# MONOGRAFIA

# ESTADO ACTUAL DEL CIBERCRIMEN EN COLOMBIA CON RESPECTO A LATINOAMÉRICA

**LUISA FERNANDA ACUÑA LOPEZ**
**SANDRA MILENA VILLA MOTATO**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA**
**CIENCIAS BASICAS RISALRALDA**
**ESPECIALIZACION SEGURIDAD INFORMATICA**
**CEAD DOSQUEBRADAS - RISARALDA, PEREIRA**
**2018**

# ESTADO ACTUAL DEL CIBERCRIMEN EN COLOMBIA CON RESPECTO A LATINOAMÉRICA

**LUISA FERNANDA ACUÑA LOPEZ**
**SANDRA MILENA VILLA MOTATO**

**Monografía para optar por el título de especialista en seguridad informática**

**Director:**

**Martin Camilo Cancelado**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA**
**CIENCIAS BASICAS RISALRALDA**
**ESPECIALIZACION SEGURIDAD INFORMATICA**
**CEAD DOSQUEBRADAS - RISARALDA, PEREIRA**
**2018**

**CONTENIDO**

## LISTA DE TABLAS

## LISTA DE FIGURAS

## CONTENIDO DE ANEXOS

## 1. TITULO

Estado actual del Cibercrimen en Colombia con respecto a Latinoamérica

# 2. DEFINICIÓN DEL PROBLEMA

## 2.1 Antecedentes del problema

La poca existencia de análisis de datos en esta rama, la cantidad de información, la disponibilidad de herramientas de ataque automatizadas de fácil acceso fluctuante como el desarrollo de estas acciones y variables se han ido incorporando e impactado a través de los años analizando su influencia e impacto en Colombia, teniendo presente esto en contraste con los demás países por medio de la revisión de las nuevas legislaciones aplicada a los delitos informáticos que se están implementando en Colombia; se hace imperativo, tener claridad sobre la intención de la ley, sus postulados y la razón de ser de las penas que contempla, como se tipificado en Latinoamérica sin dejar de observar el resto del mundo.[1] Considerando todas las temáticas expuestas, una vez adquirido el conocimiento se podrá generar posibles recomendaciones y sugerencias para las diferentes organizaciones que en un momento dado puedan afrontar el cibercrimen como enfrentar y poder estar preparados con los crecientes cambios en las telecomunicaciones e interconectividad.

En Colombia como en todos los países de Latinoamérica las tecnologías de la información y las comunicaciones se han ido incorporando a un ritmo acelerado, siendo usado en cosas como: búsquedas en internet, compras, correo electrónico y juegos por nombrar algunos, por otro lado, la comunicación es más rápida y más confiable que en el pasado, pero el problema reside en que tan expuestos estamos a las amenazas, riesgos o vulnerabilidades[2][3]y el cibercrimen, donde son inevitables las consecuencias, de quienes habitan la región se ven obligados a enfrentar un importante desafío al momento de proteger la información, garantizando la disponibilidad, integridad, trazabilidad, autenticidad y confiabilidad de los servicios prestados a través de Internet, donde la infraestructuras y sistemas críticos cada día son más exigentes causando en muchos caso que las empresas pierden su capital principal4por no tener presente los principios de la seguridad de la información.

[1] Guzmán a, clara lucía. “contextualización del cibercrimen en Colombia - tecnología en redes 130-472—1” {2009}
[2] Cybercrime news, artículos y actualizaciones {en línea}, disponible en: (https://www.scmagazine.com/cybercrime/topic/47218/)
[3]Yagub, mimi, “cybercrime in Colombia: ¿an underestimated threat?” {en línea} (2014) disponible en: (http://www.insightcrime.org/news-analysis/cyber-crime-colombia-underestimated-threat)
[4] Mari, angélica - brasil tech, “latin america braces for rise in cybersecurity threats” {2016} {en línea} disponible en: (http://www.zdnet.com/article/latin-america-braces-for-rise-in-cybersecurity-threats/)

Ahora en contraposición y analizando que procesos realiza Colombia a nivel jurídico y legal donde se cuenta con "*la Ley 1273 del 05 de enero de 2009*", la cual requiere ser revisada con respecto a las leyes de los países vecinos, para crear un ambiente balanceado estableciendo una comparación beneficiosa que enriquezca la formulación de las nuevas normas ya que actualmente, está por el momento contempla puntos que hacen referencia a aquellas conductas o modalidades delictivas que van enfocadas a la afectación del patrimonio económico de los colombianos, entre ellas el hurto por medios informáticos o electrónicos, y la transferencia no consentida de activos[5]

Por ende, la seguridad informática se convirtió en un fuerte dolor de cabeza para las organizaciones. y en Colombia, particularmente, reside en el desconocimiento, porque es sorprendente lo poco que se sabe al respecto y más aún cuando las empresas, aunque saben sus riesgos o han enfrentado perdidas debido al delito informático guardan silencio y en parte es intencional, por temor a dañar su reputación y asustar a los clientes, además del menosprecio por el impacto de las amenazas cibernéticas hacen que los costos que pagan sean más altos; haciendo imperativo, determinar las falencias existentes en la norma sobre delitos informáticos (cibercrimen) a la luz de otras legislaciones y de tratados internacionales, que permitan proyectar leyes adecuadas y efectivas que cumplan con su misión de proteger, donde se debe buscar puntos de vista que favorezcan o amplíen la visión de la problemática, para lo cual se buscarán en las fuentes que se especializan en el estudio de estas áreas y temáticas relacionadas, donde los delito cibernéticos no reconocen fronteras nacionales y que se requiere un esfuerzo multilateral y multidimensional para abordar la cantidad de amenazas informáticas para las empresas y usuarios en general, porque como se decía previamente, todavía el cibercrimen es tratado como temas apartes en los diferentes lugares de Latinoamérica, cuando realmente son los mismos ataques y vulneraciones a las que día a día se enfrentan las empresas, y por ende con el fin de poder entender el estado actual del cibercrimen y que pueden hacer las organizaciones al respecto y estar mejor preparados para enfrentar esta creciente oleada de cibercrimen que cada día afecta más y más a las empresas donde se hace imperativo crear, implementar y generar conciencia en cuanto a seguridad informática se refiere.

[5]Infolaft, "lo que debe saber sobre el cibercrimen en Colombia", {2014} {en línea} disponible en: (http://www.infolaft.com/es/art%c3%adculo/lo-que-debe-saber-sobre-el-cibercrimen-en-colombia)

## 2.2 Formulación del problema

¿Cómo la identificación del estado actual del cibercrimen en Colombia con respecto a Latinoamérica ayudara a plantear mejoras de seguridad en las empresas?

## 2.3 Descripción del problema

Este proyecto pretende revisar, contrastar por medio de una revisión bibliográfica el incremento del cibercrimen en Colombia realizando algunos comparativos, el cual tendrá como enfoque los diferentes ataques informáticos, nuevas formas de instrucción, vulneración o las distintas amenazas latentes en el ciberespacio, la poca protección de las empresas donde por el desconocimiento[6] de cómo protegerse utilizando con las metodologías, los programas y políticas[7] que los países diseñan para evitar ataques sobre la información y la realización de planes de contingencia, de las implantaciones de seguridad de las pymes, pueden mejorar su seguridad y por ende garantizar sus servicios y activos, además de revisar los conceptos de ciberseguridad y ciberdefensa, desde su manejo e impacto en Colombia en comparación con Latinoamérica.

[6] Bolaños, Andrés días, universidad nacional abierta y a distancia UNAD. "análisis comparativo sobre delitos informáticos en Colombia - con relación a seis países de Latinoamérica - escuela de ciencias básicas, tecnología e ingeniería. {2014}

[7] Symantec, organización estados americanos, "tendencias de seguridad cibernética en américa latina y el caribe "{2014}

## 3. JUSTIFICACIÓN

El cibercrimen es un asunto que concierne a todos: sector público o privado, las empresas y los usuarios, ya que todos tiene un rol papel fundamental para contrarrestar los delitos informáticos los cuales suelen dejar billonarias pérdidas en el mundo. Actualmente los delitos informáticos han aumentado considerablemente al punto de ser necesario legislarlos para que tengan una justa penalización que pueda controlar su difusión y crecimiento. 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 presente monografía se desarrolla para analizar e identificar las falencias existentes en la legislación Colombiana en cuanto a delitos informáticos y el impacto que ha tenido en las empresas con respecto a los países de Latinoamérica, desde la perspectiva y lineamientos del "*Convenio de Ciberdelincuencia de 2001*, convenios existentes sobre ciberdelincuencia y ciberdelito en Colombia y las leyes colombianas implementadas que los tipifiquen, porque el especialista de Seguridad Informática necesita conocer la posición que ha tomado su país en la defensa y preservación integral de los sistemas informáticos en contra de los ciberdelincuentes, como personas y desde cualquier campo de la ciencia, cada colombiano está llamado a realizar aportes que contribuyan al fortalecimiento de la seguridad, y desde la Ingeniería de Sistemas, aún más, desde el punto de vista de los Especialistas en Seguridad Informática debe existir una preocupación más alta por formular alternativas de mejora y es que, seguridad cibernética debería no ser algo de cada país individual ya que una nación por sí sola no puede asegurar adecuadamente sus redes.

La cooperación es esencial de ahí que es muy importante realizar comparativos sobre que está haciendo Colombia en contraste con sus países vecinos, que podría aprender de ellos y que puede enseñarles[8]; por ende, con el fin de poder demostrar cómo la ciberseguridad y la ciberdefensa permiten evidenciar que en el ciberespacio existen amenazas latentes a la seguridad de un estado o una organización. A lo largo del mismo, se busca ofrecer una explicación sobre estos términos, y que sea lo más entendible posible y dar una visión clara, realizando una compilación de varios documentos que hablan sobre el tema. Tocando la terminología relacionada como: amenazas y vulnerabilidades abarcando su utilización titilación, prevención y distintos métodos de protección, luego que manejo le dan los diferentes países, analizando diferencia, similitudes entre Colombia y Latinoamérica al combatirlas, y proteger información valiosa[9].

[8] INFORME CIBERSEGURIDAD – "Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?" {2016} –{en línea} Disponible en: (http://observatoriociberseguridad.com/)
[9] VARGAS V, Edisson Mauricio, "ciberseguridad y ciberdefensa: ¿qué implicaciones tienen para la ¿seguridad nacional?" {2014}

# 4. OBJETIVOS

## 4.1 Objetivo general

Realizar análisis de la situación de Colombia con respecto a Latinoamérica de las amenazas, utilizadas por los cibercriminales para atacar las tecnologías de información y como puede esto impactar en la seguridad de las empresas

## 4.2 Objetivos específicos

- Determinar los delitos informáticos y cuáles actividades delictivas se Catalogan de acuerdo a la “Organización de las Naciones Unidas (ONU) en el Convenio de Ciberdelincuencia de 2001”.
- Revisar y exponer el panorama de los cibercrímenes que afectan en mayor medida a Latinoamérica
- Realizar un análisis del impacto negativo que tiene la ciberdelincuencia en las empresas colombiana por medio de la revisión de datos estadísticos públicos como la Fiscalía General de la Nación y la Policía Nacional.
- Determinar las diferencias y similitudes que existen entre la normatividad colombiana y las normatividades de los países analizados mediante una observación comparativa.

# 5. MARCO DE REFERENCIA

## 5.1 Antecedentes

Por medio de la tabla1. Se refleja un comparativo según la organización “PANDA SECURITY” donde se pueden observar los ataques más comunes entre 2014 - 2017[10]

**Tabla 1. Comparativo Ataques 2014-2017 según panda security**

| Ataques 2014 | Ataques 2017 |
|---|---|
| Imágenes de hollywood en la red | Filtraciones de shadow brokers |
| Ebay y paypal, los primeros afectados | Wannacry |
| Imágenes de hollywood en la red | Petya |
| Robo de 5 millones de contraseñas de Gmail | Filtración vault 7 de wikileaks |
| Viator y los datos bancarios de sus usuarios | Hackeo de la campaña de emmanuel macron |

**Fuente:** “PANDA SECURITY” donde se pueden observar los ataques más comunes entre 2014 - 2017[11]

Al revisar detalladamente, se puede mencionar aquellos ataques que están ocasionado actualmente daño, Las infraestructuras de muchas de las bases de datos de las empresas, usualmente contienen información relevante de una organización, estas bases de datos están sujetas a una amplia gama de ataques contra seguridad de sus bases de datos.

[10] Pandasecurity “la primera mitad de 2017 ha registrado un número sorprendente de ciberataques a gran escala “, {en línea} disponible en: (https://www.pandasecurity.com/spain/mediacenter/noticias/ciberataques-hasta-la-fecha/)

[11] Pandasecurity “la primera mitad de 2017 ha registrado un número sorprendente de ciberataques a gran escala “, {en línea} disponible en: (https://www.pandasecurity.com/spain/mediacenter/noticias/ciberataques-hasta-la-fecha/)

Aunque muchas de las bases de datos y sus contenidos puedes ser vulnerables a muchas series de amenazas internas y externas, es posible reducir muchos de los ataques hasta casi a cero con ayuda de las soluciones y estrategias de seguridad suministradas por diferentes organizaciones especializadas en el tema, impidiendo así que los estafadores que manejan desde técnicas de spam, pharming y phishing, que se basan en procedimientos técnicos y procesos de ingeniería social con el fin de engañar al usuario, donde el índice de víctimas día a día aumenta dramáticamente en todo el mundo.

Cuando la información de los usuarios se compromete se corre el riesgo de que sea publicada, vendida, objeto de chantaje o empleada en el acceso a cuentas bancarias; o los equipos son secuestrados y se les exige rescate, los asistentes de voz pueden ser alterados para que abran la puerta de casa o los coches pueden ser dirigidos desde la distancia.

Al analizar globalmente podemos incluso ponderar un ranking, donde lo que más se mueve en el área del cibercrimen va desde el hecho de que los ciberdelincuentes focalizan sus esfuerzos en lo que les dé más ganancias, ataques de Ransomware, donde este malware: el lucro económico es la principal motivación al ser una de las vías más sencilla y directa de obtener ganancias, los principales objetivos de estos ataques son usualmente las Empresas, ya que poseen, información más valiosa que los usuarios comunes porque en el conocido mercado negro se puede obtener bastante por la información, además si se ve desde el punto desde Internet de las Cosas (IoT): Se visualiza como la puerta sin llave a las redes corporativa de las empresas, Ataques DDoS (Distributed Denial of Service) entre otros.

Ahora en el panorama de Latinoamérica es importante revisar con que planes se cuanta destinados a contrarrestar estas nuevas técnicas, porque es evidente que los gobiernos destinan pocos recursos para mejorar la seguridad en Internet, en las redes, salvaguardar los activos y garantizar el tratamiento óptimo de los datos porque no cuentan con conocimientos especializados y experiencia para poner en marcha políticas claras y/o controles que ayuden a reducir las acciones de cibercrimen.[12]

“En Latinoamérica la regulación es incipiente, aunque hay países que se han blindado en el tema como Chile”[13]

[12] Siliconweek spain, “estudio del aumento del cibercrimen en latinoamérica” –{2012} {en línea} disponible en: (http://www.mundodigital.net/estado-del-cibercrimen-en-latinoamerica/)

[13] Azuaje, miguel, “argentina se blindará contra cyberdelitos” –{nov 10, 2017} {en línea} disponible en: (http://segundoenfoque.com/argentina-se-blindara-contra-cyberdelitos-2017-11-10)

Chile, es cuarto en tasa de cibercrimen en Latinoamérica donde virus como ransomware y/o diferentes adware son los que más lo afectan, y a nivel general estos dos delitos pasan a ser de los más comunes en el continente, donde varios de estos ataques ocurren por segundo según diferentes fuentes, ya que este tipo de virus suele ser el que está a la orden del día por las constantes actualizaciones y mejoras que tienen cada año. [14]

Argentina es uno de los países que se está regulando para poder contrarrestar el inminente crecimiento de los ciberdelitos, donde una de las acciones que se está adoptando será agregar al amplio número de tipos de pólizas de seguro, una contra ciberdelitos o ataques informáticos, cuya nueva modalidad permitirá obtener una reglamentación en el proceso, donde el objetivo principal es asegurar contra tres riesgos los cuales serían, interrupción del negocio, reputación y todo lo relacionado a demandas y reclamos de terceros en base de esos ataques informáticos, así como los costos asociados.

Ahora una pregunta que surge es: ¿Latinoamérica es atractiva para los cibercriminales y la ciberdelincuencia?

Cuando analizamos dicho interrogante nos encontramos con que el panorama actual de amenazas, priman sobre otras, como se tipifican y que planes tienes las organizaciones, las empresas y los mismos usuarios para contrarrestarlos, quedando claro que este es un problema que afecta a todos los países y regiones del planeta, no es especifico de alguno y Latinoamérica no es la excepción, donde muchas veces se ve afectada en mayor medida por el bajo nivel de medidas de protección, planes de contingencia y riesgos, salvaguardas e infraestructura especializada en seguridad, además, porque usualmente el usuario suele ser: confiado, no pone atención a la seguridad y pone sus activos en bandeja de plata para los cibercriminales los cuales sacan provecho de estas debilidades en los diferentes países para convertir las máquinas en robots y utilizarlas para diferentes tipos de ataques como puede ser envío de spam, distribución de malware, estafas, denegaciones de servicio, entre otros.[15]

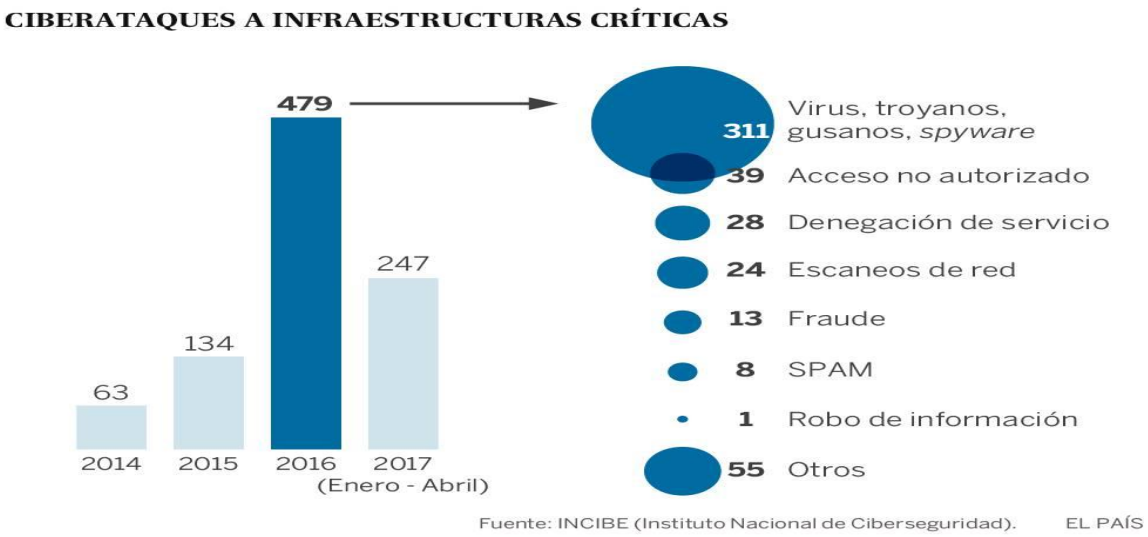
[14] Cooperativa-cl, (2016) chile, cuarto en tasa de cibercrimen en Latinoamérica – {en línea} disponible en: http://www.cooperativa.cl/noticias/tecnologia/internet/seguridad/chile-cuarto-en-tasa-de-cibercrimen-en-latinoamerica/2016-09-30/113344.html

[15] Cancino, Héctor - ciber crimen “el cibercrimen posa su mirada en américa latina” {2017} {en línea} disponible en: (https://tecno.americaeconomia.com/articulos/el-cibercrimen-posa-su-mirada-en-america-latina)

Por esta razón, Latinoamérica seria por decirlo así un destino popular para los ciberdelincuentes, y si a eso se le adiciona el hecho de que la mayoría de los países de la región toman su tiempo en reaccionar y poner en marcha los planes de contingencia, actualizar sus legislaciones, adoptar tecnología de seguridad o generar conciencia en los usuarios favoreciendo a aquellos que buscan lanzar su próximo ataque o vulnerar la seguridad en una empresa por medio del uso de malware o robo de identidad[16].

Como se puede observar en la siguiente figura 1, se puede ver un primer acercamiento a como los ciberataques han afectado las infraestructuras criticas de las organizaciones, y por ende es un tema que, hoy en día debe moverse al ritmo que lo hace el cibercrimen.

**Figura 1. Ciberataques a infraestructuras Criticas** [17]




**Fuente**: Eelpais, “los ciberataques a infraestructuras estratégicas se multiplican por siete en solo dos años” https://politica.elpais.com/politica/2017/05/24/actualidad/1495619175_136537.html)

La imagen muestra un comparativo entre los años 2014 al 2017, donde se evidencia que en los últimos años se ha incrementado, los delitos informáticos a través de los virus, los troyanos (software malicioso que permite el acceso remoto desde otro equipo) y los spyware (programas espía) estos son la amenaza más común. Se destacan los accesos no autorizados; y los ataques de denegación de servicio (DoS), "La protección de las infraestructuras críticas reside y depende en mayor medida de la seguridad que se implemente".

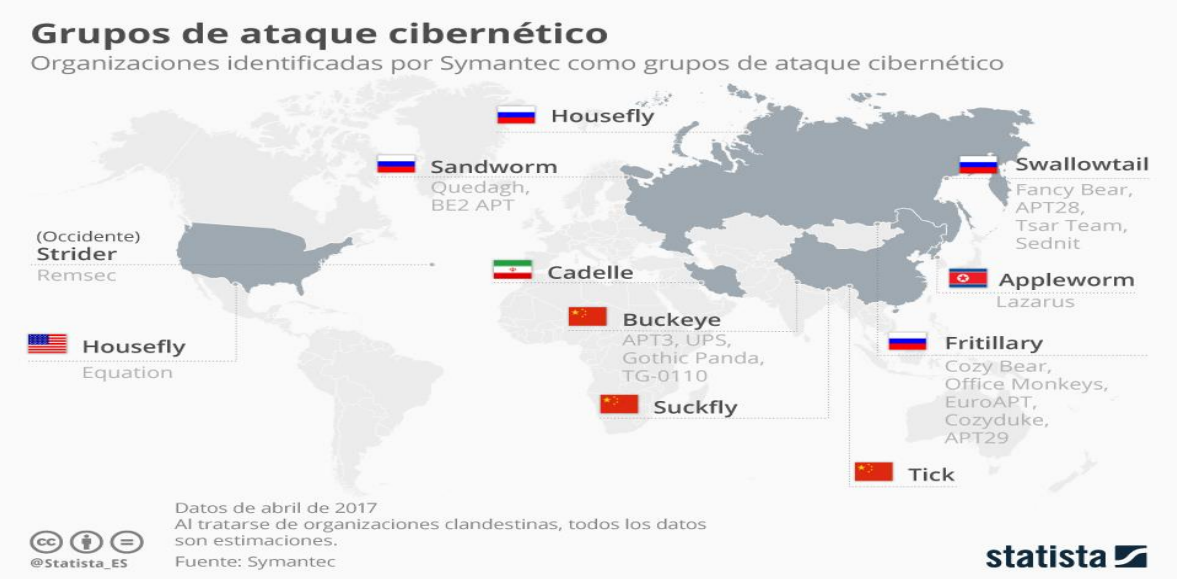
[16] Dinero, “el cibercrimen en Latinoamérica” {2014} – {en línea} disponible en: (http://www.dinero.com/actualidad/noticias/articulo/el-cibercrimen-latinoamerica/192369)

[17] Eelpais, “los ciberataques a infraestructuras estratégicas se multiplican por siete en solo dos años” {2014} {en línea} disponible en: https://politica.elpais.com/politica/2017/05/24/actualidad/1495619175_136537.html)

Los códigos maliciosos  son de los ataques más comunes donde se puede decir que para el año 2016 se  detectó un crecimiento obteniendo alrededor de un 49% que demuestra que prácticamente una de cada dos empresas latinoamericanas que participaron en este estudio fueron víctimas de algún tipo de malware.[18]

Incluso ataques como los ransomware han sido catalogados en su propia categoría y aunque, también se trata de un tipo de malware, ya se identifica como algo aparte en sí mismo. De hecho, el "*Departamento de Justicia de los Estados Unidos lo ha calificado como "la ciberamenaza más grande de 2017*".

**Figura 2. Grupos de ataque Cibernético**[19]




**Fuente**: Moreno, Guadalupe, wannacry, "lazarus es una de entre muchas", (https://es.statista.com/grafico/9409/lazarus-es-una-de-entre-muchas/)

Según la figura 2, donde por medio de las últimas investigaciones realizadas por statista y la fuente Symantec, se podría decir que muchos de los ataques son originados, desde lugares como corea del norte, china, como por ejemplo el WannaCry o Apple worm, podría provenir de un grupo de cibercrimen llamado Lazarus procedente de Corea del Norte, según ha informado la empresa de seguridad informática Securelist.

