NOV 2019

OVSIEC

Revista Trimestral del Observatorio de la Violencia

Seguridad en La Nube

Página 19

La Cultura del Miedo en Línea

Página 30

Entrevistas con la DIJ, CSIRT, IMEL y Otros

Página 67

Los Mercados Delictivos en Espacios Cibernéticos

"El delito cibernético, puede devastar totalmente las actividades comerciales de una empresa y causar pérdidas incontables al estado"

Ministerio de Seguridad Pública
Sistema Nacional Integrado de Estadísticas Criminales

Magister Ileana Turner

Directora Nacional

Maestría en Derecho Penal con énfasis en Ciencias Penales de la Universidad de Panamá, Licenciada en Derecho y Ciencias Políticas de la Universidad de Panamá, con postgrados en Derechos Humanos, Docencia Superior, Contabilidad y Finanzas y Especialización en Anti-lavado Financiero y Legal.

Equipo de Análisis

Leopoldo Lester

Analista – Sociólogo

Licenciado en Sociología de la Universidad de Panamá con estudios en Estadísticas Social y Económica, Métodos y Técnicas de Investigación del IDEN

Ana de Gracia

Analista – Técnico

Licenciada en Criminología de la Universidad Interamericana de Panamá, con estudios en Inteligencia del Centro de Capacitación y Especialización Policial (CECAESPOL)

Omar Blandón

Analista – Criminólogo

Maestría en Administración de Empresas de la Universidad Latina, Licenciado en Criminología y Planificación de Texas A&M University, con postgrados en Inteligencia, Diseño de Investigación Social y Análisis de Delitos Especializados.

Ricardo Hull

Analista – Abogado

Licenciado de Derecho y Ciencias Políticas de la Universidad de Panamá, con un postgrado en Derecho Laboral y Diplomado en Derecho Administrativo.

Jaime de Urriola

Analista – Historiador

Licenciado de Historia de la Universidad de Panamá.

Portada: Omar Blandon

Colaboración

Policía Nacional – Dirección de Investigación Judicial

- ❑ División de Delitos Contra la Propiedad Intelectual y Delitos Cibernéticos

Instituto de Medicina Legal y Ciencia Forense (IMELCF)

- ❑ Conversatorio con Personal Técnico y supervisor de Áreas Periciales de la sección de Informática Forense

Autoridad Nacional de Innovación Gubernamental (AIG)

- ❑ Entrevista con el personal técnico de la Dirección de Ciberseguridad del Centro Nacional de Respuesta a Incidentes –CSIRT Panamá

CONTENIDO

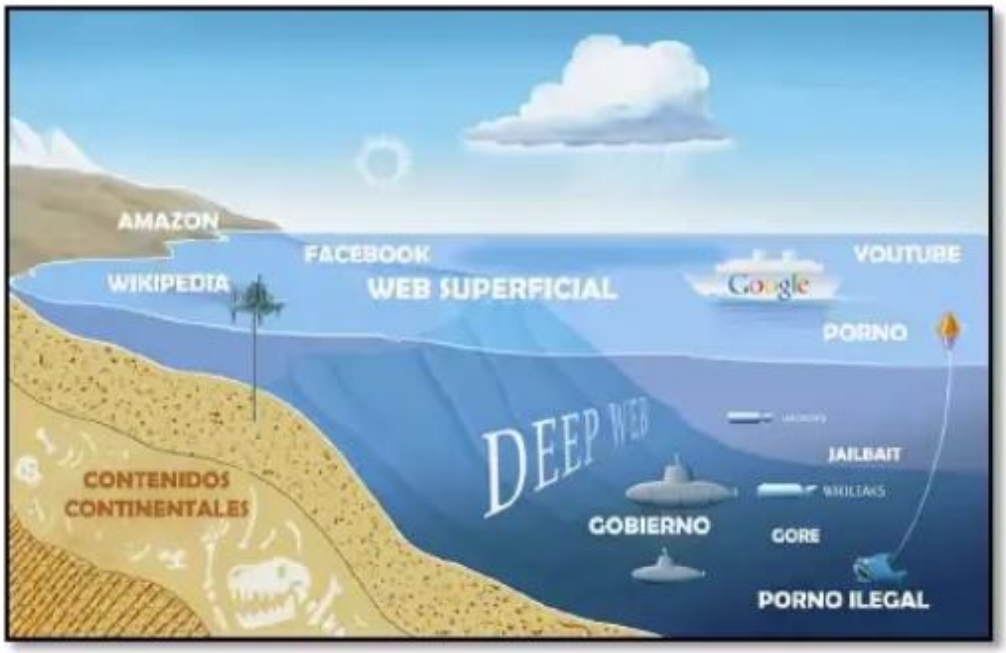
PRÓLOGO

Internet es sin duda la herramienta que le ha facilitado la vida a miles de millones de usuarios alrededor del mundo. Cuando hablamos de La Red, de aquel vasto océano de datos casi ilimitados donde podemos navegar en búsqueda de información, realizar una videoconferencia a cualquier parte del planeta o acceder a compras de artículos a través de sus innumerables tiendas virtuales haciendo nuestras vidas más llevaderas y eficientes.

Sin embargo, Internet es mucho más allá que Youtube, Facebook, Twitter o Instagram. La parte visible del ciberespacio conocida también como la Internet Superficial, representa aproximadamente el 4% de sitios rastreables.

La pregunta inmediata es: ¿Qué hay en el 96% de la *web* restante? ¿Quiénes la utilizan y con qué propósito? Es a partir de aquí, en los subniveles donde los usuarios comunes no logramos acceder, que la realidad supera a la ficción.

Podríamos definir a la *Deep Web* como todo el contenido de la Internet que no forma parte de la Internet Superficial, es decir, aquella que no está indexada a los motores de búsqueda de la red y que en ella se esconde el 80% del contenido real de la Internet donde se pueden encontrar páginas olvidadas, información clasificada e incluso sitios de organizaciones delictivas dedicadas a todo tipo de negocios oscuros y mórbidos.



PRÓLOGO

Para tener una mejor comprensión de lo inmensa que es la red, tomaremos como ejemplo el motor de búsqueda más famoso en la actualidad: Google. Desde su aparición en 1998, albergaba aproximadamente unos 2.4 millones de sitios web y para el 2018 ya alcanzaba la asombrosa cifra de 1.6 billones de *websites* y la cual continúa creciendo exponencialmente en este instante. Si definimos esa cifra en almacenamiento de datos, podríamos decir que Google tiene un tamaño de 19 Terabytes de información contenida en sus servidores actualmente.

Estos datos podrían resultarnos gigantescos si no mencionáramos que la *Deep Web* posee un tamaño 500 veces mayor. Informes de la Universidad de California en Berkeley, estiman que la red profunda contiene alrededor de 7500 Terabytes de información, lo que se traduciría en aproximadamente 550 billones de contenidos individuales.

Es en este espacio inmensurable donde se han desarrollado las más complejas e inimaginables formas de mercado negro y demás modalidades del crimen organizado jamás vistas hasta ahora (pornografía infantil, trata de personas, tráfico de drogas, falsificación de documentos e identidades, asesinatos en vivo, entre otros).

Dichas características hacen de la *Deep Web* un lugar atractivo para actividades que desean permanecer en la oscuridad, por lo que muchos criminales cibernéticos se reúnen en foros privados donde el acceso es restringido.

La *Deep Web* adquirió mayor relevancia en el año 2011 con el nacimiento de la famosa Ruta de la Seda mejor conocida como *Silk Road*. Creada por el hacker estadounidense Ross Ulbricht, el sitio actuaba como un mercado negro en línea para la venta de cualquier tipo de drogas y negocios ilícitos. Desde su creación en 2011 hasta el momento de su cierre por el FBI en octubre de 2013, el sitio web poseía un catálogo en línea de 13,000 artículos (la mayoría de ellas drogas), y logró generar ganancias por 9.5 millones de bitcoins, cuyo equivalente en dólares americanos sería de 1.2 billones de dólares.

Panamá, como una plataforma de servicios y punto de desarrollo estratégico en el ámbito comercial y financiero, no está exenta de los peligros que conllevan dichas acciones que pondrían en riesgo nuestro centro bancario y de negocios. Es por esta razón que las legislaciones de los países han reforzado sus leyes para combatir y hacerle frente a esta nueva modalidad de delito cibernético.

En ese sentido, nuestro país tiene la obligación internacional de adecuar su legislación penal conforme a los estándares regulados en el Convenio de Budapest, lo que implica elaborar reformas al Código Penal y Código Procesal Penal.

Actualmente, Panamá cuenta con el CSIRT-Panamá bajo la estructura de la AIG (Autoridad Nacional para Innovación Gubernamental) creada a través del Decreto Ejecutivo 709 de 2011. Dicha unidad tiene como objetivo principal prevenir e identificar ataques e incidentes de seguridad a los sistemas informáticos de la infraestructura crítica del país.

Mediante la presente publicación, no solo trataremos de abordar el ciberdelito como una simple conducta criminal, por el contrario, analizaremos el concepto de seguridad informática como parte de una política criminal y reflexionaremos sobre las intervenciones que son necesarias para la protección de la información de las personas y sus derechos en el ámbito digital.

EL INTERNET Y SUS OPORTUNIDADES PARA CREAR MERCADOS DELICTIVOS

INTRODUCCIÓN

El delito cibernético, le cuesta a las empresas y a los estados miles de millones de dólares anualmente en activos robados y pérdida de negocios. Este delito puede devastar totalmente las actividades comerciales de una empresa y causar pérdidas incontables al estado, debido al hecho que cada día más dependemos de la tecnología y el internet para hacer la gran mayoría de nuestras transacciones comerciales. Como resultado, una empresa puede perder negocios si se percibe que es vulnerable al delito cibernético. Dicha vulnerabilidad puede conducir a una disminución en el valor de mercado de la empresa, debido a preocupaciones legítimas de analistas financieros, inversores y acreedores. (Anderson, 2013)

Por otro lado, la información que es robada de las empresas tanto privadas como estatales representa un mercado delincuencial en crecimiento que, mediante el uso de herramientas de encubrimiento de identidad en el internet produce un mercado “negro” virtual, que se explicará a fondo en el presente artículo. Estos mercados utilizan como moneda de intercambio el ahora muy conocido método de pago llamado **criptomoneda** , siendo la más estable y confiada la moneda conocida como, ***Bitcoin***.[2] (Abeslamidze, 2018)[1]

El comercio electrónico es una parte fundamental de la actividad comercial internacional y según los pronósticos de muchos especialistas, la mayoría de las transacciones a futuro serán por medios electrónicos. (McCarthy, 2016) La mayoría del comercio electrónico tiene lugar en los sitios web de las empresas, en este ambiente virtual, el término "ciberespacio" se refiere al medio electrónico de las redes informáticas, principalmente la Web, en la cual se viabiliza la comunicación en línea entre Empresas a Usuarios o “B2C” en inglés o entre dos personas “P2P” para concretar una transacción comercial. Un desafío al interrumpir la facturación es que

1. La criptomoneda o criptodivisa es un tipo de moneda digital que utiliza la criptografía para proporcionar un sistema de pagos seguro. Estas técnicas de cifrado sirven para regular la generación de unidades monetarias y verificar la transferencia de fondos. No necesitan de un banco central u otra institución que las controle. (Economipedia, 2019)

2. Verbatim, de la Pagina Web de Bitcoin, 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. (Org., 2019)

se genera grandes pérdidas en concepto de gravámenes, gastos en costosos medios investigativos fiscales y la pérdida de confianza en los controles legales, todo hechos que, si no se lleva adelante un mínimo de control, pueden conducir a la inclusión a las notorias listas de los llamados paraísos fiscales y países no seguros en el ámbito tecnológico. (Gregory, 2007)

El cibercrimen le cuesta a la economía internacional más de $ 6 mil millones de dólares por año (Accenture Security, 2019)[3]. Estos activos monetarios lamentablemente pueden ser robados, literalmente con solo presionar un botón. El presente artículo examina los tipos de delitos informáticos y cómo afectan la actividad comercial legitima y brinda mayor información del mercado "negro" ilegitimo.

Además, el estudio revisa distintos estudios que tendrán como objetivo contestar las siguientes preguntas de investigación abordadas en el artículo que incluyen:

¿Cuáles son algunas formas en que el delito cibernético afecta la actividad comercial legitima?

El Internet merece una atención especial en la criminología, así como en el derecho y las políticas penales, debido a varias características: es global, instantánea, intrínsecamente transfronteriza, digital y permite el procesamiento automatizado de la información.

Debido a estas características, ¿Qué ámbitos, ofrece el Internet para cometer delitos cibernéticos y delitos comunes? Delitos en que las redes informáticas son el objetivo o una herramienta sustancial.

El artículo, esboza algunas tipologías de la ciberdelincuencia y enumera factores de riesgo del Internet que, en combinación, proporcionan una estructura de oportunidades única para la delincuencia. Incluye un análisis del llamado "Red Oscura"[4] y su vasto mercado delictivo, ilustrando temas que debe preocupar las autoridades.

