Revisión de la clasificación, categorías, métodos y efectos de la ciberdelincuencia en Colombia en la última década

Review of the classification, categories, methods and effects of cybercrime in Colombia in the last decade

Isabel Cristina Trochez Arias[1]
isabel.trochez00@usc.edu.co

Universidad Santiago de Cali, Facultad de Ingeniería, Programa de Tecnología en Sistemas de la Información (1)

Resumen
El avance en la tecnología informativa y la globalización del internet ha permitido a los delincuentes tener un nuevo campo de acción, generándose así nuevas modalidades de delitos o facilitado la comisión de los delitos tradicionales, ciberdelincuencia. Este concepto es muy amplio, por lo cual la literatura ha dado diversas clasificaciones para ayudar a definir el tema de manera más limitada. Este documento muestra las diferentes definiciones y clasificaciones que se da a la ciberdelincuencia, tambien, se analiza los métodos de ciberdelincuencia más utilizados en Colombia, así como, algunas prácticas o estrategias para evitar ser víctima de los ciberdelincuentes.

Palabras Clave: Ciberdelincuencia, Ciberdelito, Ciberseguridad, Ransomware, Grooming, Doublepulsar, ColCERT, CSIRT, Phishing, Smishing, Vishing**,** Cyber-Stalking.

Abstract
The advance in information technology and the globalization of the internet has allowed criminals to have a new field of action, generating new forms of crime or facilitating the commission of traditional crimes, cybercrime. This concept is very broad, so the literature has given various classifications to help define the subject in a more limited way. This document shows the different variations and classifications that are given to cybercrime, also, analyzes the most used cybercrime methods in Colombia, as well as, some practices or strategies to avoid being victims of cybercriminals.

Keywords: Cyberdelinquency, Cybercrime, Cybersecurity, Ransomware, Grooming, Doublepulsar, ColCERT, CSIRT, Phishing, Smishing**,** Vishing, Cyber-Stalking.

1. INTRODUCCIÓN

La palabra ciberdelito en los últimos años se ha convertido en una palabra de uso común, pero sigue siendo difícil definirla con precisión, porque al igual que el crimen "tradicional" la ciberdelincuencia tiene muchas caras y se realiza en distintos ambientes. Por ejemplo (Council of Europe, 2001) firmó en Budapest el "Convenio de Ciberdelincuencia del Consejo de Europa" donde usa el término "ciberdelincuencia" para describir delitos que van desde delitos contra los datos y sistemas informáticos hasta delitos de violación de derechos de autor. También la Brigada de Investigación Tecnológica de la Policía Nacional Española va más allá y cubre delitos como fraude, sabotaje, pornografía infantil. La ley de delitos informáticos de (Colombia, 2009) inserta crímenes tales como, la suplantación de sitios web para capturar datos personales, acceso no autorizado sistema informático protegido, entre otros. Igualmente (Kamariah Musa, Ismail, Abd Ghadas, & Md Radzi, 2015) incluye cyberstalking en su definición de ciberdelincuencia.

Como se puede ver la ciberdelincuencia es muy amplia y puede ocurrir de muchas maneras. Como dice (Kamariah Musa, Ismail, Abd Ghadas, & Md Radzi, 2015) ciberdelincuencia son crímenes, que son perpetrados por el uso de una computadora o a través de las tecnologías de la información y la comunicación, o como comentan otros autores la ciberdelincuencia es usada para referirse a cualquier crimen que involucra computadoras, redes o dispositivos de hardware (Gordon & Ford, 2006).

No hay una definición universal aceptada sobre ciberdelincuencia, pero (Wall, Hunting shooting and Phishing: New Cybercrime Challenges for Cybrecanadians in the 21st Century, 2008) comenta que para definir adecuadamente ciberdelincuencia se debe conocer el impacto que han tenido las tecnología de la información y comunicación en la transformación del mundo. Además el mismo autor (Wall, Cybercrime:the transformation of Crime in the Information Age, 2007) refiere que la ciberdelincuencia no es un término jurídico, sino un término genérico para describir una serie de hechos cometidos contra o a través del uso de datos o sistemas informáticos (13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal., 2015).

La ciberdelincuencia es un área del crimen de rápido crecimiento, dado que el aumento de los delitos informáticos en parte se debe al incremento de los usuarios profesionales en informática (Murashbekov, 2015) y que gracias al internet les han dado la oportunidad de cometer crímenes de manera más eficaz y sin mucho riesgo, tanto los se denominan como "tradicionales" o nuevos tipos de delitos.

