LOS DESARROLLOS TECNOLÓGICOS Y SU INFLUENCIA EN EL CRECIMIENTO DE LOS CIBERDELITOS EN COLOMBIA

Martínez Moya Carlos Andrés
carlosmartinez555@gmail.com
Universidad Piloto de Colombia

Abstract—Since the beginning of internet, commerce in general saw in cyberspace an opportunity to present their products on a large scale, increasing their income. With this situation, cybercriminals saw a great opportunity to make a profit by the same means, with attacks that generate income without much effort. This article aims to show the reader as technological developments contribute to the growth of cybercrime in Colombia, current threats that are attacking cyberspace, multimillion-dollar losses caused by cybercrime, and a glimpse of what you can expect to Colombia in the coming years in technological advances and cybercrime.

Resumen—Desde los inicios de internet, el comercio en general vió en el ciberespacio una oportunidad para presentar sus productos a gran escala, incrementando sus ingresos. Con esta situación, los ciberdelincuentes vieron una gran oportunidad de obtener beneficios económicos por el mismo medio, con ataques que generan ingresos sin mucho esfuerzo. Este artículo tiene como objetivo mostrar al lector como los avances tecnológicos contribuyen al crecimiento de la delincuencia informática en Colombia, las actuales amenazas que están acechando el ciberespacio, las pérdidas de millones de dólares causadas por los delitos informáticos y una visión de lo que puede esperar a Colombia en los próximos años en los avances tecnológicos y los delitos informáticos.

Índice de Términos—APT**,** ciberbullying**, c**iberdelincuentes ciberdelitos, delito informático, grooming, IoT, malware, phishing, sexting.

I. INTRODUCCIÓN

La evolución constante de las tecnologías de información, la necesidad naciente de la economía de ofrecer sus servicios y productos a través de internet y la dependencia de la tecnología para desenvolvernos adecuadamente en una sociedad cada vez más consumista, muestran la necesidad de mantener la integridad, confidencialidad y disponibilidad de los datos, su correcto almacenamiento, canales adecuados para su transmisión, concienciación en los usuarios, sin embargo, no son medidas suficientes; así como la forma de protección de la información avanza, también lo hacen los métodos para atacarla.

Hoy día, donde el uso de internet ha cambiado el modus vivendi del mundo entero, donde día a día se utiliza el ciberespacio para realizar multimillonarias transacciones, muchas de estas con las medidas de seguridad adecuadas, otras no tanto, donde la interrelación de las personas por medio de las redes sociales es cada vez mayor, muchos de ellos sin tomar las medidas de seguridad adecuadas y caen en las redes de los ciberdelincuentes, que ven en estas fallas una gran oportunidad. De ahí el crecimiento inesperado de los delitos informáticos que utilizan el ciberespacio para su actuar.

Colombia no ha sido ajena a la ciberdelincuencia, en 2013, seis millones de usuarios fueron víctimas de algún delito informático y se espera que en los años siguientes se siga dando una tendencia de crecimiento, debido principalmente al desconocimiento de los colombianos en principios básicos de seguridad de su información, fallas en los sistemas de información en las empresas y la pobre regulación existente en el país para temas relacionados con delitos informáticos en el ciberespacio.

Entre las técnicas más utilizadas para el ciberdelito en Colombia se encuentran el “spyware”; el “ransomware”; el “phishing”; el “DDoS” y recientemente el “sexting”, “grooming” y “ciberbullying”, los cuales serán analizados durante el desarrollo del presente documento, lo anterior se da principalmente porque los ciberdelincuentes se aprovechan de la ingenuidad de los usuarios de los sistemas informáticos para atacarlos, capturar su información y comercializarla en el mercado negro. En otra proporción, atacan las fallas de seguridad presentes en los sistemas de información de empresas, con el fin de recibir una ganancia por ello.

Los nuevos desarrollos como las aplicaciones móviles y el IoT (internet de las cosas), están abriendo grandes puertas a los cibercriminales para atacar y aprovecharse de las nuevas vulnerabilidades, con el fin de obtener algún beneficio.

En Colombia existe la Ley 1273 de 2009 para judicializar los ciberdelitos y la Ley 1581 de 2012 para la protección de datos personales, sin embargo, aún la legislación es muy pobre, adicional a esto, el desconocimiento en el tema por parte de los juristas y la perfección del delito hacen muy difícil el recaudo de las pruebas y la judicialización de los ciberdelincuentes.

La mejor forma de minimizar los ciberdelitos es generando conciencia en la población, en los colegios, universidades y empresas enseñando la importancia de mantener actualizado su sistema operativo, no comprar software ilegal, mantener sus equipos de cómputo con un buen antivirus, no ser tan ingenuos con aquellos correos electrónicos de supuestos bancos con los que se tiene relación y donde solicitan actualización de datos, o aquellos correos electrónicos con ofertas o “regalos” que llegan, y que con solo un clic, puede ver más información del premio.

Mientras no se genere conciencia en este tema, los ciberdelitos seguirán creciendo exponencialmente año tras año, teniendo en cuenta los esfuerzos que el gobierno nacional está haciendo para llevar muchos servicios estatales a internet y el impulso de la empresa privada para promocionar el comercio virtual de sus productos en eventos como ciberlunes en Colombia, o servicios bancarios cada vez más virtualizados y gratuitos.

