Informe:

Amenazas del **Cibercrimen** en Colombia **2016** -2017

@caivirtual caivirtual.policia.gov.co

CENTRO CIBERNÉTICO POLICIAL

I Análisis del CIBERCRIMEN

INTRODUCCIÓN

La dinámica del Cibercrimen y su constante evolución exponencial, ha propiciado que delincuentes que hasta hace poco actuaban de manera aislada, sin coordinación, con un alcance local, en la actualidad constituyan organizaciones trasnacionales complejas de Cibercrimen.

La diferenciación de roles en las estructuras criminales, el fácil acceso al mercado ilegal de tecnología para el Cibercrimen, la dificultad del rastreo de actividades ilícitas en la internet profunda o Dark Net[1], las transacciones a través de monedas virtuales, el mercado ilegal de datos y el crimen como servicio, así como la débil armonización de la persecución penal internacional, han facilitado este escenario.

> **"Las Redes Tor se utilizan como suburbios de la criminalidad y en ella figuran todo de tipo de servicios: carding, pornografía infantil, búsqueda de potenciales víctimas o redes de lavado."**
> ***Luis de Eusebio Director - Adjunto de Europol***

Aunque han pasado ya más de treinta años desde que comenzó a hablarse de la criminalidad informática, y más de veinte desde que se acuñó el término *Cibercrimen*, parece que el fenómeno de la criminalidad relacionada con el uso de las Tecnologías de la Información y la Comunicación sigue siendo totalmente novedoso y por ello, parcialmente incomprendido por la sociedad en general y, en particular, por las instituciones encargadas de la prevención de esta amenaza.[2]

El Cibercrimen forma parte ya de la realidad criminológica de nuestro mundo, pero en muchas ocasiones se exagera la amenaza que el mismo supone y en otras no se percibe el riesgo real al que el uso de las TIC conlleva. La lógica de que esta «novedad» dure tanto, es la revolución de las TIC, como concepto amplio, abierto y dinámico que engloba todos los elementos y sistemas utilizados en la actualidad para el tratamiento de la información, su intercambio y comunicación en la sociedad actual, en la que se enmarca el fenómeno del Cibercrimen. No ha terminado todavía, ni lo hará en mucho tiempo, lo que supone que la cibercriminalidad o delincuencia asociada al ciberespacio seguirá expandiéndose y evolucionando en las próximas décadas.[3]

Obviamente, esta evolución del Cibercrimen, conlleva un cambio en sus protagonistas esenciales: los criminales y las víctimas; del ya mítico *hacker*[4] estereotipado en el adolescente introvertido y con problemas de sociabilidad, encerrado en su casa, a convertirse en un genio informático capaz de lograr la guerra entre dos superpotencias usando sólo su ordenador, hasta llegar a las mafias organizadas de cibercriminales que aprovechan el nuevo ámbito para aumentar sus actividades ilícitas y sus recursos.

1. Red utilizada para compartir información y contenido entre nodos que no se encuentra indexada en motores de búsqueda, preservando el anonimato de quienes intercambian información.
2 y 3. El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio. Fernando Miró Llinares. 2012.
4. Del verbo to *hack*, cortar en inglés. Persona experta en alguna rama de la tecnología, a menudo informática, que se dedica a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo.

CENTRO CIBERNÉTICO POLICIAL

Análisis del CIBERCRIMEN

Y al no ser los cibercrímenes únicamente los motivados con ánimo económico, también varían los perfiles de cibercriminales que cometen delitos que no son más que réplicas en el ciberespacio de los que ejecutarían en el espacio físico. Lo mismo sucede con las víctimas; las empresas siguen siendo objeto de victimización debido tanto al uso generalizado de las TIC en ellas como a sus recursos económicos objeto de deseo por los cibercriminales.[5]

Pero la aparición de los cibercrímenes sociales, convierten a cualquier ciudadano, que se relacione en Internet, que contacte con otros, envíe mensajes, charle en foros o comparta sus fotos, en objeto de un ciberataque personal a su honor, intimidad, libertad sexual o similares bienes jurídicos. Lo mismo sucede con otras instituciones supranacionales en relación con los cibercrímenes políticos o ideológicos cometidos con intención de desestabilizar un Estado o de difundir un determinado mensaje político aprovechando las posibilidades de comunicación masiva que ofrece el ciberespacio: la ciberguerra, el *hacktivismo*[6] o el ciberterrorismo y que han convertido a los Estados, a los recursos públicos que ofrecen a los ciudadanos a través de Internet, en objetivo de ataques de denegación de servicio, de infecciones de *malware*[7] u otros que pueden llegar, como ha sucedido, a paralizar la actividad de importantes instituciones de un país.

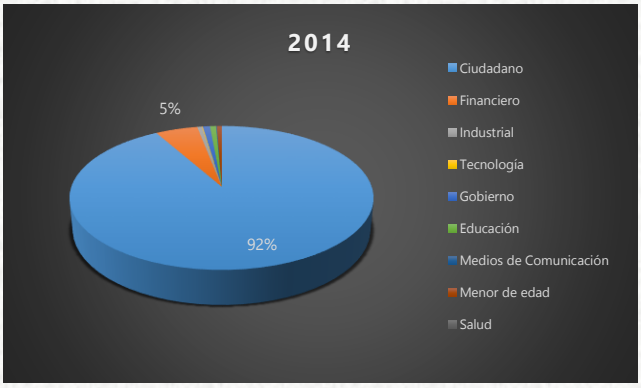
La transnacionalización del delito y los nuevos escenarios determinados por los procesos de globalización, plantean nuevos desafíos en materia de seguridad digital que generan la necesidad de implementar y desarrollar de estrategias bajo el principio de corresponsabilidad con el ánimo de hacer frente a los requerimientos nacionales y globales que enfrentamos.

Por tal motivo y con el fin de brindar atención a incidentes cibernéticos que afectan a la ciudadanía en el país, el Centro Cibernético Policial de la DIJIN ha dispuesto de un **@caivirtual** 24/7 para la prevención, orientación y atención de incidentes informáticos que afectan a los distintos sectores (públicos y privados), así como a la ciudadanía en general a través del portal de servicios: caivirtual.policia.gov.co en las cuales se difunden alertas de ciberseguridad de las distintas modalidades utilizadas por los ciberdelincuentes.