[18] Mendoza, miguel ángel, "seguridad corporativa en Latinoamérica: causas de incidentes y controles utilizados", {2017} –{en línea} disponible en (https://www.welivesecurity.com/la-es/2017/04/27/seguridad-corporativa-en-latinoamerica/)

[19] Moreno, Guadalupe, wannacry, "lazarus es una de entre muchas", {16/05/2017} –{en línea} disponible en (https://es.statista.com/grafico/9409/lazarus-es-una-de-entre-muchas/)

Como se pretende mostrar con el documento por medio de comparativos y casos de estudio enfocados en este tema, sigue siendo un campo inexplorado a grandes rasgos en lo que respecta a Latinoamérica, siendo poco lo que las organizaciones conocen, y las que lo hacen, tardan en querer hacerlo, y solo cuando sus activos se ven afectados, es que logran ver la importancia de la seguridad, de los procesos estandarizados y la implementación de políticas ligadas.

Como podemos ver existen diferentes ataques informáticos que incluso no son visto como tales porque sus supuestos fines son lucrativos para el usuario o les dan un "beneficio", pero que a la larga está exponiendo información delicada el usuario o si darse cuenta están siendo usados para fines mayores, lavado de dinero, o financiando otros delitos mayores.

Por su parte otros países han ido adoptando estrategias para contrarrestar también de distintas formas la creciente oleada de cibercrimen que se viene en paralelo a la tecnología y sus beneficios[20].

Y si se revisa los ataques generados por delincuentes informáticos en Colombia, estos se enfocan cada vez más hacia las empresas, organizaciones o entidades cuya información sea de interés, donde su efectividad es mayor y con estos podrán generan una mayor ganancia para dichas organizaciones en pro del ciberdelito. Por ende como punto de partida se cuenta con las conclusiones del informe del centro cibernético de la policía "*Amenazas del Cibercrimen en Colombia 2016-2017*" donde se muestra un análisis de la situación actual del país en materia de seguridad cibernética[21].

Como se muestra en la figura3. Podemos apreciar un poco como se encuentra Colombia respecto a países como México y Brasil.

[20] Explainer: fighting cybercrime in Latin America (2013) Rachel glickhouse
{en línea} disponible en: (http://www.as-coa.org/articles/explainer-fighting-cybercrime-latin-america)
[21] Globalservices, "amenazas del cibercrimen en Colombia", {2016-2017} {en línea} disponible en:
(https://www.globalservices.bt.com/latam/es/blog/amenazas-del-cibercrimen-en-colombia-2016-2017)

**Figura 3. Ataques Cibernéticos Principales países[22]**


**Fuente:** La republica.co Colombia se pierden cerca de US$ 600 millones por el cibercrimen:(https://imgcdn.larepublica.co/cms/2017/03/02232524/al-ataquesciber0303.jpg)

## 5.2 Marco teórico

El desarrollo de las tecnologías informáticas ofrece un aspecto negativo, a pesar de todos los beneficios que ha traído y es el hecho de que abre la puerta a conductas antisociales y delictivas. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas para infringir la ley y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.[23] Sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse.

Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda, huella de los hechos, por nombrar algunas estafas, robos, sobornos, tráfico ilícito entre otros.

Es en si todo lo que englobe actividades e incursiones ilícitas en las redes informáticas privadas, ya sea de individuos particulares o de instituciones públicas o privadas, gubernamentales o no, cometidas por un solo individuo, o por grupos aficionados o expertos y organizados. Incluso se toma el cibercrimen como un instrumento y que de algún modo contribuyan a la expansión y empoderamiento de los grupos dedicados al crimen organizado transnacional.

[22]La republica.co Colombia se pierden cerca de US$ 600 millones por el cibercrimen- {en línea} Disponible en: 2017 (https://imgcdn.larepublica.co/cms/2017/03/02232524/al-ataquesciber0303.jpg)

[23] Eumed “los delitos informáticos. tratamiento internacional” {2012} {en línea} disponible en: (http://www.eumed.net/rev/cccss/04/rbar2.htm)

Es importante entender en primera instancia que el delito cibernético se considera como aquellas actividades que se realizan de forma ilegal o que en algunas partes consideran ilícitas y que pueden realizarse a través de redes electrónicas, digitales de forma personal, nacionales o mundiales; donde estos se típica como crímenes cibernéticos donde se involucra algún dispositivo y desde él se realizan dichas actividades delictivas siendo una parte integral y necesaria del crimen[24], en esto tenemos a los atacantes o responsables de vulnerar la seguridad o es su contra parte defenderla, protegerla y salvaguardarla, ahora por el lado de los atacantes estos desarrollan cada día tecnologías y tácticas cada vez más sofisticadas, creando infraestructuras back-end (se refiere a la separación de preocupaciones entre la capa de presentación (front end) y la capa de acceso a datos (back end)) sólidas para el lanzamiento y soporte de sus campañas. Los ciberdelincuentes están perfeccionando sus técnicas para obtener dinero de sus víctimas y para evitar ser detectados mientras continúan robando datos y propiedad intelectuales,[25] a nivel mundial, y es que en el mundo muchas naciones, han tenido que verse frente a frente y mejorar sus esfuerzos doblando la seguridad con el fin de evitar manipulación política y sabotaje dirigido.

Al mismo tiempo, los cibercriminales han causado niveles sin precedentes de interferencia, enfocándose en herramientas de TI y servicios en la nube relativamente sencillos[26]

Estos delitos cibernéticos, cibercrímenes o ciberdelitos tiene entre sus características que permiten a sus ejecutores actuar a nivel global y de manera anónima, adquiriendo así una capacidad y un alcance que no tiene fronteras, dando pie a la instauración de redes mundiales de ciberdelincuencia.

Estas nuevas ventajas que traen consigo las herramientas TI han generado en el crimen organizado transnacional se ha adaptado a los distintos cambios en la sociedad con el fin de garantizar su existencia en el tiempo tomando un interés en la gran variedad de aplicaciones que la tecnología y los nuevas herramientas de la información proporciona a sus actividades, teniendo en ellas un perfecto instrumento de expansión de su enriquecimiento e influencia a nivel mundial, complementando sus ya conocidas actividades tradicionales.[27]

---

[24] Pladna - brett, east Carolina university “the lack of attention in the prevention of cyber crime and how to improve it”- {en línea} disponible en: (http://www.infosecwriters.com/text_resources/pdf/bpladna_cybercrime.pdf)

[25] cisco, “informe anual de seguridad” - {2016}

[26] Cancino, Héctor - ciber crimen, “el cibercrimen posa su mirada en américa latina”, {2016} –{en línea} disponible en: https://tecno.americaeconomia.com/articulos/el-cibercrimen-posa-su-mirada-en-america-latina

[27] GESI – Universidad de Granada – {2017} La cibercriminalidad como instrumento para la expansión y empoderamiento del crimen organizado {en línea} disponible en: ( http://www.seguridadinternacional.es/?q=es/content/la-cibercriminalidad-como-instrumento-para-la-expansi%C3%B3n-y-empoderamiento-del-crimen )

La ciberdelincuencia se ha logrado expandir por diferentes medios como la ingeniería social, o el internet de las cosas, que multiplica las amenazas a las cuales se exponen ya las organizaciones y usuarios.

El principio del internet de las cosas es la operación remota e interconectividad donde cada uno de los objetos conectados a Internet tiene una IP específica y mediante esa IP puede ser accedido pare recibir instrucciones. Así mismo, puede contactar con un servidor externo y enviar los datos que recoja.

Con este ecosistema formado por numerosos procesos y dispositivos conectados, la principal fuente de amenazas es que "es muy difícil actualizar todos estos a la vez dejando vulnerabilidades visibles para los delincuentes, y especialmente cuando esta está integrada a una red junto a otros muchos dispositivos".[28]

Dentro los ciberdelitos más conocidos a los que se puede exponer cualquier organización se puede mencionar algunas modalidades tales como: el robo de información, afectación del sistema, y falsificación en las transacciones.

Las organizaciones no están aún concienciadas de la dimensión, real del problema, donde por ejemplo el Internet de las Cosas es sólo un tema más a tener en cuenta cuando se habla de ciberseguridad, la protección de los datos generados por estos dispositivos y la identificación de datos sensibles que están expuestos, donde se estima que son en gran medida los riesgos a los que se exponen y por donde se pueden generar mayores ataques en los diferentes entornos que las organizaciones poseen.[29]

### 5.3 Marco legal

La ciberseguridad es un factor crítico para garantizar la transformación digital de Europa, imprescindible para el avance tecnológico. En estos momentos es clave desarrollar un sector fuerte con tecnología propia, porque en caso contrario estaremos expuestos a ciberataques cada vez más complejos y con mayor impacto en nuestra sociedad.

[28] Eleconomista –{2018} Check Point: "La ciberdelincuencia del internet de las cosas busca sobre todo el dinero" {en línea} disponible en: ( https://www.eleconomista.es/tecnologia/noticias/8930004/02/18/Avi-Rembaum-Check-Point-La-ciberdelincuencia-IoT-busca-sobre-todo-el-dinero-no-se-diferencia-de-otras-actividades.html )

[29] Investigación VIU- Universidad de Valencia - Informe-Ciberseguridad – Ciberseguridad Tendencias 2017 - {2017}

Y es que se entiende que el acceso no autorizado al sistema se constituye en un problema de seguridad grave ya que una persona o software puede extraer información de gran importancia desde un repositorio o base de datos, y posteriormente generar perjuicios a la organización de diversas formas, cuando se habla de que una amenaza, ataque, herramienta puede ingresar sin la debida validación y autenticación se puede pensar que se trata de un gusano, un troyano o, en general, de un virus.

Se puede decir que inclusive a nivel organizacional se describe un futuro sombrío para las cuales no están preparadas las entidades y los diferentes países para lidiar con este desarrollo y crecimiento las vulnerabilidades y el riesgo de seguridad en la información, que esto conlleva.

Ahora si se habla de que están haciendo países como Colombia, para contrarrestar o prepararse para enfrentar los diferentes ataques, vulnerabilidades y riesgo, se puede decir que fue el primer país latinoamericano en adoptar una estrategia nacional integral de ciberdefensa. En julio de 2011, el "*CONPES 3701*" -el marco de defensa cibernética del país- estableció una unidad policial para investigar el delito cibernético, un comando cibernético conjunto para respuestas militares a ataques cibernéticos en las fuerzas armadas y "*colCERT*", una oficina gubernamental para coordinar medidas de ciberseguridad.

Países como Colombia que muestran ser un blanco fructífero para los delincuentes, ha empezado a despertar y ver como tema importante el involucrase con todas estas nuevas políticas, capacitaciones y convenciones, donde puede aprender de países que ya pasaron por este proceso e implementarlo también en el país; Como se muestra en la figura4 .la cual refleja una invitación de Europa para Colombia en temas de delito cibernético.

**Figura 4. Consejo de Europa invitó a Colombia a adherir a la Convención sobre Delito Cibernético[30]**


**Fuente:** Cancillería , "consejo de Europa invitó a Colombia a adherir a la convención sobre delito cibernético" (http://www.cancilleria.gov.co/newsroom/news/consejo-europa-invito-colombia-adherir-la-convencion-sobre-delito-cibernetico )

[30] Cancillería , "consejo de Europa invitó a Colombia a adherir a la convención sobre delito cibernético" {2013} {en línea} disponible en: (http://www.cancilleria.gov.co/newsroom/news/consejo-europa-invito-colombia-adherir-la-convencion-sobre-delito-cibernetico )

Por ende, se hace importante revisar, no solo el cibercrimen desde el punto de vista del delito en si sino también desde las leyes y decretos que regulan, penalizan y los tipifican según su gravedad.

En países europeos como España, la seguridad y el manejo que se le da es a través de la legislación sobre delitos informáticos y los artículos del código penal español referentes a delitos informáticos, (*ley-orgánica 10/1995, de 23 de noviembre/boe número 281, de 24 de noviembre de 1.995*)[31], en países como estados unidos se ha implementado es la ley de Protección de Datos la cual se ocupa de la seguridad de la transmisión electrónica de datos personales, aunque los Estados Unidos no tienen ninguna legislación formal centralizada a nivel federal con respecto a este tema, sí aseguran la privacidad y protección de los datos a través de la Ley de Privacidad de los Estados Unidos, la Ley de Puerto Seguro y la Portabilidad y Responsabilidad del Seguro Médico.[32]

Los Delitos Informáticos reciben un tratamiento Internacional bajo una Doctrina y práctica donde es importante el análisis de los aspectos doctrinales que avalan el Sistema de Protección Mundial a esta desde las nuevas figuras jurídicas en la Comunidad Mundial de Naciones, quienes han insertado los principios de las políticas de protección, utilización a las nuevas tecnologías y servicios informáticos.

Por ejemplo, en la tabla 2. A través de la revisión de las leyes descritas en la página de Iberoamérica sobre protección de datos podemos generar un cuadro comparativo entre los diferentes países allí descritos.[33]

[31]Delitosinformaticos.com {2000-2012} “legislación sobre delitos informáticos España” {en línea} disponible en: (https://delitosinformaticos.com/legislacion/espana.shtml)

[32] Hg.org - hgexperts.com “data protection”. {1996-2017} {en línea} disponible en: (https://www.hg.org/data-protection.html)

[33] Redipd –“red iberoamericana de protección de datos” {2009} -{en línea} Disponible en: (http://www.redipd.es/index-ides-idphp.php)

**Tabla 2. Comparativo - de leyes según la página de red iberoamericana de protección de datos – Parte 1**

| PAIS | LEYES | AÑO | TIPO DE LEGISLACION | LEGISLACION |
|---|---|---|---|---|
| COLOMBIA | Ley Estatutaria Nº 1581 | 2012 | general | promueven y buscan con fin la protección de datos personales |
| | Ley Estatutaria Nº 1266 | 2008 | general | Son todas aquellas disposiciones generales del hábeas data y como este es regulado, dependiendo del manejo que este le dé a información que este inmersa en las bases de datos personales, analizando tipo, clasificación y características de estas. |
| | Ley 1712 | 2014 | sectorial | Se encarga de definir, determinar y revisar la forma en la cual los operadores de los bancos de datos de información de índole financiera, crediticia, comercial, de servicios o la proveniente de terceros deben presentar la información de los titulares de la información y que tratamiento de datos estas deben tener. |
| | Decreto 1377 y Decreto 886 del 134 | 2013 / 2014 | General / sectorial | Reglamenta parcialmente la Ley Nº 1581 / Registro Nacional de Bases de Datos. |
| | Artículo 15. | | Constitución | Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. |
| | Artículo 20. | | Constitución | Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación |
| | Ley 1.273 (2009), | 2009 | Código Penal | Modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos". |

Fuente: Redipd –"red iberoamericana de protección de datos" - (http://www.redipd.es/index-ides-idphp.php) [34]

[34] Redipd –"red iberoamericana de protección de datos" {2009} -{en línea} Disponible en: (http://www.redipd.es/index-ides-idphp.php)

Otras leyes que valen la pena mencionar están:

Ley No 599 de 2000: Por la cual se expide el código penal. Artículo No 192, donde se ratifica la conducta punible de violación ilícita de comunicaciones y se incluyen algunas conductas relacionadas con el delito informático, tales como el ofrecimiento, venta o compra de equipos para interceptar la comunicación entre personas

Ley No 1341 de 2009: Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones (TIC).

Decreto No 2364 de 2012 el cual habla sobre la firma electrónica y otras disposiciones.[35]

***Tabla 3.*** **Comparativo - de leyes según la página de red iberoamericana de protección de datos – Parte 2**

| **COMPARATIVO - DE LEYES SEGÚN LA PAGINA DE RED IBEROAMERICANA DE PROTECCION DE DATOS** | | | | |
|---|---|---|---|---|
| **PAIS** | **LEYES** | **AÑO** | **TIPO DE LEGISLACION** | **LEGISLACION** |
| BRASIL | Artículo 5 | | Constitución | "habeas data" |
| | Ley Nº 9.296 | 1996 | sectorial | interceptación de comunicaciones telefónicas |
| | Ley Nº 9.507 | 1997 | sectorial | Derecho de Acceso a la Información y reglamenta el "habeas data" |
| | Ley Complementaria 105 | | sectorial | Secreto de las operaciones de instituciones financieras |
| | Ley Nº 8078/90 | 1990 | sectorial | Código de Protección y defensa del Consumidor. |
| MEXICO | articulo 6 /articulo 16/ articulo 73 | | Constitución | preceptos constitucionales |
| | Leyes | | | De trasparencia protección al consumidor, defensa del usuario de servicios financieros, acceso a la información |

**Fuentes**: El autor y generado a partir de información encontrada en Redipd –"red iberoamericana de protección de datos" [36]

[35] Universidad militar granada facultad de ciencias económicas- importancia de la implementación del concepto de Ciberseguridad organizacional en las organizaciones tipo Pymes –[2015]

[36] Redipd –"red iberoamericana de protección de datos" {2009} -{en línea} Disponible en: (http://www.redipd.es/index-ides-idphp.php

Como se aprecia, en la tabla es un comparativo, entre 3 países iberoamericanos que muestran cómo se manejan las leyes, y es que, cada país se enfoca de manera distinta, en algunos describen todo en pocas leyes otros lo dividen en decretos, pero el punto es como se enfocan que tipifican y en qué caso aplican.

Por ende, aunque estas estén, debe crearse conciencia, así como los cibercriminales usan la ingeniería social, y los gustos de la gente para general los diferentes ataques, así mismo se debe enfocar las leyes buscar que las comunidades sepan de ella porque ya la redes, el internet, los avances tecnológicos, son una realidad y como todo trae sus cosas buenas y malas por ende es proporcionar las herramientas y conocimiento para poder actuar contra ello.

Es de destacar que el principal control tecnológico que las empresas latinoamericanas implementan están orientados al uso que proveen los antivirus, bien conocido como antimalware, ya que su principal función es el de proteger de diversos tipos de códigos maliciosos, virus y amenazas. Más, sin embargo, resultar paradójico que estos sean una de las principales fuentes y puente generadores de estos ataques en primer lugar.

Como primera contramedida a tomar serian el manejo de la seguridad para prevenir ataques de intrusos es a gestión de las contraseñas y la gestión de los riegos de la información y es que se sabe que una contraseña tiene las siguientes características:[37]

- Permitir o denegar el acceso a un usuario al sistema
- Mejorar los privilegios del usuario al que les asigne su respectivo rol
- Generar, ofrecer, mejorar y optimizar políticas de seguridad enfocadas a las empresas y organizaciones.

Estas medidas son sugeridas en el contexto de que se puede hacer mucho más antes de los ataques planificando y administrando los riesgos además enfocando esfuerzos en proteger las redes, sistemas entre otros. Porque el costo de reparar los daños es usualmente mayor.

Y cuando estos sucedan aplicar dependiendo de los daños, tipos de ataques y perjuicios las leyes que Colombia tenga, para regular los acontecimientos y envergadura de cada tipo de delito.

[37] Solvetic“Tipos de ataques informáticos e intrusos y cómo detectarlos” {jun 24 2016} {en línea} Disponible en: (https://www.solvetic.com/page/noticias/s/profesionales/tipos-de-ataques-informaticos-e-intrusos-y-como-detectarlos)

## 5.4 Marco conceptual

Para entrar en contexto, se realizará una descripción de los 9 ataques más comunes en el mundo y Latinoamérica podemos ver que las vulnerabilidades se presentan desde diferentes enfoques y lugares.

1. Robos en cajeros automáticos y puntos de venta: los cuales se dan a través de malware, con el fin de clonar tarjetas, programar cajeros automáticos para arrojar el dinero entre otros.

2. Exempleados enojados con una empresa: los cuales usan lo que aprendieron para vulnerar la seguridad usualmente usando sus contraseñas antiguas “no políticas de contraseñas y control de usuarios “, quienes suelen revelar información confidencial o estratégica, principalmente trabajadores de compañías que manejan dinero".

3. Incremento de los ataques de malware contra los celulares: los cuales son un objetivo muy codiciado y exequible últimamente porque con el incremento de uso de estos dispositivos los cuales poseen acceso a casi todo lo relacionado con el usuario, incluyendo cuentas de banco entre otros datos que son sensibles y privados.

4. Infecciones de ransomware: este tipo de malware se ha vuelto muy popular debido a que lo que hace es un software malicioso que delincuentes instalan en un PC sin consentimiento y que les da la capacidad de bloquear un equipo de forma remota, bloqueando el acceso a los datos, de ahí se pide una suma por devolver el control de este.

5. Ataques regionales dirigidos: el cual funciona por medio del uso de técnicas de cifrado y de cuan protegida la información se encuentra y por quienes es exequible aprovechando las tecnologías para proteger pero que pueden ser usadas y por ende por motivos de privacidad para comunicarse y generar problemas a los demás[38].

6- Las botnets ilegales: que permiten a los usuarios tomar el control remoto de una computadora sin el consentimiento del propietario, son una de las herramientas favoritas entre los hackers criminales[39].

[38]CNN –“Las 5 formas de cibercrimen que marcarán el 2016 en América Latina” {2016} - {en línea} Disponible en: (Http://cnnespanol.cnn.com/2015/11/20/las-5-formas-de-cibercrimen-que-marcaran-el-2016-en-america-latina/)

[39] organized crime in the Americas, “¿Can Latin American Governments Keep Up with Cyber Criminals? “, (2016) insight Crime, {en línea} Disponible en: (http://www.insightcrime.org/news-analysis/can-latin-american-govt-keep-up-with-cyber-criminals)

7- Las estafas vía vishing y smishing: corresponden a ataques que se generan por medio de la difusión de un mensaje o correo y posterior llamada del delincuente, los premios por parte de operadores de telefonía celular y almacenes de cadena, las falsas ofertas en bolsas de empleo virtuales y la falsa llamada del sobrino retenido[40].

8- Uso de monedas virtuales: como formas de pago: conocidas también como criptomonedas el cual es conocido actualmente como el fenómeno revolucionario relacionado a comercio y movimientos económicos donde recientemente, han alcanzado una variedad de más de 175 tipos diferentes, siendo el Bitcoin la más popular hasta el momento, estas tienen la particularidad de que no son generadas ni reguladas por ningún banco, autoridad central o entidad monetaria y el cual presenta variaciones haciéndola muy inestable, lo que hace que las criptomonedas se convierten en una opción viable y usada por los ciberdelincuentes en muchos casos, con el fin de recolectar el pago de sus víctimas sin correr el riesgo de ser vistos o de mostrar quienes son, permitiendo así su uso directo entre pares y diversos lugares sin control[41].

9- Uso de plataformas EBAY Y PAYPAL: como puente para ataques de phising y pahrming los cuales se dieron en mayo del 2014, eBay parecía estar pidiendo a los usuarios de PayPal, cambiar las contraseñas de acceso.[42], donde hay reportes que dicen que la compañía un par de meses antes había sido atacada por ciberdelincuentes, donde fueron las bases de datos lo que se vio afectado siendo las bases relacionadas a las cuentas privadas de algunos usuarios, dándole acceso a lo que sería la red interna, donde allí se genera el ataque, extrayendo de la base de datos los nombres de usuarios, teléfonos, direcciones de correo electrónico y contraseñas.
Además, es importante mirar la temática desde la prevención, y esto se logra proponiendo metodologías, controles y políticas de Protección contra los malware, ataques, amenazas, e implementando planes preventivos y medidas a considerar contra las diferentes vulnerabilidades y riegos que se puedan presentar.

[40] Gadelha, Silvia, Head of Financial Lines, Brasil at XL Catlin “Cybercrime in Latinoamérica” {2016}, {en línea} Disponible en: (Http://xlcatlin.com/fast-fast-forward/articles/cybercrime-in-latin-america)
[41] Enter.co s.a.s, “el nuevo blanco de los cibercriminales en Colombia son las empresas” (2017) {en línea} disponible en: (http://www.enter.co/chips-bits/seguridad/empresas-el-nuevo-blanco-de-los-cibercriminales-en-colombia/)
[42] Pandasecurity” los 6 ataques de seguridad más famosos de 2014 {2014} - {en línea} disponible en: (https://www.pandasecurity.com/spain/mediacenter/seguridad/los-6-ataques-de-seguridad-mas-famosos-de-2014/)

Vulnerabilidades y Amenazas: La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo, que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño[43]

Una Amenaza: es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los Elementos de Información.

Y de ahí que esta busque sobre toda la cosa mantener y preservar lo que se conoce como:

Las dimensiones de la seguridad informática: está conformada principalmente en:

- Confidencialidad
- Integridad
- Disponibilidad

Además, pueden tenerse en cuenta estas otras dimensiones que aportan a la seguridad informática dos aspectos importantes:

- Autenticidad
- Trazabilidad

La confidencialidad busca que la información que se considera importante o valiosa sea protegida, que se mantenga intacta y lejos de las personas que no tienen permitido el acceso a ella

La integridad de la información implica que los datos no tengan errores, no sean modificados sin permiso, o estén incompletos en pocas palabras estén corruptos.