II. DESARROLLOS TECNOLÓGICOS Y CIBERDELITOS

A. ¿Por qué los nuevos desarrollos tecnológicos están influenciado el crecimiento de los ciberdelitos en Colombia?

Desde el nacimiento de internet, personas inescrupulosas con conocimientos en programación han diseñado pequeños programas dañinos conocidos como virus, con el fin de afectar el rendimiento de los equipos de cómputo. Con los avances de la tecnología, unas pocas empresas comenzaron a utilizar Internet para el comercio, desde este mismo momento, también surgieron los cibercrímenes. Hoy día, el cibercrimen en todo el mundo ha traído pérdidas económicas calculadas en 113 billones de dólares, afectando a más de 400 millones de cibernautas, lo que lleva a que el cibercrimen sea más rentable que el narcotráfico.

Como si fueran comerciantes, los cibercriminales venden la información obtenida fraudulentamente en el mercado negro, donde una cuenta de skype puede llegar a costar USD$25, conocer los datos de acceso de una cuenta de Facebook USD$200, detalles de una tarjeta de crédito USD$10, robar un personaje virtual de un juego por internet USD$150, por eso es tan rentable el cibercrimen. [16]. Pero Colombia no es indiferente a esta situación, la penetración de las nuevas tecnologías en el país, y el incremento de los ciudadanos que acceden a los servicios de internet en los lugares más recónditos del país, como uno de los propósitos del gobierno nacional, la implementación de servicios financieros y gubernamentales virtuales y el desconocimiento de los usuarios de internet de los peligros inherentes que se presentan en la red y la despreocupación por la seguridad de su información en la web, han llevado a que se presente un crecimiento abismal del cibercrimen en el país.

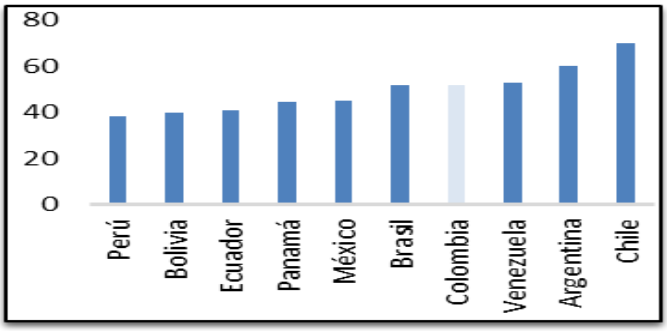

Fig. 1. (Porcentaje de individuos utilizando internet en Latinoamérica en el 2013) Fuente: Coyuntura TIC – CCIT y Fedesarrollo

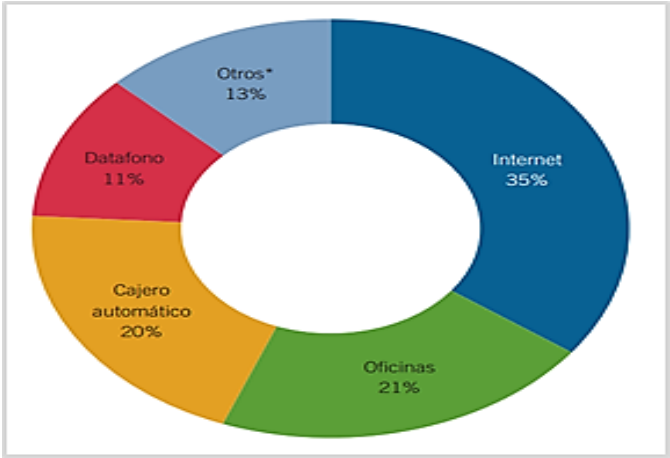

Fig. 2 (Medios utilizados en Latinoamérica para realizar operaciones bancarias). Fuente: Coyuntura TIC – CCIT y Fedesarrollo

Sergio Silva, presidente de Microsoft Colombia, alertó que "el cibercrimen aumentará cada año un 50%, por lo que más de un millón de personas están siendo afectadas por estos delitos y llevándolo aún más allá, cada segundo doce personas están siendo afectadas por este delito". Firmas expertas en seguridad como Symantec, presentaron en su reporte de 2013 para Colombia, cifras realmente preocupantes.

Fig. 3 (Reporte comparativo de las experiencias con el cibercrimen en Colombia y el mundo) Fuente: Reporte Norton 2013

Los correos electrónicos son uno de los principales vectores de propagación de códigos maliciosos, a lo largo de los últimos años se han visto múltiples reportes de campañas de correos masivas, relacionadas con troyanos bancarios a través de documentos de ofimática con macros maliciosas, o la propagación de ransomware, que llegaron a las bandejas de entrada de los usuarios.

Otro de los medios de propagación más usuales son los dispositivos extraíbles como USB, tarjetas de expansión, donde fácilmente propagan la amenaza a otros equipos.

A continuación se mencionan algunos de los métodos utilizados por los cibercriminales que actualmente están afectando la disponibilidad, confidencialidad e integridad de la información de las personas y organizaciones en el ciberespacio:

• *Phishing*: Es un delito cibernético con el que por medio del envío de correos se engaña a las personas invitándolas a que visiten páginas web falsas de entidades bancarias o comerciales. Allí se solicita que verifique o actualice sus datos con el fin de robarle sus nombres de usuarios, claves personales y demás información confidencial. (Glosario TIC, s.f.).

• *Spyware:* Programa maligno que recolecta información privada de un computador. Generalmente, para robar la información no se necesita usar el computador, y el dueño de éste no lo nota. (Glosario TIC, s.f.)