CARACTERIZACIÓN DEL CIBERCRIMEN

Durante los últimos 3 años a través de las plataformas dispuestas por Centro Cibernético Policial se recibieron **15.565**[8] incidentes informáticos. A partir del análisis de información, se identificaron aspectos comunes que permiten caracterizar el delito informático en Colombia, así:

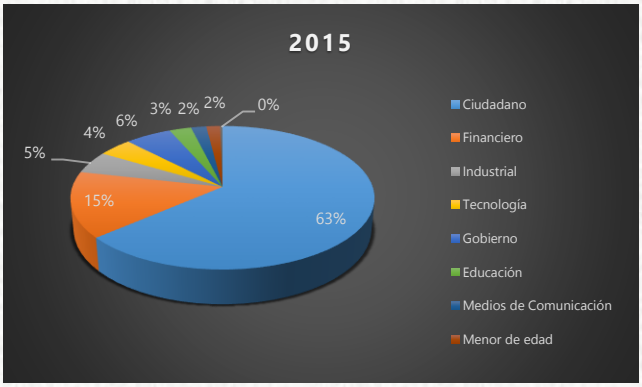
1. El cambio en la selección de las víctimas, pasando del ciudadano común a las grandes empresas del sector público-privado, las cuales generan una mayor rentabilidad a la actividad criminal.

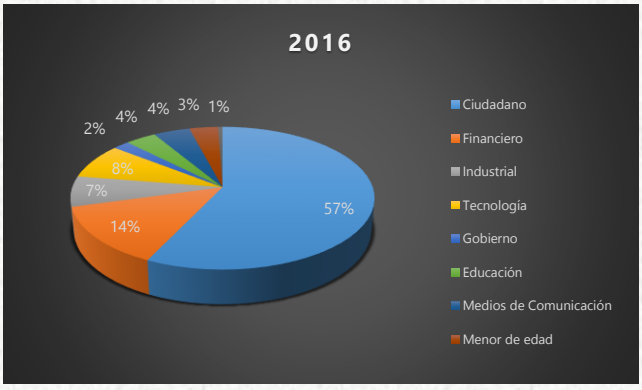


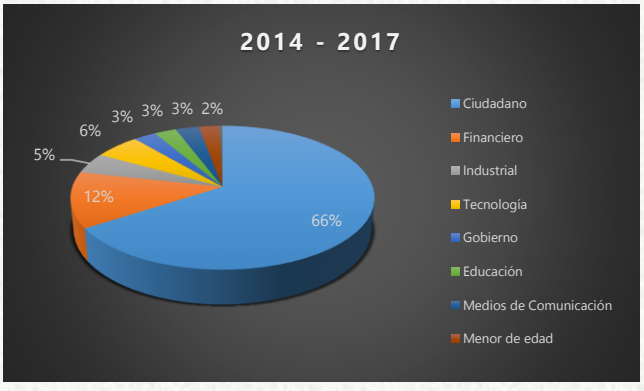
5. El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio. Fernando Miró Llinares. 2012.
6. Forma de protesta realizada por aficionados o profesionales de la seguridad informática (Hackers) con fines reivindicativos de derechos, promulgación de ideas políticas o quejas de la sociedad en general, haciendo uso de los fallos de seguridad de las entidades o sistemas gubernamentales. *revistadigital.inesem.es.*
7. Software malicioso.
8. Estadística Centro Cibernético Policial. Plataforma de atención a incidentes 24/7 @caivirtual. A fecha 10/03/2017.

CENTRO CIBERNÉTICO POLICIAL

Análisis del CIBERCRIMEN

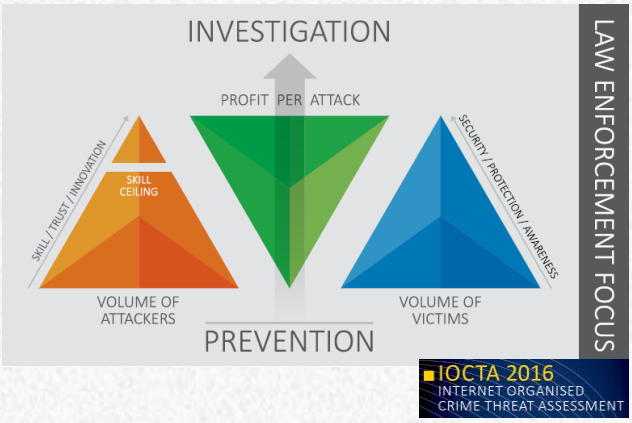






En el 2014, del total de incidentes atendidos, el 92% afectaban a los ciudadanos del común, para el 2015 el 63% y en el 2016 el 57%, presentando una **disminución del 35%**. Mientras tanto, el sector empresarial pasó de un 5% a un incremento del 28% en los reportes atendidos[9].

Estas cifras ratifican lo planteado en el documento IOCTA 2016[10] (Internet Organised Crime Threat Assessment) del European Law Enforcement Agency de EUROPOL[11], referente a la Tricotomía del delito, en donde se estipula que a mayor volumen de ataque, con mayor número de víctimas, donde su nivel de seguridad y protección es bajo, el beneficio por ataque es menor. Pero si por el contrario, el ataque se realiza a un sector reducido o especializado, por ejemplo, el sector financiero, con un ataque más sofisticado, que requiera de mayor habilidad y destreza, con niveles de innovación alto, el beneficio por ataque será mucho mayor.



