayor cantidad de colombianos para conectarlos a internet, como son gobierno el línea, Kiosko Vive Digital, proyecto 1000 zonas Wifi para regiones rurales, entre otros, pero conocemos el nivel de seguridad y los planes de convergencia que estos proyectos tienen para garantizar la privacidad de los usuarios?, cada día más usuarios adquieren más dispositivos para conectarse a internet, entre los que podemos encontrar, los “Wereables, Relojes inteligentes, manillas y anillos inteligentes, zapatos deportivos con posibilidad de conectarse a internet, entre otros” todos estos dispositivos tienen consigo un sistema embebido que permiten conectarse a otros dispositivos y a la red de redes, es ahí donde los hackers ven una gran oportunidad de hacerse con miles de datos de usuarios para sacar de alguna manera provecho a la situación, a su vez el mismo diario indica que es

preocupante la poca cantidad de recursos que se destinan a la protección de la información, es solo el 10% en el mejor de los casos, por otro lado los ataques informáticos incrementan entre un 50 y 60% con relación a años anteriores, el general Bautista ofrece cifras interesantes con respecto a la cantidad de denuncias por delitos informáticos, anualmente se formalizan alrededor de 7200 denuncias por este tipo de delito, cifra que aumenta cada año entre el 30 y 40%, de los cuales una cantidad de 4500 casos están relacionados con hurtos informáticos (robo de identidad, alteración y suplantación de datos personales, robo de cuentas de correo, robo de cuentas bancarias, entre otros), a su vez, cerca de 1200 casos se relacionan con accesos indebidos a infraestructuras tecnológicas de las empresas y acceso a equipos personales, con el fin de obtener información relevante, por otro lado cerca de 900 casos, se relacionan con suplantación de identidad, 300 casos con transferencia de activos y datos de accionistas, 200 casos se relacionan con phishing o suplantación de sitios web, la mayoría de estos ataques van dirigidos con fines económicos.

7.2 PERFIL ÉTICO Y PSICOLÓGICO DE LOS CIBERDELINCUENTES

Definir un perfil de un 'delincuente informático' es una manera muy amplia y generalizada, Kevin Mitnik, pionero de esta actividad lo define como 'Un hacker es una persona que utiliza y desarrolla su inteligencia para generar más conocimiento; y su arma más letal es su propia curiosidad'.

Según fuentes periodísticas, Colombia ha sido uno de los tres países con más denuncias por delitos informáticos[26], tomando el riesgo de que cada vez el número de denuncias vayan en aumento.

[26] https://www.semana.com/nacion/articulo/delitos-informaticos-han-aumentado-colombia-advierten-especialistas/267571-3

7.2.1 Ataques informáticos, Una mirada desde la Ética

Es muy interesante todo lo que comprende un estudio sobre los hackers que actúan por factores psicológicos, pues estos tienen un mayor detalle en cosas mínimas, es importante mencionar que la mayoría de hackers poseen un alto nivel de abstracción y retención, es por esto que pueden comprender y aprender técnicas avanzadas que muchas personas no puede hacer, pero cuando se trata de este tipo, los hackers con factores psicológicos tienen algo más que les permite incluso aplicar técnicas avanzadas con detalles muy mínimos que a su vez son el factor fundamental de su actividad.

De manera general el análisis en cuanto a delitos informáticos se torna más complejo cuando vemos qué tipos de delitos informáticos se ven a diario a nivel global, sin embargo, simplificando este tema podemos ver cuál es el caso en Colombia, el avance de la tecnología, los proyectos gubernamentales de los entes encargados, la aplicación de la tecnología en cada ámbito, tales como académico, desde las instituciones de educación de básica primaria, hasta instituciones de educación doctoral, en la salud, en lo laboral, en lo cotidiano, todo esto implica que la tecnología esté involucrada en cada aspecto de la vida de los individuos, es ahí donde personas suficientes conocimientos de estos pueda ver un panorama ideal para realizar o aplicar sus conocimientos con fines propios y personales, mayormente con el cumplimiento de sus objetivos sean académicos, pues conocemos casos de hackers que han tomado copias de manera ilegal a muchas bibliotecas de universidades a nivel mundial, objetivos políticos.

El perfil criminal de una persona, independiente de su naturalidad, es usualmente de característica multidisciplinar, un delincuente no se enfoca solo en una acción, este fija un objetivo, pero muchos factores interactúan entre sí para lograr componer todas las piezas que lo lleven a demandar un acto o acción, los perfiles

criminológicos se definen a lo largo de un ciclo emocional como una estimación que corresponde a una característica del individuo más allá de su composición histórica como ser y de su estilo de vida en una serie de hechos delictivos graves o leves y que aún no hayan sido identificados, estas características pueden provenir desde un contexto social, psicológico e incluso familiar.

El contexto psicológico de un ciberdelincuente se empieza a construir desde su niñez, estos primeros años son muy importantes para el desarrollo cognitivo y experimental de un hacker, empiezan a adquirir rasgos de personalidad que se desarrollan a medida que interactúan con su entorno, la comunicación tiende a ser menos espontánea y más analítica, los hackers tienden a escuchar y prestar más atención al detalle antes de dirigir una opinión.

Kevin mitnick uno de los hackers más importantes de la historia decía '*La información es publica, es de todos, y nadie tiene derecho a ocultarla*'[27], el cuándo fue detenido sostenía que no se consideraba un hacker, ya que un hacker era solo una persona curiosa que le gusta investigar.

El hacker es una persona apasionada por el conocimiento y aplicaciones, el termino hacker viene desde la década de los 60, no solamente se denomina hacker a una persona con altos niveles de conocimiento en el uso y adopción de sistemas informáticos, sino también a personas que dedican sus conocimientos a otras disciplinas, como por ejemplo un carpintero, un pintor, su esencia no radica en la capacidad de corromper un sistema, sino en como este aplica sus conocimientos y su pasión para descubrir nuevas rutas que lleven a un camino más ágil y eficiente para realizar una acción, los hackers no son personas que usan una herramienta o medio para sacar provecho de las vulnerabilidades que pueda tener, sino que utiliza sus conocimientos para mejorar el entorno que rodea un sistema, sin embargo, existen también personas que sacan provecho de sus conocimientos para beneficio

[27] Douglas Terán (2013); "El Perfil Criminal de los delincuentes Informáticos"; Diario de los Andes; Recuperado de: http://diariodelosandes.com/content/view/227662/105960/

propio, entre ellos los ‘crackers’, los hackers son usualmente asociados con personas superdotadas o genios, sin embargo su pasión y dedicación es lo que en la mayoría de ocasiones llevan a un hacker más allá de la media.

La motivación es lo que lo impulsa a ir más allá en sus actividades cotidianas, aprender constantemente, compartir el conocimiento y conectarse con otras personas entorno a un tema específico es satisfacción para los hackers, las comunidades de hackers son grandes y robustas, además comparten temas de interés donde cada uno realiza un aporte significativo que permite estar a la vanguardia y crecer el mar de conocimientos, es por ello que la motivación los ayuda a continuar, a seguir investigando y aprendiendo, estas personas pueden realizar una contribución a un sistema por largos periodos de tiempo sin tener como objetivo principal una remuneración económica de su actividad, para ellos es más importante compartir sus conocimientos y aportar a la comunidad que obtener mucho dinero por lo que hacen, una característica arraigada de los hackers es que son personas muy inteligentes y dedicadas, además muy curiosos y tienen la capacidad de analizar y entender situaciones abstractas.