Fig. 4. **(**Correo electrónico ficticio donde se solicita descargar una supuesta factura que viene comprimida, pero que al dar clic sobre ella, se ejecuta un software espía que sin saberlo, comienza a capturar información del equipo. Imagen obtenida del correo electrónico del autor

• *Ransomware***:** Es un tipo de malware (software malintencionado) que los criminales instalan en su PC sin su consentimiento. Ransomware les da a los criminales la capacidad de bloquear su equipo desde una ubicación remota. Luego presentará una ventana emergente con un aviso que dice que su ordenador está bloqueado y afirma que no podrá acceder al mismo a no ser que pague. (Microsoft Corporation, s.f.).bcdb cvb

Es fácil reconocerlo debido a que este no le permitirá ingresar a su equipo, es necesario siempre verificar que el equipo, el sistema operativo y todo lo que se use en el computador se encuentre actualizado para así minimizar el riesgo, debido a que este siempre se va a encontrar la idea es optimizar las herramientas y así evitar que el computador sea atacado.

Fig. 5. (Cifrado de la información de un equipo, donde se da un tiempo para pagar y el costo del secuestro, el cual debe ser cancelado en bitcoins). Imagen obtenida de Internet.

• *DDoS:* Es un ataque informático que aprovecha los límites de capacidad específicos que se aplican a los recursos de red, como la infraestructura sobre la que se basa el sitio web de una empresa. El ataque DDoS enviará gran cantidad de solicitudes al recurso web atacado con el fin de superar la capacidad del sitio web para gestionar tantas solicitudes y evitar así que este funcione correctamente. (Kaspersky Labs, s.f.).

Para la ejecución de este ataque se infectan un gran número de ordenadores conectados a la red para obtener suficientes recursos y lograr que el ataque sea exitoso. De esta manera forman lo que se denomina una botnet o una red de ordenadores infectados o bots. En el momento del ataque se hace uso de todas las máquinas infectadas para generar un inmenso número de conexiones simultáneas hacia un objetivo concreto, la página Web de la compañía en cuestión. [1]

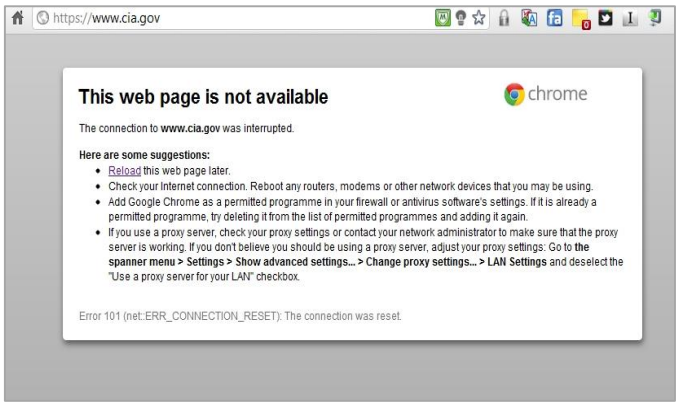

Fig. 6. (Ataque de Denegación de Servicio Distribuido al portal de la Agencia Central de Inteligencia CIA)**.** Imagen obtenida de internet.

• *Defacement:* Es la sustitución o modificación no autorizada del contenido de un sitio web.

Fig. 7. (Ataque de defacement al Portal Web del Servicio Nacional de Aprendizaje SENA). Imagen obtenida de internet.

- *Fuga de información:* La fuga de información es una de las amenazas más críticas para una organización. El mal uso de los sistemas de la organización y sus datos, la pérdida de dispositivos o de información impresa, la falta de control de acceso en las instalaciones o los errores misceláneos (como podría ser divulgar datos privados en una red pública o enviar un correo electrónico a destinatarios equivocados) podrían comprometer la información de la organización. Sin una adecuada gestión de estas amenazas, podríamos incurrir en graves multas cuando se trata de datos de alto nivel de seguridad ante las normativas de protección de datos, como por ejemplo datos personales o de salud. [6]

En los años recientes, los criminales han perfeccionado su accionar, aprovechando las nuevas oportunidades y fallas de seguridad para obtener provecho o ridiculizar a personas y empresas. A continuación se relacionan algunos de los más recientes tipos de ataques:

- *Sexting:* Es una práctica que consiste en tomarse fotos de carácter erótico o sexual a sí mismo con el fin de enviarla, mediante un mensaje de texto desde un dispositivo móvil a los amigos o personas cercanas, perdiendo el carácter de privado y puede suceder que el receptor de la imagen la haga circular a través de los correos electrónicos, la suba a las redes sociales o la reenvíe por mensaje de texto, situación que expone al protagonista de la fotografía a una serie de consecuencias indeseables. [2]

- *Ciberbullying:* Es el uso de los medios como el Internet, telefonía móvil y videojuegos online principalmente para ejercer el acoso psicológico entre iguales. Estamos ante un caso de ciberbullying cuando un o una menor atormenta, amenaza, hostiga, humilla o molesta a otro/a mediante el uso de estas tecnologías. [3]

- *Grooming:* Son el conjunto de acciones que lleva a cabo un adulto a través de las TIC para ganarse la confianza de un menor, con el fin de obtener un posterior beneficio de índole sexual. Se diferencia claramente del ciberbullying precisamente por sus principales características:
– Hay una diferencia de edad significativa entre el agresor y la víctima.
– Busca obtener de los menores beneficios de índole sexual.