La disponibilidad es lo que permite que la información siempre este activa, funcional y disponible en momento que se requiere, que no sea borrada por error o que sufra algún error.

La autenticidad es lo que nos permite identificar el gestor de la información. Como por ejemplo saber que quien manda la información es realmente de donde se generó, evitando suplantación de identidad.

[43] Gestión de Riesgo en la Seguridad Informática - amenazas vulnerabilidades - {en línea} Disponible en: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

La trazabilidad nos permite determinar todas y cada una de las acciones que realiza cada usuario, un histórico de los procedimientos a los que ha sido sujeto el archivo, dato o información. [44][45]

Criminalidad: son todas las acciones, causado por la intervención humana, que violan la ley y que están penadas por esta; y ciber crimen está relacionado a la cibernética o espacio digital.

Malware es un software escrito específicamente para dañar e infectar el sistema host. El malware incluye virus junto con otros tipos de software como troyanos, gusanos, spyware y adware. El malware avanzado como el ransomware se usa para cometer fraude financiero y extorsionar a los usuarios de computadoras,[46] estos entre otras amenazas, al tener diversos propósitos de uso, permite que los atacantes continuamente evolucionen las técnicas para propagar e infectar los sistemas informáticos, lo que hace que estas nuevas amenazas adapten su naturaleza y se vuelven cada vez más sofisticadas, aumentando en cantidad, complejidad y diversidad.

Virus: como se explicó, Virus es un tipo específico de malware por sí mismo. Es una pieza contagiosa de código que infecta el otro software en el sistema host y se propaga una vez que se ejecuta. Su actuar puede compararse como lo hace un parásito.

Adware: también se conoce como software compatible con publicidad. Es un software que genera anuncios con el fin de generar ingresos para su autor. Los anuncios se publican en la pantalla presentada al usuario en el momento de la instalación. El Adware está programado para examinar qué sitios de Internet, el usuario visita con frecuencia y para presentar e incluir anuncios relacionados. No todo el adware tiene una intención maliciosa, pero se convierte en un problema de todos modos porque daña el rendimiento del equipo y llega a ser molesto.

Spyware: este tipo de software malicioso, le espía, rastrea sus actividades en Internet. Ayuda al pirata informático a reunir información sobre el sistema de la víctima, sin el consentimiento de la víctima.

Worms: este tipo de malware se replica y destruye la información y los archivos guardados en la PC host.

[44] Seguinfo dimensiones de un sgsi - {en línea} (2007) Disponible en: <https://seguinfo.wordpress.com/2007/08/21/dimensiones-de-un-sgsi/>

[45] Las dimensiones de la seguridad de la información - {en línea} Disponible en: https://www.seguridadycontinuidad.com/las-dimensiones-de-la-seguridad-de-la-informacion

[46] Malware vs Virus: ¿Cuál es la diferencia? – antivirus cómodo {en línea} (2018) Disponible en: antivirus.comodo.com

Troyano: los troyanos son un tipo de virus diseñado para hacer que un usuario piense que es un programa seguro y ejecutarlo. Pueden estar programados para robar información personal y financiera, y luego hacerse cargo de los recursos de los archivos del sistema de la computadora host.

Ciberseguridad Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.[47]

Ciberdelincuencia son aquellas amenazas que por medio del uso de virus informáticos, malware y troyanos creados por estudiantes, jóvenes y desarrolladores entre otros entes, los cuales pueden dañar su ordenador.[48]

Hablando un poco de las políticas y controles que una organización puede implementar para gestionar y garantizar la protección de sus activos las cuales podría ser bajo la (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), la Gestión del Riesgo:[49]

1. Establecer una Política de la Organización al respecto: directrices generales de quién es responsable de cada cosa.
2. Establecer una Norma: objetivos a satisfacer para poder decir con propiedad que la amenaza ha sido conjurada.
3. Establecer unos Procedimientos: instrucciones paso a paso de qué hay que hacer.
4. Desplegar salvaguardas técnicas que efectivamente se enfrenten a las amenazas con capacidad para conjurarlas.
5. Desplegar controles que permitan saber que todo lo anterior está funcionando según lo previsto.

[47] Welivesecurity - ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia {en línea} (2015) Disponible en: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

[48] Kaspersky - Ciberdelincuencia y Ciberdelitos {en línea} (2012) Disponible en: https://www.kaspersky.es/resource-center/threats/computer-vandalism

[49] MAGERIT is the methodology of analysis and risk management developed by the High Council of Electronic Administration {en línea} (2012) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en#.Wqmh2ujOXDc

- Conviene llegar a un cierto equilibrio entre:

    - Salvaguardas Técnicas: en aplicaciones, equipos y comunicaciones.
    - Salvaguardas Físicas: protegiendo el entorno de trabajo de las personas y los equipos.
    - Medidas de Organización: de prevención y gestión de las incidencias.
    - Política de Personal: que, a fin de cuentas, es el eslabón imprescindible y más delicado política de contratación, formación permanente, organización de reporte de incidencias, plan de reacción y medidas disciplinarias.

## 6. METODOLOGIA UTILIZADA

El presente proyecto es una monografía que se basa en la revisión bibliográfica y analítica, por medio del desarrollo del tema de delitos informáticos y el cibercrimen a través de comparativos a partir de una línea base de investigación sobre el tema escogido. Por otro lado, se tomó como herramienta de recolección y análisis de información el análisis documental, desde las normas de tipificación de delitos informáticos, normatividad y revisión de convenios internacionales como el CONPES, comparativos de los distintos delitos y casos reales, análisis de la ley colombiana contra las leyes de Latinoamérica y otros países externos.

# 7. DETERMINAR LOS DELITOS INFORMÁTICOS Y CUÁLES ACTIVIDADES DELICTIVAS SE CATALOGAN DE ACUERDO A LA "ORGANIZACIÓN DE LAS NACIONES UNIDAS (ONU) EN EL CONVENIO DE CIBERDELINCUENCIA DE 2001"

## 7.1 Análisis y Comparativo Inicial

En este documento se pretende por medio de una revisión bibliográfica de la tipificación de los delitos informáticos en Colombia, así como la clasificación de los mismos según los artículos de la ley, el convenio de CONPES y que otras leyes o decretos se ven relacionados cuando se comenten dichos delitos, de ahí generar un análisis final sobre ellos. [50]

Como cualquier principio legislativo estipula no existe que delito sí para ello no existe sanción, es decir, se puede realizar una acción mientras no esté sancionada en la Ley, por ello es necesario que se identifiquen las acciones que pueden estar afectando al individuo o sociedad y que estas acciones sean catalogadas como delito para que sobre ellas se impongan sanciones, de ahí que se revisaran casos sucedidos en los últimos años y se tipificaran según la ley colombiana y los decretos que estén afectando, y desde el punto de vista del creciente uso de la tecnología informática y donde cada vez más se encuentra presente en muchos aspectos de la vida cotidiana; tales como: transacciones comerciales, procesos mecánicos industriales y laborales, domesticas. Constantemente nos vemos expuestos a ser víctimas de ataques informáticos,

Para poder analizar y determinar los delitos informáticos y como son catalogados según la ONU en el convenio de ciberdelincuencia del 2001 también conocido como CONPES y luego según la actual ley en Colombia, donde se analiza desde los conceptos de criminalidad o delincuencia informática, la forma de ser juzgados y penalizados desde el ámbito legal según las legislaciones de cada país y como este explica su envergadura. [51]

[50] Documento Conpes Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA {en línea} (2001) Disponible en: https://www.dnp.gov.co/CONPES/documentos-conpes/Paginas/documentos-conpes.aspx

[51] Convenio sobre ciberdelincuencia - {en línea} (2001) Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

El análisis jurisprudencial de los escasos supuestos que han llegado a los Juzgados y Tribunales penales, sobre todo en Colombia, se ha venido efectuando mayoritariamente desde una perspectiva clásica del Derecho Penal, en donde "lo digital, electrónico o informático", se ha venido tratando como una complementación a la inicial perspectiva tradicional, determinando consecuentemente su punibilidad o su impunidad legal penal , incluso su posible subsunción o no en los tipos delictivos existentes.[52]

Este convenio de Ciberdelincuencia De 2001. Se discute el tema de delito Informático con el fin de definir los diferentes delitos informáticos, como precedente a lo que sería en adelante la fuente principal para legislar acerca de este tipo de problemática que desde entonces cobraba fuerza y que se ha ido extendiendo y desarrollándose a la par de los diferentes avances tecnológicos. la tipología y tipificación de los Delitos informáticos, y como se deben manejar, y gracias a este ha permitido un mayor entendimiento en el área, [53] por parte de Colombia uno de los pioneros en implementar leyes que los clasifican y los tipifican.

El Convenio de Ciberdelincuencia define los Delitos Informáticos distribuidos, así:

1. Delitos contra la confidencialidad, la integridad, y la disponibilidad de los datos y sistemas informáticos.
   Art 1: Glosario de términos
   Art. 2: Acceso ilícito
   Art. 3: Interceptación ilícita
   Art. 4: Interferencia en los datos (Ataques a la integridad de los datos)
   Art. 5: Interferencia en el sistema (Ataques a la integridad del sistema)
   Art. 6: Abuso de los dispositivos

2. Delitos informáticos.
   Art. 7: Falsificación informática
   Art. 8: Fraude informático

3. Delitos relacionados con el contenido.
   Art. 9: Delitos informáticos relacionados con la pornografía infantil

[52] Caracterización de los delitos informáticos en Colombia [en línea] 2012 {disponible en} http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewFile/126/149

[53] Council of Europe, (2014).Convention on Cybercrim CETS No.: 185.Recuperado de http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=E

4. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.
   Art. 10: Delitos relacionados con infracciones de la propiedad intelectual y de los derechos [54]

### 7.2 Análisis de artículos incluidos en el documento de CONPES

Artículo 2: Acceso ilícito: “Acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático

Artículo 3: Interceptación ilícita: “la interceptación deliberada e ilegítima, por medios técnicos, digitales o electrónicos”.

Artículo 4: Interferencia en los datos: “la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos”

Artículo 5: Interferencia en el sistema: “la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños que de alguna forma que interfiera con su integridad”

Artículo 6: Abuso de los dispositivos: “La comisión deliberada e ilegítima que permita la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de

Artículo 7: Falsificación Informática: “cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos

Artículo 8: Fraude Informático: “los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante cualquier medio que tenga la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona”

Artículo 9: Delitos relacionados con la Pornografía Infantil: Todo lo relacionado a la Producción de Pornografía Infantil, oferta, difusión o transmisión, adquisición, posesión, utilizando sistemas informáticos

[54]Delitos relativos a la propiedad intelectual [en línea] {disponible en} http://www.portaley.com/delitos-informaticos/delitos-intelectual.shtml

## 7.3 Legislación en Colombia

La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes

La importancia de esta ley reside en lo que abarca y es desde la Protección de la información y de los datos que divide en dos capítulos: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos y De los atentados informáticos y otras infracciones.[55]

## 7.4 Análisis OTAN

Los lazos entre las diversas fuerzas armadas que conforman la OTAN están orientados en mejorar aspectos de campos específicos “como la mitigación de los efectos y las consecuencias de los desastres naturales originados por el cambio climático, la ciberdefensa, la cooperación en materia de guerra cibernética hasta los procedimientos militares, la gestión de riesgos y en el desminado”.[56]

Este tipo de acuerdo no es bilateral, sino uno de seguridad. Llamado Acuerdo de Seguridad de la Información entre Colombia y la OTAN, se firmó el 25 de junio de 2013 y el proceso se llevó a cabo durante los siguientes años hasta hacer oficial en el 2018 que Colombia entra a hacer parte como socio .[57]

el ingreso de Colombia a esta categoría que es muy específica, donde ya se encuentran países como Japón, como Australia, que es el de socio global. No quiere decir eso que sean miembros plenos” pero si es un avance en tema de defensa para Colombia. [58]

[55] ley de delitos informáticos en Colombia {en línea} 1997 - 2017 j. c. daccach. delta asesora disponible en: http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia
[56]Colombia formalizó su ingreso a la OTAN y se convierte así en el primer socio global latinoamericano http://www.france24.com/es/20180531-colombia-otan-bruselas-latinoamerica
[57] Cinco aspectos clave del ingreso de Colombia como socio de la OTAN {en línea} 2018 {disponible en}: http://misionverdad.com/TRAMA-GLOBAL/cinco-aspectos-sobre-colombia-como-socio-global-de-la-otan
[58] Colombia va a tener un estatus privilegiado de cooperación con la OTAN, de gran interés y utilidad para el país: Presidente Santos {en línea} 2018 {disponible en}: http://es.presidencia.gov.co/noticia/180528-Colombia-va-a-tener-un-estatus-privilegiado-de-cooperacion-con-la-OTAN-de-gran-interes-y-utilidad-para-el-pais-Presidente-Santos

## 7.5 Que son los delitos informáticos y que son las políticas de seguridad

Delitos Informáticos" son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático.[59]

El delito Informático implica actividades criminales que un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc., sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho.[60]

Las políticas de seguridad informática van siempre de la mano en cada país con la promulgación de leyes estatutarias incluidas en el código penal, en donde se pretende imponer sanciones de tipo penal y económico, a todo tipo de comportamientos ilícitos que traen consigo las nuevas formas de delincuencia cibernética que causa pérdidas económicas y de información.

En Colombia eso no es la excepción, donde para dar cumplimiento a esto se creó: La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las organizaciones se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales, divididos en dos capítulos:

[59] ciberdelincuentes y cibervictimas {en línea} 2010 (disponible en:) https://www.ehu.eus/documents/1736829/2010409/clc+91+ciberdelincuentes+y+cibervictimas.pdf

[60] caracterización de los delitos informáticos en Colombia {en línea} 2012 (disponible en:) http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewfile/126/149

**Primer capitulo**

- artículo 269a: acceso abusivo a un sistema informático.
- artículo 269b: obstaculización ilegítima de sistema informático o red de telecomunicación.
- artículo 269c: interceptación de datos informáticos.
- artículo 269d: daño informático
- artículo 269e: uso de software malicioso.
- artículo 269f: violación de datos personales.
- artículo 269g: suplantación de sitios web
- artículo 269h: agravaciones

**Segundo capitulo**

- artículo 269i: hurto por medios informáticos y semejantes.
- artículo 269j: transferencia no consentida de activos.

A parte de estas leyes Colombia posee leyes y decretos que permiten regular la información y datos relacionados al manejo, tratamiento, trasmisión y protección tales como por ejemplo:[61][62]

Ley 1712 de 2014“Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.

Código Penal Art. 199. Espionaje Art. 258. Utilización indebida de información[63]

- Art. 418. Revelación de Secreto
- Art. 419. Utilización de asunto sometido a secreto o reserva
- Art. 420. Utilización indebida de información oficial
- Artículo 431. Utilización indebida de información obtenida en el ejercicio de la función pública
- Artículo 463. Espionaje

[61] Los delitos informáticos desde el punto de vista del Derecho {en línea} 2017 (disponible en:) https://www.kennedy.edu.ar/noticia/los-delitos-informaticos-desde-el-punto-de-vista-del-derecho/

[62] Delitos informáticos: mal uso de Tecnologías de Información y Comunicación {en línea} 2009 (disponible en:) http://noticias.universia.net.co/vida-universitaria/noticia/2009/09/04/236295/delitos-informaticos-mal-uso-tecnologias-informacion-comunicacion.html

[63] Colombia el primer país que penaliza los delitos informáticos- la patria [disponible en] (en línea) http://repository.unad.edu.co/bitstream/10596/2668/5/76323713.pdf

Tipos de Amenazas

- Virus
- Gusanos
- Bomba lógica o cronológica

Tipo de delitos

- Sabotaje informático
- Acceso no autorizado a sistemas o servicios
- Reproducción no autorizada de programas informáticos de protección legal.
- Manipulación de datos de entrada y/o salida
- Manipulación de programas
- Fraude efectuado por manipulación informática.

La Ley 1266 de 2008 definió el término dato personal como "cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica". Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la ley obliga a quien "sustraiga" e "intercepte" dichos datos a pedir autorización al titular de los mismos.

También es bueno mencionar otras leyes que regulan el tratamiento de la información y los datos en Colombia tales como

- Constitución Política Artículo 15. Reconoce como Derecho Fundamental el Habeas Data Artículo 20. Libertad de Información[64]
- Ley 527 de 1999. "Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"
- Ley 1266 de 2008. "Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países
- Ley 1273 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"

[64] Santiago Cisneros- normas y leyes que existen en Colombia para delitos informáticos –(en línea) [disponible en]https://www.slideshare.net/santiagocisneros6/normas-y-leyes-que-existen-en-colombia-para-delitos-informaticos

- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la Protección de Datos Personales”, esta última tiene como desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.
- Ley 527 de agosto de 1999: Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación (parte de una PKI) y se dictan otras disposiciones
- Decreto 1747 de septiembre de 2000: Se reglamenta parcialmente la ley 527 en lo relacionado con las entidades de certificación, los certificados y las firmas digitales65 Leyes las cuales aún todavía requieren revisión porque entre ella existen ciertas discrepancias. [666768]

A través de la información, se han podido identificar diferentes tipos de delitos informáticos que se cometen en nuestro país, entre los que se encuentran aquellos que:

- Afectan el patrimonio económico: banca virtual, phishing, key logers, falsas páginas, venta a través de portales de compra y venta, falsos premios.
- Buscan el abuso de menores: comercializan videos, fotografía, audio, texto, falsas agencias, salas de chat.
- Afectan la propiedad intelectual: descargas de programas y comercialización de obras sin pagar derechos de autor.
- Afectan la información como bien jurídico: como por ejemplo cuando algunos empleados usan sus privilegios o permisos para acceder a información que es secreto de la empresa y luego entregarla a la competencia, teniendo como base el desarrollo que han tenido. Robos de información privilegiada. [69]

Colombia es uno de los países pioneros en reglamentación respecto al trámite de mensajes digitales (comercio electrónico).

---

[65] banrep leyes- {disponible en][en línea] http://www.banrep.gov.co/es/temas/6923
[66] la patria {disponible en][en línea http://www.lapatria.com/tecnologia/colombia-el-primer-pais-que-penaliza-los-delitos-informaticos-1980
[67]secretaria de gobierno {disponible en] 2012 [en línea http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html
[68] ¿por qué las personas cometen delitos informáticos?, por bobby stocks {en línea} 2001-2018, leaf group ltd (disponible en:) https://techlandia.com/personas-cometen-delitos-informaticos-sobre_96220/
[69] Comunidad americana -edu. Articulo realizar {en línea} (disponible en: ) http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewfile/126/149

El marco legal colombiano comprende: entre los delitos informáticos de mayor prevalencia en los países, latinoamericanos se tiene: abuso de los dispositivos, falsedad informática, fraude o estafa informática, interceptación ilícita, atentado contra la integridad del sistema, acceso ilícito, pornografía infantil, atentado contra la integridad de los datos. [70]

Identificando las normativas vigentes en Colombia y por medio de un análisis que pretende relacionar e investigar sobre casos reales verificables ocurridos en Colombia y Latinoamérica sobre algunos delitos informáticos elegidos:

Grooming Es una nueva forma de acoso y abuso hacia niños y jóvenes que se ha venido popularizando con el auge de las TIC, principalmente los chats y redes sociales. Inicia con una simple conversación virtual, en la que el adulto se hace pasar por otra persona, normalmente, por una de la misma edad de víctima con el fin de extorsionar al menor, e incluso llegar a la parte de pornografía infantil si este solicitase imágenes del menor.

El grooming se está empezando a tipificar como un delito preparatorio para otro de carácter sexual más grave como lo es el abuso sexual de menores de edad.[71]

Ejemplo en algunos países como: Alemania se pena con privación de libertad de 3 meses a 5 años al que ejerza influencia sobre el menor por medio de la exhibición de ilustraciones o representaciones pornográficas o por dispositivos sonoros de contenido pornográfico o por conversaciones en el mismo sentido.

Australia también pena con 15 años de prisión el uso de Internet para buscar actividades sexuales con personas menores de 16 años de edad.[72]

El grooming aún “no está tipificado como delito en Colombia” aunque el acto del mismo puede llegar a consecuencias más agravantes como el abuso de los menos y pornografía infantil.

Caso Real:

El imitador de cantantes: Este hombre de 23 años –sin identificar aún por parte de las autoridades– contaba con dos perfiles falsos en Facebook, a nombre del cantante Maluma. A través de estas presencias en línea se ganaba la confianza de niñas de entre 9 y 12 años, a quienes pedía fotografías y videos en que aparecieran desnudas o en ropa interior.

---

[70] Estudios psicológicos de los delincuentes informáticos (aproximación a los perfiles de personalidad de los sujetos que realizar {en línea} 2006-2016 (disponible en:)

[71] Es groorming un delito – internet-gromming {en línea} (disponible en:) https://internet-grooming.net/es-un-delito-el-grooming/

[72] camilo Gutiérrez Amaya Welivesecurity los 10 delitos informáticos por lo que se dieron condenas en la historia {en línea} 2013 disponible en: https://www.welivesecurity.com/la-es/2013/11/12/top-10-condenados-por-delitos-informaticos-quienes-fueron-primeros-historia/

Una vez las menores de edad le enviaban el material que él solicitaba, las amenazaba con publicar las imágenes o enviárselas a sus padres a menos que accedieran a sostener relaciones sexuales con él. En el momento de la captura, la Policía realizó la incautación de 15 discos duros, 5 tabletas, 9 celulares, 15 memorias micro SD y 2 memorias USB, que utilizaba para almacenar y distribuir las imágenes.

Ley colombiana que lo tipifica

- Artículo 269F: Violación de datos personales.

Tipificación según CONPES:

- Artículo 9: Delitos relacionados con la Pornografía Infantil

Ingeniería Social: Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social.

Los ataques informáticos que usan ingeniería social no aprovechan una falla en el software, sino que usan técnicas de ingeniería social para conseguir las credenciales necesarias para vulnerar la seguridad informática.

Por eso, a veces poco importa las medidas de seguridad tecnológicas que implementes si las personas están mandando su clave por correo electrónico. Como parte de la estrategia de seguridad de tu compañía, tienes que hacer un gigantesco esfuerzo para evitar que los criminales informáticos implementen técnicas de ingeniería social para entrar a tus sistemas.[73]

Caso Real:

Los casos aquí abundan y no hacen más que demostrar cuánto les rinde a los cibercriminales aprovechar noticias de famosos fallecidos o incluso inventar que murieron, gracias a lo cual consiguen que cientos de usuarios curiosos hagan clic en enlaces engañosos. Por mencionar algunos ejemplos, tenemos la falsa muerte del cantante Ricardo Arjona y también la del automovilista Michael Schumacher, el suicidio del actor Robin Williams o el rumor de que Michael Jackson estaba vivo.

[73] Enter.co – Guías lleva a tu negocio a internet ingeniería social {en línea} (disponible en:) http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/

Ley colombiana que lo tipifica

- Artículo 269I: Hurto por medios informáticos y semejantes.
- Artículo 269J: Transferencia no consentida de activos.

Tipificación según CONPES:

- Art. 5: Interferencia en el sistema (Ataques a la integridad del sistema)

Botnets: Un botnet es una serie de sistemas comprometidos entre los cuales podemos encontrar, servidores, redes, servicios móviles, los cuales usualmente se les conoce como computadoras zombis las cuales al estar infectas y utilizando programas maliciosos como malware permiten realizar ataques controlados.

Las botnets se utilizan comúnmente para enviar spam de correo electrónico, fraude con solo dar clics y generar tráfico malicioso para ataques distribuidos de denegación de servicio. , los botnets son muy populares en el mundo del malware porque estos pueden propagar infecciones usando los recursos del sitio web, donde los bots son propagados utilizando medios de trasporte como ejemplo gusanos con correos electrónicos o utilizando huecos en el sistema.[74]

Una Bonet es un conjunto de Pc infectados y controlados por un artífice de forma remota, a cada equipo de esa red se le llama bots o zombi pueden existir 2 métodos para atacar por páginas web vulnerable o vía email.

Caso Real:

El control de miles de ordenadores mediante este tipo de software malicioso se realiza a través de un panel de control desarrollado por delincuentes. A la estructura creada por miles de computadoras infectadas se les denomina botnets.

El ciclo de vida de una botnet es complejo. Pueden estar activas unos pocos meses o durante años. La ONU estima que en 2011 más de un millón de direcciones IP únicas dirigían y controlaban botnets a nivel mundial.

Ley colombiana que lo tipifica

- Artículo 269C: Interceptación de datos informáticos.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.

[74]Botnets, techtarget {en línea} 2017 (disponible en:) http://searchsecurity.techtarget.com/definition/botnet

Tipificación según CONPES:

- Artículo 3: Interceptación ilícita: “la interceptación deliberada e ilegítima, por medios técnicos, digitales o electrónicos”.