Los ciberdelincuentes tienen como preferente el Sistema Operativo Linux, ya que este comparte una filosofía ideológica que se centra en el conocimiento como el poder humano más valioso, así como el gran filósofo Francis Bacon compartía en su obra *Meditaciones Sacrae* escrito en el año 1597 escribía lo siguiente ‘*ipsa scientia potestas est*’ lo cual significo las primeras apariciones de ‘*el conocimiento en su poder*’, Aristóteles también defendía esta teoría (384-322 a.C) en su obra *Ética de Nicomano* como el conocimiento sensible y el saber productivo.

Andrés Sepúlveda uno de los hackers más reconocidos en Colombia y además uno de los más polémicos, desde que se efectuó su captura en 2014, realizo acciones que podrían sospecharse si se hubiera hecho un seguimiento a su cuenta de Twitter con anterioridad, el lugar donde expresaba su ser, sus posiciones y pensamientos,

realizo diferentes trinos que dejo perplejo al país, entre sus trinos más polémicos están,

- '*Matar es un arte que no admite sutilezas*'
- '*Solo guiño mi ojo izquierdo para apuntar mejor*'
- '*Hoy comeremos en el infierno*'
- '*Me gusta el olor a muerte*'
- '*Nelson, Mandela un peligroso comunista menos*'
- '*Pero recuerden, los quiero matar a todos*'
- '*Grande Uribe!*'
-

Sepúlveda describía su perfil biográfico en Twitter como un hacker 'ético' y aliado del ciberterrorismo y la guerra cibernética[28], y seguidor de la derecha en Colombia, quien en ese año fue señalado de cometer 4 delitos, entre ellos, (violación ilícita de comunicaciones, uso de software malicioso, interceptaciones ilegales y espionaje).

En sus trinos se puede analizar que Sepúlveda era una persona impulsiva, con intenciones personales y de un temperamento fuerte y radical, sin embargo, según el médico psiquiatra, Álvaro Romero, director del Departamento de Medicina de la Universidad de la Sabana, "es muy difícil definir a una persona por los tweets que manda, sin embargo, es posible decir que de acuerdo con lo escrito y la frecuencia con que lo hacía, Andrés Sepúlveda es probablemente una persona impulsiva que puede tender a la agresividad e imposición".

[28] Es un radical de derecha y seguidor del expresidente Álvaro Uribe varios de los trinos eran retweeteados por Sepúlveda en muestra de aprobación y apoyo. http://www.vanguardia.com/actualidad/colombia/258878-quien-es-el-hacker-andres-sepulveda

7.3 SISTEMA DE DEFENSA QUE EL GOBIERNO TIENE COMO CONTINGENCIA EN CASO DE RECIBIR ATAQUES DE TIPO INFORMÁTICO

El gobierno nacional a través de la CONPES (Consejo nacional de política económica y social), une sus esfuerzos con entidades como coICERT (Grupo de respuestas a emergencias en Colombia) el cual coordina aspectos como ciberseguridad y ciberdefensa, también hace parte de este grupo de defensa el Comando Conjunto Cibernético CCOC de las fuerzas militares proporciona estrategias que permiten prevenir o contrarrestar amenazas que afecten los intereses nacionales, al igual que el CCP Centro Cibernético Policial el cual ofrece información, apoyo y protección ante delitos cibernéticos, este implemento a su vez un CAIV (Comando de Atención Inmediata Virtual) el cual recibe reportes de delitos informáticos, por lo tanto las entidades responsables de la seguridad ante delitos informáticos son, CONPES (Consejo Nacional de Política Económica y Social), coICERT (Grupo de respuestas a emergencias en Colombia), CCOC (Comando Conjunto Cibernético), CCP (Centro Cibernético Policial), CAIV (Comando de Atención Inmediata Virtual).

Según la Policita Nacional de Colombia en el año 2015 la mayor cantidad de delitos informáticos registrados corresponden a las siguientes categorías:

- Claves programáticas espías, son softwares maliciosos diseñados especialmente para espiar la actividad de los usuarios, entre estos esta, troyanos, spyware, adware.
- Estafas en línea, se presentan mediante la oferta de productos a través de internet, generalmente a un costo más bajo que lo normal, este tipo de transacciones no tienen un control regulado por entidades reconocidas, es uno de los delitos más comunes.
- Spam, los correos no deseados son cada vez más comunes.
- Pornografía infantil, Se divulgan a través de foros, páginas pornográficas, comunidades virtuales, entre otras modalidades.

- Software pirata, ofrecen software legitimo con licencia de tipo propietario con una herramienta que permite legalizar dicho software, las herramientas para activar el software son diseñadas por usuarios con altos conocimientos en programación y usualmente infectan la máquina del usuario.

El Gobierno a través del proyecto de acuerdo 271 de 2014 mediante el Consejo de Bogotá, menciona los siguientes acuerdos

Acuerdo 037 de 2013, 'Por medio del cual se establece la Estrategia de Ciberseguridad para enfrentar ciberdelitos y amenazas contra el Distrito Capital'.
Este proyecto de acuerdo se establece a través de una estrategia de ciberseguridad en la capital, como una forma de enfrentar las amenazas cada vez más frecuentes ante entidades gubernamentales, ya que a la fecha se habían reportado ataques a las bases de datos, infraestructura y a los equipos de cómputo de la institución[29], entre los casos mencionados están.

- Ataque masivo de hackers contra la registraduría,

Conforme lo cita la fuente de El Universal, (2012)[30] "Pese a que un informe del Cuerpo Técnico de Investigación de la Fiscalía (CTI), elaborado en mayo de 2010, determinó que hubo un ataque masivo de hackers al programa informático de la Registraduría Nacional durante las elecciones parlamentarias del 2010, que a la postre hizo colapsar al sistema de datos; la Fiscalía decidió archivar la investigación por considerar que las pruebas no eran suficientes."

Por otro lado el Observatorio Nacional de Seguridad participa en un proyecto para

[29] Algunas entidades del Estado, como del Distrito Capital, han padecido ataques a sus bases de datos, información, infraestructura y equipos de sistemas y cómputo (informáticos), http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=59602

[30] Caso de la registraduría cera cerrado, El universal, http://www.eluniversal.com.co/cartagena/politica/caso-de-ataques-de-hackers-la-registraduria-sera-cerrado-65633

realizar el estudio de viabilidad el cual tiene como objetivo el impulso y apoyo al fortalecimiento de la seguridad digital con el apoyo de Colciencias a través de convocatorias realizadas por el Ministerio de Tecnologías y Telecomunicaciones MinTIC, con esto el gobierno busca generar un impacto positivo en cuanto a la disminución de los delitos, con el fin de proteger las PyMES, entidades financieras, las infraestructuras críticas, y la defensa nacional, también la protección ante delitos como.

- Ciudadanía digital
- Población menor de edad
- Cyberbullying
- Ciberespionaje a empresas
- Transacciones electrónicas

La OEA (Organización de Estados Americanos) en su documento de la Misión Técnica (Conclusiones y recomendaciones, 2014), "Desafío 1": "Los esfuerzos de Colombia para abordar la ciberseguridad están limitados por la falta de una visión general clara."; adicionalmente establece la recomendación de "desarrollar una visión global para la ciberseguridad"[31].