La mayor parte de las veces se centran en conseguir imágenes o vídeos del menor con contenido sexual, pero en otras ocasiones se persigue el tener un contacto real con el menor para abusar de él sexualmente. El grooming está claramente relacionado con la pederastia y la pornografía infantil. El grooming es pues el "engatusamiento" que el agresor lleva a cabo para engañar a la víctima y obtener de él lo que busca, imágenes, vídeos o un contacto real para abusar sexualmente. [4]

- *APT (Advanced Persistent Threats):* Es un ataque sofisticado y de larga duración que se ejecuta contra una entidad objetivo concreta. Por su propia definición, la APT no es la amenaza "normal" a la que se enfrenta: Avanzada. El atacante dispone de las capacidades técnicas importantes que se requieren para aprovechar la debilidad del objetivo, entre las que se incluyen las habilidades de codificación y la capacidad de descubrir y aprovechar las vulnerabilidades ya conocidas. Persistente. A diferencia de los ataques aislados de corta duración que sacan provecho de las oportunidades temporales, las APT a menudo se desarrollan en cuestión de años, emplean varios aspectos y combinan las infracciones de seguridad cometidas a lo largo del tiempo para acceder a mayor cantidad de datos importantes. Amenaza los individuos, los grupos y las organizaciones que llevan a cabo las APT cuentan con la motivación, la capacidad y los recursos necesarios para lograr su efectividad. **[5]**

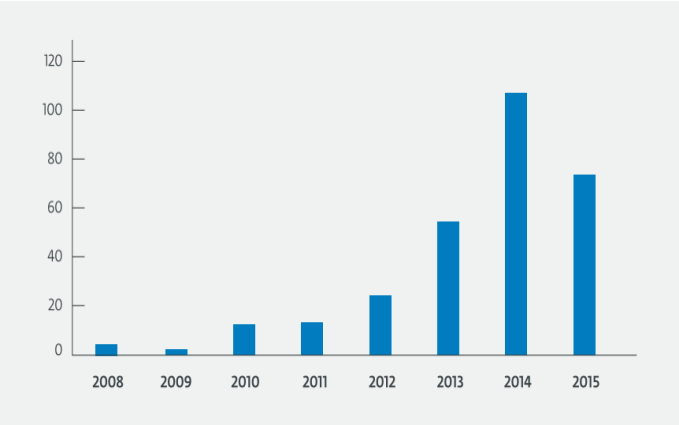

Fig. 8. (Cantidad de reportes de APT´s). Fuente: Informe Tendencias 2016 – (IN) Security Everywhere ESET

- *Páginas Web*: Los ataques a páginas Web se basan principalmente en comprometer credenciales de usuario mediante fuerza bruta o robo y/o en explotar vulnerabilidades en el software o infraestructura que soporta dicha aplicación Web, como por ejemplo los gestores de contenidos o plataformas de comercio electrónico. La mayoría de las empresas ponen a disposición de sus clientes y sus empleados plataformas Web necesarias para el negocio pero que pueden poner en riesgo la información de la empresa. [1]

- *TPVs y Copia Tarjetas de Crédito:* Cuando se refiere a ataques a Puntos de Venta (TPV) o Point of Sales (PoS), los atacantes tratan de comprometer servidores o los dispositivos PoS con el objetivo de obtener información de pago. Las empresas que más sufren este tipo de ataques son las de ventas al consumidor de a pie como las del sector de hostelería. Otra amenaza relacionada es la instalación de terminales falsos en los

cajeros automáticos para robo de tarjetas de crédito, lo que afecta principalmente a entidades bancarias. Para evitar éste tipo de fraude, Visa y MasterCard diseñaron una norma de obligado cumplimiento (PCI-DSS) con el objetivo de aumentar la seguridad de los datos y de las operaciones realizadas con tarjetas de crédito, la cual afecta a todas aquellas compañías (y comercios) que procesan, transmiten y/o almacenan dichos datos. [6]

Adicional a las amenazas anteriormente citadas, el cibercrimen está tomando nuevos rumbos, la nueva tendencia es atacar los dispositivos móviles, donde ha visto una gran oportunidad para capturar información personal de los usuarios, quienes, en su mayoría, no le tienen ningún software de seguridad como antivirus o antispyware en sus dispositivos móviles, o muchas de las aplicaciones que se descargan son virus disfrazados.

Mientras los smartphones y tabletas concentran cada vez más servicios encargados de procesar información sensible, esta se vuelve más atractiva a los ojos de los cibercriminales, donde los principales escenarios de riesgo son la pérdida del dispositivo móvil y la instalación de aplicaciones maliciosas por descuido del usuario, donde las consecuencias de un ataque se vuelven exponencialmente más críticas.

Según la consultoría de Gartner, los móviles con sistema operativo android tiene la dominancia en el mercado actual de dispositivos móviles, con el 81,9% del mercado mundial entre julio y septiembre del 2015, así mismo, fueron detectados en este mismo período de tiempo alrededor de 700.000 nuevos virus para este sistema operativo móvil, lo que se asegura que 1 de cada 5 aplicaciones son programas maliciosos.

Fig. 9. (Crecimiento de troyanos en Android durante el 2015)**.** Fuente: Informe Tendencias 2016 – (IN) Security Everywhere ESET

En este sentido, los cibercriminales iniciaron una etapa de diversificación y complejización de sus amenazas, por lo que ahora es posible apreciar campañas de difusión de malware móvil más organizadas, que abarcan nuevos vectores de infección y buscan dificultar la remoción de las amenazas. A lo largo del año 2015 se encontraron una gran cantidad de vulnerabilidades y la explotación de las mismas se convirtió en un mecanismo cada vez más vigente entre los atacantes para ganar el control de los dispositivos. Este último punto plantea nuevas presiones para la rápida actualización de plataformas, lo que puede devenir en una importante falencia para sistemas operativos como android, donde existe tal cantidad de proveedores de equipos que las actualizaciones pueden tardar demasiado en ser desplegadas a los usuarios finales.