DoS: Un ataque de denegación de servicio distribuido (DDoS) es un intento de hacer que un servicio en línea no esté disponible al abrumarlo con tráfico de múltiples fuentes. Apuntan a una gran variedad de recursos importantes, desde bancos hasta sitios web de noticias, y presentan un gran desafío para asegurarse de que las personas puedan publicar y acceder a información importante.[75]

Los ataques distribuidos de denegación de servicio (DDoS) son una subclase de ataques de denegación de servicio (DoS). Un ataque DDoS implica múltiples dispositivos conectados en línea, conocidos colectivamente como botnet, que se utilizan para abrumar a un sitio web objetivo con tráfico falso. A diferencia de otros tipos de ataques, estos no intentan violar su perímetro de seguridad. Por el contrario, su objetivo es hacer que su sitio web y servidores no estén disponibles para usuarios legítimos. DDoS también se puede usar como pantalla de humo para otras actividades maliciosas y para eliminar dispositivos de seguridad, incumpliendo el perímetro de seguridad del objetivo.[76]

Un ataque DDoS exitoso es un evento muy notable que afecta a toda la base de usuarios en línea. Esto lo convierte en un arma popular de elección para hacktivistas, ciber vándalos, extorsionadores y cualquier otra persona que busque hacer un punto o defender una causa.

Los asaltos DDoS a menudo duran días, semanas o incluso meses a la vez, lo que los hace extremadamente destructivos para cualquier organización en línea. Entre otras cosas, los ataques DDoS pueden conducir a la pérdida de ingresos, erosionar la confianza del consumidor, forzar a las organizaciones a gastar fortunas en compensaciones y causar daños a la reputación a largo plazo.

Caso Real:

Con tan solo cuatro días de diferencia, se registraron los dos ataques “distribuidos de denegación de servicio” (DDoS, por sus siglas en inglés) más grandes de los que se haya tenido registro hasta el momento. El primero de ellos ocurrió el miércoles 28 de febrero, cuando GitHub quedó fuera de servicio desde las 17:21 a las 17:26 (UTC) y fuera de servicio, pero de manera intermitente, desde las 17.26 a las 17:30 horas, explicó la empresa en una publicación realizada en su página web.

[75]Ddos attack definitions - ddospedia {en línea} 2017 (disponible en:) radware ltd. https://security.radware.com/ddos-knowledge-center/ddospedia/botnet/

[76] What is a ddos attack? ©2013 ddos data https://www.digitalattackmap.com/understanding-ddos/

El segundo fue el pasado lunes 4 de marzo, cuando la empresa de seguridad y monitoreo Arbor Networks afirmara que su sistema de datos de amenazas DDoS y tráfico global, llamado ATLAS, registró un nuevo ataque de esta naturaleza contra el sitio web de sus clientes, cuyo nombre no fue develado, en Estados Unidos.

Ley colombiana que lo tipifica

- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. - artículo 269d: daño informático
- Artículo 269E: Uso de software malicioso.[77][78]

Tipificación según CONPES:

- Artículo 3: Interceptación ilícita: “la interceptación deliberada e ilegítima, por medios técnicos, digitales o electrónicos”.

Vishing**:** Variante del tradicional phishing, conocido también como phishing a través de VoIP. La víctima se le indica mediante una llamada, grabación o mensaje de texto, un número de teléfono al que comunicarse, utilizando un señuelo como que sus tarjetas de crédito han sido utilizadas fraudulentamente, o que se requiere actualización de datos, ofreciendo productos u ofertas, obsequios, entre otros engaños y lograr que el usuario suministre información al delincuente que le permita realizar compras y transacciones por internet o vía telefónica.

El Vishing se basa en la ingeniería social que establece que en cualquier sistema "los usuarios son el eslabón débil". En la práctica, comúnmente se practica este tipo de ciberdelito fingiendo ser un empleado de un banco o organización, un compañero de trabajo, un técnico o un cliente. Se utiliza el envío de solicitudes que requieren la renovación de permisos de acceso a páginas web, documentos falsos solicitando respuestas que revelan información sensible, o vulneran las políticas de seguridad.

Caso Real:

El Grupo de Delitos Telemáticos de la Guardia Civil alerta en su portal de una variante del tradicional phishing (suplantación de la identidad…) conocido como vishing o phishing a través de VoIP (Voice over IP). El phishing tradicional es una modalidad de delito por Internet en el que se nos intenta hacer creer que el banco nos ha remitido un correo electrónico para conseguir que vayamos a una web que simula ser la del banco, e introduzcamos nuestras claves de acceso, el número de tarjeta u otros datos confidenciales.

[77] Distributed denial of service (ddos) attack -2000 - 2017, techtarget {en línea} 2017 (disponible en: http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack

[78]What does ddos mean? 2017 imperva {en línea} 2017 (disponible en: https://www.incapsula.com/ddos/denial-of-service.html

Ley colombiana que lo tipifica

- Artículo 269A: acceso abusivo a un sistema informático.

- Artículo 269b: obstaculización ilegítima de sistema informático o red de telecomunicación.

Tipificación según CONPES:

- Art. 5: Interferencia en el sistema (Ataques a la integridad del sistema)
- Art. 6: Abuso de los dispositivos

El Hacking, es descrito como una conducta que describe el acceso no autorizado a un equipo o sistema informático cuyo objetivo tiene por objetivo la violación de derechos intelectuales, sería bueno agregarle algo más sobre hacking y cracking

Caso Real: Con la aparición de las nuevas tecnologías también se han desarrollado formas de estafa, robos o ataques a través de internet. En los últimos años, algunos de los llamados 'hackers' han caído luego de los seguimientos policiales a sus ciberdelitos, como 'Oroboruo', el paisa que atacó días antes de las votaciones del plebiscito a la Registraduria.[79]

El caso está a la espera de ser judicializado y Será procesado por los delitos de acceso abusivo a un sistema informático y daño informático", indicó el director general de la Policía Nacional, general Jorge Hernando Nieto Rojas.[80]

Ley colombiana que lo tipifica

- artículo 269a: acceso abusivo a un sistema informático y artículo 269h circunstancias de agravación punitiva. y artículo 269d: daño informático

[79] El tiempo delito de hackers Colombia {en línea} (disponible en:) http://www.eltiempo.com/justicia/cortes/delitos-de-hackers-en-colombia-52232

[80] El tiempo delito de hackers Colombia {en línea} (disponible en:) http://www.eltiempo.com/justicia/cortes/delitos-de-hackers-en-colombia-52232

Tipificación según CONPES:

- Art. 2: Acceso ilícito

Por medio del Phishing es posible el envío de correos electrónicos que aparentan, provenir de fuentes fidedignas como por ejemplo entidades bancarias cuyo objetivo es obtener los datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude. Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsa. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador.

Caso real: El detenido y acusado, traficó con los datos de unas mil cien tarjetas de crédito y/o débito que vendía a través de foros de la llamada “darknet” o red profunda, sector de internet donde las conexiones no pueden ser rastreadas, y con los que finalmente se han defraudado en torno a 1,1 millones de euros.

Usualmente cualquier tipo de intento de fraude, como el phishing o el robo de datos de páginas web inseguras, son los delitos informáticos que más se cometen en Colombia, seguido de la pornografía infantil que, en los últimos meses, se ha llevado toda la atención por el caso del ‘Lobo Feroz’. [81]

La alerta saltó cuando la entidad bancaria BBVA detectó que se estaba haciendo un uso fraudulento de algunas tarjetas de crédito y débito, algunas de las cuales pertenecientes a empleados de la propia entidad, por lo que interpuso la correspondiente denuncia ante el cuerpo de la Policía Nacional.[82]

Ley colombiana que lo tipifica

- artículo 269e: Uso de software malicioso y
- artículo 269g: Suplantación de sitios web para capturar datos personales.

Tipificación según CONPES:

- Art. 7: Falsificación informática
- Art. 8: Fraude informático

[81] Análisis de riesgos iso 27005 vs margerit y otras metodologías {en línea} (disponible en:) https://delitosinformaticos.com/10/2009/proteccion-de-datos/analisis-de-riesgos-iso-27005-vs-magerit-y-otras-metodologias

[82] El tiempo delito de hackers Colombia {en línea} (disponible en:) http://www.eltiempo.com/justicia/cortes/delitos-de-hackers-en-colombia-52232

Evil twins: Son redes inalámbricas Wi-Fi que aparentan ofrecer conexiones a internet, pero solo son una fachada que sirve para robar cualquier número de tarjeta de crédito y contraseñas que se digite usando la conexión.

Caso Real: la técnica conocida como “Evil Twin” se basa en el hecho de que pueden existir dos AP con el mismo SSID y que utilizando utilidades como “aireplay-ng” se pueden enviar paquetes de “DeAuth” a todos los clientes conectados a un AP determinado, lo que al final puede desembocar en un ataque de denegación de servicio. Cuando un cliente se encuentra conectado en una red HotSpot, por ejemplo, en un aeropuerto, un bar, un restaurante, un MacDonalds, normalmente no existen mecanismos de autenticación intermedios, es decir, son redes que normalmente se encuentran abiertas al público en general, lo que facilita enormemente las acciones de un atacante.

Ley colombiana que lo tipifica

- Artículo 269G: Suplantación de sitios web para capturar datos personales.
- Artículo 269i: Hurto por medios informáticos y semejantes

Tipificación según CONPES:

- Art. 5: Interferencia en el sistema (Ataques a la integridad del sistema)
- Art. 6: Abuso de los dispositivos

El Pharming es conocido como un tipo de fraude en línea, el cual comparte similitudes con el phising debido a que los “agricultores o pharmers le tienen confianza al link del cual son víctimas, y esto se da porque estos sitios web fraudulentos son iguales a los conocidos, pero roban información confidencial.[83]

Caso real: la propagación de un archivo llamado “videotestimonio.mpeg.exe” que llega hasta el usuario a través de un correo electrónico simulando ser una noticia sobre un supuesto secuestro en México: El archivo descargado, detectado por ESET NOD32 como BAT/Qhost.NAT, en primera instancia, posee doble extensión, una vieja técnica de engaño que responde a una estrategia de Ingeniería Social aplicada sobre el archivo. Al ser ejecutado, se abre el navegador web predeterminado mostrando una página de YouTube.

[83]Tuabogadodefensor delitos informáticos {en línea} 2015 disponible en: http://www.tuabogadodefensor.com/delitos-informaticos/

Sin embargo, de manera transparente, el código malicioso realiza lo que se conoce como pharming local que modifica el archivo hosts con información maliciosa realizando en síntesis un ataque de pharming local orientado a re direccionar al usuario de manera subrepticia hacia un sitio web falso, en este caso, de las entidades bancarias Banamex y Bancomer de México.[84]

Ley colombiana que lo tipifica

- Artículo 269J: Transferencia no consentida de activos.
- Artículo 269g: Suplantación de sitios web para capturar datos personales.
- Artículo 269i: Surto por medios informáticos y semejantes

Tipificación según CONPES:

- Art. 7: Falsificación informática
- Art. 8: Fraude informático

Spamming: Consiste en el envío masivo de información no solicitada por medio del correo electrónico, generalmente con fines publicitarios.

Caso Real: A lo largo de 2016 el spam fraudulento usó los grandes eventos deportivos COMO el Campeonato de Europa de fútbol, los Juegos Olímpicos en Brasil y en los mundiales de fútbol de 2018 y 2022. Por lo general, los spammers enviaron avisos falsos de premios de la lotería dedicada a uno de estos eventos deportivos. El contenido de los mensajes falsos no se caracterizó por su originalidad sino los estafadores afirmaban que la lotería la llevó a cabo la organización oficial y la dirección del destinatario se había seleccionado al azar de entre millones de otras direcciones. Para recibir el dinero del premio, el destinatario tenía que responder al mensaje y proporcionar la información personal requerida.

Ley colombiana que lo tipifica

- Artículo 269J: Transferencia no consentida de activos.

Tipificación según CONPES:

- Art. 4: Interferencia en los datos (Ataques a la integridad de los datos)
-Art. 2: Acceso ilícito

[84] Camilo Gutiérrez Amaya Welivesecurity los 10 delitos informáticos por lo que se dieron condenas en la historia {en línea} 2013 disponible en: https://www.welivesecurity.com/la-es/2013/11/12/top-10-condenados-por-delitos-informaticos-quienes-fueron-primeros-historia/

Clasificación de los delitos informáticos Según la ONU

La Organización de Naciones Unidas (ONU) reconocen los siguientes tipos de delitos informáticos:

Fraudes cometidos mediante manipulación de computadoras

Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir o los que son cometidos por medio de la manipulación de programas el cual consiste en modificar los programas existentes en el sistema o en insertar nuevos programas o rutinas.

Manipulación de los datos de entrada

Donde tiene objeto cuando se alteran datos de los documentos almacenados en forma computarizada o usarse como instrumento donde las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.

Daños o modificaciones de programas o datos computarizados

Por medio de acceso no autorizado a servicios y sistemas informáticos estos accesos se pueden realizar por diversos motivos, desde la simple curiosidad hasta el sabotaje o espionaje informático, reproducción no autorizada de programas informáticos de protección legal la cual puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales.

Este problema ha logrado alcanzado dimensiones transnacionales con el tráfico de estos activos a través de las redes de telecomunicaciones modernas. Al respecto, se considera, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

Ahora, existen delitos que están apenas en análisis y tipificación en diferentes países donde, se presentan diferentes modalidades de delitos que hasta ahora se están conociendo, los cuales se cometen a través del uso de redes sociales como lo son pharming, phising e ingeniería social entre otros que aún se están tratando de clasificar para realizar un tratamiento penal contra los mismos y contra las personas que los cometen, dentro de estos se encuentran:

- Ciber Bulliying: este delito consiste en la intimidación y agresión utilizando estos medios entrando en un tipo de atentado contra la moral y la integridad de la persona.

- Perfiles falsos: este delito es un tipo de suplantación de identidad, pero en este caso la finalidad es atentar contra la dignidad e integridad moral y psicológica de las personas por medio de publicaciones que usualmente son para amedrentar al usuario.

- Pornografía infantil: este delito tiene alta incidencia, puesto que en las redes sociales abundan los pedófilos en busca de menores que inocentemente son seducidos al ser contactados por el criminal este acto que se puede tomar como preparatorio es lo que actualmente se conoce como gromming, el cual busca ganarse su confianza para luego obtener videos y fotografías de tipo sexual de los menores, material que después es difundido por internet.

- Sexting: se trata de compartir contenidos íntimos a través de mensajería móvil como por ejemplo whatsapp o chat de cualquier otra red social, en donde en primera medida se busca un encuentro sexual sin transcendencia que luego puede llegar a algo más explícito de acuerdo a la situación. Este tipo de actuaciones ponen en riesgo la intimidad del emisor del mensaje, debido a que el contenido queda expuesto a graves riesgos como la publicación de este tipo de contenidos

Lo más difícil en este tipo de delitos y ataques es más difícil ponerle un alto, porque implica la concientización de los usuarios sobre los peligros de usar su privacidad y mostrarla públicamente porque les ponen en bandeja de plata a los delincuentes toda la información necesaria o los puntos débiles, todo frente a este fenómeno creciente y más aun con el auge de las redes sociales y sus medios de comunicación que cada vez son más versátiles.

Ahora cuando se tipifica los delitos y clasificación de los delitos informáticos también es importante entender el trasfondo desde la perspectiva de “los perfiles criminológicos” que lleva a los usuarios a realizar estas acciones negativas por medio de medios digitales y electrónicos[85]

Por ende, analizaremos un poco como influye a la hora de imputar un cargo y penalizaciones a tales acciones[86]

El perfil criminológico del delincuente informático, es una persona que se puede decir que es especial, ya que utiliza su inteligencia superior a la de los demás en la parte informática, para poder realizar delitos de esta índole, suelen ser personas

[85] Caracterización de los delitos informáticos en Colombia {en línea} 2012 (disponible en:) http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewfile/126/149

[86] ¿Por qué las personas cometen delitos informáticos?, Por bobby stocks {en línea} 2001-2018, Leaf Group Ltd (disponible en:) https://techlandia.com/personas-cometen-delitos-informaticos-sobre_96220/

pocos sociables y sus delitos los comenten en las horas de la noche, donde entran a ordenadores sin permiso, requisan, copian y extraen información privada.[87]

"un hacker es solo un curioso, un investigador".

en la información encontrada sobre el tema, nos exponen que estos delincuentes informáticos desarrollan este tipo de actividades en ciudades grandes, odian las burocracias y nos dice que estas personas suelen odiar los dibujos animados, porque les pareen aburridos, estas personas critican la estructura social como la cultural, creen que los nerds son unos idiotas. Según el estudio dice que detrás de un delincuente informático hay un autodidacta, encuentran un ámbito propicio en áreas académicas, fundamentalmente en carreras de especialización tales como ingeniería electrónica, informática y en orden decreciente en la física, matemáticas, lingüística y filosofía. [88]

Estas personas por lo general tienen un alto coeficiente intelectual, son curiosos y tienen una facilidad para las abstracciones intelectuales; les gusta la novedad, y son atraídos por lo intelectual; son a veces egocéntricos y casi nunca están conformes con lo que hacen. su inteligencia la dirigen para retener gran cantidad de detalles, que luego la usaran para su provecho final, son personas adictas a la red virtual e internet jamás logran poder llegar a un grado de satisfacción, pueden pasar horas y horas tratando de encontrar algo novedoso o cometiendo su delito.[89]

[87] Perfiles de personalidad de los delincuentes informáticos psicopsi {en línea} 2014 disponible en: http://psicopsi.com/Estudios-psicologicos-de-los-delincuentes-informaticos-Aproximacion-a-los-perfiles-de-personalidad-de-los-sujetos-que-realizaron

[88] Tuabogadodefensor delitos informáticos {en línea} 2015 disponible en: http://www.tuabogadodefensor.com/delitos-informaticos/

[89] Informaticaforenseuccaraucacolombia {en línea} 2014 disponible en: http://informaticaforenseuccaraucacolombia.blogspot.com.co/2014/03/el-perfil-criminologico-del-delincuente.html

## 8. REVISAR Y EXPONER EL PANORAMA DE LOS CIBERCRÍMENES QUE AFECTAN EN MAYOR MEDIDA A LATINOAMÉRICA

### 8.1 Analizar la evolución de la criminalidad informática

A partir de comparativos, revisión bibliográfica de los acontecimientos que han venido surgiendo a través de los años, y los avances de las nuevas tecnologías tanto en la parte positiva como la implementación de ella en la evolución de los diferentes tipos de ataques y delitos informáticos con el uso de métodos y en la ampliación y extensión cualitativa y cuantitativa de las posibles víctimas de tales ataques, hacen que en los últimos años hayan aumentado considerablemente no sólo los perjuicios y daños efectivos en los ámbitos personal o de la intimidad sino que también se ha visto afectada áreas como la económica, patrimonial y de seguridad jurídica, con el agravante y exposición al peligro y riesgo en de los bienes jurídicos sociales o colectivos , Entre los delitos informáticos de mayor prevalencia en los países latinoamericanos se tiene: abuso de los dispositivos, falsedad informática, fraude o estafa informática, interceptación ilícita, atentado contra la integridad del sistema, acceso ilícito, pornografía infantil, atentado contra la integridad de los datos, desde la parte jurídica, los países latinoamericanos carecen de una homogeneización normativa penal aplicable a los delitos informáticos. Es por ello, que cada país tiene su propia base jurídica para regular ante la problemática. En su mayoría lo que han hecho es modificar los códigos penales tratando de adoptar las figuras penales clásicas a los delitos informáticos, pero aún requiere que estos sean revisados, actualizados a medida que los delitos también cambian a través de los años. “misma fin perjudicial pero nuevas formas y metodologías de aplicación y acción”

Para poder analizar el trasfondo de los delitos su evolución a través de los años es importante también entender los diferentes factores que conllevan los cometer delitos informáticos.

Los delitos informáticos se pueden catalogar por su naturaleza, y es que por medio del avance tecnológico también existe su lado negativo listo para explotar, probar o aprovecharse de los agujeros de seguridad que pueda existir, y la facilidad con la que el autor del crimen puede permanecer inadvertido o anónimo.

Es mucho más sencillo cometer un crimen y salirse con las suyas en el mundo cibernético que en el mundo real, el grado de anonimato sigue siendo tan contundente que puede conducir a que ciudadanos respetables abandonen sus valores éticos para orientarse a la búsqueda de las ganancias personales.

- Jurisdicción legal inadecuada es cuando se recibe apoyo de los gobiernos locales en el intento de llevar a cabo el espionaje de computación o el algún caso conocido como ciberterrorismo

- Crimen viejo, tecnología nueva: seria donde se aprovecha la tecnología de la computación para ayudar a facilitar o a llevar a cabo el delito, que antes se hacía de forma tradicional o de forma no digital, algunos por nombrar serian, los crímenes como la pornografía infantil, el robo de identidad y las estafas de dinero.

- Guardar rencor: Los códigos de computación maliciosos como los gusanos y virus suelen ser usados para destruir o dejar a sus objetivos imposibilitados para la satisfacción personal de ver cómo sufren los efectos del daño causado.

- La emoción del juego: La emoción y muchas veces deseo de obtener algo antes lleva a muchos a probar lo atractivo de "descifrar un código" lo que puede llevar a algunos a cometer delitos informáticos.

Los involucrados en los delitos informáticos pueden ser muy diversos y se encuentran asociados a características como falta de ética, factores psicológicos o porque desean llamar la atención, ya que los delincuentes pueden ser desde estudiantes, terroristas o figuras del crimen organizado, usuarios simples de diversas áreas, porque es muchos casos solo se requiere saber algo de informática para empezar.

Por ejemplo, delitos financieros como el fraude o el robo de información, suele ser cometido por los empleados o ex-empleados de empresas, por rencor, despido, o porque están sin trabajo eso según algunas en cuentas realizadas en diferentes organizaciones o juicios.

Ejemplo

- (2012) Albert González fue condenado a 240 meses la pena más larga impuesta hasta el momento a un cibercriminal. Albert fue el responsable de uno de los fraudes más grandes de la historia, utilizando técnicas de SQL inyección logró robar alrededor de 170 millones de números de tarjetas de crédito y claves de cajeros automáticos.

- Durante este año (2013) una condena de 24 meses fue aplicada a Lewys Martin luego de que fuera encontrado culpable de accesos no autorizados a diversos sistemas. Dentro de los sistemas vulnerados se encuentran prestigiosas universidades inglesas, sitios de policía y gubernamentales del Reino Unido y otros sitios de departamentos oficiales del gobierno de Estados Unidos.

Por eso que es se hace tan importante aprender a catalogar, definir, clasificar y tipificar los delitos informáticos desde la promulgación de esta ley, ya que con su divulgación se obtiene una herramienta importante para denunciar los hechos delictivos a los que se pueda ver afectado, un cambio importante si se tiene en cuenta que anteriormente las empresas no denunciaban dichos hechos no sólo para evitar daños en su reputación sino por no tener herramientas especiales.

Si revisamos 5 países latinoamericanos como Colombia, argentina, ecuador, chile y costa rica podemos ver claramente que cada una tipifica los delitos según sus estándares.[90]

Legislación Delitos Informáticos en Colombia:

El 5 de enero de 2009, el Congreso de la República promulgó la —Ley 1273, la cual modificó el código penal adicionando nuevas sanciones en casos relacionados con los delitos informáticos, buscando proteger la información y preservar los sistemas de tecnologías de información y comunicaciones[91]

Legislación Delitos Informáticos en Argentina:

En Argentina, en junio del 2008 se promulgó la —Ley No 26388 con reformas al Código Penal modificando delitos existentes e incluyendo el alcance de los términos documento, firma, suscripción, instrumento privado y certificado, y de esta manera contemplar el uso de nuevas tecnologías. Esta reforma contempló los siguientes delitos: La pornografía infantil mediante el uso de internet u otros medios digitales, el robo y acceso no autorizado de información almacenada.[92]

[90] Análisis comparativo sobre delitos informáticos en Colombia Con relación a seis países de Latinoamérica – Bolaños A – Narváez T, universidad nacional abierta y a distancia “unad” [en línea]2014{disponible en} http://repository.unad.edu.co:8080/handle/10596/2728

[91] Calderón R, Guzmán G, Salinas J. (2011). Diseño y Plan de Implementación de un Laboratorio de Ciencias Forenses Digitales Tesina de Seminario. Guayaquil – Ecuador. Escuela Superior Politécnica del Litoral.

[92] 24Calderón R, Guzmán G, Salinas J. (2011). Diseño y Plan de Implementación de un Laboratorio de Ciencias Forenses Digitales Tesina de Seminario. Guayaquil – Ecuador. Escuela Superior Politécnica del Litoral.

Legislación Delitos Informáticos en Costa Rica:

La Ley 9048 —Reforma de varios artículos y modificación de la sección VIII denominada delitos informáticos y conexos, del título VII del Código Pena.

Esta ley sanciona el delito de corrupción, también contempla la violación de correspondencia o comunicaciones, violación de datos personales, extorsión, estafa informática, daño informático, espionaje, sabotaje informático, suplantación de identidad, espionaje informático, instalación o propagación de programas informáticos maliciosos, suplantación de páginas electrónicas, facilitación de delito informático y difusión de información falsa.