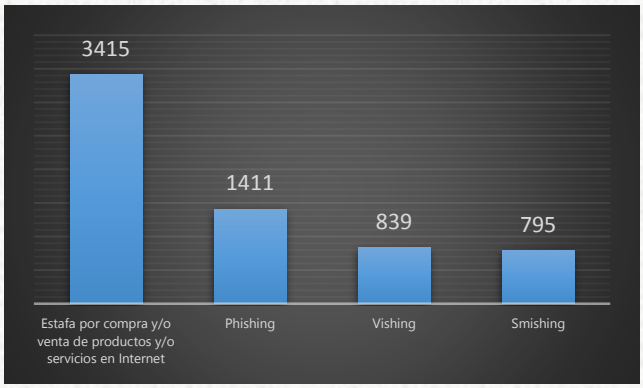
9. Estadística Centro Cibernético Policial. Plataforma de atención a incidentes 24/7 @caivirtual. A fecha 10/03/2017.
10. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016
11. EUROPOL, 28 Estados miembros de la Unión Europea en su lucha contra la gran delincuencia internacional y el terrorismo. De igual forma con numerosos estados asociados no pertenecientes a la UE y organizaciones internacionales.

CENTRO CIBERNÉTICO POLICIAL

Análisis del
CIBERCRIMEN

2. Nuevas plataformas de comercio electrónico utilizadas para estafar a través de phishing.

Generalmente, el ciudadano del común es quien más accede a reportar eventos con un 66% de los incidentes, siendo una de las principales modalidades que afectan en Colombia las **falsas ofertas** publicadas en portales web e incluso reconocidas tiendas de comercio electrónico como mercadolibre.com, OLX.com, tucarro.com, etc.



Estas estafas se originan por el incumplimiento de algunas de las partes, bien sea en el envío o recibo de productos vendidos o comprados en las plataformas, ó en el cambio de las condiciones y calidad de los mismos. Cualquier producto puede ser utilizado como mecanismo de estafa virtual.

Y es que hay una relación directa de estos eventos con el **incremento del eCommerce**[12] en Colombia, así lo demuestra el Tercer Estudio de Transacciones no Presenciales 2015 y el Estudio de Hábitos del Comprador Online 2016, presentado por la Cámara Colombiana de Comercio Electrónico[13], donde señala, que el 76% de los internautas de nuestro país en el 2014 compraron al menos un producto o servicio en línea.[14]


From: MercadoLibre <info@seguridadssl.net>
Sent: Monday, July 18, 2016 11:40 AM
To: carlosjulio_20@hotmail.com
Subject: Cuenta suspendida

mercado libre

Estimado Cliente:
Recientemente notamos un movimiento irregular en su cuenta de MercadoLibre, tales movimientos nos llevaron a suspender temporalmente su cuenta hasta que sepamos de usted.
Para activar su cuenta por favor pulse en el boton "Activar Cuenta" y llene los campos necesarios, esto hara que restablezcamos su cuenta lo antes posible.

Activar Cuenta

Saludos,
MercadoLibre

Si no quieres recibir avisos por e-mail

¡Compra y vende desde tu celular!

Disponible en App Store
Disponible en Google play

Las transacciones no presenciales o comercio electrónico, crecieron en 2015, un **64%** respecto a las de 2014. Las plataformas de pago en línea como CredibanCo, Redeban y PSE, reportaron un total de 49 millones de transacciones por $16.329 millones de dólares, que equivale al 4.08% del PIB 2015, frente al 2.63% del PIB 2014 de las transacciones respectivas[15].

Las estafas vía vishing y smishing, corresponden a la difusión del mensaje y posterior llamada del delincuente, los premios por parte de operadores de telefonía celular y almacenes de cadena, la falsas ofertas en bolsas de empleo virtuales y la falsa llamada del sobrino retenido.

Estas modalidades se pueden contrarrestar evitando dar click en enlaces y anuncios recibidos a través de correo, verificando que los portales cuenten con los protocolos de seguridad HTTPS[16], revisando periódicamente los movimientos de las tarjetas de crédito, comprando en sitios web conocidos y con buena reputación, haciendo caso omiso a llamadas y mensajes de texto sospechosos.

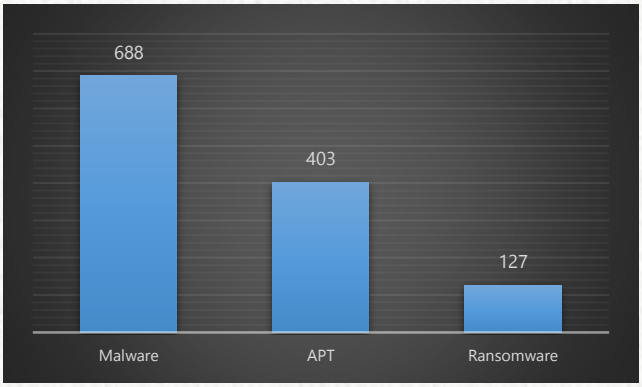
12. eCommerce, Comercio electrónico o comercio en línea.
13. CCCE, Entidad gremial que tiene como propósito consolidar el comercio electrónico y sus servicios asociados en Colombia, promoviendo las mejores prácticas de la industria.
14. https://www.ccce.org.co/sites/default/files/biblioteca/Infograf%C3%ADa%20.pdf
15. https://www.ccce.org.co/sites/default/files/biblioteca/Infograf%C3%ADa%20Tercer%20estudio%20de%20transacciones%20no%20presenciales-eCommerce%202015_0.pdf
16. HTTPS. Hypertext Transfer Protocol Secure (Protocolo seguro de transferencia de hipertexto).

CENTRO CIBERNÉTICO POLICIAL

3. Servicios de Gobierno electrónico como vector de ataque para la distribución de malware.

Ante la estrategia de **Gobierno en Línea (e-Government)**, que busca construir un Estado más eficiente, transparente y participativo gracias a las TIC, es decir, que el Gobierno prestará los mejores servicios en línea al ciudadano, los cibercriminales identificaron que estas plataformas servirían para **difundir malware** y robar información a través de estos servicios.

El ingenio de los atacantes llegó incluso a utilizar falsos correos de instituciones como la Fiscalía General de la Nación, DIAN y el SIMIT, para atraer la atención de las potenciales víctimas y lograr que dieran click sobre correos con asuntos sugestivos como "*Invitación a pagar de manera urgente sus Obligaciones.zip*", el cual al ser descargado por el usuario, ejecutaba un malware de nombre "*TrojanWin32Xtratmzc*"[17] que le permite al atacante ver todo lo que está ocurriendo en la máquina infectada.