3. Verbatim, del texto metodológico. "Para determinar el costo promedio del delito cibernético, las organizaciones encuestadas informaron sobre lo que gastaron para lidiar con los delitos informáticos durante cuatro semanas consecutivas. Una vez que los costos durante el período de cuatro semanas fueron compilados y validados, estas cifras fueron luego calculadas para determinar el costo anualizado. Estos son costospara detectar, recuperar, investigar y gestionar la respuesta al incidente. También cubierto son los costos que resultan en actividades posteriores al hecho y esfuerzos para reducir la interrupción del negocio y la pérdida de clientes. Estos costos no incluyen gastos e inversiones realizadas para mantener una postura de seguridad de la organización o cumplimiento de estándares, políticas y regulaciones." (Accenture Security, 2019)

4. La llamada deep web (internet profunda) o darknet (red oscura) es como una ciudad virtual sin ley en la que se aloja el 96% del contenido de internet. Navegar por ella no es ilegal, pero cualquier navegador convencional no sirve como puerta de entrada. (BBC, 2019)

(3) Este artículo discutirá: ¿Qué hay de la regulación de las monedas virtuales y sistemas de pago cibernéticos y que requiere mayor inquisición en su uso?

(4) ¿Cómo ha impactado en nuestra economía el uso del internet por el crimen organizado para encubrir las verdaderas identidades de algunos delincuentes y cuál es el alcance transnacional?

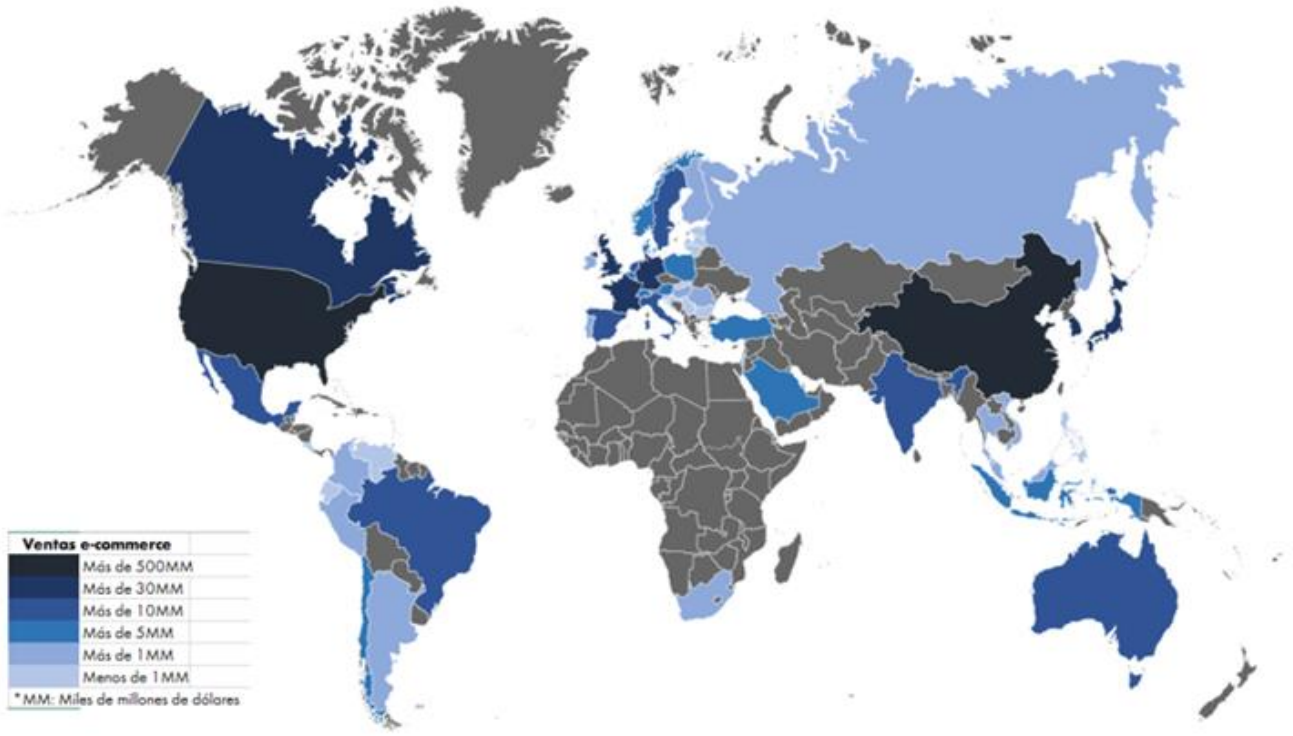
Se analizará lo poco que se sabe de los ciberdelincuentes, la ciberdelincuencia organizada y las víctimas cibernéticas, y discute brevemente los desafíos y limitaciones de la aplicación de la ley y otras contramedidas. Aunque la investigación empírica sobre la ciberdelincuencia es escasa, las ideas teóricas y las hipótesis avanzadas en la literatura justifican la conclusión de que el Internet está transformando la delincuencia de manera importante.

EL CIBERDELITO EN EL MUNDO DEL COMERCIO LEGAL

Los gerentes corporativos hoy por hoy están obligados a considerar los riesgos electrónicos y encontrar las mejores maneras de mitigarlos. Ya es una práctica común el tomar precauciones contra el fraude electrónico, frente al problema que causa los piratas informáticos, los virus y otros delitos cibernéticos. Hasta cierto punto, el negocio electrónico comenzó con las primeras computadoras en la década de 1950. Sin embargo, fue hasta el desarrollo de la World Wide Web en la década de 1990, que el negocio electrónico realmente despegó. (E-Commerce Land, 2019)

El comercio electrónico es el intercambio de bienes o servicios utilizando una infraestructura electrónica. Hace poco tiempo, el uso de Internet como una forma principal de hacer negocios se consideraba demasiado arriesgado. Hoy, el comercio electrónico es simplemente un negocio; así se hacen los negocios en el siglo moderno. El Internet es ampliamente utilizado tanto para transacciones de empresa a empresa (B2B) como para transacciones de empresa a consumidor (B2C).

FIGURA 1. VENTAS REGISTRADAS A NIVEL GLOBAL DEL COMERCIO ELECTRÓNICO



Fuente: (Linio, 2019)

El mercado B2B es de cinco a siete veces mayor que B2C. Se predice que el mercado B2B superará los $ 12 mil millones en los próximos años. (Statista, 2019) El mercado B2C está creciendo rápido, pero se caracteriza por un tamaño de transacción promedio mucho menor. (Statista, 2019) En un lapso de aproximadamente 50 años, las computadoras transformaron la forma en que las personas trabajan, juegan y se comunican.

Con todo este gran flujo de dinero intercambiando diariamente, el riesgo electrónico consecuentemente existe por el potencial de que exista problemas Financieros y tecnológicos cuando se hace negocios en la Web. Los ataques informáticos modernos abarcan un amplio espectro de actividad económica, donde distintos delincuentes cibernéticos se especializan en el desarrollo de programas informáticos maliciosos como son los exploits, botnets, mailers y servicios de distribución de malware, monetización de credenciales robadas, alojamiento web entre otros. Evaluar las relaciones entre varios de estos actores es una información esencial para discutir que estrategias económicas, técnicas y legales se deben tomar para abordar el delito cibernético.

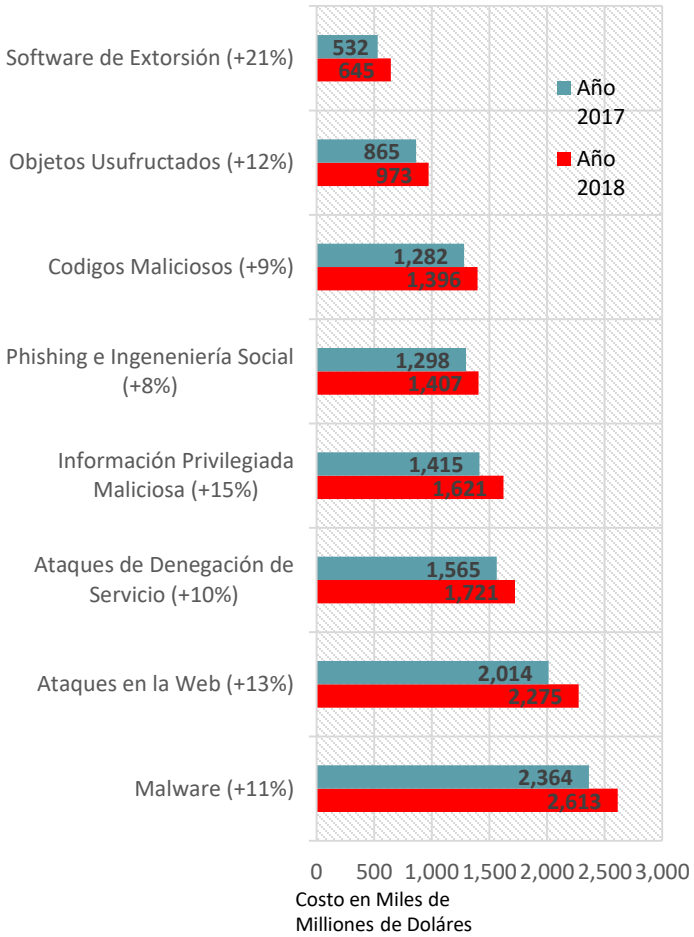
Así también, presentamos la arquitectura general de los ataques informáticos comunes y discutimos el flujo de bienes y servicios que respalda la economía subterránea. Discutimos el flujo general de recursos entre grupos criminales y víctimas, y las interacciones entre diferentes cibercriminales especializados.

❖ Mapa Económico Del Delito Cibernético

Crear un mapa económico del delito cibernético con todas las entidades posibles y sus interacciones no es trivial. Los ataques informáticos se implementan en muchas formas diferentes y su rentabilidad dependerá con frecuencia del sistema específico bajo ataque. Por ejemplo, hay una gran diferencia en atacar la data personal de una persona, usufructuar sus credenciales y tomar posesión de sus cuentas bancarias versus hacer este procedimiento en gran escala o a una empresa de grandes recursos económicos.

A nivel global se observa que el delito va en incremento de un año a otro según información disponible de fuentes de crédito mundial como el Informe Accenture de 2019. De acuerdo al informe, el Malware y Ataques en la Web son los más costosos para las empresas, sin embargo, existe otras modalidades de ataques cibernéticos que muestran serios avances con respecto a años pasados.

GRÁFICA 1. PROMEDIO DE COSTO ANUAL GLOBAL POR TIPO DE ATAQUE CIBERNÉTICO



Fuente: (Accenture Security, 2019)

Para este documento, no intentamos dar una descripción completa de los delitos informáticos; en cambio, nos enfocamos en los tipos de delitos informáticos generalizados, a gran escala y automatizados: el uso de troyanos para robar

credenciales de las computadoras de las víctimas y la infraestructura necesaria para ejecutar un botnet, ambas partes integrales en el arsenal de los temidos *hackers*[5]. Al describir estos crímenes, también debemos describir un gran ecosistema de delincuentes, incluidos los escritores de vulnerabilidades, los distribuidores de malware y los cajeros. (Broadhurst, 2014)

La explotación de las vulnerabilidades de software para obtener el control de varias computadoras es el paso fundamental en la mayoría de las empresas de ciberdelincuencia. Encontrar vulnerabilidades y escribir software de explotación [6] o exploits como comúnmente se conoce en la jerga del internet son unos de los aspectos que requiere de conocimiento especial de los ataques informáticos en comparación con otros roles de cibercrimen.

Por lo tanto, crear el mismo software que se usa para introducir códigos maliciosos a las computadoras se ha convertido en una tarea especializada. Al igual que con muchas otras partes del ecosistema del delito cibernético, existen varias herramientas de software especializadas que se utilizan para comprometer las máquinas, por ejemplo: Metasploit, Luckysploit, Gumblar, Mpack, Zeus y Neosploit. (Choo, 2013) Por lo tanto, si bien los atacantes avanzados pueden escribir su propio código de explotación, muchos otros delincuentes pueden hacer uso de estas herramientas que son fácilmente disponibles sin que el delincuente tenga conocimiento especializado en programación. Si bien muchas de estas herramientas se pueden comprar en mercados de la Red Oscura o como distribuidores para el uso sano en páginas de ventas para ingenieros de seguridad informática.