Debido a que el Internet es un servicio que se encuentra disponible alrededor del mundo y es de fácil acceso, el delito informático se convierte en transnacional, ya que no conoce fronteras, así que, dificulta hacer un análisis criminológico sobre los perpetradores y por lo tanto casi imposible detener al criminal.

Ser víctima de la ciberdelincuencia puede desencadenar una variedad de problemas que afectan la economía, la privacidad, la integridad y la salud mental de las personas; incluso empresas, generando depresión, desconfianza, aislamiento y hasta en situaciones más complejas, como el suicidio.

Esta investigación trae consigo beneficios que servirán para desarrollar e implementar mecanismos de protección nacional e internacional para hacer más efectiva la batalla contra la ciberdelincuencia y de esta forma tener una correcta cibercultura.

Es así como esta monografía pretende realizar una revisión de los impactos de la ciberdelincuencia en Colombia con el fin de proponer estrategias de mitigación, para ello busca comprender de acuerdo a la literatura existente, la clasificación de la ciberdelincuencia y sus diversos tipos, igualmente enseñar cuáles son sus categorías; métodos y herramientas utilizadas, para finalmente proponer herramientas que permiten tomar acciones de prevención.

2. CLASIFICACIÓN DE CIBERDELINCUENCIA

Dada la amplitud de la definición de ciberdelincuencia como "cualquier delito que solo se pueda cometer usando computadores, redes de computadores u otras formas de comunicación de la información (EUROPOL, s.f.)", la literatura a través de los años han dado diversas clasificaciones para ayudar a los investigadores, desarrolladores y creadores de la ley a definir el tema de manera más limitada, desarrollando esquemas que vincule los delitos informáticos con características similares en grupos similares a las clasificaciones de los delitos conocidos como tradicionales.

Para (Tatarinova, Shakirov, & Tatarinov, 2016) la ciberdelincuencia está dividida en: *crímenes contra los derechos personales, como el acoso, delitos contra la seguridad financiera –pago electrónico inseguro y delito contra la moralidad de los niños(bullying).*

Así mismo en el convenio sobre delito cibernético del (Council of Europe, 2001) y su protocolo adicional (Council of Europe: Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, 2003) clasifican la ciberdelincuencia de acuerdo a conductas legalmente prohibidas que se ajustan a la etiqueta del delito cibernético, y estas son:

Delitos contra la confidencialidad, integridad y disponibilidad de sistemas informáticos y datos; *Articulo 2: Acceso Ilegal, Artículo 3: Intercepción Ilegal, Artículo 4: Interferencia de datos, Artículo 5: Interferencia de sistemas, Artículo 6: Uso indebido de dispositivos informáticos relacionados con delitos (falsificación y fraude), Artículo 7: Falsificación Informática, Artículo 8: Fraude Informático y delitos contra el contenido, Artículo 9: Delitos relacionados con la pornografía infantil*

Delitos relacionados con infracciones de derechos de autor y derechos afines; *Artículo 10 - Delitos relacionados con infracciones de derechos de autor y derechos conexos*

Actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos; *Artículo 3: Difusión de material racista y xenófobo a través de sistemas informáticos, Artículo 4: amenazas motivadas por racista y xenófoba, Artículo 5: Insultos motivados racistas y xenófobos Artículo 6: Negación, minimización grave, aprobación o justificación de genocidio o crímenes contra la humanidad, Artículo 7: Instigar y asistir (ser cómplice)*

Por otro lado (Yar & Steinmetz, 2006) han dividido la ciberdelincuencia en cinco áreas, que muestra una serie de comportamientos y actividades en lugar de enfocarse en delitos específicos. Las cinco categorías son las siguientes:

Ciber-intrusión: *el cruce de los límites cibernéticos en los sistemas informáticos de otras personas en espacios donde ya se han establecido derechos de propiedad o título y causando daños, por ejemplo, piratería informática y distribución de virus.*

Ciber-engaños y robos*: los diferentes tipos de daños adquisitivos que pueden tener lugar dentro del ciberespacio. En un nivel se encuentran los patrones más tradicionales de robo, como el uso fraudulento de tarjetas de crédito y efectivo (cibernético), pero también existe una inquietud actual con respecto al creciente potencial para el asalto de cuentas bancarias en línea a medida que la banca electrónica se vuelve más popular.*

Ciber-pornografía**:** *el incumplimiento de las leyes sobre obscenidad y decencia.*

Ciber-violencia: *el impacto violento de las actividades cibernéticas de otros sobre la agrupación individual, social o política. Si bien tales actividades no tienen que tener una manifestación directa, la víctima, siente la violencia del acto y, como consecuencia, puede sufrir cicatrices psicológicas a largo plazo. Las actividades aquí referidas van desde el acoso cibernético y el discurso de odio hasta la charla tecnológica.*