Este proyecto de gobierno busca analizar las alternativas existentes en cuanto a materia de seguridad digital, mediante el estudio de las amenazas cibernéticas en Colombia, contextualizadas por grupos de interés, y prestar recomendaciones prácticas, prospectiva tecnológica, sensibilización y capacitación en medidas de prevención y corrección, este proyecto propone analizar la oportunidad y la viabilidad, técnico, económica y legal, de la puesta en marcha de una unidad especializada que actúe como foro de colaboración público y privada entre los

[31]En el documento elaborado como resultado de la Misión Técnica de la OEA (Conclusiones y recomendaciones, 4 de abril de 2014, Bogotá, Colombia, OEA) https://www.islsa.com/index.php/empresa/47-observatorio-nacional-de-ciberseguridad-de-colombia

actores involucrados y permita el avance y fortalecimiento de la Ciberseguridad durante los próximos años en Colombia.

Figura 7 Posición de Colombia con respecto a Latinoamérica

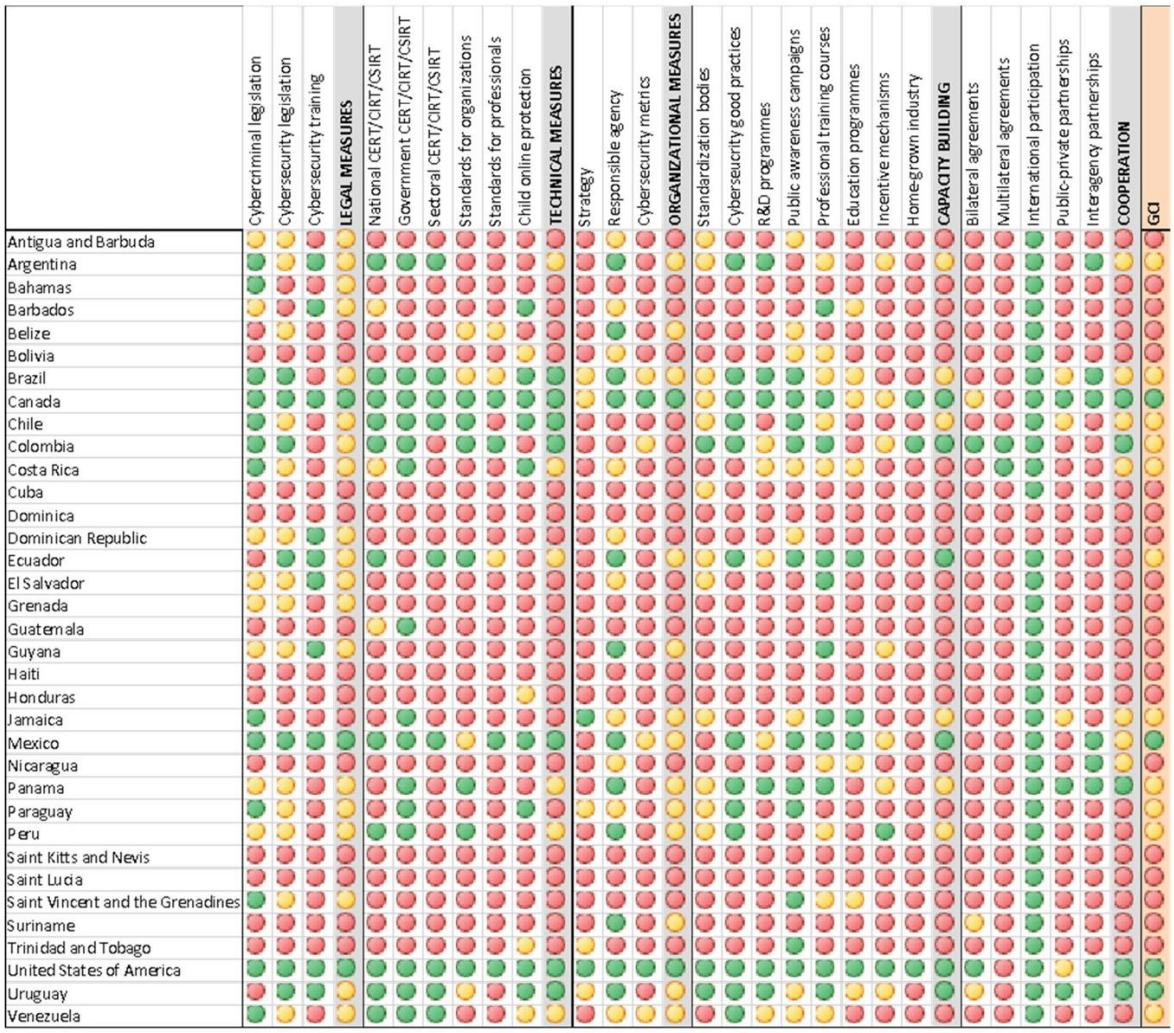
AMERICAS Region		
Country	**Score**	**Global Rank**
United States of America	0.919	2
Canada	0.818	9
Mexico	0.660	28
Uruguay	0.647	29
Brazil	0.593	38
Colombia	0.569	46
Panama	0.485	61
Argentina	0.482	62
Ecuador	0.466	65
Peru	0.374	78
Venezuela	0.372	79

Fuente: Americaeconomia tecno, https://tecno.americaeconomia.com/articulos/que-paises-lideran-la-lucha-contra-el-cibercrimen-en-latinoamerica

Según el portal Americaeconomia en el año 2017 la ITU por sus siglas en inglés (Unión Internacional de Telecomunicaciones) público un estudio el cual mide el compromiso de los países que son miembros de la ITU, en donde Colombia ocupa el puesto 6 a nivel Latinoamérica[32], este estudio busca medir el desempeño en seguridad cibernética en cuanto a indicadores legales, técnicos, organizacionales y la cooperación, por medio de indicadores que evalúan diferentes ítems a través de los colores verde, amarillo y rojo, el cual verde significa que cumple con la totalidad, amarillo cumple parcialmente y rojo no cumple.

[32] Colombia ocupa el puesto 6 a nivel Latinoamérica en cuanto a seguridad de la información, 9 agosto de 2017, https://tecno.americaeconomia.com/articulos/que-paises-lideran-la-lucha-contra-el-cibercrimen-en-latinoamerica

Figura 7 Región de las Américas



Fuente: Global Cybersecurity Index (GCI), 2017

En el grafico se observa que Colombia incumple parcialmente en 5 ítems los cuales son,

- Medidores legales
- Métricas de ciberseguridad
- Programas R&D
- Mecanismos de incentivos
- GCI

Del total de 31 ítems evaluados Colombia tiene 17 en color verde, 5 en amarillo y 9 en rojo.

- **Aspectos Técnico** Colombia cuenta con 4 ítems en verde y 2 en rojo, por lo tanto, pasa el examen en este aspecto, debido a que cuenta con un equipo de respuesta para emergencias cibernéticas del Ministerio de Defensa (ColCERT) y (CSIRT), también se suman a ellas DigiCSIRT, SOC (Comando de operaciones Cibernéticas, y (CCIT), Cámara Colombiana de Informática y Telecomunicaciones.
- **aspectos organizacionales**, Colombia es deficiente en estos aspectos, ya que tiene 3 ítems en rojo y solo uno en amarillo, solo siendo aprobado en cuanto a las métricas de seguridad.
- **Capacidad de crear,** Es uno de los aspectos más sobresalientes de Colombia ya que cuenta con 6 ítems en verde, 2 en amarillo y 1 en rojo, las buenas prácticas en seguridad han aportado un valor agregado a las políticas de seguridad Nacional, a ello se suma las campañas para la concientización de la seguridad digital, el programa de Investigación y Desarrollo aporta un importante valor en cuanto a políticas públicas y buenas prácticas.
- **Cooperación internacional,** En este aspecto Colombia está en la mediana ya que presenta 3 ítems en verde y 2 en rojo, en cuanto a la valoración positiva están los acuerdos laterales y bilaterales, y en cuanto a los aspectos negativos esta la interacción entre entidades privadas y públicas.