Una vez que los atacantes tienen acceso a herramientas de explotación, aún necesitan encontrar computadoras vulnerables para explotar. Tradicionalmente, había dos métodos principales para encontrar estas computadoras vulnerables en sitios remotos: (1) Un atacante probaría las redes para identificar computadoras vulnerables, o (2) un atacante

5. Un hacker es una persona que por sus avanzados conocimientos en el área de informática tiene un desempeño extraordinario en el tema y es capaz de realizar muchas actividades desafiantes e ilícitas desde un ordenador. (Akhgar, 2014)

6. Un programa o código que se aprovecha de un agujero de seguridad (vulnerabilidad) en una aplicación o sistema, de forma que un atacante podría usarla en su beneficio (Akhgar, 2014)

enviaríaspam con archivos adjuntos de malware. Si bien estas dos formas de encontrar computadoras vulnerables todavía están activas, actualmente, la forma[5] más común de comprometer las nuevas computadoras es a través de malware basado en la web. En este tipo de ataque, los ciberdelincuentes se apoderan de un servidor web, lo convierten en un sitio controlado por malware y "atraen" a los usuarios de computadoras vulnerables para que visiten su sitio web. Para "atraer" a los usuarios a visitar su servidor, los ciberdelincuentes utilizan programas afiliados que pagan a otros delincuentes por la cantidad de tráfico referido a su servidor de malware. (Choo, 2013)

Una técnica muy popular para dirigir el tráfico al servidor malicioso es infectar sitios web legítimos y agregar un iframe[7] que apunta al servidor malicioso. Además, los ciberdelincuentes pueden convencer a los desarrolladores de sitios web malintencionados de que incorporen código malicioso en sus sitios web, o pueden distribuir widgets[8] maliciosos "gratuitos" de terceros como un contador de visitantes del sitio web que los desarrolladores de sitios web incorporan en su propio sitio. El 80% de los sitios web señalados como maliciosos por los índices de antivirus y motores de búsqueda son negocios legítimos que fueron abusados para redirigir el tráfico a sitios maliciosos. (Gercke, 2014)

❖ Monetizando Computadoras Comprometidas

Una vez que un atacante explota una vulnerabilidad en una computadora, obtiene el control sobre ella y puede instalar cualquier programa. Uno de los primeros programas que instalan los atacantes es el software con la capacidad de realizar un seguimiento de todas sus computadoras comprometidas. Un conjunto de computadoras comprometidas bajo el control de una sola autoridad generalmente se denomina botnet. Al controlar una botnet, un atacante tiene muchas formas de monetizar las computadoras comprometidas. Las fuentes de ingresos incluyen el robo de información privada, demandas de extorsión a través de ataques DDoS[9], spam, envenenamiento de

7. iFrame es la abreviatura de Inline Frame y es un elemento poderoso en el diseño web. Probablemente hayas visto innumerables videos de YouTube insertados en sitios distintos a YouTube. Un iFrame puede insertar todo tipo de medios. Entonces si te preguntas cómo lo hicieron, lo más probable es que el diseñador web haya puesto un elemento iFrame dentro de esa página. (Broadhurst, 2014)

8. Los Widgets son una serie de pequeños programas que se utilizan para añadir funciones, simplificar o automatizar aquellas acciones que se lleven a cabo con frecuencia dentro de una web. (BBC, 2019)

9. Un ataque DDoS tiene como objetivo inhabilitar un servidor, un servicio o una infraestructura. Existen diversas formas de ataque DDoS: por saturación del ancho de banda del servidor para dejarlo inaccesible, o por agotamiento de los recursos del sistema de la máquina, impidiendo así que esta responda al tráfico legítimo (Gercke, 2014)

motores de búsqueda y fraude de clics. Si bien los ataques de spam, phishing y DDoS pueden considerarse parte del modelo de negocio de botnet, los describimos con más detalle en secciones separadas debido a su notoriedad.

1. Ataques Cibernéticos Y Sus Mecanismos Para El Robo De Credenciales

El phishing comenzó como un método de fraude por correo electrónico en el que el autor envía correos electrónicos legítimos que contienen enlaces a sitios web falsificados en un intento de obtener información financiera confidencial de los destinatarios. Los sitios web que son frecuentemente falsificados por los phishers incluyen PayPal, eBay y las instituciones financieras más conocidas del mundo. Con frecuencia, se engaña a los usuarios para que brinden información confidencial haciendo clic en los enlaces de correos electrónicos que aparentemente provienen de instituciones financieras legítimas que les piden que actualicen su información de contacto e inicio de sesión. Una vez que se registra esa información, los ciberdelincuentes pueden obtener el control de la cuenta. Si bien todavía se realizan varios ataques de phishing de esta manera, los están siendo reemplazados por troyanos que roban credenciales. Este tipo de troyano utiliza keyloggers[10] y screenloggers[11] instalados en las computadoras de las víctimas para recopilar información personal, esta última modalidad ha sido encontrado a menudo en el campo de trabajo por los expertos en peritaje del ***Instituto de Medicina Legal de Panamá.***

Los programas de explotación Zeus y Torpig son algunos de los muchos ejemplos de troyanos que roban los datos de los usuarios. Además del monitoreo pasivo, muchos de estos troyanos obtienen activamente información confidencial de sus víctimas. Por ejemplo, cada vez que la máquina infectada visita uno de los dominios especificados en el archivo de configuración del troyano (por ejemplo, un sitio web bancario), El virus emite una solicitud a un servidor de inyección que proporciona un formulario en la página de inicio de sesión, solicitando al usuario información confidencial.

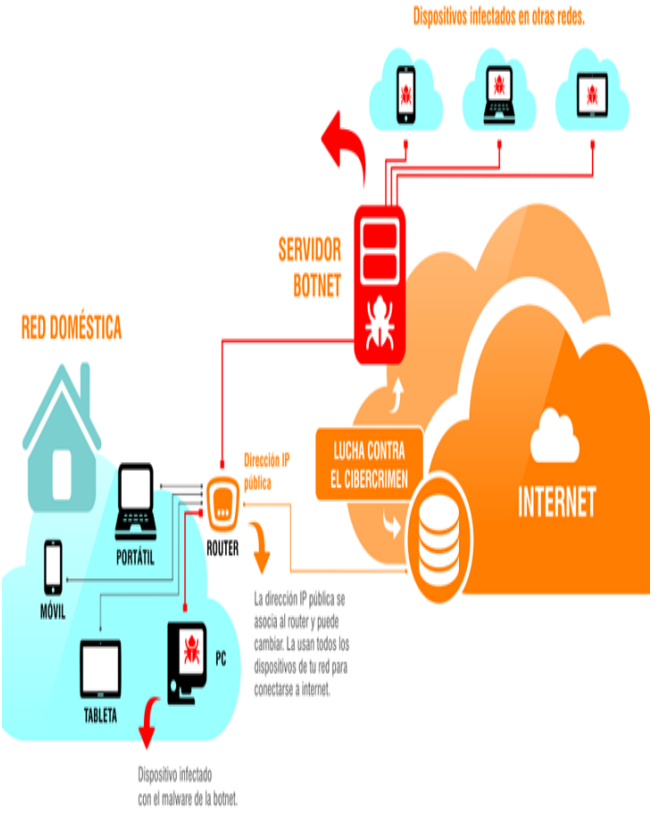
10. Los keyloggers realizan un seguimiento y registran cada tecla que se pulsa en una computadora, a menudo sin el permiso ni el conocimiento del usuario. (Choo, 2013)

11. ScreenLogger es una herramienta para aquellos que quieran llevar un registro de lo que pasa en la PC, por ejemplo, para aquellos padres que temen que sus hijos puedan estar en algo raro, para novios o novias celosos/as, o para alguna empresa que necesite llevar algún tipo de supervisión. (Broadhurst, 2014)

Estos, a veces llamados ataques man-in-the-browser[12], son esencialmente ataques man-in-the-middle[13] entre el usuario y los mecanismos de seguridad del navegador. Además de las credenciales bancarias, estos troyanos recopilan otra información. Por ejemplo, el servidor de comando y control para que el virus distribuye módulos que se inyectan en aplicaciones populares en la computadora infectada. Las aplicaciones incluyen el administrador de control de dispositivos, navegadores web, clientes ftp, clientes de correo electrónico, mensajería instantánea y programas del sistema. Después de la inyección, estos virus pueden inspeccionar todos los datos manejados por estos programas y pueden identificar y almacenar información interesante, como credenciales para cuentas en línea y contraseñas almacenadas. (Akhgar, 2014)

Una vez que los troyanos han interceptado información de interés, la suben a "sitios de colocación" como en el “Darkweb”. Por ejemplo, Zeus se pone en contacto con su servidor cada 20 minutos para cargar datos robados. Los troyanos de phishing y robo de credenciales están en el centro de muchas actividades criminales.

Figura 2. Arquitectura de un Ataque Informático



12. El ataque Man In The Browser (MITB) consiste en uno del tipo Man In The Middle (MITM) pero particularmente en el navegador web. La técnica consiste en situarse en medio de las comunicaciones para interceptarlas por lo que permite el robo de información e inyectar código malicioso para tomar control del equipo de la víctima. Una vez que sabe qué sitios son visitados por la víctima, puede duplicarlos para redirigir su visita a un sitio falso y robar sus credenciales. (Akhgar, 2014)

13. El ataque Man-in-the-Middle. Como sugiere su nombre en inglés, es cuando un intermediario (el cibercriminal o una herramienta maliciosa) entre la víctima y la fuente: una página de banca online o una cuenta de correo electrónico. (Akhgar, 2014)

Primero, para instalar sus troyanos en las computadoras, requieren herramientas de explotación, pagan programas afiliados o compran botnets a los pastores. También deben pagar a los ISP[14] y a los registradores de nombres de dominio para alojar servidores de comando y control de contactos y colocar ubicaciones. Los phishers también necesitan usar servicios de spam para publicitar sus sitios web fraudulentos. Finalmente, después de que se recopila información confidencial de usuarios desprevenidos, necesitan vender esta información o utilizar los servicios de mulas, cajeros o carders.[15]

2. Pasos Finales Del Negocio

Para monetizar la información confidencial recopilada por troyanos, keyloggers, campañas de phishing, los ciberdelincuentes requieren de la compra de esta información por carders, ladrones de identidad y otros estafadores profesionales. El robo de identidad se usa para cometer diferentes tipos de fraude. Hay distintas variaciones importantes del fraude financiero, que principalmente se distinguen en dos distintas modalidades:

1) El fraude de cuentas nuevas, que es cuando un impostor abre líneas de crédito utilizando la información personal de otra persona. Esto puede incluir nuevas cuentas de tarjeta de crédito, hipotecas o servicios públicos, como cuentas de teléfonos inalámbricos.

2) En la adquisición de cuentas, que es cuando un impostor hace usufructo de una de las cuentas existentes de la víctima. Por ejemplo, el impostor puede robar un número de tarjeta de crédito de la víctima y usarlo sin autorización.

El robo de identidad es un delito lucrativo y de bajo riesgo, pero requiere mucho trabajo cuando se realiza a gran escala. Los ladrones de pequeña escala pueden usar de manera oportunista la tarjeta de otra persona, o hacer cargos en sus propias cuentas y afirmar que fueron hechos por impostores. Las operaciones a gran escala requieren la cooperación de múltiples actores y cierta experiencia técnica. En fraudes de cuentas nuevas, el impostor intenta obtener líneas de crédito. Para comenzar este proceso de manera efectiva, el impostor debe obtener credenciales a nombre de las víctimas, organizar la entrega de correos para la recolección de tarjetas de crédito y obtener cuentas telefónicas para la activación de las tarjetas.

14. ISP, es un proveedor de servicio de internet suelen ser una empresa.

15. Es el nombre que se da al delito tecnológico en el que se involucran fraudes con tarjetas de crédito. Hablamos del uso ilegitimo, con ánimo de lucro, de las tarjetas de crédito de otra persona, un delito muy común dentro del binomio delincuencia-nuevas tecnologías. El objetivo del carder es hacerse con los datos numéricos de la tarjeta, incluido el de verificación. (BBC, 2019)

Los impostores pueden crear credenciales falsas u obtener credenciales reales de una autoridad estatal, pero ambas opciones son cada vez más difíciles de lograr, debido a los avances en la tecnología de credenciales y las medidas antifraude que han adoptado varios estados.

❖ COSTO SOCIAL DEL DELITO CIBERNÉTICO

A nivel nacional para planificar el nivel apropiado de recursos para combatir el cibercrimen, necesitamos una mejor comprensión de los costos del cibercrimen. Del mismo modo, para comprender los incentivos de los ciberdelincuentes, es igualmente importante investigar el producto de los ataques informáticos.

Para desarrollar un modelo económico de cibercrimen también necesitamos estimar la pérdida social neta de las víctimas y que nos cuesta implementar una estrategia de seguridad creando los estamentos de seguridad necesarios y preparados para combatir este flagelo. Que al mismo tiempo lleva ante la justicia casos bien investigados. Podemos obtener datos anecdóticos sobre algunas de las ganancias del delito cibernético de los casos donde se dieron enjuiciamientos. Sin embargo, como se menciona en otros artículos casi todos estos casos de alguna manera están conectados a esquemas más grandes de crimen organizado y de corrupción.

Si bien los casos de enjuiciamiento pueden darnos cierta verdad sobre diferentes actividades, no está claro cuán representativos de la economía clandestina son estos informes anecdóticos.

Porque después de todo, solo se informa una fracción de los delitos, y de los casos denunciados solo se investiga y se procesa una fracción. Para tener una mejor idea de la cantidad de dinero que ingresa a la economía subterránea, requerimos más información de las instituciones que son víctimas del cibercrimen.