Crimen contra el estado: *son los delitos que abarca aquellas actividades que violan las leyes que protegen la integridad de la infraestructura de la nación, como el terrorismo, el espionaje y la divulgación de secretos oficiales.*

De igual forma para (Gordon & Ford, 2006) el computador o dispositivo puede ser el agente del delito, el facilitador del delito o el objetivo del delito, por lo tanto intentaron definir un marco conceptual que pueda ser usado desde perspectiva técnica como social. La ciberdelincuencia la clasifican en tipo I y tipo II:

El primer tipo tiene las siguientes características:

- *Generalmente es un evento singular o discreto desde la perspectiva de la víctima.*
- *A menudo se ve facilitado por la introducción de programas de software criminal como registradores de pulsaciones de teclas, virus, rootkits o caballos de Troya en el sistema informático del usuario.*
- *Las introducciones pueden, pero no necesariamente, ser facilitadas por vulnerabilidades.*

El segundo tipo que incluye actividades como el acoso cibernético, el chantaje, la manipulación del mercado de valores, el espionaje corporativo complejo y la planificación o realización de actividades terroristas en línea; tiene las siguientes características:

- *Generalmente es facilitado por programas que no se ajustan a la clasificación de la delincuencia. Por ejemplo, las conversaciones pueden tener lugar usando IM (mensajería instantánea) y los clientes o archivos pueden transferirse usando el protocolo FTP.*
- *Generalmente hay contactos o eventos repetidos desde la perspectiva del usuario.*

Y en la ley 1273 de delitos informáticos de (Colombia, 2009) clasifican la ciberdelincuencia en:

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos; *Artículo 269A: Acceso abusivo a un sistema informático*, *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 para capturar datos personales.*

De los atentados informáticos y otras infracciones; *Artículo 269I: Hurto por medios informáticos y semejantes, Artículo 269J: Transferencia no consentida de activos.*

3. MÉTODOS DE LA CIBERDELINCUENCIA

La masificación del Internet brinda nuevos escenarios de riesgo, debido a la facilidad de producir material ilícito en segundos de un servidor host a otro, y de ser accedido/descargados en todo el mundo, constituyendo así nuevas formas de delito y potenciando las tradicionales.

Colombia es el tercer país en Latinoamérica en recibir ciberataque, solo en el 2019 recibió 40 billones de intentos en ciberataques (El Universal, 2019). Los delitos informáticos más frecuentes en Colombia son:

3.1. PHISHING

Es una forma de ingeniería social en la que un atacante intenta obtener de manera fraudulenta información confidencial, al hacerse pasar por un tercero confiable. Los ataques de phishing en la actualidad suelen emplear "señuelos" generalizados (Jagatic, Johnson, Jakobsson, & Menczer, 2005) para realizar el fraude.

Los mensajes de phishing parecen provenir de organizaciones legítimas, sin embargo, se trata de imitaciones. Los correos electrónicos solicitan al usuario de carácter urgente a que actualice, valide o confirme la información de una cuenta, sugiriendo a menudo que hay un problema. Entonces se le redirige a una página web falsa para que así facilite información sobre su cuenta (avast).

En los correos electrónicos que utilizan los estafadores conocidos como phisher, se falsifican la dirección del remitente, los mensajes contienen logotipos e imágenes del sitio web real al que hace referencia, además, los textos amenazan con una pérdida, ya sea económica o de la propia cuenta existente, si no se siguen las instrucciones indicadas, y siempre se muestra un enlace que lleva al sitio fraudulento (Universidad Nacional de Luján: Dirección General de Sistemas).

El Internet Security Threat Report de (Symantec, 2019) reporta que el principal señuelo para el phishing son los correos que aparentemente contiene facturas; las industrias de agricultura, finanzas, seguros y bienes son los más atacados; los países de Arabia Saudita, Noruega y Holanda son lo que más sufren por Phishing; encontrándose Colombia en la posición número 34 a nivel mundial y segundo en Latinoamérica, con 1 caso en 4,619 correos electrónicos. La misma investigación (Symantec, 2019) reporta que los niveles de phishing disminuyeron de 1 en 2,995 correos electrónicos en 2017, a 1 en 3,207 correos electrónicos en 2018. Y que el 78% de las personas son conscientes de los riesgos de los enlaces desconocidos en los mensajes de correo, sin embargo, les dan click.