A nivel nacional Colombia ocupa el puesto 46 con un color amarillo, este ranking lo lideran Estados Unidos, Canadá y México.

En Colombia existen unos nodos que se encargan de crear buenas prácticas en cuanto a aspectos de seguridad, el nodo de seguridad se ajusta al documento CONPES 3701 con el fin de minimizar el nivel del riesgo al que la información está expuesta para, fortalecer la posición estratégica en el ciberespacio y asegurar la infraestructura del estado y la protección de los servicios que provee a los

ciudadanos, así como también enfrentar de formar adecuada los riesgos en ciberseguridad

Figura 8 Nodo de seguridad del CONPES

Fuente: Ministerio de Tecnologías y Telecomunicaciones

7.4 FALENCIAS DE LA LEY 1273 DE 2009

La ley 1273 de 2009 es la única ley en Colombia que abarca en gran medida las faltas contra la propiedad intelectual, el abuso de sistemas informáticos, daños y corrupción de la información, acceso no autorizados a sistemas informáticos, uso

de software malicioso, violación de datos personales, suplantación de identidad y sitios web, entre otros, presentados a través del artículo 269A al 269G dentro de la constitución, sin embargo, la información al igual que la tecnología se ha transformado en múltiples aspectos, cada día se conocen nuevas maneras de transmitir datos, al igual que nuevas maneras de vulnerar los mismos, por lo tanto, aunque existe una ley que regula y penaliza todo acto que atente a la integridad, y confidencialidad tanto de la información como del individuo, esta tiene una serie de falencias que deben ser consideradas.

en la cual se enfoca en el ciberespacio, esta es la Ley 1273 la cual se conoce así "mediante la cual la se modifica el Código Penal, se crea un nuevo derecho legal, denominado '*protección de la información'*. y los datos y sistemas que usan información y comunicaciones sobre tecnologías son totalmente conservado, entre otras disposiciones[33]" exige una pena de prisión o multas grandes para cualquier persona condenada por información sobre sistemas o telecomunicaciones sobre delitos en la red. La ley cubre áreas como el acceso ilegal a información personal, la intercepción de datos, la destrucción de datos o el uso de software malicioso.

[33] http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Sin embargo, Colombia presenta diferentes falencias con respecto a otros países entre las que deben ser revisadas

Por medio del siguiente cuadro se hace un análisis de las fortalezas y debilidades de la ley 1273 de 2009.

Tabla 1 Fortalezas y debilidades de la ley 1273 de 2009

Ley 1273 de 2009	Fortalezas	Debilidades
Artículo 269A ***ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.*** Acceso no autorizado a un sistema informático, sanción de hasta 96 meses de prisión y 1000 SMMLV	Es una de las sanciones más drásticas en la región.	Otorga la posibilidad a un usuario de conseguir un permiso legal para acceder de manera autorizada a un sistema informático.
Articulo 269B ***OBSTACULIZACIÓN ILEGITIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.*** Quien sin estar facultado impida el uso adecuado de un sistema de información. Sanción de hasta 96 meses de prisión y 1000 SMMLV	Este articulo permite sancionar a una persona quien con intereses propios altere y no permita el acceso adecuado de un sistema informático	No ofrece una descripción clara y precisa sobre la actividad la cual será penalizada.
Artículo 269C. ***INTERCEPTACIÓN DE DATOS INFORMÁTICOS*** Quien sin estar autorizado realice interceptación de datos para para beneficio propio. Sanción de hasta 72 meses de prisión	Este articulo brinda protección a la información de los usuarios, permitiendo tener garantías en la protección de datos sensibles.	No penaliza delitos por manipulación de datos con fines de extorsión o interceptación de datos.

Ley 1273 de 2009	Fortalezas	Debilidades
Artículo 269D*.* ***DAÑO INFORMÁTICO.*** Quien sin estar facultado para ello destruya, modifique, borre o altere un sistema informático diferente de su propiedad. Sanción de hasta 96 meses de prisión y 1000 SMMLV.	Penaliza y sanciona a las personas que realicen acciones malintencionadas a otro sistema informático.	No sanciona de manera explícita a las personas que obtengan o extraigan o destruyan pruebas que puedan incurrir a una penalización.
Artículo 269E. ***USO DE SOFTWARE MALICIOSO.*** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos. Sanción de hasta 96 meses de prisión y una multa de hasta 1000 SMMLV.	Este articulo penaliza a quienes realicen la instalación de virus o programas que puedan afectar un sistema para beneficios propios.	No especifica de manera detallada que tipo de software malicioso son penalizados, por lo tanto, una persona puede no caer en un delito si utiliza un software que no es categorizado como malicioso, pero realice tales afines.
Articulo 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 p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes. Sanción de hasta 96 meses de prisión y hasta 1000 SMMLV.	Colombia es uno de los primeros países en decretar este articulo y de esta manera protege los datos de los afectados.	El articulo esta detallado por lo tanto no ofrece debilidades a destacar.

Ley 1273 de 2009	Fortalezas	Debilidades
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. Sanción de hasta 96 meses de prisión y hasta 1000 SMMLV de multa.	Brinda protección al ciudadano que haya sido víctima de este tipo de delito.	No detalla de manera específica que tipo de suplantación es penalizada, es importante reconocer que hay diferentes tipos de suplantación entre ellos, vía telefónica, mensaje de texto, entre otros.

Fuente: Autor.

8 CONCLUSIONES

La evolución de la tecnología implica un avance a la humanidad en diferentes sentidos, la tecnología avanza de tal manera que es importante estar a la vanguardia de cada cambio los teléfonos celulares o “Smartphone” rápidamente se convirtieron en una parte fundamental de nuestra vida cotidiana, estos dispositivos están diseñados para hacer casi cualquier función de las actividades diarias, se ha convertido en un aliado perfecto para la productividad en cuestiones laborales y también para el entretenimiento, sin embargo, la tecnología significa un potencial peligro para los usuarios, es necesario estar conscientes de los riesgos que rodean la tecnología, especialmente su vía más rápida y global, el internet.

El primer objetivo hace referencia a un estudio el cual analiza y documenta los ataques informáticos más importantes teniendo como objetivo el gobierno Nacional en los últimos 5 años, en este documento se presenta el estudio de varios ataques informáticos dirigidos a diferentes entidades del gobierno, uno de los casos más conocidos fue el del hacker Andrés Sepúlveda, este caso estremeció al país en época de elecciones presidenciales del 2014.

Posteriormente se hace un estudio del alcance de estos ataques, durante el año 2014, el país fue cómplice de un acto de corrupción perpetuado a través de un equipo de cómputo, se buscó obtener ventaja de las habilidades de un hacker para denigrar la reputación e imagen de los candidatos opositores a la presidencia del mismo año.