Durante el 2016 hubo un incremento del **114.4% en ataques de malware** en el país, en relación al 2015 (153 incidentes reportados en el 2015, 328 incidentes reportados en el 2016).

Las APT (Amenazas Persistentes Avanzadas) permiten al ciberdelincuente fijar sus objetivos utilizando software malicioso, para explotar vulnerabilidades en los sistemas, se recibieron 48 incidentes en el 2015 y 286 en el 2016 respecto a esta modalidad.

De la misma forma el Ransomware tuvo un incremento de ataques del 500% en comparación del 2016 a 2015, es decir, se paso de 14 incidentes atendidos en el 2015, a 84 en el 2016, siendo esta modalidad, una de las principales tendencias del Cibercrimen en el 2017.[18] Se estima que el 76% de las infecciones de Ransomware se da a través del correo electrónico y spam.[19]

La prevención es clave para identificar los riesgos y poder combatirlos; como, por ejemplo, proteger todos los dispositivos que se conecten a Internet, eliminar todo archivo o correo sospechoso, pensar dos veces antes de dar click sobre links o archivos adjuntos en correos inesperados y realizar copias de seguridad "backups" de su información de manera periódica.

17. Este es el nombre de la familia de malware que llega por el correo electrónico disfrazado de una supuesta factura.
18. Estadística Centro Cibernético Policial. Plataforma de atención a incidentes 24/7 @caivirtual. A fecha 10/03/2017
19. http://globbsecurity.com/ransomware-cifras-38969/

CENTRO CIBERNÉTICO POLICIAL

Análisis del
CIBERCRIMEN

4. La participación activa de personas con acceso a información privilegiada o sensible de la víctima a través de BEC.

BEC (Business Email Compromise) se define como una estafa sofisticada, destinada a las empresas que trabajan con proveedores extranjeros y/o con empresas donde se llevan a cabo los pagos a través de transferencias electrónicas internacionales.

La estafa compromete cuentas de correo electrónico de negocios legítimos a través de técnicas de ingeniería social o del acceso a la información para llevar a cabo transferencias no autorizadas de fondos. De acuerdo con un informe del FBI publicado en mayo de 2016, las víctimas perdieron $3mil millones de dólares a través de BEC.[20]

Colombia no es ajena a este modalidad, donde la principal característica es, **el fraude CEO**, en el que los ciberdelincuentes falsifican la dirección de correo ejecutivo de una organización, con el fin de iniciar una transferencia de fondos a sus propias cuentas. Se estima que por cada caso de BEC que afecte en Colombia, existe una perdida de 130mil dólares.

De: juan.ochoa@cultivosfl.com 1
Enviado: Thursday, February 23, 2017 3:18 PM
Para: ana.arias@cultivosfl.com
Asunto: Proceso de pago INMEDIATO 2

Buenas tardes,

Ana, le pido que se comunique con el Dr. [redacted].com a la brevedad, y le pida instrucciones acerca de una transferencias que debemos realizar.

Es un asunto reservado, y así debe mantenerse hasta su conclusión. 3

Me mantiene informado luego de cada transferencia, a este correo.
juan.ochoa.duarte@directors.com.co

Cordialmente,
JUAN OCHOA DUARTE
Director Operativo 4

La anterior imagen es un caso de BEC y el siguiente análisis contiene los aspectos a tener en cuenta para no ser víctima de esta estafa:

1. *Un dominio de remitente falso.* Los ciberdelincuentes suelen registrar un dominio similar a su destino.

2. *Un asunto del correo electrónico urgente solicitando la transferencia de fondos inmediatos.* Suelen utilizar líneas de asunto, que implican urgencia con respecto a las consultas sobre pagos o transferencias de fondos, tales como: Pago-Importante, Aviso de pago, Proceso de pago, Solicitud rápida, Fondo Recordatorio de pago, Solicitud de transferencia bancaria, etc.

3. *Cuerpo del correo electrónico.* En el fraude CEO, los estafadores hacen aparentar que se necesita urgentemente la transferencia de fondos y debe ser ejecutada tan pronto como sea posible. Además, se deben tener en cuenta los correos electrónicos mencionados, pidiendo la transferencia de fondos o la información de la transacción a una cuenta que es diferente al utilizado normalmente.

4. *Posición del remitente del correo electrónico.* Los cibercriminales que utilizan el fraude CEO normalmente se hacen pasar por alguien influyente en una organización.

Siempre vale la pena confirmar los detalles de la comunicación, especialmente cuando se trata de mensajes que impliquen transferencias de fondos. También es importante tener en cuenta que algunos sistemas usan BEC de una cuenta hackeada, lo que subraya aún más la necesidad de protocolos que incluyen la verificación de información distintos al de correo electrónico. En lugar de hacer click en "Responder", utilice la función "Nuevo correo" y seleccione de la lista de contactos, la dirección de correo electrónico de la persona que está respondiendo, esto es para asegurarse de que no se está respondiendo a una dirección falsa.

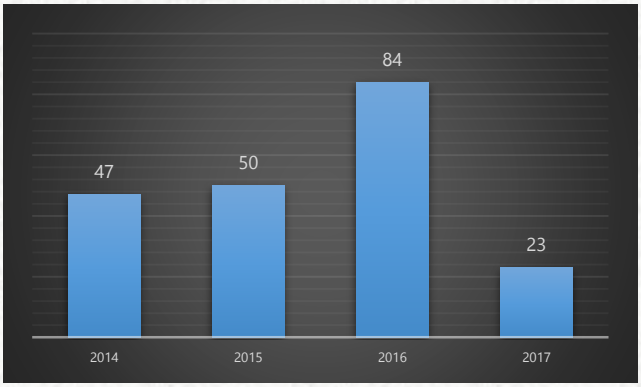
20. https://www.ic3.gov/media/2016/160614.aspx

CENTRO CIBERNÉTICO POLICIAL

Análisis del
CIBERCRIMEN

5. Vinculación cada vez más frecuente de ciudadanos extranjeros en las organizaciones criminales con injerencia en Colombia.