Dado que el phishing se aprovecha de las vulnerabilidades técnicas y sociales, y que los phisher se está volviendo más inteligentes, se han producido nuevas modalidades como el **Spear-Phishing**, el cual busca los grupos de personas más vulnerable, es decir se ataca a grupos específicos y determinados. Está requiere técnicas avanzadas de piratería y una gran cantidad de investigación sobre sus objetivos, porque buscan datos más valiosos como información confidencial, secretos comerciales. De acuerdo al Internet Security Threat Report (Symantec, 2019) el 65% de los phisher usaron el Spear-Phishing como el vector primario de infección y que el 96% de la motivación principal continúa siendo la recolección de inteligencia. Las otras muy populares en Colombia; las preferidas por los delincuentes, es el **Smishing** (Noticias Caracol, 2018), que como mencione anteriormente es un tipo de phishing mediante la cual alguien intenta obtener información privada a través de un mensaje de texto o SMS (Norton, 2019). Este tipo de modalidad es muy preocupante porque las personas tienden a confiar mucho en los mensajes de texto que llegan a su celular. Y el **Vishing** donde se hace uso del Protocolo Voz sobre IP –VoIP– y la ingeniería social para engañar a personas, recreando una voz automatizada parecida al de las entidades bancarias (BBVA, 2015) o como explica Maximiliano Cantis, experto en seguridad informática de ESET Colombia son falsos call centers que se ponen en contacto con miles de personas (Noticias Caracol, 2018).

3.2. CYBER-STALKING (CIBERACOSO)

El Ciberacoso es similar al acoso, involucra comportamientos amenazantes o de acoso por parte de un individuo contra otro, con la excepción de que este acto en particular hace un uso completo de Internet (Tatarinova, Shakirov, & Tatarinov, 2016), ¿ pero qué es el acoso?.

El acoso es un comportamiento agresivo y no deseado causado por una persona, en contra de otra que involucra un desequilibrio de poder real o percibido (stopbullying, 2019), con la intención de provocar miedo y preocupación en la víctima , esté puede ser verbal, psicológico-moral, o físico. Siendo el más común el psicológico, debido a que el acoso como delito no requiere la presencia de un elemento físico, sino que se concentra más en elemento mental (Kamariah Musa, Ismail, Abd Ghadas, & Md Radzi, 2015). Algunas conductas pueden ser, observar el comportamiento de la víctima, merodear o hacer seguimientos repetitivos, recopilar información, entre otros. En esencia, es la exposición a conductas de violencia psicológica intensa, dirigidas de forma reiterada y prolongada en el tiempo, con el fin de crear un ambiente hostil o humillante que asuste, perturbe y aterrorice la vida de la víctima (Universidad de la Rioja:Servicio de Prevención de Riesgos Laborales, 2017). El Ciberacoso se vale de las mismas conductas del acoso, pero esta vez en línea. El acosador no está en presencia directa de su víctima, sino que se acerca sigilosamente a ella en línea, monitoreando las actividades y al mismo tiempo haciendo amenazas y otras formas o intimidación verbal en el mundo virtual entre ellas: email, mensajería instantánea, redes sociales, blogs, mensajes de texto, sitios web difamatorios (Kamariah Musa, Ismail, Abd Ghadas, & Md Radzi, 2015).

Entre los tipos de comportamientos que constituyen el ciberacoso, se pueden encontrar las acusaciones falsas, el daño a datos o equipos, la solicitud de menores con fines sexuales; grooming. etc.

El ciberacoso es cada vez más frecuente y especialmente entre la población escolar, según cifras reveladas por la Organización de Naciones Unidas y la Fundación Telefónica, el 55 % de los jóvenes han sido víctimas de ciberacoso (MinTIC).

En Colombia el año 2017 la Universidad de Boyacá realizó una investigación donde encontró que 15,38% de los jóvenes entre 17 y 20 años de edad, han sido en algún momento víctimas del acoso cibernético, por WhatsApp y por Redes Sociales, pues estas redes facilitan el anonimato y existe una menor probabilidad de detección del acosador. Las mujeres fueron las más afectadas (Caracol Radio, 2017).

En el 2018 la universidad EAFIT y Tigo-Une realizaron un estudio en instituciones educativas de Medellín, Bogotá, Barranquilla, Bucaramanga, Cartagena, Cali, Pereira y Manizales, donde encuestan a 485 niños y jóvenes entre 9 y 16 años (50% mujeres y 50% hombres). El informe da cuenta de que el 12% de los niños y adolescentes ha sido víctima de ciberacoso. El 20% de los encuestados dijo que ha recibido mensajes con contenido sexual (enTICconfio: MinTc, 2018).