Legislación Delitos Informáticos en Chile:

Fue uno de los países pioneros en expedir una ley contra los delitos informáticos en Latinoamérica, Ley19223 del 28 de Mayo de 1993, la cual consta de cuatro artículos en los que se castigó conductas ilícitas como: la inutilización o destrucción de un sistema de tratamiento de información o sus componentes afectando el correcto funcionamiento del sistema, al igual que la interferencia, intercepción o acceso a un sistema de información con el fin de apoderarse de datos almacenados en el mismo, también sancionó el daño o destrucción de datos, así como la revelación o difusión de datos contenidos en un sistema de una manera malintencionada.

Legislación Delitos Informáticos en Ecuador:

Dentro del nuevo Código Penal del Ecuador ya se especifican varios tipos de delitos informáticos. Los artículos que los tipifican son el 229 y el 234. Se toman en cuenta delitos por revelación ilegal de base de datos, transferencia electrónica por activo patrimonial, intercepción ilegal de datos, ataque a la integridad de sistemas informáticos, delitos contra la información pública reservada, y acceso no consentido a un sistema informático.

## 8.2 Evolución legislativa de diferentes países

Desde 1959 en adelante, países como los Estados realizaron y organizaron nuevas acciones contra la manipulación informática y el espionaje de datos, para los que no había legislación penal. En esos años, el debate se centró en la elaboración de una respuesta jurídica y documentaria de desde la creación y recuperación de información relacionados a las (Leyes, Jurisprudencia, Doctrina).

Debido a que con el robo de información no solo se podía obtener datos importantes, sino también, mediante programas, verdaderos actos jurídicos como: certificaciones, contratos, mandatos judiciales, etcétera. Así nació a fines de los años sesenta la informática jurídica en cuestión y el afán de su protección.

Por ejemplo, si analizamos también la evolución de la legislación argentina frente a los delitos informáticos, en ese país al principio no era considerada la información como algo tangible, por lo tanto, solo estaban protegidos los lenguajes de bases de datos y algunas plantillas de cálculo y dentro de su código penal no fueron consagrados aquellos hechos delictivos pero con el auge de la tecnología y a su vez con el avance de la delincuencia informática se vio la necesidad de modificarlos y crear nuevos instrumentos jurídicos que dieran respuesta a esta problemática, respaldado debido a la promulgación de leyes que comprendieran temas como la protección de datos, la privacidad, la propiedad intelectual, promoción de la industria del software y por último los delitos informáticos y ciberseguridad.

Protección de datos personales y privacidad. La ley mediante la cual se ampara estos dos aspectos en Argentina es la Ley 25.326, en la cual se dictan las disposiciones generales y especificas por las cuales se protege la privacidad, se hace alusión a la protección de datos y también se consagran aspectos como derechos, uso y responsables del registro de datos, así como también se sancionan de manera penal y económica.

Seguridad Informática. La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.[93]

Los 3 delitos informáticos más astutos de la historia

La organización de hackers ShadowCrew

En 2006, la organización de hackers ShadowCrew, violaba la endeble seguridad de las redes inalámbricas de varias tiendas de pequeñas cadenas en estados unidos, donde se infiltraban por medio de sniffers o keyloggers con el fin de apoderarse de la información bancaria de los usuarios lucrarse de la venta de estos en el mercado negro.

[93]La comisión International Electrotechnical Commission (IEC): 41 Ley 19.628 Protección de datos de carácter personal disponible en: http://www.leychile.cl/Navegar?idNorma=141599 42 Ley 19.223 Ley Relativa a delitos informáticos disponible en: http://www.leychile.cl/Navegar?idNorma=30590 43 Ley 19.799 Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma disponible en: http://www.leychile.cl/Navegar?idNorma=196640 44

Se requirió de la colaboración de ciertas instituciones para lograr atrapar el perpetrador de dichos delitos informáticos.

¿Activismo cibernético o tráfico de información?

Probablemente el caso más famoso y controversial de los últimos años es la aparición de información confidencial de distintos y aunque usualmente suelen, denominar este tipo de trabajo como activismo cibernético, el publicar documentos obtenidos de manera ilegal, se catalogan como vulneración de la seguridad de los sistemas de distintos gobiernos, sino que va siempre un paso adelante al descifrar el encriptado de dicha información.[94]

Los alcances de una violación a la seguridad empresarial

En 2014, Apple, sufrió un golpe a la seguridad de la nube conocida como icloud, Para demostrar la vulnerabilidad del sistema de manera contundente, violaron la seguridad y se apoderaron del control de su sistema de bloqueo remoto y puso al descubierto la posibilidad de un importante robo de información masiva por la falta de atención a las fallas en el sistema de seguridad.

A pesar de algunos de los delitos que se comenten tiene distintas razones de ser evidencia que hoy en día, la moneda más valiosa se está volviendo la información.

Por ello, cada día se generan nuevas herramientas en materia de seguridad cibernética y se mejoran las existentes, como el manejo de firmas y la encriptación de documentos, ya que utilizar recursos de vanguardia para proteger la información puede hacer la diferencia.

### 8.3 7900-vulnerabilities que no se tuvieron en cuenta para el año 2018

El año pasado rompió el récord histórico anterior de la mayor cantidad de vulnerabilidades reportadas, con 20,832 de ellas catalogadas.

Según un análisis de VulnDB y Risk Based Security se descubrió que 7.900 de las vulnerabilidades quedaban fuera del rango del radar, no se informaban al ser catalogadas como vulnerabilidades o exposiciones comunes según MITRE (CVE) y la base de datos de vulnerabilidades nacional (NVD).[95]

[94]Los-3-delitos-informaticos-mas-astutos-de-la-historia [en línea] 2017 {disponible en:} http://blogs.adobe.com/latinoamerica/2017/11/14/los-3-delitos-informaticos-mas-astutos-de-la-historia/

[95]7900 Vulnerabilidades no entraron en la base de datos CVE en [en línea] 2017 {disponible en} https://www.infosecurity-magazine.com/news/7900-vulnerabilities-didnt-make-it/

*"Las organizaciones que rastrean y clasifican los parches de vulnerabilidad no vieron alivio en 2017, ya que fue otro año récord para las divulgaciones de vulnerabilidad*", basta con mirar el número de infracciones de datos de piratería informática y web informadas regularmente a menudo lleva a algunos a creer que las vulnerabilidades importantes están cubiertas, y ese tampoco es el caso.

Además, de las más de 18,000 identificaciones de CVE que fueron asignadas o asignadas a las Autoridades de Numeración de CVE (CNA), casi 7.000 se encontraban en estado de reserva, a pesar de que 1.342 de ellas tenían una divulgación pública.

"Desde los sistemas operativos y el software instalados en los sistemas cliente y servidor hasta los dispositivos Iota y SCADA, las vulnerabilidades continúan siendo una gran preocupación", y más aún cuando la capacidad de utilizar correctamente los datos de vulnerabilidad para ayudar con el proceso de toma de decisiones es importante además de cerciorarse de que esté integrado en la solución que ofrece VulnDB ".

### 8.4 Ciberterrorismo

El ciberterrorismo podría definirse como el uso de recursos informáticos para intimidar o coaccionar a otros. Un ejemplo de ciberterrorismo podría ser la intrusión en un sistema informático para dañar su infraestructura crítica y con ello afectar a los usuarios relacionados.[96]

Esta actividad se encuentra en auge y crecimiento continuo donde los delincuentes se aprovechan el internet y los dispositivos son tan utilizados hoy en día, lo que la convierte en una amenaza constante contra la que de momento no se dispone de los suficientes recursos,

El ámbito es donde se mueve el ciberterrorismo, tanto en lo concerniente a la difusión de simple propaganda, como en lo que se refiere a la comunicación, difusión o transmisión de elementos más concretos, como puede ser un manual para la elaboración de explosivos o un chat se enfoca en el intercambio de ideas funcione como una especie de escuela virtual de adoctrinamiento, propaganda para la captación y adiestramiento de adeptos hasta la financiación de sus actividades, es necesario actuar de una manera global para cegar esos canales.

[96]Telcelsoluciones - que-es-el-ciberterrorismo-y-por-que-debe-preocuparte [en línea] 2017 {disponible en:} http://www.telcelsoluciones.com/articulos/que-es-el-ciberterrorismo-y-por-que-debe-preocuparte

El ciberterrorista parte del supuesto de que el acceso a internet es fácil, el flujo de información en la red está poco regulado (apenas existen mecanismos de control) y, por consiguiente, sabe que potencialmente cuenta con una gran audiencia en todo el mundo, con la que se puede comunicar de manera virtual desde el anonimato.[97]

El ciberterrorismo alude a la eventual comisión de delitos de terrorismo a través de los medios y sistemas informáticos. El terrorismo más que a una conducta definida hace referencia a un propósito cuyo objetivo es aterrorizar de forma indiscriminada a una población determinada; de ahí que las conductas puedan ser múltiples.

De ahí se desprende la clasificación de lo que se conoce como: Ciberconductas por ejemplo: el cracking, el hacking, el phising, pharming, Ddos, botnets, Ataque a infraestructuras críticas, malware o apología, entre otras.[98]

### 8.5 CiberWarface

La guerra cibernética es un conflicto informático o de red que involucra distintos ataques motivados por lo que se conoce como política de un estado-nación en otro estado-nación. Este tipo de ataques, donde los actores del estado-nación intentan interrumpir las actividades de las organizaciones o estados-nación, especialmente con fines estratégicos o militares y ciberespionaje.[99]

La guerra cibernética puede tomar muchas formas, que incluyen:

- virus, gusanos informáticos y malware que pueden eliminar suministros de agua, sistemas de transporte, redes eléctricas, infraestructura crítica y sistemas militares.
- ataques de denegación de servicio (DoS), eventos de seguridad cibernética que ocurren cuando los atacantes toman medidas que evitan que los usuarios legítimos accedan a sistemas informáticos, dispositivos u otros recursos de red específicos.

[97] el-ciberterrorismo-una-actividad-continuo-crecimiento-articulo-523789
elespectador.com [en línea] 2014 {disponible en:} https://www.elespectador.com/noticias/actualidad/el-ciberterrorismo-una-actividad-continuo-crecimiento-articulo-523789

[98] que-es-el-ciberterrorismo ciberderecho [en línea] 2014 {disponible en:} http://www.ciberderecho.com/que-es-el-ciberterrorismo/

[99] forbes - cyber-warfare-the-threat-from-nation-states [en línea] 2014 {disponible en:} https://www.forbes.com/sites/kateoflahertyuk/2018/05/03/cyber-warfare-the-threat-from-nation-states/#2c9de18b1c78

- pirateo y robo de datos críticos de instituciones, gobiernos y empresas; y
- ransomware que mantiene a los sistemas informáticos como rehenes hasta que las víctimas paguen un rescate.[100]

La investigación de RAND proporciona recomendaciones a los responsables de tomar decisiones militares y civiles sobre los métodos de defensa contra los efectos dañinos de la guerra cibernética en la infraestructura digital de una nación.[101]

[100]searchsecurity.techtarget- cyberwarfare [en línea] {disponible en:}https://searchsecurity.techtarget.com/definition/cyberwarfare
[101] rand.org- cyber-warfare [en línea] 2014 {disponible en:} https://www.rand.org/topics/cyber-warfare.html

## 9. REALIZAR UN ANÁLISIS DEL IMPACTO NEGATIVO QUE TIENE LA CIBERDELINCUENCIA EN LAS EMPRESAS COLOMBIANA POR MEDIO DE LA REVISIÓN DE DATOS ESTADÍSTICOS PÚBLICOS COMO LA FISCALÍA GENERAL DE LA NACIÓN Y LA POLICÍA NACIONAL

### 9.1 Análisis sobre el impacto negativo que tiene la ciberdelincuencia en las empresas colombianas.

Para un país la información y los datos, así como la tecnología que la soporta, representa uno de los activos más valiosos, por lo tanto, debe ser protegida preservada y respetada, esto se logra por medio de la legislación, generación de normatividad y leyes.

En el estudio a continuación se realiza una comparación entre la legislación sobre Delitos Informáticos de distintitos países latinoamericanos, europeos y americanos con el fin de compararlos con Colombia que es el foco de estudio, e identificar las fortalezas, debilidades, falencias y sugerencias que se pueden aplicar para posteriores estudios de actualización, mejoras que se puedan presentar más adelante, desde nuevos proyectos de ley que permitan la creación de nuevos artículos o modificación que fortalezcan la Constitución Nacional.

Actualmente la información de las empresas y las personas tiende a ser almacenada en bases de datos electrónicas, lo cual ha desencadenado la aparición de diferentes formas de delitos informáticos derivados de la utilización de la información con fines lucrativos o maliciosos, o la alteración de la misma. Para tratar esos delitos se han desarrollado diferentes normativas gubernamentales, como la ley orgánica de protección de datos personales en España, o la ley 1581 de 2012 sobre protección de datos personales en Colombia.

Se puede concluir que existe interés en el tema de la legislación informática en cuanto a la privacidad de los datos personales, a pesar de que un gran porcentaje de las normativas generadas en el continente derivan de leyes y normas expedidas en países como España, Alemania, Estados Unidos de donde se adaptaron a las necesidades actuales del país, cada país tiene una visión diferente de que topología, tipificación clasificación y penalizaciones requeridas, pero es una necesidad que a fin de minimizar los vacíos jurídicos que pueden permitir a los ciberdelincuentes actuar sin temor al castigo, es implementar una estandarización legislativa más adecuada a los diferentes tipos de delito informático.

Así mismo, surge la necesidad de que las personas dedicadas a las TIC en nuestro país, conozcan de manera más profunda los acuerdos, normas y leyes que rigen la protección de los datos privados para dar trámite adecuado a las implementaciones que así lo requieran. [102]

Estos vacíos legales o ambigüedades dentro de la ley 1273 de 2009, permite mostrar como los delincuentes pueden evadir las sanciones penales y económicas, amparados en la falta de instrumentalización de la ley y en la ambigüedad en la definición técnica de los delitos que castiga en algunos de sus artículos, sin tener en cuenta que muchos según su cometido pueden ser más graves que otros, aunque el medio fuese el mismo.

En la tabla siguiente se presenta una relación motivación vs que afecta y como se refleja eso en los pilares de la información.

**Tabla 4 motivación VS pilar o dimisión de la información que se puede ver afectado**

| Motivación | Pilar o dimensión de la información que se puede ver afectado y tipo de daño |
|---|---|
| Fraude | Autenticación – Integridad |
| Acceso no Autorizado | Autorización – Autenticación - disponibilidad |
| Curiosear | Privacidad – Datos Reservados-. Confidencialidad |
| Alteración de Mensaje | Integridad – disponibilidad - Confidencialidad |

**Fuente:** El autor

La comprensión de los elementos de seguridad y como ellos trabajan en el mundo físico, puede ayudar para explicar cómo estos daños y dimensiones se encuentran en el mundo de la red y dónde se sitúan las dificultades, desde el punto de vista de su protección.

Medidas de seguridad de la red.

Existen numerosas técnicas para proteger la integridad de los sistemas. Lo primero que se debe hacer es diseñar una política de seguridad. En ella, definir quiénes tienen acceso a las diferentes partes de la red, poner protecciones con contraseñas adecuadas a todas las cuentas, y preocuparse de hacerlas cambiar periódicamente (Evitar las passwords "por defecto" o demasiado obvias).

[102] MChaparro - Legislación informática y protección de datos en Colombia, comparada con otros países [en linea] 2014 {disponible en} http://biblioteca.uniminuto.edu/ojs/index.php/Inventum/article/download/1014/953

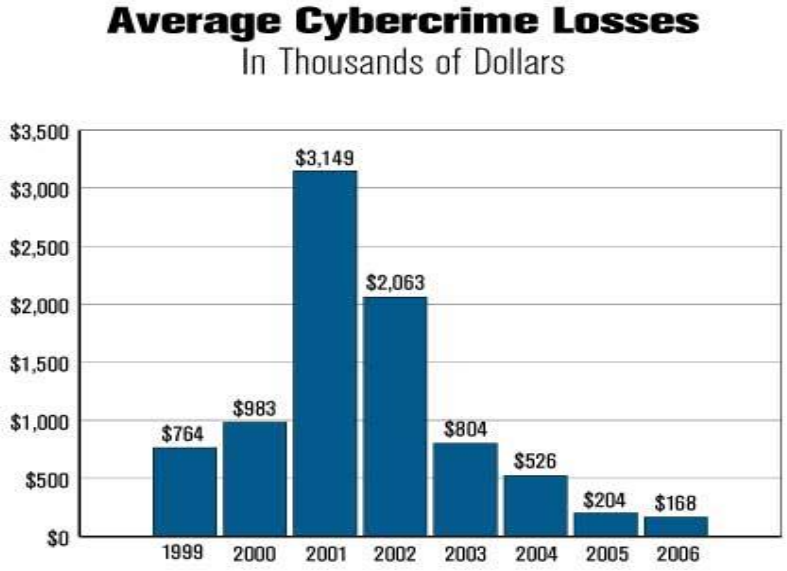
Firewalls.

Existen muchas y muy potentes herramientas de cara a la seguridad de una red informática. Una de las maneras drásticas de no tener invasores es la de poner murallas. Los mecanismos más usados para la protección de la red interna de otras externas son los firewalls o cortafuegos.

El análisis del promedio de las pérdidas económicamente por el cibercrimen

En la figura siguiente se muestra el promedio de pérdidas en un estudio realizado en el 2006 donde a través de un estudio realizado por CSI/FBI en un estimado de 8 años

**Figura 5. NetSec CSi/FBI imagen[103]**




**Fuente:** Link.springer.com [en línea] {disponible en}: https://link.springer.com/chapter/10.1007/978-3-642-39498-0_12

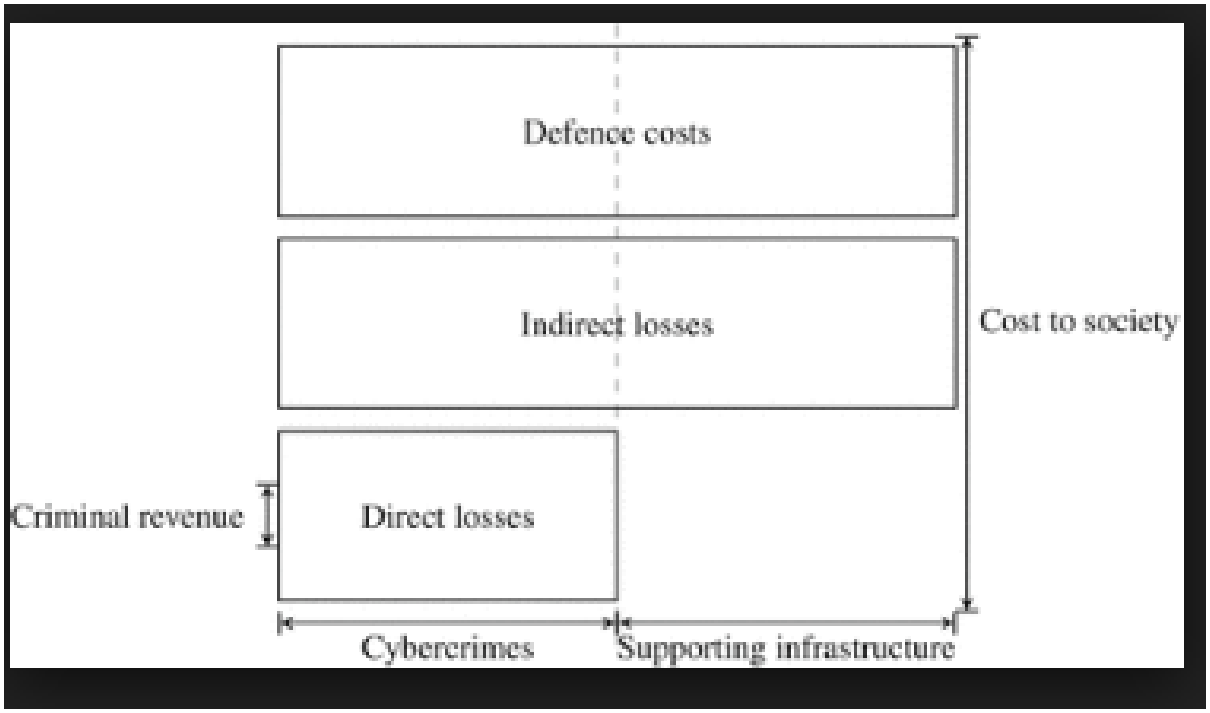
Estos resultados fueron proporcionados por la conferencia NetSec de junio en Scottsdale, Arizona donde se brindó la oportunidad de brindarles a los asistentes una vista previa de los resultados de la Encuesta sobre seguridad y delitos informáticos de CSI / FBI

[103] Link.springer.com [en línea] {disponible en}: https://link.springer.com/chapter/10.1007/978-3-642-39498-0_12

Las pérdidas varían donde su pico más alto fue el 2001, y luego de la implementación de normatividad legislativa se puede ver un decremento en la incidencia de pérdidas monetarias, gracias a las políticas, legislación y salvaguardas que dan mejor protección y garantiza la continuidad del negocio.

Sin embargo, lo que los informes de Symantec nunca han demostrado es una situación de delito cibernético que está fuera de control.

**Figura 6 . Costos de defensa, costos indirectos, los costos de la sociedad**




**Fuente:** Informe sobre ataques informáticos en Colombia y al sector financiero http://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370

En la imagen siguiente podemos ver en un cuadro estructurado como funciona, costos de defensa, costos indirectos, los costos de la sociedad, las pérdidas directas, que comprende los cibercriminales, la infraestructura de soporte y los ingresos de los criminales. [104]

[104] Informe sobre ataques informáticos en Colombia y al sector financiero [en línea] {disponible en}: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370

## 9.2 Revisión de datos estadísticos públicos como la fiscalía general de la nación y la policía nacional

Según la policía al responder los interrogantes, ¿Para los ciberinvestigadores, ¿es fácil detectar de dónde proviene un mensaje amenazante o resulta imposible hacerlo?, se da por medio de la identificación de estos ataques, los cuales varían y dependen de la modalidad y del vector utilizado por el ciberatacante. Un ataque mediante spam que se ejecuta usando servidores de correos electrónicos requiere capacidades técnicas diferentes a las que se usan para la identificación de falsos perfiles en redes sociales como Facebook y Twitter. La cooperación internacional entre agencias y el sector privado es fundamental para contener e investigar estas actuaciones criminales. La Policía Nacional es referente, a nivel regional, en estas pesquisas gracias a sus capacidades tecnológicas y a la experiencia adquirida mediante la transferencia de conocimientos que provienen de las agencias extranjeras que luchan contra el cibercrimen.[105]

¿Con cuáles organismos cuenta el Estado colombiano para mantener el orden en el mundo virtual?

Colombia tiene tres organismos en este campo: el Colcert, que depende del Ministerio de Defensa y que se dedica a mitigar el riesgo y a dar respuestas inmediatas a la violación o amenaza inminente contra las políticas de seguridad informática del país. Las entidades estatales reportan al Colcert las vulnerabilidades o incidentes que se presenten en cualquiera de ellas. Además, el Estado cuenta con el Centro Cibernético Policial que actúa bajo la supervisión de la Dirección de Investigación Criminal e Interpol (Dijín) y que está encargado de la ciberseguridad; y con el Comando Conjunto Cibernético, que se hace cargo de la ciberdefensa de la nación.

[105]"CIBERATAQUES A LA MEDIDA"
Un oficial del Centro Cibernético Policial de Colombia explica estrategia para elecciones [en línea] 2018 [disponible en] https://www.elespectador.com/noticias/judicial/un-oficial-del-centro-cibernetico-policial-de-colombia-explica-estrategia-para-elecciones-articulo-737056

Según estadísticas del Grupo de Investigación de Delitos Informáticos de la Dirección Central de Policía Judicial (DIJIN), el cual se dedica a la investigación de conductas delictivas derivadas del uso de la tecnología y telecomunicaciones, el hurto a través de Internet es uno de los mayores delitos que se presentan en Colombia (Grupo Investigativo de Delitos Informáticos - GRIDI, 2009).[106]

Para contrarrestar este tipo de delincuencia, la Dijin trabaja en tres aspectos:

• Preventivo: A través de la página en Internet: www.delitosinformaticos.gov.co, donde expertos en el cibercrimen atienden las inquietudes de los ciudadanos y dan recomendaciones para no ser víctima de los delincuentes.

• Investigativo: Coordinando todas las actividades con la Fiscalía y las autoridades competentes para recopilar el material probatorio.

• Político: Participando en la promulgación y elaboración de proyectos de ley que permitan tipificar estas prácticas y disminuir este tipo de delincuencia.

[106] Caracterización de los delitos informáticos en Colombia Characterization of cybercrime in Colombia http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewFile/126/149

## 10. DETERMINAR LAS DIFERENCIAS Y SIMILITUDES QUE EXISTEN ENTRE LA NORMATIVIDAD COLOMBIANA Y LAS NORMATIVIDADES DE LOS PAÍSES ANALIZADOS MEDIANTE UNA OBSERVACIÓN COMPARATIVA.