El fraude electrónico en cajeros automáticos ATM en Colombia ha sido uno de los vectores más explotados dentro de las entidades financieras, destacándose por su crecimiento en los últimos tiempos. Existen diversas técnicas con las cuales los ciberdelincuentes logran hacerse de una copia de la banda magnética o chip correspondiente a una tarjeta de crédito o débito, la cual es utilizada para consumar un hecho delictivo, realizando compras o directamente retirando dinero de cuentas bancarias.[21]



Esta modalidad conocida como skimming, registró 84 incidentes en el 2016, y 23 en lo corrido del presente año, teniendo una creciente injerencia de bandas internacionales de países como Rumania, que llegan a Colombia, principalmente a ciudades con gran afluencia de turistas, instalan dispositivos de alta tecnología con micro-cámaras, micrófonos y otros elementos en cajeros electrónicos, que permite almacenar la información y posteriormente ser magnetizada.[22]

En el 2016 fueron capturados 18 ciudadanos de nacionalidades extrajeras, por delitos informáticos en el país.[23]

Es por esto, que antes de utilizar un cajero, es necesario verificar que no exista ningún aparato o dispositivo extraño instalado, especialmente en la ranura de ingreso de la tarjeta, ocultar el registro de la clave de posibles micro-cámaras y desconfiar de personas extrañas al momento de realizar las transacciones.

6. Presencia de usuarios Colombianos en Deep Web.

La Deep Web ya no es algo novedoso, de hecho, es un tema del que ha tomado fuerza desde hace un par de años. Pero en cierta forma, se ha convertido en tabú, porque sólo se habla de la gran cantidad de información de tipo malicioso que se puede encontrar allí.

La Deep Web no es más que la parte de Internet que no ha sido indexada por algún tipo de buscador, por lo que la única forma de llegar a este tipo de información es conociendo la dirección exacta. Las razones por las cuales alguien podría no querer indexar su información, abarcan un gran abanico de posibilidades, de las cuales no todas son necesariamente ilegales. De hecho, para una empresa puede ser importante que la página de acceso a algún servicio web no sea conocida en Internet.[24]

La red Tor (también conocida como nivel 4 de la Deep Web) se compone actualmente por aproximadamente 30.000 sitios web ".onion" activos, lo cual la hace mucho más pequeña de lo que se pensaba anteriormente.

21. http://www.welivesecurity.com/la-es/2015/04/06/que-es-skimmer-como-proteger-tarjeta/
22. Copiar la información en las bandas magnéticas de las tarjetas.
23. Cifras SIEDCO - Plataforma Estadística se Criminalidad y Operatividad de la Policía Nacional. A fecha 10/03/2017
24. http://www.welivesecurity.com/la-es/2014/09/05/mitos-realidades-deep-web/

CENTRO CIBERNÉTICO POLICIAL

Este tipo de anonimato en internet ha servido para que criminales puedan realizar cualquier tipo de comercialización de productos ilegales como drogas, armas, imágenes con contenido de abuso sexual infantil, trata de personas y de órganos, falsificación de moneda, documentos (pasaportes, cedulas, visas), mercado de datos y de información.

En Colombia se han detectado mas 280 páginas para la comercialización de drogas, accediendo a través de buscadores como Tor. Ofreciendo la droga sólo a ciudadanos extranjeros en el país, la transacción se realiza a través de correo electrónico cifrado, el pago a través de monedas virtuales y tanto el vendedor, como el comprador, no tendrían contacto físico para la entrega del producto ya que es dejado en un lugar que con posterioridad se le da a conocer al comprador por parte del vendedor.

De igual forma en redes sociales se han identificado grupos y perfiles que comercializan estupefacientes y drogas sintéticas en pequeñas cantidades, haciendo uso de plataformas de mensajería instantánea como Whatsapp, BBM, Telegram para concretar las formas de pagos de la compra y la entrega del producto, siendo estos últimos los medios de comunicación para la negociación y las redes sociales para la oferta.

7. Uso del Internet como herramienta de amenazas e instigación a delinquir.

El uso de internet va en aumento, es una herramienta fácil de usar y accesible para personas de todas las edades, donde son muchas las posibilidades que nos ofrece: conectarnos con amigos y familiares, acceder a información con fines educativos, entretenernos y aprender cosas nuevas; en fin es una herramienta de la que se pueden obtener grandes beneficios.

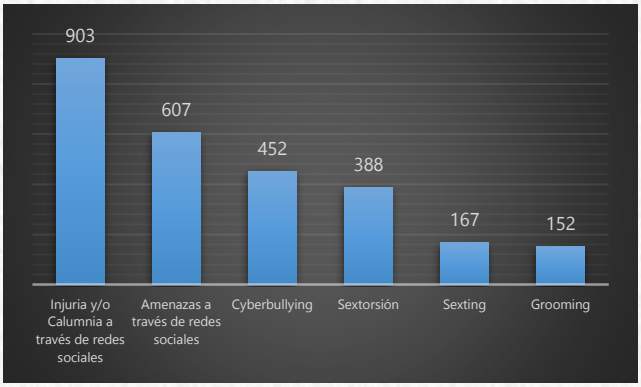
El cierre del primer trimestre del año 2016, arrojó un total de suscriptores a Internet en el país que alcanzó los 13.707.151, cifra compuesta por suscriptores a Internet fijo y móvil, lo que representa un índice de penetración del 28,1%, según el boletín trimestral del Ministerio TIC.[25]

Sin embargo, personas inescrupulosas han promovido un mal uso de internet, dando cabida a delitos y comportamientos indebidos como el Ciberbullying en todas sus formas: burlas, ridiculización, intimidación, amenazas, extorsión, etc. Así mismo la instigación a delinquir, apología al delito, suplantación de identidad, sextorsión, grooming, entre otros comportamientos inaceptables.