Si bien la estimación de las ganancias de los delincuentes cibernéticos es diferente a la estimación de las pérdidas debidas al delito cibernético, solo una fracción de las pérdidas del delito cibernético se traduce en ganancias para los delincuentes cibernéticos; la parte restante de las pérdidas se distribuye entre recuperación, litigios, daños a la marca y muchos otros efectos colaterales; si exigimos a las instituciones financieras que informen las pérdidas directas del delito cibernético es posible que podamos estimar la entrada de efectivo que respalda la economía subterránea.

AVANCES IMPORTANTES EN LA TECNOLOGÍA QUE AMPLÍAN LOS RIESGOS ASOCIADOS AL DELITO CIBERNÉTICO

La evolución de la tecnología digital ha dado lugar a muchas aplicaciones nuevas, sin contar con las que ya observamos que son vulnerables al delito cibernético. Como consecuencia de estos avances, se considera importante que se discute algunos de estos y cómo han sido o podrían ser explotados con fines criminales, para luego entrar en la sección que describe el mercado de la Red Oscura que los alberga.

Telefonía Móvil

Aunque la telefonía móvil fue creada en pequeña escala hace décadas atrás, su uso hoy por hoy ha crecido dramáticamente en los últimos diez años. La primera red 3G del mundo se lanzó en Japón en 2001, y las redes europeas datan de 2003. La Unión Internacional de Telecomunicaciones (UIT) estima que había 6.800 millones de suscripciones de telefonía móvil a fines de 2012, el total se triplicó, desde 2005. Hoy en día, se conoce que un número creciente de países tiene más teléfonos que personas.

Al evolucionar desde simples comunicaciones de voz, los móviles ahora permiten la transmisión de texto, imágenes, música y combinaciones multimedia; Facilitan el acceso a Internet y la navegación por satélite. Sin embargo, a pesar de todos los beneficios de la telefonía móvil, en la última década el teléfono móvil se volvió instrumental en una variedad de actividades delictivas, desde la detonación remota de dispositivos explosivos hasta la transmisión de solicitudes fraudulentas y la distribución de imágenes ilícitas de niños.

Ahora es posible obtener el control remoto de un teléfono móvil y usarlo como dispositivo de escucha, o clonar su tarjeta SIM para usarla en delitos posteriores. La piratería telefónica para obtener acceso no autorizado a la data de voz se convirtió en un problema importante cuando en los últimos años se han dado casos de Corrupción a nivel nacional, muchos de estos casos han caído porque no contaron con la debida autorización legal, gastando incontables recursos financieros y perdiendo de vista elementos críticos para la presentación de evidencia no viciada a los tribunales de justicia de Panamá.

Un área de crecimiento reciente parece involucrar el uso de aplicaciones falsas o apps como se conocen en la jerga móvil. Se puede acceder a las aplicaciones móviles visitando

una "tienda" en línea (Skyba, 2019) , que es controlada por ciberdelincuentes que cargan malware al celular. Cuando las víctimas descargan las aplicaciones, las mismas son capaz de recopilar datos de cuenta bancaria e inicio de sesión, y explotar el móvil de la víctima para una mayor actividad criminal. (Curtis, 2018)

Conexión Inalámbrica A Internet (Wifi)

El advenimiento de la tecnología inalámbrica ha proporcionado una alternativa conveniente a las conexiones de cable, para computar no menos que para telefonía. A pesar de todos sus beneficios, la tecnología inalámbrica está creando nuevas oportunidades criminales. A menos que estén debidamente protegidos, las redes inalámbricas de área local (LANS) son vulnerables a la penetración. Hace una década, todo lo que se necesitaba para acceder a una red inalámbrica interna era una computadora, una tarjeta de red de área local inalámbrica y un software descargable desde la Web.

Hoy en día, estas tienden a ser aplicaciones estándar que se pueden comprar con la computadora de uno. El término "conducción de guerra" se ha acuñado para referirse al acto de localizar y registrar puntos de acceso inalámbrico o "puntos calientes" mientras está en movimiento. Las tarjetas de crédito válidas y otros datos personales se pueden cosechar a granel de la red no segura de los principales minoristas. A fines de 2003, se comenzó a ver procesamientos por acceso no autorizado a sistemas inalámbricos por parte de "hackers móviles". En noviembre de ese año, dos hombres en fueron acusados de piratear la red nacional de una tienda de mejoras para el hogar desde un automóvil estacionado afuera de una de las tiendas. (Anderson, 2013)

Las innovaciones en los sistemas de pago también han creado nuevas oportunidades criminales. Las comunicaciones de campo cercano y las tecnologías de identificación por radiofrecuencia (RFID) permiten el intercambio de datos entre dispositivos que están muy cerca unos de otros. Los sistemas de pago sin contacto basados en estas tecnologías pueden ser vulnerables al escaneo de personas cercanas. El desarrollo de carteras y protectores especiales para tarjetas de crédito ha reducido esta vulnerabilidad en cierta medida aun así se sigue dando con este delito.

Computación En La Nube

La computación en la nube es un término que se refiere al almacenamiento remoto de datos, sistemas operativos y servicios de aplicaciones,

que luego pueden ser compartidos por varias partes en virtud de acuerdos de arrendamiento múltiple. El concepto data de los primeros días de la informática, dominado como estaba por los mainframes; Los sistemas de correo electrónico en línea, entre los ejemplos más comunes, existen pues los que datan más de dos décadas. La popularidad de la computación en la nube en los últimos años se debe al importante ahorro de costos que se puede lograr mediante el intercambio de recursos y el ahorro de los costos de infraestructura. Aunque el origen del término se remonta a los ejecutivos de COMPAQ Computer en 1996, la computación en la nube y la arquitectura que describe se hicieron populares una década más tarde cuando Amazon la utilizó para referirse a archivos, software y poder de la computadora que eran accesibles a través de la web en lugar de estaciones de trabajo de escritorio individuales. (Broadhurst, 2014)

A pesar de las economías que aporta a la tarea, la computación en la nube no está exenta de vulnerabilidades. El intercambio de datos y aplicaciones puede ser apropiado en empresas colaborativas a gran escala. Sin embargo, cuando la seguridad de los datos es crítica, los datos almacenados en acuerdos de arrendamiento múltiple pueden ser vulnerables a la divulgación involuntaria o al acceso no autorizado intencional. Las nubes también se utilizan para alojar contenido ilícito, como malware, software pirateado y entretenimiento, y pornografía infantil. Como servicios de alojamiento aparentemente legítimos, se les puede otorgar cierto grado de confianza. (Broadhurst, 2014)

Protocolo De Internet De Voz (Voip)

VOIP es una tecnología que admite comunicaciones de voz a través de Internet, en lugar de una red telefónica pública. Después de un período de gestación de tres décadas, su uso generalizado comenzó en 2004 y ha aumentado desde entonces. El proveedor más destacado de servicios VOIP es Skype, que fue adquirido por Microsoft en 2012.

Su popularidad fue igualada por las preocupaciones de las fuerzas del orden público sobre lo que se consideraban dificultades para monitorear e interceptar actividades sospechosas de delitos. En algunas jurisdicciones, como los Emiratos Árabes Unidos, su uso está prohibido. Sin embargo, revelaciones recientes sugieren que los gobiernos son capaces de monitorear, almacenar y analizar el contenido de VOIP.

Redes Sociales

El intercambio de información en comunidades y redes virtuales se ha vuelto cada vez más popular. Se estima que Facebook, que se fundó en 2004 tiene más de 2 mil millones de miembros activos en 2018. Estos medios de recreación e interconexión personal han enriquecido la vida de muchos usuarios, pero también han creado oportunidades para la delincuencia, así lo ha señalado la Dirección de Investigaciones Judiciales de Panamá, que conversó de una cantidad importante de personas que venden drogas por medio de esta red y otras.

Otros temas importantes de las redes sociales es el hecho que, en muchas jurisdicciones se han opuesto a lo que consideran contenido ofensivo alojado en las páginas de los miembros, esto en Panamá ha dado con casos donde se señalan a personas extranjeras burlándose de panameños por su aspecto de raza e identificación étnica. Otro problema común a nivel empresarial e institucional es el mal uso que de los empleados que pasan tiempo durante la jornada laboral en redes sociales reduciendo la productividad y aumentando la vulnerabilidad al espionaje industrial.

El volumen de detalles personales contenidos en la página de Facebook y otras redes sociales de uno puede ser explotado por extorsionistas o posibles acosadores, incluso hasta por la misma red que vende los datos personales para nefastas campañas de manipulación de la población. Sin embargo, el riesgo aún más grave, es el robo de credenciales de una víctima y la publicación de información o imágenes despectivas de ellos.

El Internet De Las Cosas

Una ventana hacia el futuro puede revelar el desarrollo de lo que se ha denominado "el internet de las cosas". Con esto se entiende la interconexión de la mayoría, si no todos los objetos, a través del internet. Esto se ha denominado "web 3.0", "web semántica", "informática ubicua" e "informática generalizada": los términos son intercambiables.

Un ejemplo muy simplista implicaría la relación de un escáner de caja de supermercado con el sistema de control de inventario. El monitoreo en tiempo real de las ventas de un producto en particular informará a los sistemas para la entrega justo a tiempo del stock de reemplazo. Otra aplicación es la búsquedapredictiva, basada en el escaneo holístico de los correos electrónicos, el calendario de citas, las redes sociales y otras actividades digitales y los datos

de ubicación geográfica. Esto puede servir como base para las notificaciones automáticas al teléfono celular; imagine que se le avisará automáticamente cuando sea el momento de partir para una reserva de cena, según la ubicación, el modo de transporte y las condiciones del tráfico en tiempo real. Estas aplicaciones ahora están con nosotros y, en muchos aspectos, hacen que nuestras vidas sean más fáciles, más seguras, mejor informadas y, en general, más agradables.

La mala noticia es que estas tecnologías están disponibles para los delincuentes no menos que para nosotros, la gente honesta. Ya varios hackers han demostrado, la inmovilización remota de automóviles en la carretera, la desactivación de los sistemas de seguridad domésticos, comerciales, gubernamentales y la desactivación de dispositivos médicos.

Otra tendencia podría describirse como la continua democratización de la tecnología. A medida que avanzamos en la era digital, las personas ahora son capaces de hacer cosas que alguna vez estuvieron más allá de su capacidad. Por ejemplo, la continua miniaturización de los componentes electrónicos ha facilitado el desarrollo de "micro-satélites". Que pronto estarán disponibles para las personas, permitiéndoles descargar imágenes a pedido. Las aplicaciones potenciales de tales tecnologías a actividades delictivas son tan diversas que aglomeran delitos como el robo, la extorsión y el terrorismo. (Akhgar, 2014)

LOS VASTOS MERCADOS DELICTIVOS DE TOR Y LA WEB OSCURA

La red oscura es la parte del Internet a la que no se puede acceder con el uso de software convencional. Incluye sitios ocultos que terminan en onion o i2p u otros nombres de dominio de nivel superior que solo están disponibles a través de navegadores modificados como TOR o software especial. El acceso a los sitios i2p requiere un programa de enrutamiento especial. El acceso a dominios de nivel superior no convencionales a través de OpenNIC requiere que el usuario cambie las direcciones del servidor DNS en su enrutador. El acceso a los sitios onion requiere Tor, además, quienes administran sitios web oscuros que terminan en onion pueden ocultar sus identidades y ubicaciones a la mayoría de los usuarios de internet, sino a todos. (Brewster, 2017)

En la mayoría de los casos, un visitante a un sitio onion nunca sabrá la identidad del anfitrión, ni el anfitrión sabrá la identidad

del visitante. Esto es muy diferente de la corriente principal de Internet, donde los sitios a menudo están asociados con una empresa o ubicación, por ejemplo, google.com está asociado con la empresa con sede en Mountain View, California y los visitantes a menudo se identifican y se controlan a través de diversas tecnologías de seguimiento como cookies, registros de cuenta, cookies Flash, direcciones IP y geolocalización.

Estas explicaciones técnicas son necesarias ya que la historia básica que surge de toda esta evidencia es que un sistema de anonimato como Tor, como con otras tecnologías, es solo una herramienta que brinda acceso a un mundo de información y mercados tanto buenos como malos. Pero que al igual que el fuego, un martillo o un automóvil, la red Tor puede mejorar la vida y proporcionar los medios para desmejorarla. Lo que importa no es la explicación técnica de la tecnología, sino cómo se usa y cuál es el efecto neto.

Enmarcado desde esta perspectiva, el foco del debate público debería alejarse de demonizar la tecnología, más bien es importante que se vaya hacia la idea de que, como cualquier otro aspecto de la sociedad humana, la Red Oscura necesita ser vigilada.

Esta recomendación es particularmente relevante para los países democráticos, donde el lado oscuro del anonimato impone los costos más altos y los beneficios de Tor son menos pronunciados. Idealmente, la vigilancia debe llevarse a cabo dentro de límites claramente definidos y basados en reglas. Eso no es diferente al resto de la sociedad.