Así mismo, conocer las leyes que están ideadas para minimizar el riesgo en Internet y concientizar a las personas de los peligros que hay en internet es una estrategia que el gobierno, en cooperación con el MinTIC han llevado a cabo a través de diferentes programas de prevención y ciberseguridad, esto representa cada vez

más un avance en la concientización con respecto a la inseguridad en la Web, es por ello que el gobierno construyo la Ley 1273 del 2009 para controlar y minimizar el impacto de los ciberataques y el número de ataques informáticos.

En los últimos 5 años, Colombia ha tenido un incremento exponencial de los delitos informáticos debido a la expansión de las nuevas tecnologías, la dependencia cada vez mayor del internet y la aceleración digital ha hecho que existan mayor exposición a los riesgos existentes en el ciberespacio.

Así también se concluye que el gobierno colombiano no ha dado la importancia necesaria al ciberespacio a pesar del alto número de delitos informáticos que se presentan a diario, sin embargo, a través de la Ley 1273 de 2009 se busca adaptar a la implementación de avances tecnológicos.

Actualmente, en algunos artículos que corresponden a la Ley 1273 de 2009 no cuentan con suficiente claridad en su descripción lo cual ha permitido que algunos delitos cometidos no hayan sido penalizados debidamente.

La falta de sensibilización y concientización a los funcionarios del gobierno ha permitido que los ciberdelincuentes encuentren una brecha de seguridad que vulnere sus sistemas de información.

No obstante, en busca de estar a la vanguardia ante la respuesta a incidentes cibernéticos, Colombia ha buscado fortalecer sus mecanismos de ciberdefensa para contrarrestar este tipo de crímenes.

9 RECOMENDACIONES

El uso de la tecnología se globalizo rápidamente con el pasar de los años, su gran alcance y compenetración con las actividades en todos los entornos de la actividad humana hace que sea el avance revolucionario más importante de las ultimas 5 décadas, con el avance tecnológico también surgen elementos que vienen consigo, entre ellos, la actividad ilícita que busca favorecerse mediante el uso de las tecnologías, en Colombia el uso de la tecnología tiene un alcance cada vez mayor, al día de hoy el uso de un dispositivo electrónico hace parte de 8 de cada 10 colombianos[34] tiene acceso directa o indirectamente de un equipo de cómputo o dispositivo electrónico, al igual que las instituciones gubernamentales confían todos sus procesos y procedimientos y su información en un dispositivo electrónico como parte del control el cual permite agilizar y mantener la información disponible en todo momento, es por ello que se realizan las siguientes recomendaciones.

- Con la dependencia cada vez más arraigada de la tecnología en todos los aspectos, es importante que las entidades gubernamentales fortalezcan la protección de la información tanto a nivel público como a nivel privado, el gobierno debe realizar un replanteamiento en las leyes que al día de hoy regulan el uso de la tecnología y del internet, por lo tanto, replantear leyes y decretos que tengan mayor rigurosidad en el momento de penalizar los delitos informáticos.
- Es importante que el gobierno y las instituciones inviertan esfuerzos y capital al fortalecimiento de las estrategias que permitan brindar a todos los internautas herramientas y bases para proteger la información más sensible,

[34] Colombia avanza en uso de tecnologías de la información, MinTIC, (2012) [En línea], https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/MinTIC-en-los-Medios/2731:Colombia-avanza-en-uso-de-tecnologias-de-la-informacion

así como hacer una concientización sobre los riesgos y peligros que hay en el uso del internet.

- Realizar talleres que permitan a los ciudadanos aprender a manejar las herramientas básicas como son, los navegadores web, el uso de la ofimática, el correo electrónico, entre otros, a su vez que conozcan los posibles peligros a los que se enfrentan al usarlas.
- Crear conciencia en el uso del internet, la mayor cantidad de delitos informáticos se hacen por medio de la propagación de software malintencionado a través de internet, una vez el gobierno realice inversiones que lleven a las instituciones a crear talleres y cursos para mejorar la seguridad en internet, los delitos informáticos se verán disminuidos de cierta forma.
- Fortalecer las leyes actuales con normativas que penalicen de manera más contundente a las personas que incurran a delitos informáticos a través del uso de las tecnologías y el internet.
- Hacer uso de software libre como uso alternativo al software propietario a lo largo de las instituciones del gobierno nacional, así como realizar campañas nacionales para promover el uso de este como alternativa para los colombianos y de esta manera no incurrir en delitos que correspondan al artículo 269E de la ley 1273 de 2009, la comunidad de software libre ofrece software en diferentes categorías como, software de ofimática, editores de texto, imagines y videos, navegadores web, entre muchos más.
- La ley que rige los delitos a través de sistemas informáticos en Colombia es la ley 1273 de 2009, esta ley aunque se sigue fortaleciendo aun cuenta con diferentes falencias las cuales deben ser fortalecidas para hacer ejercer el uso responsable de los sistemas de información, es así como el articulo 269C, Interceptación de datos informáticos, penaliza a las personas que incurran en este delito sin una orden judicial que les permita realizar este tipo de acciones, es por ellos que se sanciona con una pena de prisión de entre 36 a 72 meses los cuales representan de 3 a 5 años de cárcel, siendo una

pena alta, aun se puede pensar que una persona que este judicializada por este delito, puede pagar pena de prisión domiciliaria después de pocos meses de ingresar a la cárcel.

- El articulo 269E de la ley 1273 2009 sanciona que la persona que incurra en un delito al alterar, modificar, adquirir, vender y reproducir software con fines maliciosos debe pagar una pena de entre 48 y 96 meses de prisión, además de pagar una multa económica de hasta 1000 SMMLV, es una pena considerable para realizar este tipo de delito, sin embargo, en Colombia la actividad ilegal por medio de la piratería de software es muy alta, según una investigación del diario El Tiempo, indica que el 48% del software que se usa en Colombia es ilegal[35], siendo Colombia uno de los países con mayor índice en la región que hace uso de software pirata seguido de Venezuela con 89% de índice de ilegalidad siendo este el país que más usa software ilegal, por otro lado los países con menor índice de piratería son, Brasil con 46%, México 49% y Chile 55%, es por ello que el gobierno nacional debe poner la mira en el uso de software ilegal ya que no hay un control estricto que regule esta problemática.

[35] El 48 % del software instalado en Colombia es pirata, El Tiempo, [En línea], https://www.eltiempo.com/tecnosfera/novedades-tecnologia/estudio-revela-que-el-48-por-ciento-del-software-instalado-en-colombia-es-ilegal-228156

REFERENCIAS BIBLIOGRÁFICAS

DIAZ GARCIA, Alexander. “Proyecto de Ley de Delitos Informáticos” [En Línea]. 2008. Disponible en http://nuevastecnologiasyprotecciondedatos.blogspot.com/2008/06/proyecto-de-ley-delitos-informticos_17.html

Régimen legal de Bogotá D.C, Alcaldía mayor de Bogotá, [2014]. En Línea, disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=59602

Los sectores económicos más impactados por el cibercrimen en Colombia [En Línea]. Revista Dinero. 2017. Disponible en https://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321

Breve historia de Internet, [En Línea]. *Origines de Internet,* Disponible en, https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/#f3

Ciberseguridad entorno colombiano [En Línea]. Policía Nacional. 2014. Disponible en https://www.oas.org/juridico/spanish/cyber/cyb8_col.pdf