Como consecuencia de estos ataques mejor orquestados, los códigos maliciosos comenzaron a colarse en cientos en las plataformas oficiales para la distribución de aplicaciones legítimas. Esto plantea nuevos retos de cara al futuro, instando a las empresas de sistemas operativos móviles a desarrollar mejores métodos de detección de actividad maliciosa. El ransomware, una de las actividades más rentables del mundo del cibercrimen, se consolidó en plataformas móviles con nuevas técnicas para bloqueo de los equipos, evidenciando una ramificación en las técnicas utilizadas para comprometer los distintos dispositivos.

Finalmente, cabe destacar la utilización de aplicaciones populares en plataformas móviles como whatsapp o Facebook para aumentar el alcance de campañas de malware multiplataforma haciendo uso de viejas técnicas de ingeniería social.

Existen dos factores determinantes parar que un cibercriminal se sienta atraído a los dispositivos móviles, amenazas y vulnerabilidades. A medida que los sistemas operativos son más y más utilizados por el usuario tecnológico promedio, aumenta la cantidad de potenciales víctimas susceptibles a una única campaña de malware.

Para estos nuevos ataques no existen sistemas operativos invulnerables y que la cantidad de amenazas que se encuentran orientadas a una determinada plataforma es una medida proporcional a la cantidad de usuarios que posee.

La ingeniería social es uno de los puntos fuertes en la cantidad de fraudes a dispositivos móviles. En estos casos, nuevamente se demuestra por qué la educación es la primera barrera de protección; en ese sentido, es necesario reflexionar y alertar sobre estas nuevas tendencias que utilizan antiguas técnicas en canales como whatsapp. [7]

Las compañías de seguridad informática más importantes del mundo han identificado a China como el rey de los ataques, a Perú en Latinoamérica, y a Siria, Catar y Argelia en el Medio Oriente.

III. EL INTERNET DE LAS COSAS Y LOS MILLONES DE ACCESOS AL CIBERCRIMEN

El avance de la tecnología continúa expandiendo los límites y capacidades de dispositivos móviles a nivel mundial, cada vez hay más dispositivos que se conectan a internet y son más accesibles, por lo que la superficie de ataques creció.

Según un informe de la consultora Gartner, actualmente existen 4.9 mil millones de dispositivos conectados a internet y su número crecerá en 5 años hasta llegar a los 25 mil millones de dispositivos conectados para el 2020.

En los próximos cinco años el segmento del usuario (consumer) es el que más crecerá, ya sea por la aparición de nuevos wearables (dispositivos que se usan como accesorios en el cuerpo) como también de nuevos electrodomésticos para el hogar. Todo este crecimiento llevará a la necesidad de protegerlos para evitar incidentes de seguridad.

Categoría	2013	2014	2015	2020
Automotores	96.0	189.6	372.3	3,511.1
Usuarios	1,842.1	2,244.5	2,874.9	13,172.5
Negocios genéricos	395.2	479.4	623.9	5,158.6
Servicios(Vertical busines)	698.7	836.5	1,009.4	3,164.4
Total	**3,032.0**	**3,750.0**	**4,880.6**	**25,006.6**

Fig. 10. (Unidades de equipos de IoT por categorías, en millones)**.** Fuente: Informe Tendencias 2016 – (IN) Security Everywhere ESET

Pero la IoT abarca más que relojes y televisores; desde automóviles hasta refrigeradores ya tienen la capacidad de conectarse a internet y basar toda su operatividad en una CPU. Si bien aún no se han encontrado amenazas para estos aparatos, al existir un componente de software y una conexión a internet, es viable que los atacantes se sientan atraídos para comprometerlos y obtener algún tipo de información valiosa de ellos.

IV. ¿CÓMO SE ESTÁ COMBATIENDO EL CIBERCRIMEN EN COLOMBIA?

Con el incremento de los delitos informáticos en Colombia y ante la falta de una legislación que castigara todo delito donde se utilicen las tecnologías de información y comunicaciones para su actuar, se modificó el código penal y se creó la Ley 1273 del 5 de enero de 2009, “De la protección de la información y de los datos”. Sin embargo, a pesar de tener la legislación vigente, es difícil de implementar principalmente por las siguientes causas:

- Los ciberdelincuentes generan el ataque y eliminan su rastro, este es una de las principales características de un buen hacker.
- Los cibercrímenes son día a día más sofisticados, lo cual hace más difícil que los especialistas recopilen la evidencia correspondiente para proceder con una investigación.
- El desconocimiento del tema por parte de los juristas colombianos, quienes no saben cómo actuar frente a los cibercrímenes.

Como complemento a la Ley 1273 de 2009, y viendo la deficiencia de la ley anteriormente mencionada, y la inexistencia en Colombia de una estrategia para enfrentar las amenazas cibernéticas, el gobierno colombiano expidió el CONPES 3701. Con este documento, Colombia ha tenido una política nacional para la seguridad en el ciberespacio operando durante varios años y recientemente ha estado trabajando en una nueva estrategia integral de seguridad cibernética nacional para reflejar su compromiso de estar cibernéticamente lista en las áreas de gobernanza enfocada y liderazgo institucional a nivel nacional, con el fortalecimiento de la capacidad de respuesta a incidentes y las asociaciones público-privadas y el desarrollo de la conciencia cibernética y la profundización de la educación cibernética. [8]

Con el CONPES 3701 el gobierno colombiano estableció tres organismos con la capacidad técnica y operativa para enfrentar las nuevas amenazas en delitos informáticos. El primer organismo, se consolidó la entidad interinstitucional COLCERT, que cuenta con funcionarios del Ministerio de Defensa, Ministerio de Justicia y Ministerio de las Tecnologías de Información y Comunicaciones, y su función primordial es la de dar respuesta a incidentes cibernéticos y de la coordinación entre las partes interesadas en el ámbito nacional.