La vigilancia policial en línea, como lo demuestra el derribo de mercados ilegales como Silk Road y las redes de pedofilia infantil, es realmente posible, y es tan efectiva y conveniente como la policía fuera de línea. Un mayor movimiento en la dirección de la vigilancia policial en línea puede minimizar los costos socialmente perjudiciales de las tecnologías que otorgan el anonimato, al tiempo que permite los beneficios de tales sistemas. No es la solución ideal, pero es probable que sea lo mejor que se puede hacer.

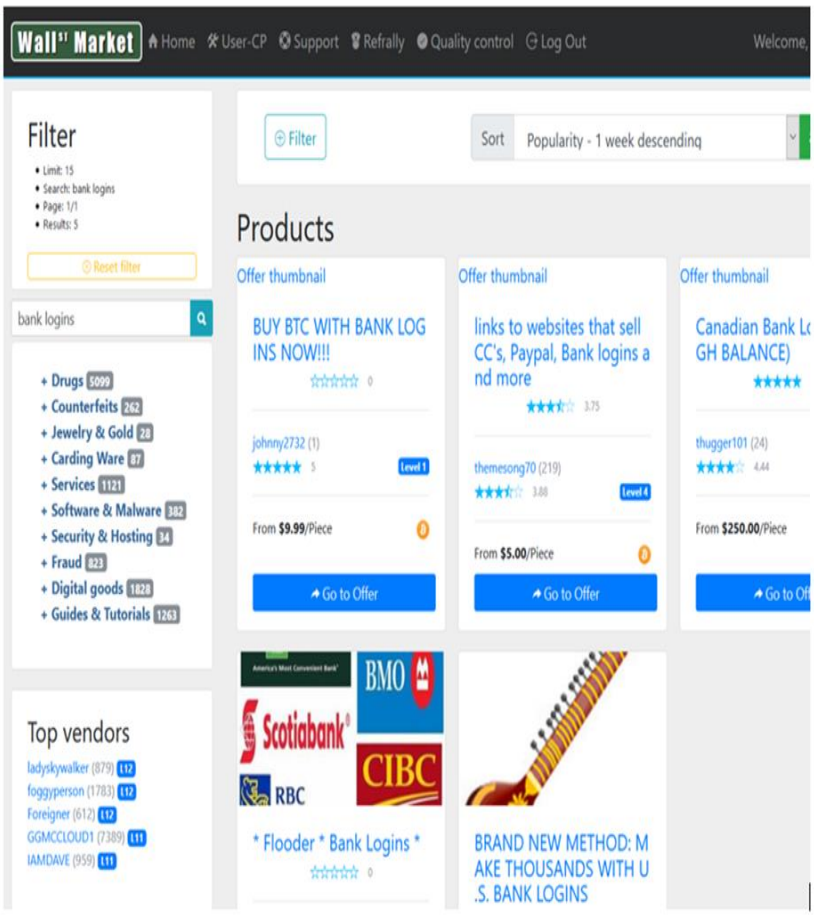
CAPTURA DE PANTALLA 1. VISTA DEL MOTOR DE BÚSQUEDA DE PAGINAS .ONION, HIDDENWIKI.NET

Fuente: (BBC, 2019)

Para conocer un poco más de la Red Oscura debemos estar claros que estos sitios web suelen ser más estrechos en el sentido que tienen menos contenido multimedia y de propaganda, muy parecido a los sitios web con el cual arrancó el internet hace años atrás, pero con un contenido mucho más profundo, en comparación con los sitios de superficie normales. Además, debido a que la mayoría de los materiales son contenidos protegidos, la calidad en general del contenido de la Web profunda suele ser mejor y más valiosa que la de la Web de Surface.

También se estima que más del 50 por ciento del contenido de Deep Web se encuentra en directorios de temas específicos (www.thehiddenwiki.net), lo que lo hace aún más accesible y relevante para las búsquedas específicas. Muy importante es el hecho que el medio de pago más comunes son las distintas criptomonedas como Bitcoin, Darkcoin o Peercoin para transacciones comerciales anónimas que se realizan dentro y en la mayoría de los mercados de la Red Oscura. Los hackers de alquiler y los mercados para tarjetas clonadas, dinero falso y otros servicios financieros también han acelerado el crecimiento.

CAPTURA DE PANTALLA 2. EJEMPLO DE MERCADO ILICITO EN LA RED OSCURA, WALL ST. MARKET



Fuente: (BBC, 2019)

Es decir que la mayoría de las transacciones no seguras que realizan las personas diariamente, donde fueron estafados o bien les robaron sus identidades, termina siendo vendido luego de una depuración de rastreo en la Red Oscura. Esta realidad lamentablemente deja a las autoridades solo con una idea de adonde ha quedado los rastros del delito.

A pesar de eso, debemos quedar conscientes de la necesidad de crear equipos que responden rápidamente ante la presencia de este delito, y que somos vulnerables.

Es importante que también las entidades bancarias y otros que comercializan a nivel nacional en el sector del comercio electrónico tengan, medidas de protección a los consumidores y que depuran personas que pueden ser sospechosos de vender información vital de las personas a terceros.

A continuación del articulo consideramos importante que se profundiza algo más sobre el uso de TOR y la Red Oscura para su debida vigilancia por las autoridades y otros interesados en conocer su funcionamiento.

CÓMO ACCEDER A LA WEB PROFUNDA Y RED OSCURA

Para explorar la Red Oscura se requiere de algunas herramientas y técnicas especiales. Algunos de ellos son similares o están estrechamente relacionados con los que usamos para explorar la web superficial. Dependiendo de los objetivos generales de uno, diferentes herramientas y técnicas ayudarán a alcanzar diferentes profundidades. Para la mayoría de los usuarios, generalmente hay dos enfoques diferentes pero relacionados para acceder a la Red Oscura:

- La Utilización de la Herramienta TOR en combinación con una red VPN
- La Utilización de un Motor de Búsqueda especial para navegar las páginas .onion

La manera más fácil y rápida de obtener acceso a la Red Oscura es utilizar motores de búsqueda alternativos especiales diseñados específicamente para ese propósito. Estos motores de búsqueda alternativos están diseñados para acceder a diferentes partes de la Red Oscura. Dado que estos sitios web no están indexados, no se encontrarán utilizando herramientas de búsqueda normales. (Gercke, 2014) Sin. embargo, sus URL se puede encontrar utilizando otros medios y, una vez que los sistemas de concesión de anonimato en línea, como TOR los verifica se permite a los usuarios acceder a la página.

REGULACIÓN DEL MERCADO ILICÍTO DE LA RED OSCURA MEDIANTE LA DIVULGACIÓN DE LOS PARTICIPANTES DE PAGOS POR CRIPTOMONEDA

A pesar que el uso de TOR y la Red Oscura, ofrecen en efecto la posibilidad de ser anónimo en línea la realidad, es que hay empresas que hacen posible discernir las identidades de los titulares de billeteras de Bitcoin mediante un proceso de divulgación de sus identidades en coordinación con estamentos de seguridad. Incluso existen varias empresas como **Chainanalysis**[16] que hacen este servicio para autoridades a nivel mundial, cuando sospechan de actividad criminal. Posteriormente discutiremos estrategias que esbozan de esta realidad en otra sección.

16. Chainalysis, con sede en Nueva York, es una empresa que se dedica a la lucha del delito en la Red Oscura, identificando conductas delictivas, como el robo de criptomonedas (como en el caso de Mt Gox) y las compras de drogas en el mercado negro (por ejemplo, en el mercado de Silk Road, ahora cerrado). (Chainanalysis, 2018)

Es importante saber que el Bitcoin está bajo vigilancia y ya científicos de la computación tienen como asociar actividades criminales con el uso de la billetera Bitcoin. Incluso es posible identificar geográficamente al usuario. Pero esto es un proceso que puede llevar tiempo y requiere de recursos para estar en constante vigilancia de la actividad criminal en la Red Oscura.

Sin embargo, nuevas criptomonedas como Monero utilizan una técnica llamada Firma de Anillo que hacen que los registros de transacciones sean altamente resistentes a la divulgación. En la criptografía, una firma de anillo es un tipo de firma digital ejecutada por cualquier miembro de un conjunto de usuarios, cada uno de los cuales tienen claves. En una firma de anillo, es matemáticamente imposible determinar qué clave se usó para crear la firma. No hay forma de desenmascarar el anonimato de una firma. De esta manera, Monero presenta así un Blockchain opaca y más difícil de rastrear. (Choo, 2013)

Ciertamente las criptomonedas como Bitcoin y Monero son las razones por la que la Red Oscura ha dado un gran impulso. Esto es evidente por la proliferación de más sitios de mercado ilícito como Silk Road y otros que reposan en la Red Oscura. Ciertamente es muy importante implementar medidas para vigilar estas actividades, ya que, según informes de la Organización Mundial de Comercio, están divulgando documentos que urgen el impulso del uso de Blockchain, la tecnología que respalda las criptomonedas como el futuro de los negocios internacionales. Podemos observar cuando citan textualmente lo siguiente:

“Blockchain es visto como un posible cambio de juego para digitalizar y automatizar procesos de financiación del comercio, en particular cartas de crédito, y para facilitar la financiación de la cadena de suministro. Las características intrínsecas de la tecnología también la convierten en una herramienta potencialmente interesante para ayudar a implementar el Acuerdo de Facilitación del Comercio (TFA) de la OMC y para facilitar los procesos de empresa a gobierno (B2G) y de gobierno a gobierno (G2G) a nivel nacional. Blockchain y los contratos inteligentes podrían ayudar a administrar los procedimientos fronterizos y las ventanas únicas nacionales (un único punto de entrada a través del cual las partes interesadas en el comercio pueden presentar documentación y otra información para completar los procedimientos aduaneros) de una manera más eficiente, transparente y segura, y mejorar la precisión del comercio

datos. El verdadero desafío será hacer que los procesos G2G transfronterizos sean más eficientes. Esto no solo requerirá resolver los problemas de interoperabilidad a nivel técnico, un problema en el que la comunidad Blockchain está trabajando activamente, sino que también requerirá estandarización y voluntad política para crear un marco regulatorio que conduzca al comercio sin papel." (World Trade Organization, 2019)

Dicho plenamente, la Organización Mundial del Comercio ve en Blockchain el futuro de las transacciones comerciales, de manera que Panamá debe mirar su regulación cuanto antes sea posible, incluso hasta considerar la creación de un ente regulador como una superintendencia.

EL IMPACTO NACIONAL DEL DELITO CIBERNÉTICO E IMPLICACIONES A LAS FUTURAS POLITICAS PÚBLICAS

Definir el impacto en Panamá del Delito Cibernético es una tarea que hoy por hoy se debe considerar por realizar por varios aspectos. Primeramente, está el hecho que no todos los delitos están tipificados en el Código Penal, y mucho menos existen capacidades dentro de los estamentos de seguridad para darle un seguimiento oportuno al mundo de Delitos que se dan.

hasta en la Web Superficial, muy pocos de estos casos llegan a la conciencia nacional porque la población en su mayoría desconoce de las distintas modalidades en que los ciberdelincuentes operan y logran apoderarse de sus identidades y bienes

De hecho, muy poco se ha reportado por parte de las empresas de la existencia de esta modalidad de delincuencia en línea porque muchas de ellas por pena o por no decepcionar a sus clientes prefieren asumir la perdida y tomar medidas posteriormente.

Si Panamá quiere primero conocer el alcance de sus problemas, puede tomar iniciativas como realizar una Encuestas a Negocios y a Personas para establecer una línea base de conocimiento de lo que está sucediendo. Después de analizar y confirmar que existen una red enorme de personas dedicada a negocios ilegales por medio del internet, habrá que crear su debida vigilancia por parte de algún estamento de seguridad o bien una organización que puede reproducir información oportuna sobre el mismo.

Lo cierto es que el futuro va traer un mundo de nuevas oportunidades para delinquir que pueden ser indetectables, ya que existe el software disponible para explotar, existe un mercado anónimo para contactar clientes y vendedores; y además existe como hacer pagos de estos servicios de manera anónima en línea.

BIBLIOGRAFÍA

1. Anderson, Ross, Chris Barton, Rainer Böhme, Richard Clayton, Michel J. G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. “Measuring the Cost of Cybercrime”, in Rainer Boehme (ed), The Economics of Information Security and Privacy, Springer-Verlag, Berlin, 2013.

2. Abeslamidze, Sofiko. “North American Bitcoin Conference Stops Accepting Bitcoin for Tickets”. Coinspeaker, 11 January 2018.

3. McCarthy, Daniel and Fader, Peter and Hardie, Bruce, Valuing Subscription-Based Businesses Using Publicly Disclosed Customer Data. October 9, 2016

4. Gregory, Gary, Munib Karavdic, and Shaoming Zou. 2007. The Effects of E-Commerce Drivers on Export Marketing Strategy. Journal of International Marketing, Vol. 15, No. 2: 30-57.