3.3. GROOMING

Es cuando un adulto acosa sexualmente a niños mediante el uso de las TIC. Los autores de este delito; criminales pedófilos, generar un perfil falso en una red social, sala de chat, foro, videojuego u otro, en donde se hacen pasar por un chico(a) y entablan una relación de amistad y confianza con el niño que quieren acosar/chantajear (Molina, y otros, 2017) o que quieren conocer y participar en comportamientos sexuales. Los pedófilos por medio de este método pueden atraer múltiples víctimas a la vez.

Hay dos tipos de Grooming:

Sin fase previa de relación y generación de confianza: El acosador logra obtener fotos/videos sexuales de los niños(as) a la fuerza, mediante el hackeo de cuentas y robo de contraseñas. Con éste material, se extorsiona al niño(a) con mostrarlo si este no le entrega más material o accede a un encuentro personal (Molina, y otros, 2017).

Con fase previa de generación de confianza: En esta fase el material es entregado por el menor y la confianza es el instrumento imprescindible. Para obtener la confianza el criminal se vale de distintas herramientas para esconder la identidad y hacerse pasar por un menor. Esto lo logra manipulando o falsificando fotos o videos, y manteniendo conversaciones en un lenguaje acorde a la edad del menor que quiera acosar. También se toman los gustos y preferencias que los chicos vuelcan en la web para producir una sensación de amistad. El criminal utiliza el tiempo como pieza clave para fortalecer la relación. Una vez capturado todo el material, se chantajea al menor pidiendo más material a cambio de no mostrar el que ya tiene (Molina, y otros, 2017).

En Colombia esté crece cada día más y una de las razones es que los niños tienen redes sociales sin supervisión, lo cual aumenta la posibilidad de ser atacados. En el 2017 se atendieron 280 casos relacionados con el grooming y en el informe Análisis del Cibercrimen, emitido por la Dirección de Investigación Judicial de la Policía, reveló que en el 2017 y en el 2018 casi a diario se recibieron denuncias de padres preocupados por sus hijos que estuvieron a punto de compartir fotografías o revelar detalles de su vida íntima por Internet a desconocidos (RCN Radio, 2018).

En el 2019 la Policía Nacional Colombiana comenta que se presentan cuatro denuncias diarias por este caso, que son 1.038 casos los que se han denunciado en el año, 290 en los que las víctimas son menores de 13 años. Los casos más frecuentes se registran en Bogotá con 292 denuncias, seguido por Medellín con 150, Cali 47, Bucaramanga 42, e Ibagué con 29 casos (RCN Noticias, 2019).

3.4. SPAM

El correo no deseado es la distribución de correos en forma masiva anunciando servicios, productos, inversiones, que en la mayoría de veces es fraude. El spam plantea un desafío global porque sigue siendo un vector importante para la difusión de los delitos. El propósito de spam es engañar a las personas para que crean que van a recibir un servicio o producto, a un precio reducido, pero en realidad el spammer antes de hacer el trato solicita dinero o que las víctimas le compartan información personal, bancaria y financiera.

Los spammer en la actualidad difunden códigos maliciosos, ya no tanto a través de URL como vector de infección primario, sino a través del uso de archivos adjuntos. Los niveles de spam en el mundo desde el 2015 ha aumentado, y en 2018 el 55% de los correos se clasificaron como spam (Symantec, 2019). Las industrias preferidas por los spammer de acuerdo Internet Security Threat Report de (Symantec, 2019) son: Minería, Finanzas, seguros y bienes raíces, Fabricación, Administración Pública; los países más atacado son Arabia Saudita, China y Brasil, encontrándose Colombia en la posición 11 a nivel mundial y la segunda de Latinoamérica.

En Colombia el 86% del malware detectado fue un troyano que se instala en los ordenadores al descargar un archivo adjunto de correo infectado (El Universal, 2019).

3.5. DOUBLEPULSAR

Es una herramienta de puerta trasera creada por la NSA para aprovecharse de una serie de vulnerabilidades conocidas en Windows con el fin de poder tomar el control de prácticamente cualquier ordenador de forma remota. Esto significa que su PC está ejecutando una versión obsoleta del servicio Compartir archivos e impresoras de Windows (SMB), que contiene una vulnerabilidad conocida como EternalBlue (avast, 2017). Esta técnica es utilizada para distribuir malware –ransomware WanaCry– y otras amenazas maliciosas.

El ransomware WannaCry ataca a las redes usando el protocolo SMBv1. La vulnerabilidad de esté se denominó MS17-010. También puede entrar en su PC mediante un adjunto de correo electrónico o a través de su navegador si visita una página web infectada. Este malware se adentra en los equipos que utilizan Windows para cifrar los archivos y restringir el acceso, se presenta una visualización en pantalla exigiendo un pago (rescate) al usuario para restaurar el acceso a su información (avast, 2018).