Colombia cuenta con una Política Nacional de Seguridad Digital [En Línea]. Ministerio de Tecnologías MinTIC, 2016. Disponible en http://www.mintic.gov.co/portal/604/w3-article-15033.html

Conoce el perfil social de un hacker, [En Línea]. disponible en, http://segured.com/conoce-el-perfil-social-de-un-hacker/

La historia de cinco hackers colombianos y sus delitos, [En Línea]. 2016, Disponible en, http://www.eltiempo.com/justicia/cortes/delitos-de-hackers-en-colombia-52232

Código de ética y práctica profesional, [En Línea]. 2015, disponible en, http://www.acm.org/about/se-code-s

Ética profesional, Polo M, [En Línea]. disponible en, http://sisbib.unmsm.edu.pe/bibvirtualdata/publicaciones/administracion/n12_2003/a08.pdf

CARDENAS CRIOLLO, Jennifer y RAMIREZ CASTILLO, Pavel, Criminalística computacional: modelo para la estructuración de evidencias [En Línea]. 2017. Universidad Libre. Disponible en http://repository.unilibre.edu.co/bitstream/handle/10901/10812/Proyecto%20Final%20CRIMINALÍSTICA%20COMPUTACIONAL%20MODELO%20PARA%20LA%20ESTRUCTURACIÓN%20DE%20EVIDENCIAS.pdf?sequence=1&isAllowed=y

¿Quién es el hacker Andrés Sepúlveda? [En línea]. 2014. Disponible en, http://www.vanguardia.com/actualidad/colombia/258878-quien-es-el-hacker-andres-sepulveda

Lineamientos de política para ciberseguridad y ciberdefensa [En Línea]. 2011. Consejo Nacional de Política Económica y Social. Disponible en http://enticconfio.gov.co/images/stories/normatividad/Conpes_3701.pdf

Definición de Delito Informático. [En Línea]. División ComputerForensic. 2012. Disponible en http://delitosinformaticos.info/delitos_informaticos/definicion.html.

GUTIÉRREZ ARRIESTA, Javier. 2013. Educación. Medidas para aumentar la seguridad informática en su centro de trabajo. [En línea]. 2013. Disponible en https://es.slideshare.net/mariorafaelquirozmartinez/medidas-para-aumentar-la-%20seguridad-informatica-en-su-centro-de-trabajo

FRANCO, David y PEREA, Jorge. Herramientas para la Detección de Vulnerabilidades basada en la identificación de servicios. [En línea]. 2016. Disponible en http://www.scielo.cl/scielo.php?pid=S0718-07642013000500003&script=sci_arttext

ESCRIVÁ, G., Romero, Seguridad Informática. Madrid, ES: Macmillan Iberia, S.A... [En línea] 19 de 02 de 2017. [Citado el: 03 de 05 de 2017.] Disponible en http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10820963&p00=seguridad+inform%C3%A1tica.

Observatorio Nacional de Ciberseguridad de Colombia https://www.islsa.com/index.php/empresa/47-observatorio-nacional-de-ciberseguridad-de-colombia

SO / IEC 27000: 2009 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Información general y vocabulario. Recuperado de https://www.iso.org/standard/41933.html.

CASABONA, CARLOS MARÍA ROMEO. 2006. Los datos de carácter personal como bienes jurídicos penalmente protegidos. El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales. ESPAÑA: Granada: Comares.

DECRETO 2573 DE. 2014. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones. [En línea] 12 de dic. De 2014. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60596

LOZANO QUINTERO, Leidy. Casos de Ciberataques en Colombia [En Línea]. Universidad Militar Nueva Granada. 2015. disponible en, http://repository.unimilitar.edu.co/bitstream/10654/7161/1/Ensayo%20para%20optar%20al%20titulo%20de%20Internacionalista%20y%20Politóloga.%20Lady%20Carolina%20Lozano%20Quintero%20.pdf

FERNANDEZ, Fernando. El peligro del voto electrónico, [En línea]. 2013. Registraduría Nacional. Disponible en https://www.registraduria.gov.co/El-peligro-del-voto-electronico.html

ANEXOS

Anexo A LEY 527 DE 1999 (agosto 21 de 1999)

"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones." [36]

Artículo 9o. INTEGRIDAD DE UN MENSAJE DE DATOS.

Para efectos del artículo anterior, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

Artículo 11. CRITERIO PARA VALORAR PROBATORIAMENTE UN MENSAJE DE DATOS.

Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente, habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

Artículo 12. CONSERVACION DE LOS MENSAJES DE DATOS Y DOCUMENTOS.

[36] Ley 527 de 1999. (1999), En Línea, http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones:

1. Que la información que contengan sea accesible para su posterior consulta.
2. Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y
3. Que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.

No estará sujeta a la obligación de conservación, la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos.

Los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta.

Artículo 28. ATRIBUTOS JURIDICOS DE UNA FIRMA DIGITAL.

Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

PARAGRAFO. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:

1. Es única a la persona que la usa.
2. Es susceptible de ser verificada.

3. Está bajo el control exclusivo de la persona que la usa.

4. Está ligada a la información o mensaje, de tal manera que, si éstos son cambiados, la firma digital es invalidada.

5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

Anexo B LEY 1341 de 2099 (julio 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 –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones."[37]

Artículo 4o. INTERVENCIÓN DEL ESTADO EN EL SECTOR DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.

En desarrollo de los principios de intervención contenidos en la Constitución Política, el Estado intervendrá en el sector las Tecnologías de la Información y las Comunicaciones para lograr los siguientes fines:

1. Proteger los derechos de los usuarios, incluyendo a los niños, niñas y adolescentes, y a la familia velando por la calidad, eficiencia y adecuada provisión de los servicios, y la promoción de la digitalización de los trámites asociados a esta provisión.

…

[37] Ley 1341 de 2009. (2009), En Linea, http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

7. Garantizar el uso adecuado y eficiente del espectro radioeléctrico, que maximice el bienestar social generado por el recurso escaso, así como la reorganización de este, respetando el principio de protección a la inversión, asociada al uso del espectro. Los proveedores de redes y servicios de telecomunicaciones responderán jurídica y económicamente por los daños causados a las infraestructuras.

…

9. Garantizar la interconexión y la interoperabilidad de las redes de telecomunicaciones, así como el acceso a los elementos de las redes e instalaciones esenciales de telecomunicaciones necesarios para promover la provisión y comercialización de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones.

Artículo 11. ACCESO AL USO DEL ESPECTRO RADIOELÉCTRICO.

El uso del espectro radioeléctrico requiere permiso previo, expreso y otorgado por el Ministerio de Tecnologías de la Información y las Comunicaciones.

El permiso de uso del espectro respetará la neutralidad en la tecnología siempre y cuando esté coordinado con las políticas del Ministerio de Tecnologías de la Información y las Comunicaciones, no generen interferencias sobre otros servicios, sean compatibles con las tendencias internacionales del mercado, no afecten la seguridad nacional, y contribuyan al desarrollo sostenible. El Ministerio de Tecnologías de la Información y las Comunicaciones adelantará mecanismos de selección objetiva, que fomenten la inversión en infraestructura y maximicen el bienestar social, previa convocatoria pública, para el otorgamiento del permiso para el uso del espectro radioeléctrico y exigirá las garantías correspondientes. En aquellos casos, en que prime la continuidad del servicio, el Ministerio de Tecnologías de la Información y las Comunicaciones podrá otorgar los permisos de uso del espectro de manera directa, únicamente por el término estrictamente necesario para asignar los permisos de uso del espectro radioeléctrico mediante un proceso de selección objetiva.