25. https://colombiatic.mintic.gov.co/602/articles-15639_archivo_pdf.pdf

CENTRO CIBERNÉTICO POLICIAL

Análisis del CIBERCRIMEN



Este tipo de modalidades afectan en su gran mayoría a los niños, niñas y adolescentes con un 75%, teniendo en cuenta que son más susceptibles al engaño y vulnerables en el ciberespacio. Por tal motivo se invita a los adultos responsables o tutores, para que presten mayor atención a los menores, brinden el acompañamiento y orientación frente a los peligros existentes en la web, promoviendo una disciplina de confianza que permita un dialogo abierto entre ambas partes.

8. Uso de monedas virtuales como formas de pago.

El fenómeno de las criptomonedas se ha vuelto la tendencia más revolucionaria en temas de e-comerce. Actualmente las criptomonedas han alcanzado una variedad de más de 715 tipos diferentes, siendo el **Bitcoin**[26] la más popular hasta el momento.

Las criptomonedas no son emitidas ni reguladas por ningún banco o autoridad central. Por otra parte, tienen un valor muy inestable, lo que a muchos inversionistas aventureros les representa la posibilidad de una rentabilidad excepcional al comprar, cuando por ejemplo, adquieren el Bitcoin si está a precios bajos y nuevamente revenderlos cuando los precios suban.

Estas criptomonedas se convierten de información meramente lógica a unidades monetarias como es el peso colombiano, a través de los servicios exchange, que vienen a ser las casas de cambio de las monedas digitales.

Otro aspecto importante a resaltar es la existencia de nuevos servicios de outsoursing para la gestión de Bitcoin, donde una persona compra Bitcoins a una empresa, esta le hace la conversión a la moneda local y automáticamente se va descontando del monedero del usuario. Lo anterior, a través de la asignación de medios de pago tradicionales como es el caso de las tarjetas de crédito o débito.

Es por esto que las criptomonedas se convierten en una opción al alcance de los cibercriminales, para recolectar el pago de sus víctimas, sin ser reconocidos, al obviar la autoridad monetaria y permitir su uso directo entre pares.

26. BITCOIN, usa tecnología peer-to-peer o entre pares para operar sin una autoridad central o bancos; la gestión de las transacciones y la emisión de bitcoins es llevada a cabo de forma colectiva por la red. https://bitcoin.org/es/

CENTRO CIBERNÉTICO POLICIAL

Análisis del CIBERCRIMEN

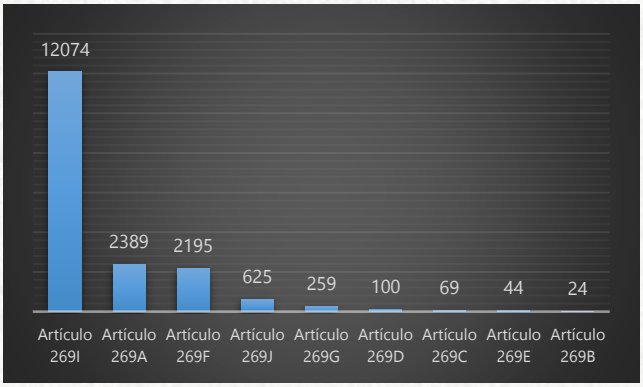
Este tipo de anonimato en internet se presta para que criminales puedan realizar cualquier tipo de transacciones debido a las avanzadas metodologías de cifrado y a la utilización de mecanismos anónimos de pago que complican la identificación de los atacantes, al punto de imposibilitar cualquier procedimiento legal.

Es aquí donde entran en juego las criptomonedas como una opción al alcance de los cibercriminales para recolectar el pago de sus víctimas, sin ser reconocidos al obviar la autoridad monetaria y permitir su uso directo entre pares.

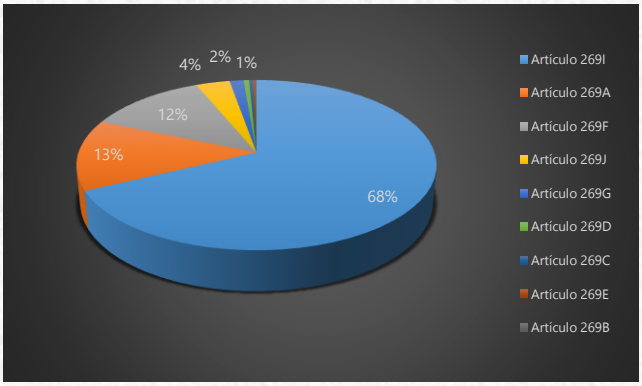
PRINCIPALES DELITOS DENUNCIADOS

Durante los años 2014, 2015, 2016 y lo que va del 2017, se han recibido 13.774[27] denuncias por violación a la ley 1273 de 2009,[28] dando un panorama de los delitos que más se denuncian en el país.

En cuanto a las tipologías criminales denunciadas ante la Policía Nacional en el citado periodo de tiempo, se evidencia un aumento significativo en el número de estas por conductas delictivas que vulneraron la integridad personal, patrimonio económico de entidades público - privadas, así como la integridad, disponibilidad y confidencialidad de la información que circula a través del ciberespacio.



Siendo el "Artículo 269I. Hurto por medios informáticos y semejantes" la tipología criminal de mayor frecuencia, equivalente al 68%, seguido de "Artículo 269A. Acceso abusivo a un sistema informático " con el 13% y "Artículo 269F. Violación de datos personales" con 12% de la muestra.