5. Bissel, Kelly, La Salle, Ryan. Ninth Annual Study on the Cost of Cybercrime, Accenture Security, MI, 2019.

6. Statista, In Depth: B2B e-commerce Report 2019, https://www.statista.com/study/44442/statista-report-b2b-e-commerce/

7. Akhgar, Babak, Andrew Staniforth and Francesca Bosco. Cyber Crime and Cyber Terrorism Investigator’s Handbook, Syngress, Waltham, 2014.

8. Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab and Steve Chon. “Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime”, International Journal of Cyber Criminology 8 (1),2014.

9. Choo, Kim-Kwang Raymond and Peter Grabosky. “Cybercrime” in Letizia Paoli. Oxford Handbook of Organised Crime. New York: Oxford UP, 2013.

10. Gercke, Marco. Understanding Cybercrime: Phenomena, challenges and legal response, ITU Publication, 2014.

11. Skyba, Mike (2013) “Fake Android Apps” http://au.norton.com/fake-android-apps/article (accessed 6 September)

12. Curtis, Sophie (2013) “Banking malware and fraudulent dating apps drive surge in mobile threats” The Telegraph, 21 August http://www.telegraph.co.uk/technology/internet-security/10257371/Bankingmalware-and-fraudulent-dating-apps-drive-surge-in-mobile-threats.html (accessed 6 September 2013).

13. Brewster (eds), Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities. Cham: Springer,2016

14. Chainanalysis, “The Changing Nature of Cryptocrime,” Report, January 2018.

15. World Trade Organization, Can Blockchain Revolutionize International Trade?, WTO Press, 2018

LA CIBERDELINCUENCIA Y LA CULTURA DEL MIEDO

Resumen

La sociedad esta atemorizada por causa del ciberdelincuente que, aunque no ataque a sus víctimas de manera directa, ni atente contra su vida e integridad física con objetos contundente, armas punzo cortantes o armas de fuego y aunque la víctima no lo vea frente a frente y aunque, estadísticamente y demográficamente sean menos que las realizadas por el delincuente común, éste delincuente viene causando más miedo en la sociedad. Sus ataques son pocos, pero certeros y peligrosos ya que, al atentar contra el Estado, ponen en riesgo a la población la cual se siente con temor de sufrir algún ataque terrorista. Se teme salir a lugares públicos por temor de que en estos puedan haber puesto artefactos explosivos que no necesariamente necesitan de personas para crear las bombas humanas ya que estas pueden ser manipuladas a control o a través de la utilización de drones.

La delincuencia y los delincuentes se han venido transformando. Ahora no solo la sociedad vive el miedo producido por la delincuencia común. Ahora también estamos viviendo en una sociedad cuyo miedo está siendo producido por un delincuente cuyo mecanismo de acción es dado por el manejo técnico que brinda el internet y que se conoce como ciber delincuente. Este no mantiene una relación de contacto físico con su víctima y ésta, la víctima no es cualquiera persona. Son empresarios, comerciantes, profesionales. La ciberdelincuencia o el cibercrimen ha venido afectando en mayor escala a aquella clase que, aunque no sean ricos ni millonarios, tienen acceso a un medio informático, ya sean celulares, tabletas o computadoras a través de las cuales han descargados informaciones personales que han utilizados esos ciberdelincuentes para presentárselos en su contra, jaqueando cuentas bancarias, robando identidad, chantajeando, bajando fotos de niños, niñas y adolescentes que los mismos familiares colocan en internet para alterarlas y y explotarlas sexualmente.

La idea de empresas integradas verticalmente dio paso, por lo tanto, a la metáfora de “redes”, que proporcionaban una base para el pensamiento contemporáneo sobre las relaciones tanto dentro de los grupos delictivos organizados como en grupos de individuos. Las definiciones

tradicionales de la delincuencia organizada se han basado en el ánimo de lucro. Sin embargo, incluso la mayoría de los observadores de la delincuencia organizada tradicional señalan el atractivo intrínseco de la emoción, el compañerismo y otros valores no materiales.
Actualmente, hay muchas organizaciones criminales (como las especializadas en el fraude y el robo de vehículos) que no practican la violencia, ni el soborno. Por otra parte, una gran cantidad de actividades de la delincuencia organizada en Internet está impulsada principalmente por consideraciones no monetarias, como la búsqueda de desafío intelectual, notoriedad individual o del grupo, la lujuria (en el caso de la actividad pedófila organizada), la ideología, la rebelión y la curiosidad.

INTRODUCCIÓN

Durante el desarrollo de la sociedad se han venido dando diversas formas de delinquir y con ésta, diversos tipos de delincuentes. En este artículo analizamos un nuevo delito, la ciberdelincuencia y, por efecto, un nuevo delincuente, el ciberdelincuentes. Una de las cosas que siempre hay que tomar en cuenta es que, desde el inicio de la vida del hombre en sociedad, ha habido delito, en diversas formas o manifestaciones y, con los mismos, también se han utilizados diversos medios o mecanismos para su ejecución. En esta nueva versión del crimen, veremos el surgimiento de un delito facilitado por las nuevas tecnologías de la información y la comunicación y de un delincuente sumamente inteligente que hace uso de esta tecnología para cometer sus actos delictivos.

Hoy día, la sociedad cuenta con el mayor desarrollo tecnológico inventado por la industria de la tecnología de la información y la comunicación llamado Internet que consiste en un conjunto descentralizado de redes de comunicación interconectadas que utilizan una serie de protocolos que garantizan que estas redes funcionen de una forma lógica con un alcance a nivel mundial"[1].

La delincuencia ha sido durante toda la existencia de la humanidad un flagelo que ha traído consigo, no solo las pérdidas de valores materiales, sino que también ha engendrado el miedo. Un miedo que se ha venido enraizando dentro de la sociedad y que se ha puesto tan normal que ha creado una nueva cultura, la cultura del miedo.

1. Recuperado de: Red de computadoras – EcuRedhttps://www.ecured.cu › Red_de_computadoras. Recuperado El 6 de noviembre 2019 A Las 11:13 A.M.

En épocas pasadas cuando se hablaba de temor, se consideraba al individuo como un loco, una persona anormal ya que las fuentes de su miedo provenían más de lo imaginario que de la realidad. La delincuencia eran formas de conductas antisociales realizadas mayormente por individuos pobres, las gentes necesitadas que no veían otra alternativa que la de robar o hurtar para poder comer y esta forma de comportamiento también generaba un miedo a las clases sociales ricas, pero no por la pérdida de su vida o de su integridad física, sino más bien por la pérdida de sus bienes materiales.

En este artículo expondremos como a través del desarrollo tecnológico por el que ha pasado la sociedad se han dado nuevas formas de delinquir y nuevos tipos de delincuentes, en este caso, los llamados delitos cibernéticos ejecutados por los que llamamos ciberdelincuentes y cómo estos han venido propiciando dentro de la sociedad una nueva cultura del miedo que, a diferencia del miedo generado por la delincuencia común, éste se agranda más por la facilidad con que vieja la noticia y el número de personas que las reciben. Constituyendo redes con las cuales mantienen un contacto a través del ciberespacio conformando grupos de interés o alternando de manera solicitaria con pares que no encuentran un lugar de pertenencia y comparten gustos, preocupaciones y que se ayudan mutuamente.

Igualmente presentamos algunos planteamientos de investigadores del comportamiento cibercriminológico de estos llamados delincuentes cibernético, al igual que de gobiernos que se valen de esta herramienta, el internet, para la realización de sus acciones delictivas, denominadas cibercrimen, así como para, de parte de los gobiernos, generar dudas en la sociedad valiéndose de los medios de información para generar noticias que provoque algún grado de inestabilidad social y genere descontentos y desconfianza en contra de adversarios políticos acusando a los mismo de ser causantes de daños producidos a la economía que ha traído como resultado el encarecimiento de los servicios o desabastecimiento de los productos por medio de los cuales se produce el caos que ellos con sus acciones a favor del pueblo resolverán.

I. DE LA DELINCUENCIA COMÚN AL CIBERDELITO

Una de las cosas que hay que tomar en cuenta es que, desde el inicio de la vida del hombre en sociedad, han existido diversas manifestaciones

de conductas antisociales que debido al daño que ocasionaban a la vida y a la integridad personal, al igual que a los bienes materiales del individuo y por los medios empleados para su ejecución, se fueron tipificando estas conductas antisociales en conductas delictivas a las cuales se les añadió una pena que debían ser cumplidas en un lugar predestinado que, a través de los tiempos, se ha venido identificando con muchos nombre entre los conocidos podemos mencionar; mazmorra, calabozo, galera, prisión, presidio, cárcel, celda, correccional y penitenciaría, entre otros.

A los individuos que cometían estas acciones delictivas se les tipificó como delincuentes de acuerdo a los tipos de actividad delictivas y la regularidad con que cometían. Entre estas clasificaciones mencionaremos las del doctor Constantino Bernaldo De Quirós[2], que realiza una clasificación de acuerdo a los grandes fundadores de la criminología comenzando con Lombroso quien clasifica al delincuente en criminales y criminaloides. Continua con Ferri quien los clasificas como locos, natos, habituales, pasionales y ocasionales y, por último, para nuestro interés tomaremos la clasificación de Garofalo en cuatro grandes tipos de delincuentes, los delincuentes privados de sentimientos de piedad, los delincuentes privados de sentimientos de probidad, los delincuentes privados de sentimientos de piedad y probidad y los delincuentes cínicos.

De acuerdo a la investigación realizada por el Mayor El Mayor RODRIGO CHAPARRO FIGUEREDO[3] en su investigación sobre la Delincuencia Común y su Incidencia en la Sociedad Colombia según la opinión de los entrevistados se llegó a la conclusión de que la mayoría de la población deduce que la delincuencia Común se debe a factores como la pobreza, el desempleo, la falta de educación y por otras circunstancias inherentes al conflicto interno que vive el país y que, de una u otra manera critican al estado por no subsanar estos problemas y por no disminuir los delitos más comunes.

Con el tiempo, de acuerdo a los estudios realizado por el Ingeniero Fernando Villarán sobre “Las causas de la delincuencia común”, establece que los factores considerados causantes de la delincuencia según Bernaldo De Quirós, se han ido decantando en siete variables

2. Doctor CANSTANTINO BERNALDO DE QUIROS, LA CLASIFICACIÓN DE LOS DELINCUENTES, Biblioteca Jurídica Virtual del Institutro de Ivestigaciones Jurídica de la UNAM. TOMADO de www.jurídicas.unam.mx ,BAJADO EL 25 DE NOVIEMBRE DE 2019, A LAS 3:11P.M.

3. MY. RODRIGO CHAPARRO FIGUEREDO, La Delincuencia Común y su Incidencia en la Sociedad de Colombia, Ensayo: Artículo de Reflexión. Universidad Militar Nueva Granada, Facultad de Relaciones Internacionales. Bogotá, D.C. MYO DE 2013)

como las más asociadas a estos dos fenómenos y que ofrecen las mayores explicaciones como los son: desigualdad, pobreza, desempleo, educación, represión, penas, y cohesión social[4].

Desde estas perspectivas la delincuencia común podría ser ejecutada por cualquier persona independientemente de su situación social o estatus económico, cualquiera podrá cometer delitos tipificados dentro de los delitos contra la propiedad, delitos contra la vida y la integridad personal, entre otros y es lo que se ha identificado como la delincuencia común. Con este tipo de delincuencia en la sociedad se empieza a formar el temor no sólo por el hecho el hecho de perder sus bienes, sino también la posibilidad de ser golpeado, maltratado, herido y hasta de perder la vida por las formas violentas y agresivas con que son realizados estos delitos al igual que por los diversos medios empleados para su ejecución, siendo unos de los temido la utilización de objetos contundes, punzo cortantes o con armas de fuego. Entre otros mecanismos utilizados para comisión de otros delitos comunes, en estos casos, los relacionados con las lesiones personales y abusos sexuales podemos mencionar la amenaza e intimidación acompañada de la fuerza física y con los ya mencionados objetos contundes, armas punzocortantes, armas de fuego, etc.

Dentro de todos estos recorridos relacionados con el surgimiento de la delincuencia común y el temor o el miedo que la misma tiene sumergida a la sociedad, surge una nueva forma de delinquir y un nuevo delincuente que dentro del mundo moderno son llamados ciberdelincuencia y ciberdelincuentes. Ahora con estos no existe el temor de ser violentado en su integridad física o en la perdida de la vida, con estas nuevas formas de ciber crimen, surge un nuevo miedo, un temor que es ocasionado por un individuo o grupos de individuos que viven ocultos en el anonimato y que se pueden encontrar en cualquier parte del mundo.

II. LOS ORIGENES CONCEPTUALES DE LA CIBERDELINCUENCIA

La delincuencia cibernética es un tema preocupante que inquieta por igual a la industria y a los gobiernos al igual que a la sociedad en general y que hoy día tiene acceso a todas las nuevas tecnologías de la información y comunicación que con el transcurrir de los años, los delincuentes cibernéticos han venido utilizando no solo para cometer delitos que

4. Fernando Villarán, Ingeniero Las causas de la delincuencia común. Bajado de, https://rpp.pe/columnistas/fernandogonzalovillarandelapuente/las-causas-de-la-delincuencia-comun-noticia-1205627 Referido el 25 de noviembre de 2019 a las 2:07p.m.

que podrían ser considerados comunes como las estafas, sino que también han servido para crear el terror en la sociedad.