En mayo de 2017 hubo gran número de ataques de ransomware y los países perjudicados fueron Rusia, China, Ucrania, Taiwán, India y Brasil. WannaCry, afectó a organismos gubernamentales, hospitales, universidades, compañías ferroviarias, empresas de tecnología y de telecomunicaciones.

En Colombia el doublepulsar estuvo entre los cuatro ciberdelitos, ciberataques, más detectados en Colombia en el segundo trimestre de 2019.

4. ESTRATEGIAS DE MITIGACIÓN DEL RIESGO

De acuerdo a la globalización del internet la ciberdelincuencia puede ocurrir desde cualquier parte del mundo, lo que hace difícil descubrir su procedencia, ya que ningún sistema es infalible, por lo tanto, se necesita la ayuda de todos – Estado, empresa privada y ciudadanos– para mitigar los riesgos.

Los países están desarrollando estrategias de ciberseguridad para tratar de conseguir un ciberespacio más seguro mediante el intercambio de información de alertas, vulnerabilidades, amenazas; la concienciación y formación de sus ciudadanos y servidores públicos en seguridad de sistemas de las TIC (Candau Romero, 2011).

Colombia ha propuesto diversas iniciativas para lograr una seguridad de la información. Algunas de estas iniciativas están regidas por el documento CONPES 3701 de 2011, el cual busca generar lineamentos en ciberseguridad y ciberdefensa para contrarrestar la ciberdelincuencia (Republica de Colombia, 2011); se crea el Grupo de Respuesta a Emergencias de Cibernéticas de Colombia ColCERT. De igual forma, la Policía Nacional por su parte creo la oficina de delitos informáticos y el Equipo de Respuesta a Incidentes Seguridad Informática de la Policía Nacional CSIRT-PONAL. La empresa privada está tomando medidas para reducir el riesgo obteniendo la certificación ISO 27001 y creando Sistemas de Gestión de Seguridad de Información (Gonzáles Hernández, 2014). Así mismo, el Estado mediante sus diferentes organismos desarrolla programas para enseñar a la ciudadanía a tener una cultura de seguridad de la información, además el congreso produjo leyes que se utilizan en seguridad informática: Ley 527 de 1999, Ley 599 de 200, Ley 962 de 2005, Ley 1150 de 2007, Ley 1341 de 2009. Tambien, la academia mediante sus cursos especializados en seguridad informática, está creando profesionales capacitados que ayudan a Colombia a tener una seguridad de la información más eficaz y eficiente.

Desde el punto vista tecnológico se deben utilizar diferentes prácticas de seguridad para proteger nuestros sistemas, como puede ser utilizar sistemas defensivos múltiples, de soporte mutuo para protegerse contra fallas de punto único – firewalls, antivirus de puerta de enlace, sistemas de detección o protección contra intrusiones(IPS)–, y como se sabe los antivirus en los endpoints no alcanza, por lo que se debe implementar sistemas integrales de seguridad en extremos con diversos niveles de protección como: usar protección del explorador para evitar ataques complejos basados en la web, configurar el control de las aplicaciones que impida que éstas y los complementos (plug-ins) del explorador descarguen contenido malicioso no autorizado, configurar los servidores de correo para bloquear o eliminar mensajes que contengan archivos adjuntos que suelen usarse para difundir virus –los servidores de correo deben estar protegidos por software de seguridad–, configurar el control de los dispositivos que impida y limite los tipos de dispositivos USB que se utilizarán, restringir los dispositivos no autorizados, tales como discos duros externos portátiles y otros medios extraíbles y en caso de que éstos estén permitidos automáticamente escanearlos en caso de virus, proteger las claves en dispositivos de hardware seguros, criptográficos y a prueba de alteraciones, asegurarse de que las contraseñas sean sólidas, con un mínimo de 8-10 caracteres de largo y alfanuméricas, cambiándolas al menos cada 90 días (Symantec, 2014). Igualmente, en las políticas de seguridad en donde el acceso a la información sensible es restringido, utilizar solución de Protección Contra Pérdida de Datos (DLP) que identifiqué y bloqué acciones sospechosas de copiado o descarga de datos sensibles.

La relación de las empresas con sus clientes es de vital importancia, por lo cual se debe fortalecer la relación de confianza escaneando el sitio web de la empresa en forma diaria para detectar malware, utilizar Certificados SSL con Validación Extendida, para mostrar la barra de direcciones del explorador en verde, establecer el marcador seguro para las cookies de la sesión y mostrar marcas de confianza reconocidas en lugares de gran visibilidad en el sitio web. Además, se debe hacer campañas de instrucción donde se educa a los usuarios acerca de los protocolos básicos de seguridad, así como, no abrir datos adjuntos si provienen de una fuente desconocida y poco confiable, tener cuidado al hacer clic en URL en mensajes de correo electrónico o en redes sociales, descargar únicamente software compartido por la empresa, o directamente del sitio web del proveedor (Symantec, 2014).