- Artículo 269A. Acceso abusivo a un sistema informático
- Artículo 269B. Obstaculización ilegítima de sistema informático o red de telecomunicación

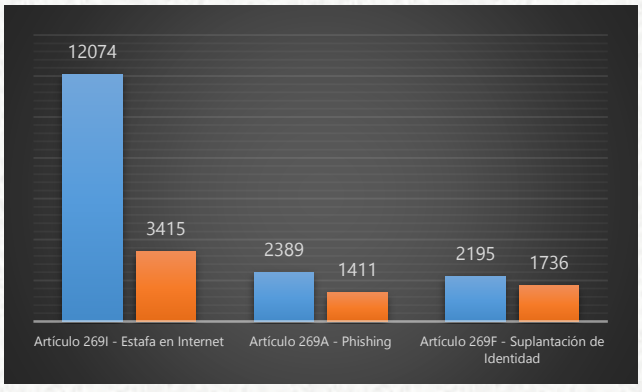
27. Cifras SIEDCO - Plataforma Estadística se Criminalidad y Operatividad de la Policía Nacional. A fecha 10/03/2017
28. Ley 1273 de 2009 por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

CENTRO CIBERNÉTICO POLICIAL

Análisis del CIBERCRIMEN

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

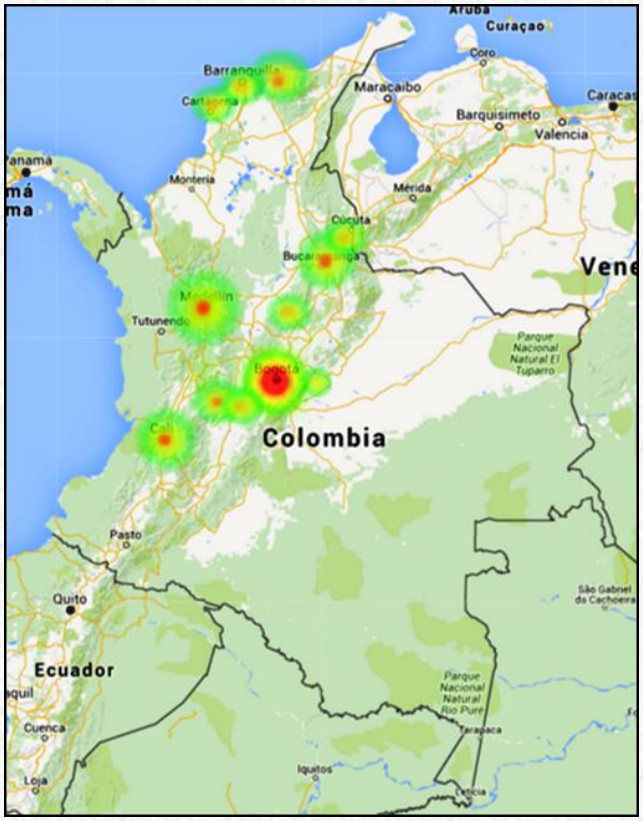
Reflejando con esto que las intenciones cibercriminales desde y hacia Colombia están ligadas principalmente a los campos comerciales y financieros, que cada vez se hacen más visibles en la cotidianidad de las personas y entidades, gracias a la masificación del uso de las tecnologías de la información y las comunicaciones a nivel nacional, como se ha mencionado anteriormente, lo que proporciona una extensión de las capacidades humanas, por lo que la interacción hombre-máquina adquiere gran protagonismo, sin dejar de lado tres aspectos primordiales que soportan el e-comercio (confianza, sistemas de pago y seguridad).



La anterior es una comparación de cifras de 3 modalidades de incidentes informáticos, con cifras de 3 delitos que se encuentran enmarcadas dentro de las conductas punibles tipificadas en el Código Penal. En cuanto a las denuncias por estafa, mas del 20% podría corresponder a estafas por medios virtuales.

MAPA DE CALOR DEL CIBERDELITO

En Colombia, la panorámica del delito informático se ve reflejada en el siguiente mapa de calor:[29]



29. Estadística Centro Cibernético Policial. Plataforma de atención a incidentes 24/7 @caivirtual. A fecha 10/03/2017

CENTRO CIBERNÉTICO POLICIAL

Análisis del CIBERCRIMEN

Las principales ciudades con más reportes de incidentes informáticos son: Bogotá 9709, Medellin 691, Cali 475, Barranquilla 240 y Bucaramanga 129[30] y las principales ciudades con mayor denuncias por Ley 1273 son: Bogotá 2607, Cali 1607, Medellin 998, Bucaramanga 594, Ibague 448 y Barranquilla 398.[31]

Lo anterior, debido a que en estas ciudades se encuentra más del 75% de suscriptores de internet fijo dedicado[32] y por mayor índice de habitantes por ciudad en el país.

COSTOS DEL CIBERCRIMEN

El Cibercrimen le cuesta al mundo hasta **US$575.000 millones al año**, lo que representa 0,5% del PIB global. Eso es casi cuatro veces más que el monto anual de las donaciones para el desarrollo internacional. En América Latina y el Caribe, este tipo de delitos nos cuestan alrededor de **US$90.000 millones al año**, el 16% del costo total mundial del delito.[33]

Datos de la compañía de seguridad RSA calcula en **US$9.100 millones** al año las pérdidas por phishing y un estudio del FBI estima en **US$2.300 millones** el daño causado en el mundo en los últimos tres años solo por ramsonware[34] y se estima que de **0,5 a 5 son los bitcoins** que solicitan los ciberdelincuentes por rescatar los archivos.[35]

La principal problemática radica en que las empresas no reconocen ser víctimas por miedo a perder clientes. El Ciberfraude en el país está generando pérdidas por **$1 billón de pesos**[36] asegura Luis Garzón, administrador de cuentas de seguridad de Cisco.

FUTURO DEL CIBERCRIMEN

- **Internet de las cosas.**

La Internet de las Cosas (IoT, por sus siglas en inglés de Internet of Things) es un tema que se popularizó hace ya algunos años, y que desde el primer momento generó polémica y debate, sobre todo dentro de la comunidad de la Seguridad Informática, puesto que **su aparición supuso (y supone) grandes y novedosos desafíos**.

El avance de la tecnología continúa expandiendo los límites y capacidades de dispositivos de este tipo; **hay cada vez más aparatos que se conectan a Internet y son más accesibles**, por lo que la superficie de ataques creció, algo que se evidenció en casos de campañas maliciosas que lograron comprometer a millones de usuarios en todo el mundo.