### La ley de protección

La ley de protección tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política;

Esto da una idea de el por qué se realizan comparativos con relación a la normativa en este campo, se encuentran relacionadas con la legislación expedida en Europa y específicamente en España, ya que tanto Europa como América Latina buscan proteger a la persona en sus derechos fundamentales, antes que, a las empresas, dándole así a la Ley un carácter más humanístico. Aunque en Colombia se promulgó la ley 1712 de marzo de 2014, por la cual "se crea la ley de transparencia y derecho de acceso a la información pública nacional y otras disposiciones", en las bases de datos consultadas no se localizaron referentes al respecto, aunque el gobierno colombiano ha generado iniciativas para su promulgación, revisión o107 Debilidad en regulación y legislación de la protección de la información y de los datos.

Pese a que existen instrumentos legales y regulatorios en seguridad de la información, persisten falencias que impiden responder oportunamente a incidentes y delitos cibernéticos, y que entre ellas se contradicen, porque una promulga el derecho a saber y el otro a protegerla de terceros, donde se debe entender en qué casos son publicables o no. Y ahí es donde se entra a clasificar los activos públicos, clasificados y públicos.

Por ello las regulaciones deberían se generadas de forma particular para poder tipificar de forma correcta todos los tipos de ataques, vulnerabilidades y a la hora de comprender su correlación con terminologías como la ciberseguridad y la ciberdefensa, sobre el cual existe muy poco en términos de alcance y operatividad.

[107]Urnadecristal septiembre [en línea] de 2014 {disponible en}: www.urnadecristal.gov.co/gestion-gobierno/dejatus-comentarios-al-decreto-que-reglamenta-ley-detransparencia

En cuanto a normatividad internacional, dentro de los instrumentos que le permitirían al país integrarse a la comunidad mundial está la Convención del Consejo de Europa en Delito Cibernético, que requiere cumplir con aspectos como el establecimiento de mecanismos de cooperación judicial como la extradición y así facilitar la investigación de acuerdo con las características y necesidades propias de su red, se creó para dichas empresas la obligación de implementar modelos de seguridad, con el fin de contribuir a mejorar la seguridad de sus redes de acceso, cumpliendo los principios de confidencialidad e integridad de datos y disponibilidad de los elementos de red, la información, los servicios y las aplicaciones, así como medidas para autenticación, acceso y no repudio, y obligaciones relacionadas con la inviolabilidad de las comunicaciones y la seguridad de la información. Sin embargo, se ha identificado, por ejemplo, que en lo que respecta a las políticas de seguridad informática van siempre de la mano en cada país con la promulgación de leyes estatutarias incluidas en el código penal, en donde se pretende imponer sanciones de tipo penal y económico, a todo tipo de comportamientos ilícitos que traen consigo las nuevas formas de delincuencia cibernética que causa pérdidas económicas y de información.

Compatibilidad de la legislación: Una forma de abordar la dimensión transnacional del delito cibernético y mejorar la cooperación internacional es desarrollar y normalizar la legislación pertinente. En los últimos años se han adoptado varias iniciativas regionales. Con distintas leyes y modelos sobre el delito cibernético e informático con la finalidad de mejorar la legislación para combatir la ciberdelincuencia e intensificar la cooperación internacional.

La Unión Europea también ha hecho esfuerzos por armonizar la legislación sobre el delito cibernético entre sus 27 Estados miembros, por ejemplo, mediante lo siguiente: la directiva 2000/31/EC del Parlamento Europeo y el Consejo sobre ciertos aspectos jurídicos de los servicios en la sociedad de la información, en particular el comercio electrónico, en el mercado interno.

La Doctrina del Derecho de la Informática, ha identificado tres alternativas de solución para hacer frente al problema jurídico que representa la sociedad informatizada, mismas que consisten en:

- La actualización de la legislación.
- La evolución jurisprudencial.
- La redacción de leyes de carácter particular.

Por ende, es importante partir de la informatización de la sociedad y los fenómenos que se desarrollan en el seno de la Sociedad de la Información, han demandado a nivel mundial la actualización de los marcos legales, a fin de que se reconstruyan las hipótesis jurídicas en que se disponen diversas conductas criminales frente al uso de la informática.

Al respecto, el ordenamiento jurídico no ha sido la excepción. En adelante, veremos cuáles son las conductas que se prevén y sancionan en el ámbito nacional. Ello permitirá, por una parte, conocer la clasificación legal de los Delitos Informáticos en México y Latinoamérica como punto de partida, y por otra, delatar la existencia de previsiones legales respecto a los denominados Delitos Informáticos.

Al realizar un análisis completo sobre la ley especial contra delitos Informáticos, es importante mencionar que su publicación se da en el año 2001 con el pasar del tiempo y los avances, tecnológicos comenzaron a realizarse actos delictivos que no podían ser castigados, al no estar estipulados en ninguna ley. Es entonces cuando se crea la ley especial contra delitos informáticos con el fin de legislar en sobre los delitos, contra las tecnologías de información.

Además de necesitar instrumentos jurídicos, la aplicación de la ley depende en gran medida de la disponibilidad de instrumentos de investigación tales como programas informáticos forenses (para reunir pruebas, registrar las pulsaciones de teclado y descifrar o recuperar ficheros suprimidos) y programas informáticos o bases de datos de gestión de la investigación (por ejemplo, con valores “hash” para imágenes de pornografía infantil conocidas

Una de las cuestiones más importantes relacionadas con el desarrollo de esos instrumentos sigue siendo la necesidad de que los encargados del desarrollo coordinen los trabajos para evitar la duplicación de información, manejo incorrecto o daño a la evidencia. Del mismo modo, deben coordinarse también los esfuerzos de las redes de puntos de contacto.

El entendimiento de los delitos informáticos no sólo puede advertirse del incremento en la cantidad de delitos cometidos, sino que, además, los mismos son cada vez más variados y complejos. La combinación de la delincuencia con las posibilidades de las nuevas tecnologías, ha generado que muchos países latinoamericanos optaran por la generación de nuevas figuras penales de acciones relacionadas a la informática por medio de análisis de la situación de los delitos informáticos en Latinoamérica donde el resultado se ha reflejado y construido un cuadro comparativo que permite identificar que delitos informáticos se encuentran tipificados penalmente en cada país abordado en el estudio. [108]

[108] Sedici.unlp {en línea} [disponible en] http://sedici.unlp.edu.ar/handle/10915/42145

**Tabla 5 Comparativo Legislación en 14 países**

| País | Legislación | Características Generales |
|---|---|---|
| **Ecuador**[109] | La ley Penal 11723 El decreto 165/94 (B.O. del 8/2/94) | El artículo 71 tipifica como conducta ilícita a "el que de cualquier manera y en cualquier forma defraudare los derechos de propiedad intelectual que reconoce esta ley" de "La propiedad Científica, literaria y artística" ha modificado los artículos 71, 72, 72 bis, 73 y 74. También dentro del Código Penal encontraremos sanciones respecto de los delitos contra el honor (109 a 117); Instigación a cometer delito incluyó al software dentro de la Ley de Propiedad Intelectual 11723. |
| **Estados unidos**[110] | Ley Federal de Protección de Sistemas de 1985. cta Federal de Abuso Computacional (18 U.S.C. Sec 1030), modificando el Acta de 1986. "entre otras leyes relacionadas a la informática que son bastante" | A Aquí se contempla la regulación de los virus (computer contaminant) conceptualizándolos aunque no los limita a los comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos. |

**Fuente**: El autor con información base en Derechos ecuador – delitos informáticos {en línea} [disponible en] https://www.derechoecuador.com/delitos-informaticos Segu-info - estados unidos delitos {en línea} [disponible en]: https://www.segu-info.com.ar/delitos/estadosunidos.htm

[109] Derechos ecuador – delitos informáticos {en línea} [disponible en] https://www.derechoecuador.com/delitos-informaticos

[110] Segu-info - estados unidos delitos {en línea} [disponible en]: https://www.segu-info.com.ar/delitos/estadosunidos.htm

**Tabla 6 Comparativo Legislación en 14 países**

| País | Legislación | Características Generales |
|---|---|---|
| **Europa**[111] | Diario Oficial de las Comunidades Europeas (DOCE series C, núm. 140, de 5 de junio de 1979). Convenio 108 del Consejo de Europa de 28 de enero de 198 Recomendación 81/679/CEE, de la Comisión de 29 de julio de 1981, Directiva 83/189/CE | Resolución del Parlamento Europeo, sobre la protección de los derechos de las personas de cara al desarrollo de los progresos técnicos en el campo de la informática, 1 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal. (Ratificado por España el 27 de enero de 1.984. Publicado en el B.O.E. nº 274 de 15 de noviembre de 1.985). relativa al Convenio del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. (DOCE nº L 246 de 29 de agosto de 1981). relativa a productos de teleinformática y a la necesidad de compatibilizar los sistemas y establecer códigos de conducta y directivas maestras para la armonización de las legislaciones de los estados miembros. |
| **Honduras** | Código Penal; Decreto 144/83 | adaptación de ciertos delitos clásicos a las nuevas modalidades informáticas. Entre ellos podremos encontrar los artículos 214, 215, 223 y 254. Por otro lado, el Decreto 144/83 incorpora algunos delitos para tipificar la pornografía infantil a través del art. 149 y sus incisos al Código Penal. |
| **México** | Reforma 75 del Código Penal Federal (1999) | Mediante reformas se crearon en el Código Penal Federal, buscaron tipificar los delitos informáticos clásicos teniendo en consideración la fecha de su incorporación. Se destaca la diferente que atentan contra los sistemas de cómputo que pueden o no, ser parte del sector financiero mexicano. Es importante destacar, que algunos Estados Mexicanos tienen además sus propias normas penales, incorporando otros delitos informáticos no analizados en este trabajo |

**Fuente**: El autor con información base en: informatice – jurídica legislación unión europea {en línea} [disponible en]: http://www.informatica-juridica.com/legislacion/union-europea/

[111] informatice – jurídica legislación unión europea {en línea} [disponible en]: http://www.informatica-juridica.com/legislacion/union-europea/

**Tabla 7 Comparativo Legislación en 14 países**

| País | Legislación | Características Generales |
|---|---|---|
| **Argentina** | Código Penal, Ley 26.388 (2008), Ley 25.326 (2000) | La Ley 26.388 conocida como la “ley de delitos informáticos” Epígrafe del Capítulo III cuyo nuevo título es "Violación de Secretos y de la Privacidad", la Ley 25.326 de Protección de Datos Personales (2000) pero fue modificado por la Ley 26.388. |
| **Bolivia** | Código Penal, Ley 1.768 (1997), Ley 3325 (2006) | La Ley 1.768 realiza una reforma general al Código Penal. Del Libro Segundo del Código Penal, el de "DELITOS INFORMÁTICOS". |
| **Brasil** | Ley 12.737 (2012), Ley 11.829 (2008) | La Ley 12.737 es una ley reciente (año 2012), en la cual se dispone la tipificación criminal de los delitos informáticos y otras providencias. la Ley 11.829 regula el Estatuto de la Niñez y la Adolescencia, para mejorar la lucha contra la producción, venta y distribución de pornografía infantil, así como tipificar como delito la adquisición y posesión de dicho material y otros comportamientos relacionados con la pedofilia en Internet. |
| **Chile** | Ley 19.223 (1993), Ley 20.009 (2005),Ley 18.168 (2002) | La Ley 19.223 es una ley “Relativa a Delitos Informáticos” La Ley 20.009 regula la responsabilidad para el caso de robo, hurto o extravío de tarjetas de crédito, en cuyo texto se sancionan algunas conductas relacionadas con estos aspectos. La Ley 18.168 (modificada por diferentes normativas) regula de manera general las telecomunicaciones, incorporando algunos tipos penales sobre la interferencia o captación ilegítima de señales de comunicación. |

**Fuente:** EL autor basado en información obtenida en Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado.
http://webcache.googleusercontent.com/search?q=cache:http://conaiisi.unsl.edu.ar/2013/82-553-1-DR.pdf
Delitos informáticos – delitos Venezuela https://www.delitosinformaticos.com/estafas/delitosvenezuela.shtml

**Tabla 8. Comparativo Legislación en 14 países**

| País | Legislación | Características Generales |
|---|---|---|
| Colombia | Ley 1.273 (2009), Ley 1366 (2009), ley 1587 | La ley 1.273, de reciente sanción legislativa (año 2009), modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos". Se afirma que dicha normativa busca preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones CAPITULO I, titulado "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", utilizando medios informáticos, electrónicos o telemáticos". ley 1587 de protección de datos |
| Costa Rica[112] | Ley 9.048 (2012) | La Ley 9048 es una modificación importante del Código Penal de este país. y 288 de la Ley Nº 4573. Modifica la sección VIII del título VII del Código Penal, titulándolo "Delitos informáticos y conexos", donde regula desde el art. 230 hasta el art. 236. En esta modificación bastante integral, agrega una importante cantidad de delitos informáticos al Código Penal, desde los más tradicionales hasta algunos más modernos como la Suplantación de Identidad (art. 230) o el espionaje cibernético (art. 231). |
| Venezuela[113] | Oficial N° 37.313 del 30 de octubre de 2001) | La Ley define los términos tecnología de la información, sistema, data, documento, computadora, hardware, firmware, software, programa, procesamiento de datos o de información, seguridad, virus, tarjeta inteligente, contraseña y mensaje de datos. Se trata de una ley especial que descodifica el Código Penal y profundiza aún más la incoherencia y falta de sistematicidad de la legislación penal, con el consecuente deterioro de la seguridad jurídica. |

**Fuente:** EL autor basado en información obtenida en Delitos Informáticos en Latinoamérica: http://webcache.googleusercontent.com/search?q=cache:http://conaiisi.unsl.edu.ar/2013/82-553-1-DR.pdf Delitos informáticos – delitos Venezuela https://www.delitosinformaticos.com/estafas/delitosvenezuela.shtml

[112] Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. {en línea} [disponible en] http://webcache.googleusercontent.com/search?q=cache:http://conaiisi.unsl.edu.ar/2013/82-553-1-DR.pdf

[113] Delitos informáticos – delitos Venezuela {en línea} [disponible en] https://www.delitosinformaticos.com/estafas/delitosvenezuela.shtml

**Tabla 9. Comparativo Legislación en 14 países**

| País | Legislación | Características Generales |
|---|---|---|
| **Perú** | la Ley 30096 o ley de delitos informáticos | El 22 de octubre de 2007, el Congreso de la República de dicha nación emite la Ley 30096 o ley de delitos informáticos, la cual tiene por objeto prevenir y sancionar toda conducta ilícita cometida a través de la utilización de tecnologías de la información o comunicación que puedan llegar a afectar sistemas, datos informáticos y otros bienes jurídicos penalmente importantes. |
| | la Ley 30171, la cual modifica la Ley 30096, ley de delitos informáticos | El 10 de marzo de 2014, el Congreso de la República del Perú emite la Ley 30171, la cual modifica la Ley 30096, ley de delitos informáticos, con el objeto de incorporar la calidad de "deliberada" e "ilegítima" a las conductas delictivas, sancionadas en la tipificación de los delitos informáticos regulados. |
| **Paraguay** [114] | El 26 de noviembre de 1997, Ley 1160, la cual tipifica algunos delitos informáticos | El 26 de noviembre de 1997, el Congreso de la Nación Paraguaya publica su Código Penal mediante la sanción de la Ley 1160, la cual tipifica algunos delitos informáticos, la comisión de otras conductas punibles a través de las nuevas tecnologías y otros tipos penales relacionados con la delincuencia informática |

**Fuente:** EL autor basado en información obtenida Analysis of the criminalization of cybercrime in Spanish-speaking countries Análise da criminalização do cibercrime nos países de lingual española. {en línea} [disponible en]: http://revistalogos.policia.edu.co/index.php/rlct/article/view/339/html

[114] Analysis of the criminalization of cybercrime in Spanish-speaking countries Análise da criminalização do cibercrime nos países de lingual Española. {en línea} [disponible en]: http://revistalogos.policia.edu.co/index.php/rlct/article/view/339/html

## 11. CONCLUSIONES

En conclusión el continuo avance de las Tecnologías de la información, además traer múltiples beneficios para la sociedad, donde las ventajas y las necesidades del flujo nacional e internacional de datos se pueden satisfacer, generando incremento económico en países como Colombia, pero también se evidencia un incremento del uso de estas tecnologías para fines incorrectos, por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

Esto implica que es importante que los países realicen la caracterización de los delitos informáticos, en Colombia se debe definir cada aspecto de manera correcta, su tipificación, que abarcan o acarrean por medio de su uso y sus efectos. Para poder ejecutar los cargos acordes a ello.

La falta de cultura informática ya sea en las organizaciones o los usuarios es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en las buenas prácticas de tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.

Debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que, a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área. Desde el punto de vista de la Legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática.

Desde la creación de decretos, leyes y penalizaciones a quienes comentar dichos delitos, se puede concluir que dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras o dispositivos electrónicos es importante y conveniente fijar mecanismos sincronizados para la puesta en vigor de instrumentos de cooperación internacional para contrarrestar eficazmente la incidencia de la criminalidad informática.

Debido a que muchos de los delitos pueden ser cometidos desde otros países gracias a las posibilidades de conexión y acceso, además se puede observar el gran potencial de la actividad informática como medio de investigación, especialmente

debido a la ausencia de elementos probatorios que permitan la detección de los ilícitos que se cometan mediante el uso de los ordenadores.

Finalmente, debe destacarse el papel del Estado, que aparece como el principal e indelegable regulador de la actividad de control del flujo informativo a través de las redes informáticas.

Regulando con la continua tipificación, mejoras en las leyes que abarcan que una manera más directa los distintos tipos de delitos y le den la debida importancia porque aún falta más rigor en ellos.

La legislación colombiana y diferentes organizaciones como la ONU o CONPES comparten su objetivo y fin de:

- Proteger a la ciudadanía de las amenazas y/o delitos cibernéticos desde la clasificación, tipificación y penalización de estos.
- Responder operativamente ante los delitos cibernéticos, desarrollando labores coordinadas de prevención, atención, investigación y de apoyo a la judicialización de los delitos informáticos en el país.
- Dar asesoría sobre vulnerabilidades y amenazas en sistemas informáticos.
- Divulgar información a la ciudadanía, que permita prevenir lo concerniente a pérdida de disponibilidad, integridad y/o confidencialidad de la información.

Fomentando la concientización en las empresas y usuarios sobre la inclusión de políticas de seguridad cibernética, en coordinación con los actores involucrados y la gran importancia que sigue teniendo este tema y los serios retos que plantea, donde en los últimos 50 años se han examinado y elaborado diversas soluciones para hacer frente a la cuestión del delito cibernético. En parte, el tema sigue difícil de analizar porque la tecnología evoluciona constantemente y los métodos utilizados para cometer esos delitos también cambian.

En 1997, varios países aprobaron una estrategia innovadora en la guerra contra el delito con metodología y modos de determinar rápidamente la proveniencia de los ataques e identificar a los cibercriminales, también se están en negociaciones para unir fuerzas en las diferentes instituciones para resguardar las diferentes tecnologías, activos, implementaciones digitales e infraestructuras con el fin de desarrollar sistemas de información para identificar casos de uso indebido de las redes, perseguir a los infractores y recabar pruebas.

Se pudo determinar también que Impacto en la Identificación de Delitos a Nivel Mundial y las dificultades que enfrentan las autoridades en los diferentes países demuestra la necesidad de una cooperación mundial para modernizar las leyes nacionales, las técnicas de investigación, la asesoría jurídica y las leyes de extradición para poder alcanzar a los delincuentes, debido a que en muchas ocasiones un delito informático se puede cometer desde otro país impactando ambas jurisdicciones y las penalizaciones pueden diferir entre ellos.

Por ejemplo, en Europa existe una guía sobre delitos en la tecnología de la informática ha publicado un Manual sobre el delito por computadora, en el que se enumeran las leyes pertinentes en los diversos países y se exponen técnicas de investigación, al igual que las formas de buscar y guardar el material electrónico en condiciones de seguridad.

Incluso se están realizando colaboraciones con las universidades, la industria y los medios de comunicación y con expertos técnicos en seguridad y asesores jurídicos de los gobiernos, agentes del orden y organizaciones encargadas de proteger la intimidad a fin de combatir los virus, ataques, delitos, fraude electrónico y la explotación de datos personales.

Incluso, estos países también se han propuesto disponer centros de coordinación encargados de hacer cumplir la ley. Estos centros apoyan las investigaciones de otros Estados mediante el suministro de información vital o ayuda en asuntos jurídicos, tales como entrevistas a testigos o recolección de pruebas consistentes en datos electrónicos.[115]

Es importante entender, que las ofensas tradicionales como el fraude económico o social cuestan al ciudadano alrededor de cientos de dólares al año; los fraudes transitorios cuestan un poco más de unos cuantos cientos de dólares; mientras que los nuevos delitos informáticos cuestan en decenas de centavos pero que a la larga genera más ganancia, ejemplo si por cada transacción de una cuidad se carga 1 centavo por cada persona que la realice a una cuenta en unos pocos días tendrá un estimado grande, otro ejemplo es por medio del uso de botnet el cual se usó para generar al menos un tercio del spam enviado en 2010 el cual genero a sus perpetradores una gran suma, pero cualquiera de estos ejemplos se comparan pero

[115]Monografías – Trabajos [en línea] {disponible en}: http://www.monografias.com/trabajos6/delin/delin2.shtml#ixzz5evosszrt

sin ser ni siquiera la mitad de lo gastado en prevención anti spam y es que aún es muy ineficientes los esfuerzos y la lucha contra el delito cibernético;

Esto se da porque de alguna forma los delitos cibernéticos son globales y tienen fuertes externalidades, mientras que los delitos tradicionales como el robo de automóviles y robos comunes son locales, y los equilibrios asociados han surgido después de muchos años de optimización.

En cuanto a la pregunta más directa de qué se debe hacer, nuestras cifras sugieren que deberíamos gastar menos anticipándonos al cibercrimen (en antivirus, firewalls, etc; como se mencionaba previamente).[116]

La investigación del cibercrimen se centra principalmente en evidencia digital, por ejemplo, en el contenido de mensajes de correo electrónico, en las direcciones empleadas para enviar los e-mails, en los archivos logs o ficheros de texto de actividad computacional, y en los datos almacenada en los computadores personales o portátiles. Estas evidencias son muy frágiles, fáciles de destruir o alterar, con sólo programar rutinas para eliminar los archivos logs relativos a la actividad de los sistemas, los cuales pudieran contener evidencia para investigar un delito informático.[117]

Para finalizar es importante mencionar el impacto que puede el mejorar las leyes, decretos y políticas relacionadas a la seguridad y lucha contra el cibercrimen a nivel organizacional, donde se requiere que las organizaciones se alineen con las políticas de ciberseguridad emitidas por los respectivos Ministerios o entidades que lideran los diferentes sectores de las infraestructuras críticas. Por ejemplo, en el sector financiero, la entidad encargada de liderar estos procesos es la Superintendencia Financiera de Colombia; en el caso de las Pymes es importante que, de acuerdo con el sector de la economía al cual pertenezcan, identifiquen la entidad reguladora y se enteren de las políticas, normas y directrices emitidas en materia de ciberseguridad y ciberproteccion, a fin de estar alineados y incrementar los esfuerzos para enfrentar este tipo de amenazas que crecen día a día a la par de las nuevas tecnologías.

---

[116] link.springer.com - [en línea] {disponible en}: https://link.springer.com/chapter/10.1007/978-3-642-39498-0_12

[117] Mary angélica Carvajal avellaneda - Nataly Rangel Ruíz - universidad libre de Colombia seccional Cúcuta biblioteca Manuel José Vargas Duran - Análisis comparativo del tratamiento jurídico dado a los delitos informáticos en el derecho penal colombiano y español. {en línea} [disponible en] http://repository.unilibre.edu.co/bitstream/handle/10901/9330/trabajodegradodelitosinformaticos.docx?sequence=1

## 12. RESULTADOS

Todo lo que abarca la ciberdelincuencia y la tipificación de las normas y como regula los métodos, procesos de cooperación internacional en la lucha contra la ciberdelincuencia. Es importante establecer que se creen normatividad de cooperación porque muchos de los delitos informáticos son difíciles de tipificar y penalizar porque pueden ser cometidos desde diferentes partes, en aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos.[118]

Alguno de estos delitos sin tipificar correctamente en Colombia abarcarían: interceptación ilícita de archivos gubernamentales, gromming, pornografía infantil, ataques a la integridad, disponibilidad del sistema, autenticación de los certificados, en donde ésta queda corta al tratar estos temas o lo hacen de manera superficial sin darle la importancia real y porque los artículos actuales no logran englobar la temática y deja algunos de estos puntos por fuera, por ejemplo es el caso de la pornografía infantil o gromming no se contemplan de manera directa, siendo que son delitos graves por tratarse de menores de edad y violación a los derechos y esto se evidencia porque si se realiza un análisis a los actuales, son tratados como agravios, más que como un delito en toda la palabra, el gromming ya es incluso tipificado como delito en algunos países de Europa incluso es tomado en cuenta en algunos de latino américa, y esto se puede evidenciar en algunos comparativos realizados en los capítulos previos donde se contrasta las leyes en varios países.