En la asignación de las frecuencias necesarias para la defensa y seguridad nacional, el Ministerio de Tecnologías de la Información y las Comunicaciones tendrá en cuenta las necesidades de los organismos de seguridad del Estado. El trámite, resultado e información relativa a la asignación de este tipo de frecuencias tiene carácter reservado. El Gobierno nacional podrá establecer bandas de frecuencias de uso libre de acuerdo con las recomendaciones de la UIT. Así mismo, podrá establecer bandas exentas del pago de contraprestaciones para programas sociales del Estado que permitan la ampliación de cobertura en zonas rurales.

Anexo A LEY 1273 DE 2009 (ENERO 5 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 que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

El CONGRESO DE COLOMBIA DECRETA:

Artículo 1. Adicionase el **Código Penal** con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor.

CAPITULO PRIMERO

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269B. OBSTACULIZACIÓN ILEGITIMA 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, a los

datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 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, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

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, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269E. USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envié, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

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, envié, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 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 envié páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a

noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. la pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 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 la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para si o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO SEGUNDO

De los atentados informáticos y otras infracciones

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, incurrirá en las penas señaladas en el artículo 240 de este Código.

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, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Artículo 2. Adiciónese al artículo **58** del **Código Penal** con un numeral 17, así: ***Articulo 58 CIRCUNSTANCIAS DE MAYOR PUNIBILIDAD.*** Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera:

(...)

17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos ó telemáticos.

Artículo 3. Adiciónese al artículo 37 del ***Código de Procedimiento Penal*** con un numeral 6, así:

Artículo 37. DE LOS JUECES MUNICIPALES. los jueces penales municipales conocen:

(...)

6. De los delitos contenidos en el titulo VII Bis.

Artículo 4. La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias, en especial el texto del artículo 195 del Código Penal.

Anexo B Formato RAE

Título: Estudio sobre casos de cibercrimen en entidades gubernamentales de Colombia en los últimos 5 años.
Autor: TIGREROS MOJICA, Steven
Fecha de Realización: 21/10/2019
Palabras Claves: Cibercrimen, intrusión, investigación, hacking ético, contraseña, ciberseguridad, seguridad informática, delito informático, gobierno de Colombia.
Descripción: Trabajo de grado para optar por el título de Especialista en Seguridad informática.
Fuentes: DIAZ GARCIA, Alexander. “Proyecto de Ley de Delitos Informáticos” [En Línea]. 2008. Disponible en http://nuevastecnologiasyprotecciondedatos.blogspot.com/2008/06/proyecto-de-ley-delitos-informticos_17.html Régimen legal de Bogotá D.C, Alcaldía mayor de Bogotá, [2014]. En Línea, disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=59602 Los sectores económicos más impactados por el cibercrimen en Colombia [En Línea]. Revista Dinero. 2017. Disponible en https://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321 Breve historia de Internet, [En Línea]. *Origines de Internet,* Disponible en, https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/#f3 Ciberseguridad entorno colombiano [En Línea]. Policía Nacional. 2014. Disponible en https://www.oas.org/juridico/spanish/cyber/cyb8_col.pdf

Colombia cuenta con una Política Nacional de Seguridad Digital [En Línea]. Ministerio de Tecnologías MinTIC, 2016. Disponible en http://www.mintic.gov.co/portal/604/w3-article-15033.html

Conoce el perfil social de un hacker, [En Línea]. disponible en, http://segured.com/conoce-el-perfil-social-de-un-hacker/

La historia de cinco hackers colombianos y sus delitos, [En Línea]. 2016, Disponible en, http://www.eltiempo.com/justicia/cortes/delitos-de-hackers-en-colombia-52232

Cuidado con el voto electrónico, Carolina botero, 2018, [En Línea], disponible en, https://www.elespectador.com/opinion/cuidado-con-el-voto-electronico-columna-793175

Código de ética y práctica profesional, [En Línea]. 2015, disponible en, http://www.acm.org/about/se-code-s

Ética profesional, Polo M, [En Línea]. disponible en, http://sisbib.unmsm.edu.pe/bibvirtualdata/publicaciones/administracion/n12_2003/a08.pdf

CARDENAS CRIOLLO, Jennifer y RAMIREZ CASTILLO, Pavel, Criminalística computacional: modelo para la estructuración de evidencias [En Línea]. 2017. Universidad Libre. Disponible en http://repository.unilibre.edu.co/bitstream/handle/10901/10812/Proyecto%20Final%20CRIMINALÍSTICA%20COMPUTACIONAL%20MODELO%20PARA%20LA%20ESTRUCTURACIÓN%20DE%20EVIDENCIAS.pdf?sequence=1&isAllowed=y

¿Quién es el hacker Andrés Sepúlveda? [En línea]. 2014. Disponible en, http://www.vanguardia.com/actualidad/colombia/258878-quien-es-el-hacker-andres-sepulveda

Lineamientos de política para ciberseguridad y ciberdefensa [En Línea]. 2011. Consejo Nacional de Política Económica y Social. Disponible en http://enticconfio.gov.co/images/stories/normatividad/Conpes_3701.pdf

Definición de Delito Informático. [En Línea]. División ComputerForensic. 2012. Disponible en http://delitosinformaticos.info/delitos_informaticos/definicion.html.

GUTIÉRREZ ARRIESTA, Javier. 2013. Educación. Medidas para aumentar la seguridad informática en su centro de trabajo. [En línea]. 2013. Disponible en https://es.slideshare.net/mariorafaelquirozmartinez/medidas-para-aumentar-la-%20seguridad-informatica-en-su-centro-de-trabajo

FRANCO, David y PEREA, Jorge. Herramientas para la Detección de Vulnerabilidades basada en la identificación de servicios. [En línea]. 2016. Disponible en http://www.scielo.cl/scielo.php?pid=S0718-07642013000500003&script=sci_arttext

ESCRIVÁ, G., Romero, Seguridad Informática. Madrid, ES: Macmillan Iberia, S.A... [En línea] 19 de 02 de 2017. [Citado el: 03 de 05 de 2017.] Disponible en http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10820963&p00=seguridad+inform%C3%A1tica.

Observatorio Nacional de Ciberseguridad de Colombia https://www.islsa.com/index.php/empresa/47-observatorio-nacional-de-ciberseguridad-de-colombia

SO / IEC 27000: 2009 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Información general y vocabulario. Recuperado de https://www.iso.org/standard/41933.html.

CASABONA, CARLOS MARÍA ROMEO. 2006. Los datos de carácter personal como bienes jurídicos penalmente protegidos. El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales. ESPAÑA: Granada: Comares.