Lo que en un pasado se inició como un juego, como bromas para desquite, se convirtiendo en acciones de maldad y ahora, ya no solo es la comisión de bromas, desquites o maldades, ahora el ciberdelito se fue enfocando hacia el espionajes industriales, las violaciones de seguridad protocolos de nacional y bancaria, el robo de identidades, jaqueo de cuentas bancarias, de archivos personales, en fin, ahora están siendo utilizada para la siembra del miedo ciudadano en las luchas políticas y religiosas que llevan en algunos países, grupos rebeldes que han sido identificados como terrorista, han exportado ese terror a otras latitudes fuera de su territorio.

La sociedad esta atemorizada por causa del ciberdelincuentes que, aunque no ataque a sus víctimas de manera directa, ni atente contra su vida e integridad física con objetos contundente, armas punzo cortantes o armas de fuego y aunque la víctima no lo vea frente a frente y aunque, estadísticamente y demográficamente sean menos que las realizadas por el delincuente común, éste delincuente viene causando más miedo en la sociedad. Sus ataques son pocos, pero certeros y peligrosos ya que, al atentar contra el Estado, ponen en riesgo a la población la cual se siente con temor de sufrir algún ataque terrorista. Se teme salir a lugares públicos por temor de que en estos puedan haber puesto artefactos explosivos que no necesariamente necesitan de personas para crear las bombas humanas ya que estas pueden ser manipuladas a control o a través de la utilización de drones.

Pero el MIEDO no solo se ha enfocado desde el aspecto político ya que han surgido otros tipos de delincuentes cibernéticos que han venido utilizando estas tecnologías para el desarrollo de otros tipos de delitos cibernéticos que igualmente están sembrando el miedo en la sociedad ya que se trata de violentar la integridad física, económica y familiar enviando amenazas, o imágenes con las cuales realizan chantajes y extorciones. En estos días, aunque no sean cifras significativas que se comparen, en cuanto al número, con los delitos comunes, se han venido proliferando los delitos de robo de identidad, extorsión, hakeos a cuentas bancarias y la explotación sexual comercial de niños, niñas, jóvenes adolescentes y adultos, por organizaciones criminales que han hecho de estos delitos cibernéticos acciones muy lucrativas.

La delincuencia y los delincuentes se han venido transformando. Ahora no solo la sociedad vive

el miedo producido por la delincuencia común. Ahora también estamos viviendo en una sociedad cuyo miedo está siendo producido por un delincuente cuyo mecanismo de acción es dado por el manejo técnico que brinda el internet y que se conoce como ciber delincuente. Este no mantiene una relación de contacto físico con su víctima y ésta, la víctima no es cualquiera persona. Son empresarios, comerciantes, profesionales.

La ciberdelincuencia o el cibercrimen ha venido afectando en mayor escala a aquella clase que, aunque no sean ricos ni millonarios, tienen acceso a un medio informático, ya sean celulares, tabletas o computadoras a través de las cuales han descargados informaciones personales que han utilizados esos ciberdelincuentes para presentárselos en su contra, jaqueando cuentas bancarias, robando identidad, chantajeando, bajando fotos de niños, niñas y adolescentes que los mismos familiares colocan en internet para alterarlas y explotarlas sexualmente.

III. CULTURA DEL MIEDO

El desarrollo de la ciberdelincuencia ha traído también un desarrollo de una nueva cultura denominada “cultura del miedo” generada por la tecnología de la información y la comunicación en donde ahora hay que tener cuidado no solo en lo que se hace sino también en dar información sobre datos personales o familiares. Al igual que la tecnología de la información y la comunicación han contribuido a mejorar las diversas relaciones sociales que se manifiestan dentro de un conglomerado social, también han servido para que éste mismo conglomerado social empiece a desarrollar una cultura del miedo por todo los delitos y acciones cibernéticas que los ciberdelincuentes han venido realizando, ya sea actuando de manera individual o conformando grupos de crimen organizado.

Vale la pena preguntarnos ¿Qué es el miedo? Según la Real Academia de la Lengua Española, el miedo es “la angustia por un hecho real o imaginario”[5]. En realidad, en la actualidad podríamos expresar, que el miedo es un sentimiento o una percepción subjetiva que depende de muchos factores y evidentemente de las vivencias de cada individuo. El miedo es una

5. La cultura del miedo y la inseguridad artificial en nuestra Sociedad. Publicado el 30 abril, 2017 por Daniel Saavedra. BAJADO DE https://www.iniseg.es/blog/seguridad/la-cultura-del-miedo-y-lainseguridad-artificial-en-nuestra-sociedad/ RECUPERADO EL 30 DE OCTUBRE DE 2019 A LAS 02:36 P.M.

sensación de angustia provocada por la presencia de un peligro real o imaginario[6] como el miedo a la oscuridad, el miedo a los espacios abiertos o cerrados, el miedo a las alturas, también el miedo lo definen como un sentimiento de desconfianza que impulsa a creer que ocurrirá un hecho contrario a lo que se desea, como el miedo a que algo salga mal (una fiesta, la presentación de un examen, un discurso en público, etc.) Identificado con estas acciones, el miedo es una persección común de miedo y ansiedad que puede afectar la manera de interacción de las personas.

El miedo es un sentimiento que siempre ha estado acompañando al hombre, desde sus inicios y gracias a este miedo, se han logrado alcanzar logros impensados y dentro de esos logros alcanzados, podemos mencionar todas las revoluciones que durante el desarrollo de la sociedad se han venido dando, cambiando las formas de vida del individuo desde la revolución agrícola, en donde el hombre, deja la recolección y el nomadismo para convertirse en un ser sedentario empieza a la producción de su comida, manteniendo la caza como una de sus actividades. Este sedentarismo les sirvió para vivir en comunidad y juntos ´poder protegerse de los embates de los animales salvajes, así como de los eventos naturales que no tenían explicaciones, así como de los mismos hombres que se disputaban entre ellos dominios territoriales y las mujeres y las cosechas obtenidas de la agricultura.

Seguida por las diversas revoluciones industriales en donde gracias a las nuevas formas de producción generadas por las fábricas se da un salto del campo a la industria, el abandono del campo por el hombre que emigra a las nuevas formas de organización social llamadas las ciudades industriales y con esta un mayor desarrollo de la criminalidad y nuevos tipos de delincuentes, hasta llegar a la revolución tecnológica industrial y de la comunicación.

Esta conducta hizo del hombre el peor enemigo del hombre y ser el sujeto de la humanidad que inspiró mayor temor a su propia especie. El hombre ha logrado, gracias al desarrollo industrial vencer el miedo a los animales y a hasta a las fuerzas sobrenaturales, pero no así al hombre. De los animales se han inventado tantas armas que ha generado en su destrucción masiva que hoy día se han creado organismos y legislatura para la protección de los mismo. De las fuerzas naturales, se han inventariado artefactos que miden el desarrollo de estos actos los cuales se han enviado al espacio por sus

6. BAJADO DE https://www.wordreference.com definición › miedo miedo - Definición - WordReference.com RECUPERADO EL 7 DE NOVIEMBRE DE 2019 A LAS 3:26P.M..

pronósticos y prepararse ante cualquier eventualidad. Pero en cuan to al hombre, su dominio y control ha sido, hasta estos días, más que imposible.

En su afán de poder, el hombre inicio conquista de territorios y dominio de otros hombres al grado de convertirlos en esclavos. Pero para lograr esto, tuvo que inventar nuevas armas de destrucción con las cuales infringiera miedo y temor. El desarrollo tecnológico ha traído consigo el desarrollo de las armas de destrucción para el mismo las cuales se han venido utilizando para las diversas guerras que han surgidos a través de la historia de la humanidad. Generando un temor en la sociedad de que con esas armas se llegue la destrucción de la humanidad.

En el campo de la criminalidad, el miedo también se ha venido transformando. Todos tenemos miedo a ser criminalizado, más en estos tiempos en donde la conducta criminal del delincuente común se ha tornado violenta y los del crimen organizado, en asesina. Si se tiene la mala suerte de ser asaltado por un delincuente común que podría ser un drogadicto o un individuo que sufre de alguna adicción y sus delitos lo realizan para obtener un dinero con los cuales pueda poder sufragar sus vicios y si la persona victimizada no cuenta con dinero son capaz de agredirla como producto de un enojo y frustración al no conseguir el dinero y de la ansiedad provocada por el deseo del consumo de la cosa producto de su adicción.

El crimen organizado por su parte también ha venido ´provocando miedo en la sociedad creando un sentimiento de desconfianza de salir a divertirse o pasear con su familia, o de ni siquiera salir de su casa o al balcón de su casa por las muertes que se han venido dando por los llamados ajustes de cuentas en donde los ahora sicarios que encuentran en panamá, no les importan a cuantas personas o las personas puedan matar siempre y cuando logren su objetivo de matar a su víctima.

IV. LA CULTURA DEL MIEDO INSTITUCIONALIZADA

El miedo también se ha venido institucionalizado, los gobiernos, con el fin de mantener unos lineamientos políticos, o ir en contra de un adversario político o proyectar unas medidas económicas, se hacen de los medios de información y comunicación para difundir noticias engañosas que vayan conduciendo a la sociedad hacia la adopción de pensamientos temerosos con la finalidad de estas acepten cono necesarias las medidas que se hayan a emplear. Igual acción realizan los adversarios políticos,

difundiendo noticias contrarias a las posiciones gubernamentales con la finalidad de que la sociedad pierda credibilidad en las medidas establecidas por el gobierno como necesaria.

“Entre los que tienden a argumentar que la cultura del miedo está siendo intencionadamente elaborada por el gobierno con la finalidad de mantener a la sociedad engañada y temerosa, podrían mencionarse al lingüista Noam Chomsky, al sociólogo Barry Glassner, a cineastas políticos tales como Adam Curtis y Michael Moore o reporteros como Judith Miller. Los motivos expuestos para tal plan premeditado de alarmismo varían, pero dependen del potencial incrementado de control social, que una población desconfiada y recíprocamente atemorizada, puede ofrecer a aquellos en el poder.

En estos términos, los miedos son cuidadosos y repetidamente creados y alimentados por cualquiera que desee infundir temor, frecuentemente a través de la manipulación de palabras, hechos, noticias, fuentes o información, a fin de inducir ciertos comportamientos personales, justificar acciones o políticas gubernamentales (en el país o el extranjero), mantener a la gente consumiendo, elegir políticos demagogos o distraer la atención pública de supuestas problemáticas sociales más urgentes como la pobreza, la seguridad social, el desempleo, el crimen o la contaminación. Dichos comentaristas sugieren que existe una escala de procesos culturales que pueden considerarse como "técnicas" deliberadas para alarmar” .[7]

“Al otro extremo del rango, una cultura del miedo es planteada como una susceptibilidad que surge de cada rincón de la sociedad contemporánea, de forma natural. Frank Furedi, profesor de sociología en la Universidad de Kent (Gran Bretaña), quien también fundó el Partido Comunista Revolucionario, ejemplifica este margen del rango con sus libros, Culture of Fear: Risk-taking and the Morality of Low Expectations (1997).(Cultura del miedo: toma de riesgos y la moralidad de las bajas expectativas). y Politics of Fear: Beyond Left and Right (2005) (Política del miedo: más allá de la izquierda y la derecha). Furedi sitúa el origen del fenómeno en lo que él caracteriza como una 'falla de la imaginación histórica', un síntoma que identifica como la extenuación de los sistemas de significado político del siglo XX.