Actualmente este organismo se encuentra elaborando los borradores de protocolos para la seguridad de la información y lidera la identificación del mapa de riesgos de la infraestructura crítica en el país. El segundo organismo, se desarrolló el Comando Cibernético Policial (CCP) de la Policía Nacional y dentro de sus funciones se encuentra la de investigar todos los casos en los que se ha visto comprometida la ciberseguridad de las entidades del gobierno y del sector privado del país. El tercer organismo es el Comando Conjunto Cibernético (CCOC) en cabeza del Comando General de las Fuerzas Militares, donde sus funciones son las de prevenir y contrarrestar todo ataque de naturaleza cibernética que afecte los intereses nacionales.**¡Error! No se encuentra el origen de la referencia.**

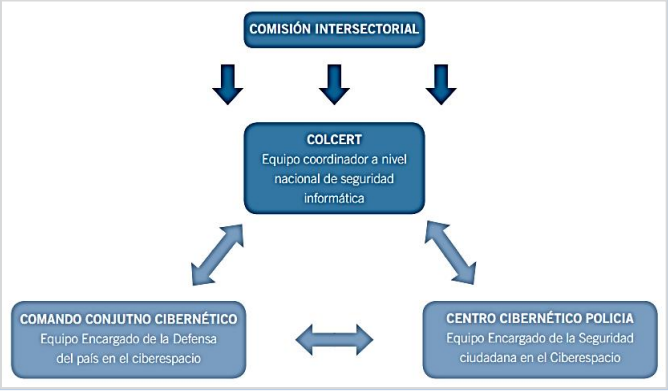

Fig. 11. (Tridente de la ciberseguridad y ciberdefensa establecido por el CONPES 3701) Fuente: Coyuntura TIC – CCIT y Fedesarrollo

V. ¿QUÉ LE ESPERA A COLOMBIA CON EL CIBERCRIMEN?

Sin duda alguna, el cibercrimen va a seguir creciendo, por el afán del gobierno de aumentar la cobertura de internet en el país, y de los comerciantes que ven en la web una opción para publicitar y vender sus productos. Sin embargo, mientras no exista un verdadero compromiso para concienciar a las personas usuarias de internet, el cibercrimen no va a disminuir.

Pese a los importantes avances de Colombia contra el cibercrimen en los últimos años, persisten falencias y muchas tareas pendientes que impiden responder de manera eficiente al elevado nivel de vulnerabilidad del país ante estas nuevas amenazas. Con base en esto, se hace necesario implementar medidas más efectivas que impongan una barrera al incremento de la delincuencia informática, la afectación del normal

funcionamiento en la prestación de servicios y la persistencia de impunidad para manejar este tipo de delitos.

Todo lo anterior brinda un nuevo andamiaje donde emergen al menos cuatro ejes fundamentales en los cuales Colombia y en especial sus autoridades deberían concentrarse. El primer eje fundamental consiste en mejorar la institucionalidad nacional, ya que si bien el CONPES representó un gran progreso, actualmente los esfuerzos de Colombia para abordar temas de ciberdelitos encuentran un techo por la falta de una visión integral de largo plazo, así como la descoordinación en las iniciativas realizadas por las diferentes entidades. En ese sentido, resulta de vital importancia actualizar el marco institucional, de tal forma que se regulen las responsabilidades entre los diferentes organismos y se permita realizar una evaluación exhaustiva de la situación de riesgo general en todo el país.

En esta misma línea, es necesario establecer un órgano de coordinación permanente, el cual tenga la autoridad legal para actuar y la responsabilidad de dirigir la formulación de política pública a nivel nacional. Adicionalmente, se deben fortalecer las capacidades de las entidades encargadas de la ciberseguridad y la ciberdefensa, en la medida que la gran mayoría de estas organizaciones no cuentan en la actualidad con la autoridad o los recursos suficientes para atender los ataques provenientes del ciberespacio. Los agentes involucrados en la seguridad del país contra el cibercrimen deben contar con una sólida capacidad analítica y técnica. En ese sentido, el gobierno colombiano deberá desarrollar e invertir en un ecosistema académico, donde se brinden las herramientas fundamentales para capacitar y certificar a los encomendados para estos temas.

De otro lado, resulta definitivo implementar una nueva regulación, eficiente y ágil sobre la investigación de los delitos informáticos. En este frente, la misión de la OEA aconseja la creación de unidades especializadas de fiscales con preparación específica para la investigación y el ejercicio de la acción penal, respecto de los ciberdelitos.

En tercera instancia, pese a que existen numerosos avances en materia de cooperación internacional, Colombia todavía se encuentra rezagado en la adhesión a los diferentes instrumentos internacionales, de hecho, ni Colombia, ni ningún país de América Latina, han firmado y/o ratificado los instrumentos internacionales jurídicos vinculantes, los cuales cuentan con obligaciones legales para todos los países miembros. De esta forma, urge la necesidad de reformar la legislación colombiana, de tal forma que se armonice con la Convención de Budapest, especialmente en lo referido a las cuestiones de derecho procesal.