En pocas palabras, durante los próximos años seguirá en aumento la cantidad de dispositivos que generan, almacenan e intercambian datos con los usuarios para mejorar su experiencia y simplificar muchas de las tareas que realizan.[37]

Existen 4.9 mil millones de dispositivos conectados a Internet y su número ascenderá en 5 años hasta llegar a los 25 mil millones de dispositivos conectados a Internet para el 2020

- **Wearables.**

Durante 2015 y 2016 se realizaron gran cantidad de reportes sobre vulnerabilidades en los **wearables (dispositivos que se usan como accesorios en el cuerpo)**, en donde se desarrollaban casos que permitirían a un atacante robar y filtrar información desde el mismo dispositivo.

30. Estadística Centro Cibernético Policial. Plataforma de atención a incidentes 24/7 @caivirtual. A fecha 10/03/2017
31. Cifras SIEDCO - Plataforma Estadística se Criminalidad y Operatividad de la Policía Nacional. A fecha 10/03/2017
32. https://colombiatic.mintic.gov.co/602/articles-15639_archivo_pdf.pdf
33. https://publications.iadb.org/bitstream/handle/11319/7449/Ciberseguridad-Estamos-preparados-en-America-Latina-y-el-Caribe.pdf?sequence=7
34. http://www.dinero.com/edicion-impresa/tecnologia/articulo/las-cifras-que-mueven-el-cibercrimen-a-nivel-global/241593
35. http://globbsecurity.com/ransomware-cifras-38969/
36. http://www.elespectador.com/noticias/economia/ciberfraude-cuesta-1-billon-colombia-articulo-621635
37. http://www.welivesecurity.com/wp-content/uploads/2016/12/Tendencias-2017-eset.pdf

CENTRO CIBERNÉTICO POLICIAL

Análisis del CIBERCRIMEN

Entre los vectores de ataques utilizados, se han encontrado fallas en las aplicaciones y en el uso de las tecnologías de comunicación, como en el caso de Bluetooth y los códigos pin de seis dígitos.[38]

- **Jackware.**

Secuestrar sistemas informáticos y archivos de datos (mediante ataques de Ransomware); denegar el acceso a datos y sistemas (con ataques de Denegación de Servicio Distribuido o DDoS); e infectar dispositivos que forman parte de la Internet de las Cosas son las principales tendencias para el 2017.

Algunos ejemplos pueden ser, utilización de los dispositivos IoT infectados para **extorsionar sitios web** con la amenaza de lanzar un ataque de DDoS, o bloquear los dispositivos IoT para pedir el pago de un rescate, a lo que se llamaría "**jackware**".[39]

- **Malware para móviles.**

En un principio, se esperaba que los dispositivos móviles evolucionasen hasta convertirse en computadoras de bolsillo, tan capaces como cualquier equipo de escritorio.

Es claro que hoy nuestros teléfonos y tabletas inteligentes han trascendido este propósito, generando nuevas maneras de interacción tecnológica antes inimaginables.

Acompañando el aumento en la cantidad de nuevas variantes de códigos maliciosos, una gran preocupación para los usuarios móviles serán las vulnerabilidades no sólo del sistema operativo sino también de las aplicaciones que utilizan.

A medida que estas apps concentran datos que pueden poner en peligro la integridad física de sus usuarios, será un desafío para sus creadores el adoptar prontamente procesos de desarrollo seguro que garanticen la minimización del riesgo de exposición, por ejemplo, mediante API incorrectamente diseñadas.[40]

CENTRO CIBERNETICO POLICIAL - @caivirtual

El Centro Cibernético Policial es la dependencia de la Dirección de Investigación Criminal e INTERPOL encargada del desarrollo de estrategias, programas, proyectos y demás actividades, requeridas en materia de investigación criminal contra los delitos que afectan la información y los datos.

Para dar respuesta a los incidentes de ciberseguridad, la Policía Nacional implementó el "@caivirtual", que nace en el año 2007 como primera iniciativa online de atención policial contra el delito cibernético en Latinoamérica, y garantiza una respuesta inmediata a los requerimientos de los ciudadanos 24/7.

Como resultado de nuestras actividades, se ha logrado fomentar conciencia ciudadana en temas como seguridad de la información y seguridad informática en coordinación con los actores involucrados.

DESPLIEGUE INTERAGENCIAL

- **Centro Europeo Contra el Cibercrimen EC3 Europol**

La Policía Nacional de Colombia se ha vinculado a los diferentes grupos de expertos (Focal Point) del EC3 desde el año 2014, participando en operaciones contra la ciberdelincuencia transnacional y el crimen organizado en sus diferentes blancos.

38, 39 y 40. http://www.welivesecurity.com/wp-content/uploads/2016/12/Tendencias-2017-eset.pdf

Permitiendo un despliegue de capacidades técnicas y humanas para enfrentar estas amenazas globales, fortaleciendo la cooperación policial internacional.

Joint Cybercrime Action Taskforce "J-CAT" del EC3 Europol: El grupo de tarea conjunta contra el Cibercrimen es una iniciativa del EC3 de Europol, que consta de (13) oficiales de enlace expertos en Cibercrimen, cuya responsabilidad, es liderar y articular acciones conjuntas contra redes cibercriminales transnacionales. La participación de Colombia data desde el año 2015 siendo nuestro país el único representante de Latinoamérica en esta mesa de expertos en Europol.

- **INTERPOL**

La presidencia del Grupo de jefes de unidades para la lucha contra la ciberdelincuencia en la región de América Latina, ha permitido, a la Policía Nacional de Colombia, liderar acciones conjuntas de prevención y articulación operacional con los homólogos policiales en la región, asimismo el uso eficiente de los canales de cooperación policiales con esta agencia, nos ha permitido mejorar los tiempos de respuesta ante solicitudes de apoyo investigativo en la región.

- **AMERIPOL**

A través de la unidad nacional de Ameripol en Colombia, se está articulando las capacidades tecnológicas para enfrentar la amenaza del Cibercrimen a nivel continental, siendo Colombia, un referente en el despliegue de acciones operativas contra el fraude por medios informáticos, la lucha contra el contenido de abuso sexual infantil en línea y otras amenazas de carácter informático como el Ransomware y Botnets en la región.