Como se sabe los ciberdelincuentes se vuelven más astutos e inteligentes a medida que avanza el mundo civilizado, creando nuevas amenazas, por lo cual como profesionales la mejor técnica de protección es mantenernos actualizados sobre las diferentes tendencias a nivel mundial en tecnología, información, legislatura y seguridad.

5. CONCLUSIONES

Con la masificación del internet y el desarrollo de las TICS, los delincuentes tienen un campo muy amplio para actuar y cometer crímenes de manera más fácil, eficaz y sin mucho riesgo, desencadenado una serie de problemas en la seguridad, integridad, economía y privacidad del Estado, la empresa privada y las personas. Lo cual, nos exige a responder de manera rápida, para impedir o mitigar los daños. Se muestra que la literatura y diferentes países a través de los años ha dado diversas definiciones y clasificaciones para ayudar a los investigadores, a los profesionales en seguridad informática y a los creadores de la ley, a crear esquemas que permitan que estos nuevos tipos de delitos y sus características, se agrupen en los delitos que se conocen como tradicionales –estandarizar– para dar una penalización más adecuada. Claro está que cada día aparecen un nuevo dispositivo tecnológico y nuevas amenazas, por eso debemos actualizarnos con regularidad –Estado, empresa privada, ciudadanos– sobre las nuevas tendencias en seguridad y legislación a nivel mundial.

Colombia, aunque no está al nivel de los EEUU o de algunos países europeos en seguridad informática, está creando diferentes leyes, programas, iniciativas y mecanismos para contrarrestar la ciberdelincuencia. De igual manera, se muestra un interés del país en reducir la brecha de las vulnerabilidades y debilidades de nuestros sistemas informáticos. Así mismo, se da cuenta que los ciberdelincuentes se aprovechan de la confianza –herramienta principal de la ingeniería social– y el desconocimiento de las personas para cometer el ciberdelito, por lo que se está instruyendo, pero sobretodo concientizando a la ciudadanía de utilizar políticas y prácticas de seguridad informática –cibercultura– y así tener un fuerte unido, y poder decir que tenemos un verdadero sistema de defensa.

6. REFERENCIAS

13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. (12-19 de abril de 2015). *Seminario 3: El fortalecimiento de las respuestas de prevención del delito y justicia penal frente a las formas de delincuencia*, 22. Doha. Obtenido de https://www.unodc.org/documents/congress/Documentation/IN_SESSION/ACONF222_L6_s_V1502123.pdf

avast. (s.f.). *Phishing*. Obtenido de https://www.avast.com/es-es/c-phishing

avast. (2017). *Actualizar Windows para reparar la vulnerabilidad EternalBlue y evitar el ataque DoublePulsar*. Obtenido de https://support.avast.com/es-co/article/EternalBlue-vulnerability

avast. (2018). *WannaCry*. Obtenido de https://www.avast.com/es-es/c-wannacry

BBVA. (26 de Noviembre de 2015). *¿Que es el Vishing?* Obtenido de https://www.bbva.com/es/vishing-la-imaginacion-los-estafadores-no-limites/

Candau Romero, J. (2011). Estrategias nacionales de ciberseguridad. Ciberterrorismo. 257-232. La Rioja, España. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=3837524

Caracol Radio. (10 de Julio de 2017). *El ciberbullying es una realidad en Colombia*. Colombia. Obtenido de https://caracol.com.co/radio/2017/07/10/regional/1499686270_201237.html

Colombia. (5 de Enero de 2009). Ley 1273 de 2009."De la Protección de la información y de los datos". *Ley de delitos informaticos*. Colombia.

Council of Europe. (23 de Noviembre de 2001). *Council of Europe.* Obtenido de https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Council of Europe: Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. (28 de 1 de 2003). *Council of Europe.* Obtenido de https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

El Universal. (9 de Septiembre de 2019). *Colombia sufrió 42 billones de intentos de ataques cibernéticos*. Colombia. Obtenido de https://www.eluniversal.com.co/tecnologia/colombia-sufrio-42-billones-de-amenazas-de-ciberataques-IF1698794

enTICconfio: MinTc. (13 de Agosto de 2018). *Así usan redes sociales los niños y jóvenes en Colombia*. Colombia. Obtenido de https://www.enticconfio.gov.co/Asi-usan-redes-sociales-los-ninos-y-jovenes-en-colombia

EUROPOL. (s.f.). Obtenido de https://www.europol.europa.eu

Gonzáles Hernández, M. (2014). Actualidad de Colombia en Seguridad de la Informacon. Obtenido de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2882/00001886.pdf?sequence=1

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *J Comput Virol.* Obtenido de https://usc.elogim.com:2782/content/pdf/10.1007%2Fs11416-006-0015-z.pdf

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (12 de Diciembre de 2005). Social Phishing. Indiana, EEUU.