Con el fin de facilitar el intercambio rápido de datos, Colombia deberá adherirse al sistema I-24/7, el cual brinda acceso a todas las bases de datos criminales de la INTERPOL, así como promover su entrada a los Equipos de Respuesta en Caso de Incidente de Seguridad (FIRST, por sus siglas en inglés), la asociación más numerosa en el mundo de equipos de esta índole.

Para finalizar, Colombia afronta el reto de crear conciencia en su población de la dimensión de esta problemática en la actualidad. La ciberdelincuencia es una amenaza cada vez más latente en nuestra sociedad, la cual atenta no solo a las más grandes industrias y entidades gubernamentales, sino que también afecta a todas las personas conectadas al ciberespacio. Por lo anterior, se debe incorporar una cultura de seguridad de la información generalizada, que se base en la capacidad de todas las personas de gobernar y administrar los incidentes que se presentan día a día. Esta cultura deberá estar orientada no solo a preservar la información sino también a asegurar la confidencialidad y disponibilidad de todos los sistemas de información existentes.

Es importante mencionar que la responsabilidad de política no recae exclusivamente en el gobierno. La población colombiana debe ser consciente que la ciberdelincuencia es una problemática que nos afecta a todos y que diariamente destruye cada vez más la estabilidad mundial. Por eso es tan necesario fortalecer las campañas de concienciación en seguridad de la información todas las esferas de la sociedad colombiana, estudiantes, empresarios, personas del común, que tienen en su mano la posibilidad de contribuir en la disminución o crecimiento de los ciberdelitos en el país.

Un ejemplo de lo anterior, y que se ha tratado durante el presente artículo, es el estudio de Symantec, donde muestra que en el mundo hay 378 millones de víctimas del cibercrimen al año, casi la totalidad de habitantes de América del Sur, 1 millón de víctimas por día y 12 víctimas por segundo. A lo anterior se suma que el 64% de los colombianos ha experimentado ser blanco de la ciberdelincuencia. En este contexto, la cultura de la seguridad de la información se erige como un baluarte en las políticas de cada individuo de la sociedad, para poder evitar así cualquier ataque que atente contra nuestra privacidad, seguridad o bienestar. [9]

Aunque hay que tener en cuenta que bajo estos riesgos que siempre existirán, Colombia junto con Chile son los dos países Latinoamericanos que mejor están enfocando la lucha contra el cibercrimen y los delitos informáticos según Luis Ortiz, experto en seguridad de Intel Security para América Latina. [10] debido a que ya varias empresas están generando planes de acción y muchas compañías de seguros están incluyendo productos para proteger esta información. Aunque no se puede negar que para competir mundialmente en sistemas de reacción para estos ataques la seguridad cibernética es muy básica, la idea es llegar a un nivel de respuesta rápido y conocer así cuando tenemos un ataque y que respuesta dar. [10].

Para hacerle contrapeso a los ciberdelincuentes, la Policía Nacional ha dispuesto a la ciudadanía en general un CAI Virtual como canal especializado en prevención de delitos cibernéticos, donde se ofrece orientación y atención de incidentes informáticos en línea, para atender a los distintos sectores de la sociedad, tomando especial valor los requerimientos ciudadanos, a través del portal de servicios http://www.ccp.gov.co y su cuenta de twitter @CaiVirtual.

A través del Centro Cibernético de la Policía, la DIJÍN investigó cerca de 5 mil denuncias recibidas a través del CAI virtual en 2015, dentro de las que se destacan casos de usurpación de identidad, *phishing*, estafas en línea, entre otras.

Como resultado, capturas por delitos de interceptación, hurto, o suplantación de datos personales ascendieron a 237 en ese mismo año.

Desde el grupo de INTERPOL, adscrito a la DIJIN, también se han realizado numerosos operativos en conjunto con agencias homólogas internacionales, con las cuales se ha logrado desmantelar redes de delincuentes informáticos alrededor del planeta y en especial, redes dedicadas a la pornografía infantil.

Ante la estrecha relación que existe entre el uso de software ilegal e infecciones de malware con potencial riesgo de ataque, otras autoridades se unen a la lucha contra la piratería. Es así como la Dirección de Impuestos y Aduanas Nacionales DIAN sostiene que mantendrá las acciones de control y fiscalización para detectar el uso de software ilegal a lo largo de 2016. Además, afirma que 110 empresas actualmente responden a procesos judiciales por casos relacionados con propiedad intelectual, enfrentando penas hasta de 8 años de cárcel, y multas hasta de mil salarios mínimos legales mensuales vigentes. [11]

REFERENCIAS

[1] Maria Ángeles Caballero Velasco MAPFRE, «Gerencia de Riesgos y Seguros,» [En línea]. Available: http://gerenciaderiesgosyseguros.com/122/ciberdelincuentes-la-gran-amenaza/. [Último acceso: 14 Septiembre 2016].

[2] Ministerio de Tecnologías de Información y Comunicaciones, «En TIC confío,» [En línea]. Available: http://www.enticconfio.gov.co/sabes-que-es-y-en-que-consiste-el-sexting. [Último acceso: 11 Septiembre 2016].

[3] Ministerio de Educación Nacional - República de Colombia, «Colombia aprende,» [En línea]. Available: http://www.colombiaaprende.edu.co/html/productos/1685/w3-article-300311.html. [Último acceso: 11 Septiembre 2016].