De este modo, se puede concluir la ley 1273 de 2009 esta desactualizada y requiere que se le dé un estudio por parte de las autoridades responsables, en el cual se pueda contemplar adiciones, ajustes tanto a los actuales artículos como la generación de los faltantes, con el fin de dar una tipificación acorde al delito, afección y perjuicio, estas mejoras a la ley de delitos informáticos podría establecer un bien reglamentario y judicial que vaya de la mano con las necesidades, penalizaciones que cada delito realmente se merezca, y es que un factor de ciberdelincuencia actual es que se dejan pasar muchas cosas que aunque mínimas son el inicio de delitos más graves.

[118] Mary angélica Carvajal avellaneda - Nataly Rangel Ruíz - universidad libre de Colombia seccional Cúcuta biblioteca Manuel José Vargas Duran - Análisis comparativo del tratamiento jurídico dado a los delitos informáticos en el derecho penal colombiano y español. {en línea} [disponible en] http://repository.unilibre.edu.co/bitstream/handle/10901/9330/trabajodegradodelitosinformaticos.docx?sequence=1

Se logró identificar que dentro de este contexto, no solamente existen falencias y/o ambigüedades, sino que también no es clara la competencia de las diferentes autoridades que pueden procesar las denuncias que se reciben a diario frente a esta problemática, así por ejemplo se puede decir, que falta capacitación a las autoridades o entes encargados y el diseño claro de un apartado de competencia que defina quien debe seguir el debido proceso en suceso que involucre la parte digital/información y todo lo relacionado con TI, medios informáticos o transmisión de activos, teniendo en cuenta el origen del lugar a partir de que se comete el delito y el lugar donde se llega a ejecutar como tal. Por esta clase de circunstancias los procesos se pueden pasar de una autoridad a otra como se analizó en las sentencias dentro de este proyecto y de esta manera dejan la posibilidad de terminación de términos que pueda favorecer en ese caso al delincuente y no a la víctima.

Por lo anteriormente expuesto, se puede confirmar y observar que la ley colombiana 1273, a pesar de haber sido creada para dar un tratamiento de carácter jurídico frente a la aparición de ciberdelincuencia este aun es ambiguo porque ya se quedó pequeño frente a todo lo que abarca la ciberdelincuencia, cibercrimen y términos relacionados a la seguridad informática, , ya que desde hace varios años ha ido creciendo en todo el territorio nacional, por lo que es imperativo generar nuevas estrategias contra los delitos informáticos y el fortalecimiento del bien jurídico y a su vez integre las medidas que deben aplicarse en cuanto a seguridad informática, con el fin de reducir, prevenir o mitigar el daño causado por esta problemática.

Para finalizar la identificación y la falta de un artículo de definiciones aún es muy insipiente porque crear un glosario que abarque todos estos términos informáticos sería un anexo larguísimo pero que a la larga serviría como un punto de base para entender todo lo que tiene por dentro un proceso de delincuencia informática, según sea contemplado por la autoridad competente, con ello se evitaría que cierto delitos cometidos mediante el uso de aplicaciones o dispositivos informáticos sean juzgados por error de manera ordinaria saltándose la ley vigente para estos casos.

Hacer frente a los desafíos requiere de esfuerzos diplomáticos y la cooperación internacional. Para que la seguridad cibernética sea efectiva y de forma adecuada la cooperación es esencial.[119]

[119] Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? - Informe Ciberseguridad 2016

Dentro del desarrollo de este proyecto se muestran y analizan las diversas técnicas de cibercriminalidad que se cometen con más frecuencia en Colombia, teniendo en cuenta el origen y evolución de las nuevas tecnologías en el ámbito informático, los nuevos métodos implementados y mejorados a través de las diferentes versiones de los métodos, técnicas o herramientas que pueden ser aplicados y desarrollados de forma que facilite a los delincuentes las diferentes actividades ilícitas, ya sean de robo, suplantación, estafa y demás delitos que puedan estar clasificados dentro de la lista creciente de las nuevas formas criminales de atentar contra la confidencialidad, integridad y disponibilidad de la información, así mismo que atentan contra los bienes de tipo mueble e intangibles con valor económico de las personas que son víctimas de estos ataques. Por lo que es posible evidenciar que Colombia aún tiene huecos y baches en los que se pueden cometer delitos difícilmente tipificarles y no contemplados en la ley actual, pero que son bastante graves y delicados por sus características en los ámbitos de seguridad informática y que se puedan sancionar correctamente, algunos que pueden incluso dejar daños irreparables en todos los entornos de desarrollo y crecimiento de los diferentes países de Latinoamérica, Colombia las organizaciones y sus usuarios.

## 13. RECOMENDACIONES.

Se requiere de un estudio e investigación de las leyes, políticas y normas colombianas frente a la seguridad de datos de la información, con el objetivo de promover la protección de la misma por medio de generación y proposición de medidas o estrategias que permitan un buen manejo de los activos información y de las nuevas tecnologías, así mismo proponer sanciones que vayan acordes a la problemática. Es esencial transmitir desde el nivel nacional políticas de seguridad informática que puedan adaptarse a las necesidades de las empresas colombianas y en cada una de ellas, brindar la capacitación necesaria a sus funcionarios para poder implementarlas y lograr disminuir, prevenir o corregir los daños causados por los ataques y delitos informáticos.[120]

También es importante contar con el interés de equipos interdisciplinarios delegados por ententes gubernamentales, personal TI y personal capacitado en derecho con el fin de generar las mejoras continuas y ajustes a la normatividad actual que permita tipificar de mejor manera los delitos informáticos, según su envergadura.

Esto conlleva a la humanidad a establecer convenios multilaterales para vencer las barreras que existen y cumplir el reto que se tiene a gran escala con la creación de legislaciones más multidimensionales, concisas y que sean manejadas con un idioma universal que pongan un poco de orden y permitan a los usuarios desde cualquier nación saber cómo protegerse no importando en qué lugar este, porque, así como la tecnología, las comunicaciones y la era del internet de las cosas es universal así lo sea el modo de protección y de legislación.

[120] Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia Zulay Nayiv Sánchez castillo – universidad nacional abierta y a distancia —unadll escuela de ciencias básicas e ingeniería especialización en seguridad informática Chiquinquirá 2017

## 14. NOMBRE DE LAS PERSONAS QUE PARTICIPAN EN EL PROYECTO

En las tablas siguientes se describe las dos personas que participan en el proyecto

Tabla 2 y tabla 3

**Tabla 10. Participante 1**

| Nombre del estudiante: Luisa Fernanda Acuña López | | | | | |
|---|---|---|---|---|---|
| Identificado con | C.C x | C.E | Otro | Número: 1088283569 | |
| Programa Académico | | Especialización en Seguridad informática | | Correo Electrónico | umianimeluisa@gmail.com |
| No. de Créditos Aprobados del plan de estudios: | | 25 | | Promedio Acumulado: | 4.6 |
| Dirección residencia: cl. 12#28-38 álamos edificio virrey apto 403 | | | | | Municipio / Departamento Pereira / Risaralda |
| Teléfono / Celular 3122461362 | | | | Zona Occidente | CEAD Dosquebradas |

***Tabla 11. Participante 2***

| Nombre del estudiante: Sandra Milena Villa Motato | | | | | |
|---|---|---|---|---|---|
| Identificado con | C.C. x | C.E | OTRO | Número: 42118465 | |
| Programa Académico | | Especialización en Seguridad informática | | Correo electrónico | sandra.mvillam@gmail.com |
| No. De Créditos Aprobados y porcentaje de créditos aprobados frente al plan de estudio: | | 25 | | Promedio Acumulado: | 4.7 |
| Dirección: villa roció Manzana 3 -26 casa 17 | | | | | Municipio / Departamento Pereira / Risaralda |
| Teléfono / Celular 3173951308 | | | | Zona Occidente | CEAD Dosquebradas |

## 15. BIBLIOGRAFÍA.


1. Guzmán a, clara lucía. “contextualización del cibercrimen en Colombia - tecnología en redes 130-472—1” {2009}
2. Cybercrime news, artículos y actualizaciones {en línea}, disponible en: (https://www.scmagazine.com/cybercrime/topic/47218/)
3. Yagub, mimi, “cybercrime in Colombia: ¿an underestimated threat?” {en línea} (2014) disponible en: (http://www.insightcrime.org/news-analysis/cyber-crime-colombia-underestimated-threat)
4. Mari, angélica - brasil tech, “latin america braces for rise in cybersecurity threats” {2016} {en línea} disponible en: (http://www.zdnet.com/article/latin-america-braces-for-rise-in-cybersecurity-threats/)
5. Infolaft, “lo que debe saber sobre el cibercrimen en Colombia”, {2014} {en línea} disponible en: (http://www.infolaft.com/es/art%c3%adculo/lo-que-debe-saber-sobre-el-cibercrimen-en-colombia)
6. Bolaños, Andrés días, universidad nacional abierta y a distancia UNAD. “análisis comparativo sobre delitos informáticos en Colombia - con relación a seis países de Latinoamérica - escuela de ciencias básicas, tecnología e ingeniería. {2014}
7. Symantec, organización estados americanos, “tendencias de seguridad cibernética en américa latina y el caribe “{2014}
8. INFORME CIBERSEGURIDAD – “Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?” {2016} –{en línea} Disponible en: (http://observatoriociberseguridad.com/)
9. VARGAS V, Edisson Mauricio, “ciberseguridad y ciberdefensa: ¿qué implicaciones tienen para la ¿seguridad nacional?” {2014}
10. Pandasecurity “la primera mitad de 2017 ha registrado un número sorprendente de ciberataques a gran escala “, {en línea} disponible en: (https://www.pandasecurity.com/spain/mediacenter/noticias/ciberataques-hasta-la-fecha/)
11. Pandasecurity “la primera mitad de 2017 ha registrado un número sorprendente de ciberataques a gran escala “, {en línea} disponible en: (https://www.pandasecurity.com/spain/mediacenter/noticias/ciberataques-hasta-la-fecha/)
12. Siliconweek spain, “estudio del aumento del cibercrimen en latinoamérica” –{2012} {en línea} disponible en: (http://www.mundodigital.net/estado-del-cibercrimen-en-latinoamerica/)
13. Azuaje, miguel, “argentina se blindará contra cyberdelitos” –{nov 10, 2017} {en línea} disponible en: (http://segundoenfoque.com/argentina-se-blindara-contra-cyberdelitos-2017-11-10)

14. Cooperativa-cl, (2016) chile, cuarto en tasa de cibercrimen en Latinoamérica – {en línea} disponible en: http://www.cooperativa.cl/noticias/tecnologia/internet/seguridad/chile-cuarto-en-tasa-de-cibercrimen-en-latinoamerica/2016-09-30/113344.html
15. Cancino, Héctor - ciber crimen “el cibercrimen posa su mirada en américa latina” {2017} {en línea} disponible en: (https://tecno.americaeconomia.com/articulos/el-cibercrimen-posa-su-mirada-en-america-latina)
16. Dinero, “el cibercrimen en Latinoamérica” {2014} – {en línea} disponible en: (http://www.dinero.com/actualidad/noticias/articulo/el-cibercrimen-latinoamerica/192369)
17. Eelpais, “los ciberataques a infraestructuras estratégicas se multiplican por siete en solo dos años” {2014} {en línea} disponible en: https://politica.elpais.com/politica/2017/05/24/actualidad/1495619175_136537.html)
18. Mendoza, miguel ángel, “seguridad corporativa en Latinoamérica: causas de incidentes y controles utilizados”, {2017} –{en línea} disponible en (https://www.welivesecurity.com/la-es/2017/04/27/seguridad-corporativa-en-latinoamerica/)
19. Moreno, Guadalupe, wannacry, “lazarus es una de entre muchas”, {16/05/2017} –{en línea} disponible en (https://es.statista.com/grafico/9409/lazarus-es-una-de-entre-muchas/)
20. Explainer: fighting cybercrime in Latin America (2013) Rachel glickhouse {en línea} disponible en: (http://www.as-coa.org/articles/explainer-fighting-cybercrime-latin-america)
21. Globalservices, “amenazas del cibercrimen en Colombia”, {2016-2017} {en línea} disponible en: (https://www.globalservices.bt.com/latam/es/blog/amenazas-del-cibercrimen-en-colombia-2016-2017)
22. La republica.co Colombia se pierden cerca de US$ 600 millones por el cibercrimen- {en línea} Disponible en: 2017 (https://imgcdn.larepublica.co/cms/2017/03/02232524/al-ataquesciber0303.jpg)
23. Eumed “los delitos informáticos. tratamiento internacional” {2012} {en línea} disponible en: (http://www.eumed.net/rev/cccss/04/rbar2.htm)
24. Pladna - brett, east Carolina university “the lack of attention in the prevention of cyber crime and how to improve it”- {en línea} disponible en: (http://www.infosecwriters.com/text_resources/pdf/bpladna_cybercrime.pdf)
25. cisco, “informe anual de seguridad” - {2016}
26. Cancino, Héctor - ciber crimen, “el cibercrimen posa su mirada en américa latina”, {2016}

27. –{en línea} disponible en: https://tecno.americaeconomia.com/articulos/el-cibercrimen-posa-su-mirada-en-america-latina
28. GESI – Universidad de Granada – {2017} La cibercriminalidad como instrumento para la expansión y empoderamiento del crimen organizado {en línea} disponible en: ( http://www.seguridadinternacional.es/?q=es/content/la-cibercriminalidad-como-instrumento-para-la-expansi%C3%B3n-y-empoderamiento-del-crimen )
29. Eleconomista –{2018} Check Point: "La ciberdelincuencia del internet de las cosas busca sobre todo el dinero" {en línea} disponible en: ( https://www.eleconomista.es/tecnologia/noticias/8930004/02/18/Avi-Rembaum-Check-Point-La-ciberdelincuencia-IoT-busca-sobre-todo-el-dinero-no-se-diferencia-de-otras-actividades.html )
30. Investigación VIU- Universidad de Valencia - Informe-Ciberseguridad – Ciberseguridad Tendencias 2017 - {2017}
31. Cancillería , “consejo de Europa invitó a Colombia a adherir a la convención sobre delito cibernético” {2013} {en línea} disponible en: (http://www.cancilleria.gov.co/newsroom/news/consejo-europa-invito-colombia-adherir-la-convencion-sobre-delito-cibernetico )
32. Delitosinformaticos.com {2000-2012} “legislación sobre delitos informáticos España” {en línea} disponible en: (https://delitosinformaticos.com/legislacion/espana.shtml)
33. Hg.org - hgexperts.com “data protection”. {1996-2017} {en línea} disponible en: (https://www.hg.org/data-protection.html)
34. Redipd –“red iberoamericana de protección de datos” {2009} -{en línea} Disponible en: (http://www.redipd.es/index-ides-idphp.php)
35. Redipd –“red iberoamericana de protección de datos” {2009} -{en línea} Disponible en: (http://www.redipd.es/index-ides-idphp.php)
36. Universidad militar granada facultad de ciencias económicas- importancia de la implementación del concepto de Ciberseguridad organizacional en las organizaciones tipo Pymes –[2015]
37. Redipd –“red iberoamericana de protección de datos” {2009} -{en línea} Disponible en: (http://www.redipd.es/index-ides-idphp.php
38. Solvetic“Tipos de ataques informáticos e intrusos y cómo detectarlos” {jun 24 2016} {en línea} Disponible en: (https://www.solvetic.com/page/noticias/s/profesionales/tipos-de-ataques-informaticos-e-intrusos-y-como-detectarlos)
39. CNN –“Las 5 formas de cibercrimen que marcarán el 2016 en América Latina” {2016} - {en línea} Disponible en: (Http://cnnespanol.cnn.com/2015/11/20/las-5-formas-de-cibercrimen-que-marcaran-el-2016-en-america-latina/)

40. organized crime in the Americas, “¿Can Latin American Governments Keep Up with Cyber Criminals? “, (2016) insight Crime, {en línea} Disponible en: (http://www.insightcrime.org/news-analysis/can-latin-american-govt-keep-up-with-cyber-criminals)
41. Gadelha, Silvia, Head of Financial Lines, Brasil at XL Catlin “Cybercrime in Latinoamérica” {2016}, {en línea} Disponible en: (Http://xlcatlin.com/fast-fast-forward/articles/cybercrime-in-latin-america)
42. Enter.co s.a.s, “el nuevo blanco de los cibercriminales en Colombia son las empresas” (2017) {en línea} disponible en: (http://www.enter.co/chips-bits/seguridad/empresas-el-nuevo-blanco-de-los-cibercriminales-en-colombia/)
43. Pandasecurity” los 6 ataques de seguridad más famosos de 2014 {2014} - {en línea} disponible en: (https://www.pandasecurity.com/spain/mediacenter/seguridad/los-6-ataques-de-seguridad-mas-famosos-de-2014/)
44. Gestión de Riesgo en la Seguridad Informática - amenazas vulnerabilidades - {en línea} Disponible en: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/
45. Seguinfo dimensiones de un sgsi - {en línea} (2007) Disponible en: <https://seguinfo.wordpress.com/2007/08/21/dimensiones-de-un-sgsi/>
46. Las dimensiones de la seguridad de la información - {en línea} Disponible en: https://www.seguridadycontinuidad.com/las-dimensiones-de-la-seguridad-de-la-informacion
47. Malware vs Virus: ¿Cuál es la diferencia? – antivirus cómodo {en línea} (2018) Disponible en: antivirus.comodo.com
48. Welivesecurity - ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia {en línea} (2015) Disponible en: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/
49. Kaspersky - Ciberdelincuencia y Ciberdelitos {en línea} (2012) Disponible en: https://www.kaspersky.es/resource-center/threats/computer-vandalism
50. MAGERIT is the methodology of analysis and risk management developed by the High Council of Electronic Administration {en línea} (2012) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en#.Wqmh2ujOXDc

51. Documento Conpes Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA {en línea} (2001) Disponible en: https://www.dnp.gov.co/CONPES/documentos-conpes/Paginas/documentos-conpes.aspx
52. Convenio sobre ciberdelincuencia - {en línea} (2001) Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
53. Caracterización de los delitos informáticos en Colombia [en línea] 2012 {disponible en} http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewFile/126/149
54. Council of Europe, (2014).Convention on Cybercrim CETS No.: 185.Recuperado de http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=E
55. Delitos relativos a la propiedad intelectual [en línea] {disponible en} http://www.portaley.com/delitos-informaticos/delitos-intelectual.shtml
56. ley de delitos informáticos en Colombia {en línea} 1997 - 2017 j. c. daccach. delta asesora disponible en: http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia
57. Colombia formalizó su ingreso a la OTAN y se convierte así en el primer socio global latinoamericano http://www.france24.com/es/20180531-colombia-otan-bruselas-latinoamerica
58. Cinco aspectos clave del ingreso de Colombia como socio de la OTAN {en línea} 2018 {disponible en}: http://misionverdad.com/TRAMA-GLOBAL/cinco-aspectos-sobre-colombia-como-socio-global-de-la-otan
59. Colombia va a tener un estatus privilegiado de cooperación con la OTAN, de gran interés y utilidad para el país: Presidente Santos {en línea} 2018 {disponible en}: http://es.presidencia.gov.co/noticia/180528-Colombia-va-a-tener-un-estatus-privilegiado-de-cooperacion-con-la-OTAN-de-gran-interes-y-utilidad-para-el-pais-Presidente-Santos
60. ciberdelincuentes y cibervictimas {en línea} 2010 (disponible en:) https://www.ehu.eus/documents/1736829/2010409/clc+91+ciberdelincuentes+y+cibervictimas.pdf
61. caracterización de los delitos informáticos en Colombia {en línea} 2012 (disponible en:) http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewfile/126/149

62. Los delitos informáticos desde el punto de vista del Derecho {en línea} 2017 (disponible en:) https://www.kennedy.edu.ar/noticia/los-delitos-informaticos-desde-el-punto-de-vista-del-derecho/
63. Delitos informáticos: mal uso de Tecnologías de Información y Comunicación {en línea} 2009 (disponible en:) http://noticias.universia.net.co/vida-universitaria/noticia/2009/09/04/236295/delitos-informaticos-mal-uso-tecnologias-informacion-comunicacion.html
64. Colombia el primer país que penaliza los delitos informáticos- la patria [disponible en] (en línea) http://repository.unad.edu.co/bitstream/10596/2668/5/76323713.pdf
65. Santiago Cisneros- normas y leyes que existen en Colombia para delitos informáticos –(en línea) [disponible en] https://www.slideshare.net/santiagocisneros6/normas-y-leyes-que-existen-en-colombia-para-delitos-informaticos
66. banrep leyes- {disponible en][en línea] http://www.banrep.gov.co/es/temas/6923
67. la patria {disponible en][en línea http://www.lapatria.com/tecnologia/colombia-el-primer-pais-que-penaliza-los-delitos-informaticos-1980
68. secretaria de gobierno {disponible en] 2012 [en línea http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html
69. ¿por qué las personas cometen delitos informáticos?, por bobby stocks {en línea} 2001-2018, leaf group ltd (disponible en:) https://techlandia.com/personas-cometen-delitos-informaticos-sobre_96220/
70. Comunidad americana -edu. Articulo realizar {en línea} (disponible en: ) http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewfile/126/149
71. Estudios psicológicos de los delincuentes informáticos (aproximación a los perfiles de personalidad de los sujetos que realizar {en línea} 2006-2016 (disponible en:)
72. Es groorming un delito – internet-gromming {en línea} (disponible en:) https://internet-grooming.net/es-un-delito-el-grooming/
73. camilo Gutiérrez Amaya Welivesecurity los 10 delitos informáticos por lo que se dieron condenas en la historia {en línea} 2013 disponible en: https://www.welivesecurity.com/la-es/2013/11/12/top-10-condenados-por-delitos-informaticos-quienes-fueron-primeros-historia/
74. Enter.co – Guías lleva a tu negocio a internet ingeniería social {en línea} (disponible en:) http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/
75. Botnets, techtarget {en línea} 2017 (disponible en:) http://searchsecurity.techtarget.com/definition/botnet

76. Ddos attack definitions - ddospedia {en línea} 2017 (disponible en:) radware ltd. https://security.radware.com/ddos-knowledge-center/ddospedia/botnet/
77. What is a ddos attack? ©2013 ddos data https://www.digitalattackmap.com/understanding-ddos/
78. Distributed denial of service (ddos) attack -2000 - 2017, techtarget {en línea} 2017 (disponible en:
79. http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack
80. What does ddos mean? 2017 imperva {en línea} 2017 (disponible en: https://www.incapsula.com/ddos/denial-of-service.html
81. El tiempo delito de hackers Colombia {en línea} (disponible en:) http://www.eltiempo.com/justicia/cortes/delitos-de-hackers-en-colombia-52232
82. El tiempo delito de hackers Colombia {en línea} (disponible en:) http://www.eltiempo.com/justicia/cortes/delitos-de-hackers-en-colombia-52232
83. Análisis de riesgos iso 27005 vs margerit y otras metodologías {en línea} (disponible en:) https://delitosinformaticos.com/10/2009/proteccion-de-datos/analisis-de-riesgos-iso-27005-vs-magerit-y-otras-metodologias
84. El tiempo delito de hackers Colombia {en línea} (disponible en:) http://www.eltiempo.com/justicia/cortes/delitos-de-hackers-en-colombia-52232
85. Tuabogadodefensor delitos informáticos {en línea} 2015 disponible en: http://www.tuabogadodefensor.com/delitos-informaticos/
86. Camilo Gutiérrez Amaya Welivesecurity los 10 delitos informáticos por lo que se dieron condenas en la historia {en línea} 2013 disponible en: https://www.welivesecurity.com/la-es/2013/11/12/top-10-condenados-por-delitos-informaticos-quienes-fueron-primeros-historia/
87. Caracterización de los delitos informáticos en Colombia {en línea} 2012 (disponible en:) http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewfile/126/149
88. ¿Por qué las personas cometen delitos informáticos?, Por bobby stocks {en línea} 2001-2018, Leaf Group Ltd (disponible en:) https://techlandia.com/personas-cometen-delitos-informaticos-sobre_96220/
89. Perfiles de personalidad de los delincuentes informáticos psicopsi {en línea} 2014 disponible en: http://psicopsi.com/Estudios-psicologicos-de-los-delincuentes-informaticos-Aproximacion-a-los-perfiles-de-personalidad-de-los-sujetos-que-realizaron