DECRETO 2573 DE. 2014. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones. [En línea] 12 de dic. De 2014. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60596

LOZANO QUINTERO, Leidy. Casos de Ciberataques en Colombia [En Línea]. Universidad Militar Nueva Granada. 2015. disponible en, http://repository.unimilitar.edu.co/bitstream/10654/7161/1/Ensayo%20para%20optar%20al%20titulo%20de%20Internacionalista%20y%20Politóloga.%20Lady%20Carolina%20Lozano%20Quintero%20.pdf FERNANDEZ, Fernando. El peligro del voto electrónico, [En línea]. 2013. Registraduría Nacional. Disponible en https://www.registraduria.gov.co/El-peligro-del-voto-electronico.html
Contenido del documento: El documento inicialmente aborda un tema muy importante en Colombia que está estrictamente relacionado con el uso de las tecnologías de la información y las entidades nacionales del gobierno Colombiano, el documento inicia con una introducción en el cual se puede evidenciar los diferentes tipos de ataques informáticos que el gobierno colombiano ha enfrentado durante los últimos cinco años, es importante reconocer que estos ataques no se refieren a ataques convencionales accionados por un grupo de universitarios aprendiendo nuevas herramientas de hackeo, sino, la mayoría de estos ataques corresponden a manifestaciones, formas de rechazo de ciertas decisiones que el gobierno ha tomado durante los últimos años, estos ataques son perpetuados por grupos especializados de personas con conocimientos profundos en seguridad informática y hackeo de sistemas informáticos, sin embargo, es válido aclarar que no todos los ataques tienen el mismo objetivo, algunos de ellos están direccionados hacia objetivos personales o con intereses propios. Los delitos informáticos y los casos relacionados a estos han aumentado a grandes pasos, los sectores más afectados por ataques informáticos son el sector financiero, seguidamente el sector de las Telecomunicaciones, posteriormente el sector del gobierno, y a su vez el sector energético e industrial, este documento se enfoca principalmente en los ataques dirigidos al sector gubernamental el cual

según informes del diario dinero.com este sector sufre de más de 85 mil ataques informáticos diarios.

En Colombia existen diferentes entidades especializadas en seguridad de la información con el objetivo principal de detectar cualquier tipo de intento de ataque que este dirigido tanto al sector público como a los usuarios de internet, entre estos están, el Consejo Nacional de política económica y social, CONPES, el grupo de respuestas a emergencias en Colombia, CoICERT, el Comando conjunto cibernético, CCOC, entre otros, estas entidades cuentan con servicios como el SOC (Centro de operaciones de Soporte) el cual cuenta con agentes especializados en el monitoreo de alertas que indiquen un posible ataque informático, lo cual favorece de gran manera la lucha contra los delitos informáticos, es importante mencionar que los delitos más comunes son el hurto por medios informáticos, seguido del acceso abusivo a sistemas informáticos, así como también la violación de datos personales y suplantación de identidad.

El documento aborda casos de ataques informáticos que han sido muy conocidos en los últimos años, entre estos casos se encuentra el ataque informático más mediático hasta ahora, este tuvo lugar durante las elecciones para presidencia de la república en el año 2014, cuando se encontró que uno de los candidatos contrato a un hacker de nombre Andrés Sepúlveda con el objetivo de que este hacker controlara tanto las redes sociales del candidato como también ideara formas de generar una mala percepción a los usuarios de las redes sociales con respecto a los otros candidatos, este también se encontró culpable de espinar el proceso de paz que tuvo lugar en la habana durante el mismo año, así como también fue culpable de espionaje a los otros candidatos para beneficiar al candidato quien lo contrato, de esta manera también se abordan casos muy conocidos como el ataque a la Pagina web de la procuraduría, este ataque fue efectuado por un joven conocido como alias ‘R4lph’ este hacker reemplazo la página de la procuraduría con la imagen del entonces alcance de Bogotá Gustavo Petro, durante más de 4 horas con el mensaje de ‘Petro no se va’ esto fue debido

a que la procuraduría quiso inhabilitar a Petro por gestiones realizadas durante su mandato en Bogotá.

En Colombia existen leyes que buscan regular el uso de los sistemas informáticos y la finalidad de los mismos, la Ley 1273 de 2009 cuenta con varios artículos que exponen las prohibiciones mediante el uso de los sistemas informáticos dentro del territorio Nacional, esta ley busca principalmente penalizar conductas de los usuarios que cometan infracciones o delitos informáticos a través del uso de las tecnologías de información hasta con 96 meses de prisión y multas que van desde los 100 a los 1000 salarios mínimos legales mensuales vigentes, es así como el artículo 269A penaliza acciones las cuales por medio del uso de herramientas informáticas intenten acceder de manera no autorizada a sistemas informáticos de terceros, así como también el articulo 269C. Penaliza a los usuarios que intercepten de manera indebida datos informáticos o emisiones electromagnéticas con el uso de herramientas informáticas con una pena de prisión de hasta 72 meses.

Esto a su vez la falta de rigurosidad en las penalizaciones de los delitos informáticos hace que las personas que tengan conocimientos técnicos avanzados en ciberdelincuencia y en las leyes con referencia a este tipo de actividad se permitan tener licencias para proceder con los ataques y de esta manera operar de manera libre y sin temor a ser penalizados, hemos visto en Colombia diversos ataques al sector gubernamental, sin embargo, los autores intelectuales de estos delitos en el mayor de los casos reciben penas mínimas o incluso la posibilidad de afrontar dichas penas desde sus domicilios, con una vigilancia menor sin tener en cuenta que estos pueden seguir delinquiendo, día a día surgen diversos métodos de intrusión, el robo de información, suplantación de identidad, clonación de tarjetas bancarias, accesos indebidos a equipos informáticos y cibermatoneo son casos que en Colombia suceden a diario en todo el territorio nacional, es por ello que la seguridad de la información y los

especialistas en este área continuamente están desarrollando métodos para contrarrestar estos ataques.
Metodología: Por las características del documento, este no presenta un proceso metodológico definido.
Conclusiones: Las tecnologías de las comunicaciones han desarrollado un avance que ha contribuido a la humanidad en diferentes sentidos, la tecnología avanza de tal manera que es importante estar a la vanguardia de cada cambio los teléfonos celulares o „Smartphone" r piamente se convirtieron en una parte fundamental de nuestra vida cotidiana, estos dispositivos están diseñados para hacer casi cualquier función de las actividades diarias, se ha convertido en un aliado perfecto para la productividad en cuestiones laborales y también para el entretenimiento, sin embargo, la tecnología significa un potencial peligro para los usuarios, es necesario estar conscientes de los peligros que rodean la tecnología, especialmente su vía más rápida y global, el internet. Uno de los objetivos hace referencia a un estudio el cual analiza y documenta los ataques informáticos más importantes teniendo como objetivo el gobierno Nacional en los últimos 5 años, en este documento se presenta el estudio de varios ataques informáticos dirigidos a diferentes entidades del gobierno, uno de los casos más conocidos fue el del hacker Andrés Sepúlveda, este caso estremeció al país en época de elecciones presidenciales del 2014. Posteriormente se hace un estudio del alcance de estos ataques, durante el año 2014, el país fue cómplice de un acto de corrupción perpetuado a través de un equipo de cómputo, se buscó obtener ventaja de las habilidades de un hacker para denigrar la reputación e imagen de los candidatos opositores a la presidencia del mismo año. Así mismo, conocer las leyes que están ideadas para minimizar el riesgo en Internet y concientizar a las personas de los peligros que hay en internet es una

estrategia que el gobierno, en cooperación con el MinTIC han llevado a cabo a través de diferentes programas de prevención y ciberseguridad, esto representa cada vez más un avance en la concientización con respecto a la inseguridad en la Web, es por ello que el gobierno construyo la Ley 1273 del 2009 para controlar y minimizar el impacto de los ciberataques y el número de ataques informáticos.
AUTOR: STEVEN TIGREROS MOJICA