[4] D. Cortejoso, «Bulling-acoso.com,» 22 Diciembre 2013. [En línea]. Available: http://bullying-acoso.com/definicion-y-caracteristicas-del-grooming/. [Último acceso: 11 Septiembre 2016].

[5] CA Technologies, «Defensa frente a amenazas persistentes avanzadas: Estrategias para la nueva era de ataques,» [En línea]. Available: http://www.ca.com/es/~/media/files/ebooks/ca-apt-ebook-esn.aspx. [Último acceso: 10 Septiembre 2016].

[6] M. Á. C. V. -. MAPFRE, «Gerencia de Riesgos y Seguros,» [En línea]. Available: http://gerenciaderiesgosyseguros.com/122/ciberdelincuentes-la-gran-amenaza/. [Último acceso: 14 Septiembre 2016].

[7] D. G. Bilic, «Tendencias 2016 (IN) Security Everyware ESET,» [En línea]. Available: http://www.welivesecurity.com/wp-content/uploads/2016/01/tendencias-2016-insecurity-everywhere-eset.pdf. [Último acceso: 10 Septiembre 2016].

[8] Banco Interamericano de Desarrollo (BID); Organización de Estados Americanos (OEA), «Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?,» 2016.

[9] Fedesarrollo, Cámara Colombiana de Informática y Telecomunicaciones -, «Coyuntura TIC, Avances y retos de la defensa digital en Colombia,» Noviembre 2014. [En línea]. Available: http://www.repository.fedesarrollo.org.co/bitstream/11445/2555/1/TIC_Noviembre_2014.pdf. [Último acceso: 30 Agosto 2016].

[10] Agencia EFE , «El Espectador-Tecnología,» 01 Marzo 2016. [En línea]. Available: http://www.elespectador.com/tecnologia/colombia-y-chile-los-paises-mejor-protegidos-el-cibercr-articulo-619649. [Último acceso: 14 Septiembre 2016].

[11] Asociación Colombiana de Ingenieros de Sistemas ACIS, «Las tendencias cibercriminales más peligrosas del mundo en 2016,» [En línea]. Available: http://acis.org.co/portal/content/las-tendencias-cibercriminales-más-peligrosas-del-mundo-en-2016. [Último acceso: 14 Septiembre 2016].

[12] Kaspersky Labs, «Ataques a la red distribuidos / DDoS,» [En línea]. Available: http://www.kaspersky.es/internet-security-center/threats/ddos-attacks. [Último acceso: 8 Septiembre 2016].

[13] Jorge Silva Luján, «Cada segundo 12 personas son víctimas del cibercrimen,» 03 Septiembre 2015. [En línea]. Available: http://www.dinero.com/opinion/columnistas/articulo/perdidas-genera-cibercrimen-mundo/206653. [Último acceso: 10 Agosto 2016].

[14] Microsoft Corporation, «Centro de Seguridad y Protección,» [En línea]. Available: https://www.microsoft.com/es-xl/security/resources/ransomware-whatis.aspx. [Último acceso: 18 Agosto 2016].

[15] Dinero, «Ciberdelitos le cuestan al mundo US$300.000 millones,» 30 Octubre 2014. [En línea]. Available: http://www.dinero.com/pais/articulo/costos-ciberdelitos-colombia/202720. [Último acceso: 08 Septiembre 2016].

[16] Dinero, «El cibercrimen es un delito más rentable que el narcotráfico,» 28 Septiembre 2015. [En línea]. Available: http://www.dinero.com/internacional/articulo/principales-cifras-del-cibercrimen-mundo-colombia/213988. [Último acceso: 06 Septiembre 2016].

[17] Diario El Espectador, «El cibercrimen se apoderó del 2015,» 19 Mayo 2015. [En línea]. Available: http://www.elespectador.com/tecnologia/el-cibercrimen-se-apodero-del-2015-articulo-561403. [Último acceso: 10 Agosto 2016].

[18] "Glosario TIC," [Online]. Available: http://www.enticconfio.gov.co/index.php/glossary/Tipficar-1/P/. [Accessed 07 Agosto 2016].

[19] Corporación Colombia Digital, «Reglas de seguridad para personas y organizaciones,» 29 Julio 2015. [En línea]. Available: http://colombiadigital.net/actualidad/noticias/item/8433-reglas-de-seguridad-para-personas-y-organizaciones.html. [Último acceso: 10 Septiembre 2016].

[20] Symantec, «Reporte Norton 2013 - Hoja de Datos,» 2013. [En línea]. Available: http://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-colombia.es.pdf. [Último acceso: 18 Agosto 2016].

[21] La República, «Un millón de personas han sido afectadas por el cibercrimen en Colombia,» 26 Febrero 2015. [En línea]. Available: http://www.larepublica.co/un-mill%C3%B3n-de-personas-han-sido-afectadas-por-el-cibercrimen-en-colombia_224986. [Último acceso: 18 Agosto 2016].

Autor, nació en Bogotá, Colombia en 1982. En el 2009 terminó sus estudios de Ingeniería de Sistemas en la Universidad Central de Bogotá, certificado en ISO 27001:2013, HSEQ e ITIL V3 Foundation, con experiencia laboral en seguridad de la información bajo normatividad ISO 27001 en entidades privadas y públicas del estado colombiano, experiencia en Ley 1581 de 2012, administración de centros de datos, sistemas operativos Windows, servidores, telecomunicaciones, redes, respaldos, análisis de vulnerabilidades y riesgos de activos, auditorías de sistemas de información.