90. Tuabogadodefensor delitos informáticos {en línea} 2015 disponible en: http://www.tuabogadodefensor.com/delitos-informaticos/
91. Informaticaforenseuccaraucacolombia {en línea} 2014 disponible en: http://informaticaforenseuccaraucacolombia.blogspot.com.co/2014/03/el-perfil-criminologico-del-delincuente.html
92. Análisis comparativo sobre delitos informáticos en Colombia Con relación a seis países de Latinoamérica – Bolaños A – Narváez T, universidad nacional abierta y a distancia "unad" [en línea]2014{disponible en} http://repository.unad.edu.co:8080/handle/10596/2728
93. Calderón R, Guzmán G, Salinas J. (2011). Diseño y Plan de Implementación de un Laboratorio de Ciencias Forenses Digitales Tesina de Seminario. Guayaquil – Ecuador. Escuela Superior Politécnica del Litoral.
94. 24Calderón R, Guzmán G, Salinas J. (2011). Diseño y Plan de Implementación de un Laboratorio de Ciencias Forenses Digitales Tesina de Seminario. Guayaquil – Ecuador. Escuela Superior Politécnica del Litoral.
95. La comisión International Electrotechnical Commission (IEC): 41 Ley 19.628 Protección de datos de carácter personal disponible en: http://www.leychile.cl/Navegar?idNorma=141599 42 Ley 19.223 Ley Relativa a delitos informáticos disponible en: http://www.leychile.cl/Navegar?idNorma=30590 43 Ley 19.799 Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma disponible en: http://www.leychile.cl/Navegar?idNorma=196640 44
96. Los-3-delitos-informaticos-mas-astutos-de-la-historia [en línea] 2017 {disponible en:} http://blogs.adobe.com/latinoamerica/2017/11/14/los-3-delitos-informaticos-mas-astutos-de-la-historia/
97. 7900 Vulnerabilidades no entraron en la base de datos CVE en [en línea] 2017 {disponible en} https://www.infosecurity-magazine.com/news/7900-vulnerabilities-didnt-make-it/
98. Telcelsoluciones - que-es-el-ciberterrorismo-y-por-que-debe-preocuparte [en línea] 2017 {disponible en:} http://www.telcelsoluciones.com/articulos/que-es-el-ciberterrorismo-y-por-que-debe-preocuparte
99. el-ciberterrorismo-una-actividad-continuo-crecimiento-articulo-523789
100. elespectador.com [en línea] 2014 {disponible en:} https://www.elespectador.com/noticias/actualidad/el-ciberterrorismo-una-actividad-continuo-crecimiento-articulo-523789
101. que-es-el-ciberterrorismo ciberderecho [en línea] 2014 {disponible en:} http://www.ciberderecho.com/que-es-el-ciberterrorismo/

102. forbes - cyber-warfare-the-threat-from-nation-states [en línea] 2014 {disponible en:} https://www.forbes.com/sites/kateoflahertyuk/2018/05/03/cyber-warfare-the-threat-from-nation-states/#2c9de18b1c78
103. searchsecurity.techtarget- cyberwarfare [en línea] {disponible en:} https://searchsecurity.techtarget.com/definition/cyberwarfare
104. rand.org- cyber-warfare [en línea] 2014 {disponible en:} https://www.rand.org/topics/cyber-warfare.html
105. MChaparro - Legislación informática y protección de datos en Colombia, comparada con otros países [en linea] 2014 {disponible en} http://biblioteca.uniminuto.edu/ojs/index.php/Inventum/article/download/1014/953
106. Link.springer.com [en línea] {disponible en}: https://link.springer.com/chapter/10.1007/978-3-642-39498-0_12
107. Informe sobre ataques informáticos en Colombia y al sector financiero [en línea] {disponible en}: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370
108. “CIBERATAQUES A LA MEDIDA” Un oficial del Centro Cibernético Policial de Colombia explica estrategia para elecciones [en línea] 2018 [disponible en] https://www.elespectador.com/noticias/judicial/un-oficial-del-centro-cibernetico-policial-de-colombia-explica-estrategia-para-elecciones-articulo-737056
109. Caracterización de los delitos informáticos en Colombia Characterization of cybercrime in Colombia http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewFile/126/149
110. Urnadecristal septiembre [en línea] de 2014 {disponible en}: www.urnadecristal.gov.co/gestion-gobierno/dejatus-comentarios-al-decreto-que-reglamenta-ley-detransparencia
111. Sedici.unlp {en línea} [disponible en] http://sedici.unlp.edu.ar/handle/10915/42145
112. Derechos ecuador – delitos informáticos {en línea} [disponible en] https://www.derechoecuador.com/delitos-informaticos
113. Segu-info - estados unidos delitos {en línea} [disponible en]: https://www.segu-info.com.ar/delitos/estadosunidos.htm
114. informatice – jurídica legislación unión europea {en línea} [disponible en]: http://www.informatica-juridica.com/legislacion/union-europea/
115. Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. {en línea} [disponible en]

http://webcache.googleusercontent.com/search?q=cache:http://conaiisi.unsl.edu.ar/2013/82-553-1-DR.pdf

116. Delitos informáticos – delitos Venezuela {en línea} [disponible en] https://www.delitosinformaticos.com/estafas/delitosvenezuela.shtml

117. Analysis of the criminalization of cybercrime in Spanish-speaking countries Análise da criminalização do cibercrime nos países de lingual Española. {en línea} [disponible en]: http://revistalogos.policia.edu.co/index.php/rlct/article/view/339/html

118. Monografías – Trabajos [en línea] {disponible en}: http://www.monografias.com/trabajos6/delin/delin2.shtml#ixzz5evosszrt

119. link.springer.com - [en línea] {disponible en}: https://link.springer.com/chapter/10.1007/978-3-642-39498-0_12

120. Mary angélica Carvajal avellaneda - Nataly Rangel Ruíz - universidad libre de Colombia seccional Cúcuta biblioteca Manuel José Vargas Duran - Análisis comparativo del tratamiento jurídico dado a los delitos informáticos en el derecho penal colombiano y español. {en línea} [disponible en] http://repository.unilibre.edu.co/bitstream/handle/10901/9330/trabajodegradodelitosinformaticos.docx?sequence=1

121. Mary angélica Carvajal avellaneda - Nataly Rangel Ruíz - universidad libre de Colombia seccional Cúcuta biblioteca Manuel José Vargas Duran - Análisis comparativo del tratamiento jurídico dado a los delitos informáticos en el derecho penal colombiano y español. {en línea} [disponible en] http://repository.unilibre.edu.co/bitstream/handle/10901/9330/trabajodegradodelitosinformaticos.docx?sequence=1

122. Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? - Informe Ciberseguridad 2016

123. Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia Zulay Nayiv Sánchez castillo – universidad nacional abierta y a distancia —unadǁ escuela de ciencias básicas e ingeniería especialización en seguridad informática Chiquinquirá 2017

# 16. DOCUMENTO RAE

**ANEXO 1. RESUMEN ANALÍTICO ESPECIALIZADO - RAE**

| Información General | |
|---|---|
| **Tema** | ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA |
| **Titulo** | ESTADO ACTUAL DEL CIBERCRIMEN EN COLOMBIA CON RESPECTO A LATINOAMÉRICA |
| **Tipo de proyecto** | MONOGRAFIA |
| **DIRECTOR** | MARTIN CAMILO CANCELADO |
| **Autor (es)** | LUISA FERNANDA ACUÑA LOPEZ Y SANDRA MILENA VILLA MOTATO |
| **Fuente Bibliográfica** | • Guzmán a, clara lucía. "contextualización del cibercrimen en Colombia - tecnología en redes 130-472—1" {2009}<br>• Bolaños, Andrés días, universidad nacional abierta y a distancia UNAD. "análisis comparativo sobre delitos informáticos en Colombia - con relación a seis países de Latinoamérica - escuela de ciencias básicas, tecnología e ingeniería. {2014}<br>• INFORME CIBERSEGURIDAD – "Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?" {2016} –{en línea} Disponible en: (http://observatoriociberseguridad.com/)<br>• Gadelha, Silvia, Head of Financial Lines, Brasil at XL Catlin "Cybercrime in Latinoamérica" {2016}, {en línea} Disponible en: (Http://xlcatlin.com/fast-fast-forward/articles/cybercrime-in-latin-america)<br>• Enter.co s.a.s, "el nuevo blanco de los cibercriminales en Colombia son las empresas" (2017) {en línea} disponible en: (http://www.enter.co/chips-bits/seguridad/empresas-el-nuevo-blanco-de-los-cibercriminales-en-colombia/)<br>• Seguinfo dimensiones de un sgsi - {en línea} (2007) Disponible en: <https://seguinfo.wordpress.com/2007/08/21/dimensiones-de-un-sgsi/><br>• Las dimensiones de la seguridad de la información - {en línea} Disponible en: https://www.seguridadycontinuidad.com/las-dimensiones-de-la-seguridad-de-la-informacion<br>• Documento Conpes Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA {en línea} (2001) Disponible en: https://www.dnp.gov.co/CONPES/documentos-conpes/Paginas/documentos-conpes.aspx<br>• Convenio sobre ciberdelincuencia - {en línea} (2001) Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf<br>• Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia Zulay Nayiv Sánchez castillo – universidad nacional abierta y a distancia ―unad‖ escuela de ciencias básicas e ingeniería especialización en seguridad informática Chiquinquirá 2017 |
| **Año** | 2018 |
| **Resumen** | La presente monografía se desarrolla para determinar las falencias existentes en la legislación Colombiana en cuanto a delitos informáticos el impacto que ha tenido en las empresas con respecto |

| | |
|---|---|
| | a los países de Latinoamérica, bajo los lineamientos del Convenio de Ciberdelincuencia de 2001, porque el especialista de Seguridad Informática necesita conocer la posición que ha tomado su país en la defensa y preservación integral de los sistemas informáticos en contra de los ciberdelincuentes, como personas y desde cualquier campo de la ciencia, cada colombiano está llamado a realizar aportes que contribuyan al fortalecimiento de la seguridad, y desde la Ingeniería de Sistemas, aún más, desde el punto de vista de los Especialistas en Seguridad Informática debe existir una preocupación más alta por formular alternativas de mejora y es que seguridad cibernética debería no ser algo de cada país individual ya que una nación por sí sola puede asegurar adecuadamente sus redes. La cooperación es esencial de ahí que es muy importante realizar comparativos sobre que está haciendo Colombia en contraste con sus países vecinos y que podría aprender de ellos y que puede enseñarles. |
| **Palabras Claves** | CiberCrimen, Arquitectura, protocolos, plataformas, estadísticas, delitos informáticos, ataques vulnerabilidades y riesgos, información, informática, sistemas. Legislaciones, normatividad, ciberdefensa debería ir confidencialidad integridad |
| **Contenidos** | • 7. Determinar los delitos informáticos y cuáles actividades delictivas se catalogan de acuerdo a la "organización de las naciones unidas (onu) en el convenio de ciberdelincuencia de 2001"<br>o 7.1 análisis y comparativo inicial<br>o 7.2 análisis de artículos incluidos en el documento de conpes<br>o 7.3 legislación en colombia<br>o 7.4 análisis otan<br>o 7.5 que son los delitos informáticos y que son las políticas de seguridad<br>• 8. Revisar y exponer el panorama de los cibercrímenes que afectan en mayor medida a latinoamérica<br>o 8.1 analizar la evolución de la criminalidad informática<br>o 8.2 evolución legislativa de diferentes países<br>o 8.3 7900-vulnerabilities que no se tuvieron en cuenta para el año 2018<br>o 8.4 ciberterrorismo<br>o 8.5 ciberwarface<br>• 9. Realizar un análisis del impacto negativo que tiene la ciberdelincuencia en las empresas colombiana por medio de la revisión de datos estadísticos públicos como la fiscalía general de la nación y la policía nacional<br>o 9.1 análisis sobre el impacto negativo que tiene la ciberdelincuencia en las empresas colombianas.<br>o 9.2 revisión de datos estadísticos públicos como la fiscalía general de la nación y la policía nacional<br>• 10. Determinar las diferencias y similitudes que existen entre la normatividad colombiana y las normatividades de los países analizados mediante una observación comparativa.<br>o La ley de protección |
| **Descripción del Problema de Investigación** | |

En Colombia como en todos los países de Latinoamérica las tecnologías de la información y las comunicaciones se han ido incorporando a un ritmo acelerado, siendo usado en cosas como: búsquedas en internet, compras, correo electrónico y juegos por nombrar algunos, por otro lado, la comunicación es más rápida y más confiable que en el pasado, pero el problema reside en que tan expuestos estamos a las amenazas, riesgos o vulnerabilidades y el cibercrimen, donde son inevitables las consecuencias, de quienes habitan la región se ven obligados a enfrentar un importante desafío al momento de proteger la información, garantizando la disponibilidad, integridad, trazabilidad, autenticidad y confiabilidad de los servicios prestados a través de Internet, donde la infraestructuras y sistemas críticos cada día son más exigentes causando en muchos caso que las empresas pierden su capital principal por no tener presente los principios de la seguridad de la información.

La seguridad informática se convirtió en un fuerte dolor de cabeza para las organizaciones. y en Colombia, particularmente, reside en el desconocimiento, porque es sorprendente lo poco que se sabe al respecto y más aún cuando las empresas, aunque saben sus riesgos o han enfrentado perdidas debido al delito informático guardan silencio y en parte es intencional, por temor a dañar su reputación y asustar a los clientes, además del menosprecio por el impacto de las amenazas cibernéticas hacen que los costos que pagan sean más altos; haciendo imperativo, determinar las falencias existentes en la norma sobre delitos informáticos (cibercrimen) a la luz de otras legislaciones y de tratados internacionales, que permitan proyectar leyes adecuadas y efectivas que cumplan con su misión de proteger, donde se debe buscar puntos de vista que favorezcan o amplíen la visión de la problemática, para lo cual se buscarán en las fuentes que se especializan en el estudio de estas áreas y temáticas relacionadas, donde los delito cibernéticos no reconocen fronteras nacionales y que se requiere un esfuerzo multilateral y multidimensional para abordar la cantidad de amenazas informáticas para las empresas y usuarios en general, porque como se decía previamente, todavía el cibercrimen es tratado como temas apartes en los diferentes lugares de Latinoamérica, cuando realmente son los mismos ataques y vulneraciones a las que día a día se enfrentan las empresas, y por ende con el fin de poder entender el estado actual del cibercrimen y que pueden hacer las organizaciones al respecto y estar mejor preparados para enfrentar esta creciente oleada de cibercrimen que cada día afecta más y más a las empresas donde se hace imperativo crear, implementar y generar conciencia en cuanto a seguridad informática se refiere, por lo cual es que surge la pregunta:

¿Cómo la identificación del estado actual del cibercrimen en Colombia con respecto a Latinoamérica ayudara a plantear mejoras de seguridad en las empresas?

## Objetivos

**OBJETIVO GENERAL**

- Realizar análisis de la situación de Colombia con respecto a Latinoamérica de las amenazas, utilizadas por los cibercriminales para atacar las tecnologías de información y como puede esto impactar en la seguridad de las empresas

**ESPECÍFICOS**

- Determinar los delitos informáticos y cuáles actividades delictivas se Catalogan de acuerdo a la "Organización de las Naciones Unidas (ONU) en el Convenio de Ciberdelincuencia de 2001".
- Revisar y exponer el panorama de los cibercrímenes que afectan en mayor medida a Latinoamérica
- Realizar un análisis del impacto negativo que tiene la ciberdelincuencia en las empresas colombiana por medio de la revisión de datos estadísticos públicos como la Fiscalía General de la Nación y la Policía Nacional.
- Determinar las diferencias y similitudes que existen entre la normatividad colombiana y las normatividades de los países analizados mediante una observación comparativa.

## Metodología

El presente proyecto es una monografía que se basa en la revisión bibliográfica y analítica, por medio del desarrollo del tema de delitos informáticos y el cibercrimen a través de comparativos a partir de una línea base de investigación sobre el tema escogido. Por otro lado, se tomó como herramienta de recolección y análisis de información el análisis documental, desde las normas de tipificación de delitos informáticos, normatividad y revisión de convenios internacionales como el CONPES, comparativos de los distintos delitos y casos reales, análisis de la ley colombiana contra las leyes de Latinoamérica y otros países externos

## Referentes Teóricos

El desarrollo de las tecnologías informáticas ofrece un aspecto negativo, a pesar de todos los beneficios que ha traído y es el hecho de que abre la puerta a conductas antisociales y delictivas. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas para infringir la ley y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.[121] Si no que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse.

Es importante entender en primera instancia que el delito cibernético se considera como aquellas actividades que se realizan de forma ilegal o que en algunas partes consideran ilícitas y que pueden realizarse a través de redes electrónicas, digitales de forma personal, nacionales o mundiales; donde estos se típica como crímenes cibernéticos donde se involucra algún dispositivo y desde él se realizan dichas actividades delictivas siendo una parte integral y necesaria del crimen[122], en esto tenemos a los atacantes o responsables de vulnerar la seguridad o es su contra parte defenderla, protegerla y salvaguardarla, ahora por el lado de los atacantes estos desarrollan cada día tecnologías y tácticas cada vez más sofisticadas, creando infraestructuras back-end (se refiere a la separación de preocupaciones entre la capa de presentación (front end) y la capa de acceso a datos (back end)) sólidas para el lanzamiento y soporte de sus campañas. Los ciberdelincuentes están perfeccionando sus técnicas para obtener dinero de sus víctimas y para evitar ser detectados mientras continúan robando datos y

[121] EUMED "los delitos informáticos. Tratamiento internacional" {2012} {en línea} Disponible en: (http://www.eumed.net/rev/cccss/04/rbar2.htm)

[122] PLADNA - Brett, East carolina University "The Lack of Attention in the Prevention of Cyber Crime and How to improve it"- {en línea} Disponible en: (http://www.infosecwriters.com/text_resources/pdf/BPladna_Cybercrime.pdf)

propiedad intelectuales,[123] a nivel mundial, y es que en el mundo muchas naciones, han tenido que verse frente a frente y mejorar sus esfuerzos doblando la seguridad con el fin de evitar manipulación política y sabotaje dirigido. Al mismo tiempo, los cibercriminales han causado niveles sin precedentes de interferencia, enfocándose en herramientas de TI y servicios en la nube relativamente sencillos[124]

**Referentes Teóricos y Conceptuales**

Vulnerabilidades y Amenazas: La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo, que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño[125]

Las dimensiones de la seguridad informática:

- La confidencialidad busca que la información que se considera importante o valiosa sea protegida, que se mantenga intacta y lejos de las personas que no tienen permitido el acceso a ella
- La integridad de la información implica que los datos no tengan errores, no sean modificados sin permiso, o estén incompletos en pocas palabras estén corruptos.
- La disponibilidad es lo que permite que la información siempre este activa, funcional y disponible en momento que se requiere, que no sea borrada por error o que sufra algún error.
- La autenticidad es lo que nos permite identificar el gestor de la información. Como por ejemplo saber que quien manda la información es realmente de donde se generó, evitando suplantación de identidad.
- La trazabilidad nos permite determinar todas y cada una de las acciones que realiza cada usuario, un histórico de los procedimientos a los que ha sido sujeto el archivo, dato o información. [126][127]

Criminalidad: son todas las acciones, causado por la intervención humana, que violan la ley y que están penadas por esta; y ciber crimen está relacionado a la cibernética o espacio digital.

Ciberseguridad Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.[128]

[123] CISCO, “Informe anual de seguridad” - {2016}

[124] CANCINO, Hector - Ciber crimen, “El cibercrimen posa su mirada en américa latina”, {2016} –{en línea} Disponible en: https://tecno.americaeconomia.com/articulos/el-cibercrimen-posa-su-mirada-en-america-latina

[125] Gestión de Riesgo en la Seguridad Informática - amenazas_vulnerabilidades - {en línea} Disponible en: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

[126] Seguinfo dimensiones de un sgsi - {en línea} (2007) Disponible en: <https://seguinfo.wordpress.com/2007/08/21/dimensiones-de-un-sgsi/>

[127] Las dimensiones de la seguridad de la información - {en línea} Disponible en: https://www.seguridadycontinuidad.com/las-dimensiones-de-la-seguridad-de-la-informacion

[128] Welivesecurity - ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia {en línea} (2015) Disponible en: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

Ciberdelincuencia son aquellas amenazas que por medio del uso de virus informáticos, malware y troyanos creados por estudiantes, jóvenes y desarrolladores entre otros entes, los cuales pueden dañar su ordenador.[129]

Hablando un poco de las políticas y controles que una organización puede implementar para gestionar y garantizar la protección de sus activos las cuales podría ser bajo la (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), la Gestión del Riesgo:[130]

1. Establecer una Política de la Organización al respecto: directrices generales de quién es responsable de cada cosa.
2. Establecer una Norma: objetivos a satisfacer para poder decir con propiedad que la amenaza ha sido conjurada.
3. Establecer unos Procedimientos: instrucciones paso a paso de qué hay que hacer.
4. Desplegar salvaguardas técnicas que efectivamente se enfrenten a las amenazas con capacidad para conjurarlas.
5. Desplegar controles que permitan saber que todo lo anterior está funcionando según lo previsto.

## Resultados y Conclusiones

Este documento al ser de carácter analítico, y por medio de generación de cuadros comparativos, sobre la normatividad en Colombia, la tipificación de los delitos informáticos ubicados en Latinoamérica y Colombia, y dentro del desarrollo de este proyecto se muestran y analizan las diversas técnicas de cibercriminalidad que se cometen con más frecuencia en Colombia; por lo que es posible evidenciar que Colombia aún tiene huecos y baches en los que se pueden cometer delitos difícilmente tipificarles y no contemplados en la ley actual, pero que son bastante graves y delicados por sus características en los ámbitos de seguridad informática y que se puedan sancionar correctamente, algunos que pueden incluso dejar daños irreparables en todos los entornos de desarrollo y crecimiento de los diferentes países de Latinoamérica y Colombia y sus usuarios.

De este modo, se puede concluir que la ley 1273 de 2009 esta desactualizada y requiere que se le dé un estudio por parte de las autoridades responsables, en el cual se pueda contemplar adiciones, ajustes tanto a los actuales artículos como la generación de los faltantes, con el fin de dar una tipificación acorde al delito, afección y perjuicio, estas mejoras a la ley de delitos informáticos podría establecer un bien reglamentario y judicial que vaya de la mano con las necesidades, penalizaciones que cada delito realmente se merezca, y es que un factor de ciberdelincuencia actual es que se dejan pasar muchas cosas que aunque mínimas son el inicio de delitos más graves.

Se logró identificar que dentro de este contexto, no solamente existen falencias y/o ambigüedades, sino que también no es clara la competencia de las diferentes autoridades que pueden procesar las denuncias que se reciben a diario frente a esta problemática, así por ejemplo se puede decir, que falta capacitación a las

[129] Kaspersky - Ciberdelincuencia y Ciberdelitos {en línea} (2012) Disponible en: https://www.kaspersky.es/resource-center/threats/computer-vandalism

[130] MAGERIT is the methodology of analysis and risk management developed by the High Council of Electronic Administration {en línea} (2012) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en#.Wqmh2ujOXDc

autoridades o entes encargados y el diseño claro de un apartado de competencia que defina quien debe seguir el debido proceso en suceso que involucre la parte digital/información y todo lo relacionado con TI, medios informáticos o transmisión de activos, teniendo en cuenta el origen del lugar a partir de que se comete el delito y el lugar donde se llega a ejecutar como tal. Por esta clase de circunstancias los procesos se pueden pasar de una autoridad a otra como se analizó en las sentencias dentro de este proyecto y de esta manera dejan la posibilidad de terminación de términos que pueda favorecer en ese caso al delincuente y no a la víctima.

Se puede confirmar y observar que la ley colombiana 1273, a pesar de haber sido creada para dar un tratamiento de carácter jurídico frente a la aparición de ciberdelincuencia este aun es como una prueba piloto porque ya se quedó pequeño frente a todo lo que abarca la ciberdelincuencia, cibercrimen y términos relacionados a la seguridad informática, , ya que desde hace varios años ha ido creciendo en todo el territorio nacional, por lo que es imperativo generar nuevas estrategias contra los delitos informáticos y el fortalecimiento del bien jurídico y a su vez integre las medidas que deben aplicarse en cuanto a seguridad informática, con el fin de reducir, prevenir o mitigar el daño causado por esta problemática.

Se identifica la falta de un artículo de definiciones aún es muy insipiente porque crear un glosario que abarca todos estos términos informáticos sería un anexo larguísimo pero que a la larga ser viviría como un punto de base para entender todo lo que tiene por dentro un proceso de delincuencia informática, según sea contemplado por la autoridad competente, con ello se evitaría que cierto delitos cometidos mediante el uso de aplicaciones o dispositivos informáticos sean juzgados por error de manera ordinaria saltándose la ley vigente para estos casos.

Esto nos lleva al gran reto que se tiene a gran escala y es la creación de legislaciones más detallas, concisas y que sean manejadas con un idioma universal que pongan un poco de orden y permitan a los usuarios desde cualquier nación saber cómo protegerse no importante donde este, porque, así como la tecnología, las comunicaciones y la era del internet de las cosas es universal así lo sea el modo de protección y de legislación, con el fin de garantizar que las organizaciones estén protegidas.