Kamariah Musa, M., Ismail, N., Abd Ghadas, Z. A., & Md Radzi, M. N. (17 de 09 de 2015). Cyber Stalking: Social Issues of Harassment on Internet. *American-Eurasian J. Agric. & Environ. Sci., 15(Tourism & Environment, Social and Management Sciences)*. Obtenido de http://idosi.org/aejaes/jaes15(tesms)15/2.pdf

MinTIC. (s.f.). *El 55% de los jóvenes latinoamericanos han sido víctimas de Ciberacoso según la ONU*. Colombia. Obtenido de https://www.mintic.gov.co/portal/604/w3-article-2757.html?_noredirect=1

Molina, M. P., Furnari, A., Hagelstrom, I., Ravalli, M., Passeron, E., Fainboim, L., & Palmieri, J. (Abril de 2017). Guía de sensibilización sobre Convivencia Digital. (D. Giménez, Ed.) *UNICEF*. Obtenido de

https://www.unicef.org/argentina/sites/unicef.org.argentina/files/2018-04/COM-Guia_ConvivenciaDigital_ABRIL2017.pdf

Murashbekov, O. B. (Noviembre de 2015). Methods for Cybrecrime Fighting Improvement in Developed Countries. *The Journal of Internet Banking and Commerce, 20*(S1), 24-29.

Norton. (2019). *Norton by Symantec.* Obtenido de https://co.norton.com/internetsecurity-emerging-threats-what-is-smishing.html

Noticias Caracol. (18 de Enero de 2018). *¿Sabe qué es vishing o smishing?* Obtenido de https://noticias.caracoltv.com/colombia/sabe-que-es-vishing-o-smishing-tome-nota-porque-son-dos-de-los-cibercrimenes-mas-comunes

RCN Noticias. (28 de Septiembre de 2019). *Atención padres: el grooming y sus riesgos para los niños en internet*. Colombia. Obtenido de https://noticias.canalrcn.com/tecnologia/atencion-padres-el-grooming-y-sus-riesgos-para-los-ninos-en-internet-347639

RCN Radio. (21 de Febrero de 2018). *Grooming, una amenaza cada vez mayor para los menores en Colombia*. Colombia. Obtenido de https://www.rcnradio.com/recomendado-del-editor/grooming-una-amenaza-cada-vez-mayor-para-los-menores-en-colombia

Republica de Colombia. (14 de Julio de 2011). Documento CONPES 3701. Bogotá D.C., Colombia. Obtenido de https://www.mintic.gov.co/portal/inicio/3510:Conpes-3701-de-2011

stopbullying. (2019). *stopbullying.com.* Obtenido de https://espanol.stopbullying.gov/qué-es-el-acoso-346k/índice.html

Symantec. (Junio de 2014). TENDENCIAS DE SEGURIDAD CIBERNÉTICA EN AMÉRICA LATINA Y EL CARIBE. Obtenido de https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

Symantec. (2019). *Internet Security Threat Report* (Vol. 24). Obtenido de https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

Tatarinova, L. F., Shakirov, K. N., & Tatarinov, D. V. (2016). Criminological Analysis of Determinants of Cybercrime Technologies. *International Electronic Journal of Mathematics Education, 11*(5). Obtenido de https://www.iejme.com/download/criminological-analysis-of-determinants-of-cybercrime-technologies.pdf

Universidad de la Rioja:Servicio de Prevención de Riesgos Laborales. (2017). Universidad de la Rioja, La Rioja.

Universidad Nacional de Luján: Dirección General de Sistemas. (s.f.). *Cómo protegerse del phishing.* Univerdidad Nacional de Luján, Luján. Obtenido de http://www.unlu.edu.ar/doc/seginfo/como_protegerse_del_phishing.pdf

Wall, D. S. (2007). *Cybercrime:the transformation of Crime in the Information Age.* Cambridge Polity.

Wall, D. S. (2008). *Hunting shooting and Phishing: New Cybercrime Challenges for Cybrecanadians in the 21st Century.* British Library.

Yar, M., & Steinmetz, K. F. (2006). *Cybercrime and Society.* Londres: Sage Publications Ltd.