“Fue mi experiencia del pánico a la píldora anticonceptiva de 1995 que me motivó a escribir Culture of Fear. Llevé a cabo un estudio global

7. BAJADO DE https://es.wikipedia.org/wiki/Cultura_del_miedo Recuperado el 28 de octubre de 2019 a las 10:25 a.m.

de reacciones nacionales del pánico, y rápidamente caí en la cuenta de que las respuestas diferenciales fueron culturalmente instruidas. Algunas sociedades, como la británica y la alemana, reaccionaron de una manera confusa, a modo de pavor - mientras que países como Francia, Bélgica y Hong Kong, adoptaron un enfoque más mesurado”. **8**

“Desde el punto de vista de Furedi, una percepción universal de horror pre-existe y apuntala las expresiones de alarma de los medios de comunicación y los políticos. Mientras los medios y los gobernantes pueden amplificar y sacar provecho de esta sensibilidad, sus actividades no son decisivas en su producción cultural. Furedi nivela la carga en varias voces 'anti institucionales' o 'liberales', afirmando que ellos son al menos cómplices en la explotación de ansiedades como la 'implantación' (de catástrofes ecológicas, por ejemplo), que es el asimiento más comúnmente benéfico a partir de la cultura del miedo” . **9**

8. BAJADO DE https://es.wikipedia.org/wiki/Cultura_del_miedo Recuperado el 28 de octubre de 2019 a las 10:25 a.m.

9. BAJADO DE https://es.wikipedia.org/wiki/Cultura_del_miedo Recuperado el 28 de octubre de 2019 a las 10:25 a.m.

10. BAJADO DE https://es.wikipedia.org/wiki/Cultura_del_miedo Recuperado el 28 de octubre de 2019 a las 10:25 a.m.

“Diversos periodistas sociales han presentado diferentes tesis sobre la cultura del miedo, cada uno con un énfasis distintivo. Podrían ser categorizadas a lo largo de un rango de variantes, desde aquellas en las cuales se considera al fenómeno como conscientemente dirigido - por ejemplo, una política deliberada de alarmismo -, hasta aquellas en las cuales se le trata como una emanación espontánea de desarrollos históricos, como una respuesta reflexiva a otros cambios en la sociedad” . **10**

“Las políticas de George W. Bush, especialmente su gestión retórica alrededor de su "guerra contra el terrorismo" y la invasión de Iraq, han sido el blanco principal de las críticas. En este contexto, la "cultura del miedo" es supuestamente generada por la administración de Bush y sus aliados, en un esfuerzo jerárquico para incrementar el apoyo a la fuerza militar y las operaciones de seguridad nacionales. En un amplio contexto político-nacional, muchos creen que los políticos conservadores y algunos líderes morales, hacen a la gente temerosa de cosas tales como el terrorismo, el crimen o drogas ilegales para influenciar sobre la opinión pública y la conducta personal. Es algo que muchos creen es intencionalmente exagerado por los medios a petición de los propietarios conservadores de compañías mediáticas (por ejemplo, Rupert Murdoch y Fox News).

"La idea de una sociedad en gran medida de "cultura del miedo", puede ser percibida por liberales y otros oponentes de los conservadores, como una estenografía de la manipulación cultural por parte de éstos con fines políticos. Por el contrario, los liberales también han sido acusados por su justa participación de alarmismo para aplicarlo a sus propias agendas políticas, especialmente en asuntos de protección ambiental, biotecnología y seguridad.

"Sobre cuestiones que no han sido fuertemente asociadas con la controversia política derecha/izquierda, una estampida ostentosa de miedos en el discurso público pueden ser etiquetadas por otros especialistas como "alarmistas". Síntomas típicos de una alarma incluyen una falta de educación general o científica entre el público, predisposiciones intrínsecas en la valoración de riesgos, carencia de pensamiento racional, información errónea y el dar mucha importancia a los rumores" .[11]

L. Howie afirma que "el miedo adquiere connotación política cuando existe una gran audiencia que quede sujeta a su exposición. Ningún ataque terrorista busca la exterminación de una comunidad, sino someterá la mayor cantidad posible de personas a un sentimiento de vulnerabilidad. [12]

Hoy día, la sociedad cuenta con el mayor desarrollo tecnológico inventado por la industria de la información y comunicación llamada internet. Pero, ¿qué es el internet? Internet nos es más que un conjunto descentralizado de redes de comunicación interconectadas que utilizan una serie de protocolos que garantizan que estas redes funcionen de una forma lógica con un alcance a nivel mundial.

El delincuente cibernético se vale de esta herramienta tecnológica para la realización de sus acciones delictivas, y, como se ha definido su acción no tiene límite. Igualmente puede actuar solo o conformando grupos los cuales se constituye en red. Suponen grupos de contacto que permiten reunir a las personas en el ciberespacio, desde el anonimato, a los que no encuentran un lugar de pertenencia y comparten gustos, preocupaciones, se ayudan mutuamente. El ciberdelincuentes se ha tecnificado de tal manera que para poder detenerlo se necesita de otro personaje que maneja al igual que él, las tecnologías de la información y la comunicación, o sea necesita de un "ciberpolicía".

11. BAJADO DE https://es.wikipedia.org/wiki/Cultura_del_miedo Recuperado el 28 de octubre de 2019 a las 0:25 a.m

12. Howie, L. 2012. Witnesses to Terror. NY, Macmillan

V. EL MIEDO Y LA DELINCUENCIA CIBERNETICA ORGANIZADA

En los últimos años la delincuencia cibernética se ha convertido en un tema preocupante que inquieta por igual a la industria y a los gobiernos. El hecho de que el uso delictivo organizado de Internet suponga una amenaza para la seguridad nacional o internacional depende de dos aspectos básicos: la seguridad y la delincuencia organizada. Ya se han dado algunas situaciones en las que la seguridad nacional e internacional, han sido amenazadas por la actividad de ciberdelincuencia organizada.

La extensión de las nuevas tecnologías digitales a todos los ámbitos de la vida cotidiana hace inevitable su explotación continua con fines delictivos. Parte de esta actividad puede poner en peligro la seguridad, mientras que otra no. Es importante distinguir qué actos ciberdelincuentes pertenecen a cada categoría para encontrar las respuestas adecuadas. En este apartado hemos tomado la investigación realizada por el Doctor en Criminología Abel González García[13] cuando hace interesante planteamientos sobre hechos que se refieren al miedo producido por la ciberdelincuencia en su obra ***"CIBERDELINCUENCIA: MUCHOS MITOS Y POCAS REALIDADES"*** manifestando que este miedo "está alimentado por la sobrerrepresentación que existe en los medios de comunicación de los delitos en Internet", en lo cual se pregunta si realmente existe una amenaza en contra de la vida. "Cuando nos ponemos a pensar sobre esto, nos dejamos llevar, muchas veces, por las tramas que se presentan en las películas relacionadas con amenazas o ciber ataques que amenazan la vida e integridad personal o la sociedad por grupos terroristas" [14]

En lo referente a la sobrerepresentanción que hacen los medios de comunicación de los delitos en Internet, el Doctor González analiza dos noticias, la primera que se refiere una nota de prensa emitida el 11/06/2015 por el Ministerio del Interior Español bajo el titular "Jorge Fernández Díaz subraya en la cátedra Google que el ciberdelito supone ya la tercera forma delictiva y criminal más importante a nivel mundial". Y la segunda es de una publicación echa por el Diario El País el 5/2/2015 afirmando que "España es, tras EEUU y Reino Unido, el país que sufre más ciberataques"[15]

13. González, Javier op. Cit.
14. González, Javier op. Cit.
15. González, Javier op. Cit.

"De esta manera las formas delictivas y criminales son la misma cosa, el delito tipificado en el Código Penal. Además, al afirmar que es la tercera forma delictiva, también está indicando que estamos desprotegidos, porque sólo se esclarecen 2.167 hechos de 42.437 que se conocen (no llega al 5%), según datos del propio Ministerio del Interior relativos a la cibercriminalidad. Por otro lado, en este mismo informe se explica que la ciberdelincuencia es el 1,95% de total de la delincuencia. Como pueden comprobar muy alejado del tercer puesto aducido, por lo menos en España" .[16]

En relación con la noticia referente a que España es el tercer país que sufre mayor número de ciberataques, en lo referente a la sobrerepresentación que hacen los medios de comunicación, González García considera que, "en primer lugar, sí puede ser interesante conocer qué tipo de ciberataques se producen, por ejemplo, si se realizan a infraestructuras críticas o si los sufren directamente los ciudadanos. Es decir, es muy importante conocer que existen gran variedad de ciberataques, que no todos tienen éxito y que la mayor parte de ellos son desconocidos para el público" .

16. González, Javier op. Cit.
17. González, Javier op. Cit.

en general, en este sentido, algún experto en informática no para de recalcar que la mayor parte de nosotros llevamos instalado algún tipo de malware en nuestros dispositivos y no somos conscientes de ello.[17]

Los delincuentes de la informática, están expresados en la ciberdelincuencia, tienen su propia agenda y, cual parásitos, pueden causar enormes daños a la sociedad, no solo a empresas y cualquier tipo de organización, sino también a países, sin importar su condición política o económica, por lo que estos inclusive se han visto obligados a considerarlo como amenaza de seguridad nacional. Pero a parte de todos estos también existen las victimas indefensas que se encuentran dentro del pueblo a lo que el autor se hace las pregunta ¿somos todos víctimas indefensas?, ¿somos conscientes de que somos víctimas? Debemos responder que efectivamente somos víctimas mucho más propicias en el ciberespacio por nuestro amplio desconocimiento del mismo y además, en la mayor parte de los casos, no nos damos cuenta de que estamos siendo víctimas.

. Nosotros mismos subimos a la red información ingente de nuestra vida y con eso es suficiente para ellos. Aquí debemos pararnos también a pensar en el entramado público-privado, donde las grandes empresas de Internet tienen más poder que muchos Estados, precisamente por la cantidad de datos personales que manejan. Si

todo ello es efectivo en la lucha contra la ciberdelincuencia no estoy muy seguro, de lo que sí estoy seguro es que Internet ha hecho que los gobiernos legislen para que exista una merma de libertades civiles apoyados por el miedo que tenemos a lo desconocido, ejemplo de ello es el terrorismo y el ciberterrorismo" [18]

VI. CONCLUSIÓN

La sociedad moderna se encuentra consumida por la tecnología. Hoy día, la tecnología de información y la comunicación se ha apoderado de la sociedad. Desde el más humilde hasta el más pobre cuenta con un celular. Gran parte de las comunicaciones ordinarias actuales y el mantenimiento de los registros que se almacenan en esos celulares, se basa en Internet y en las tecnologías relacionadas. Al tiempo que la tecnología digital mejora la eficiencia de las actividades legítimas ordinarias, también mejora la eficiencia de las actividades delictivas. Y con esta se va desarrollando cada vez la cultura del miedo.

Resulta un tanto irónico que la ciencia de la tecnología y de la comunicación que ha servido para acortar distancia y crear nuevos sistemas de vida más cómodo en donde las familias puedan mantener una, mejor comunicación, a pesar de las distancias en que se encuentren. Resultan irónico que esas mismas ciencias tecnológica, está ocasionando un sentimiento de temor dentro de algunos grupos sociales más vulnerables.

El delito cibernético o ciberdelito se refiere en términos generales a la actividad delictiva que utiliza los sistemas de información como instrumentos u objetivos de una ilegalidad [19]. Esto supone el acceso ilícito a los sistemas, la interferencia con su uso legal y el robo o la destrucción de la información contenida en ellos. También puede implicar la posesión o transmisión de contenido prohibido como la explotación sexual comercial de niños, niñas, adolescentes adultos.

La idea de empresas integradas verticalmente dio paso, por lo tanto, a la metáfora de "redes", que proporcionaban una base para el pensamiento contemporáneo sobre las relaciones tanto dentro de los grupos delictivos organizados como en grupos de individuos. Las definiciones tradicionales de la delincuencia

18. González, Javier op. Cit.
19. Mª José Caro Bejarano Analista Principal IEEE BAJADO DE http://www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA612013_DelincuenciaOrganizadaxInternet_MJCB.pdf RECUPERADO EL DÍA MIÉRCOLES 18 DE SEPTIEMBRE DE 2019, A LAS 11:43 A.M.

organizada se han basado en el ánimo de lucro. Sin embargo, incluso la mayoría de los observadores de la delincuencia organizada tradicional señalan el atractivo intrínseco de la emoción, el compañerismo y otros valores no materiales.

Actualmente, hay muchas organizaciones criminales (como las especializadas en el fraude y el robo de vehículos) que no practican la violencia, ni el soborno. Por otra parte, una gran cantidad de actividades de la delincuencia organizada en Internet está impulsada principalmente por consideraciones no monetarias, como la búsqueda de desafío intelectual, notoriedad individual o del grupo, la lujuria (en el caso de la actividad pedófila organizada), la ideología, la rebelión y la curiosidad.

Ya no son los hackers a los que hay que temerles, lo que debemos buscar ahora es conocer como opera el mundo de la cibercriminalidad organizada y conocer si la ciberdelincuencia organizada ha alcanzado una escala e intensidad que pudiera amenazar la seguridad nacional e internacional. Sin embargo, es necesario en primer lugar, establecer una definición de la ciberdelincuencia organizada. Al hacerlo, es importante analizar los diferentes tipos de ciberactividad que podrían considerarse "delictiva", los tipos de actores y organizaciones que persiguen los mismos, y la cuestión de si todos los actos realizados por las organizaciones y que son ilícitos pueden, de hecho, ser clasificados como “ciberdelincuencia organizada".**20**

18. González, Javier op. Cit.

CIBERCRIMEN CONTRA LAS MUJERES

RESUMEN

Los avances tecnológicos traen grandes beneficios para la sociedad, sin embargo, también acarrean nuevos retos para la seguridad pública, toda vez que las conductas delictivas se han diversificados con el uso del internet.

La doctrina entiende que una clasificación de las distintas modalidades delictivas de los delitos contra las mujeres relacionadas con la informática, debe hacerse con relación al bien jurídico protegido, y dentro de esta categoría, distinguir las acciones típicas que la vida cotidiana o la experiencia local o comparada que nos dan las noticias como hechos sociales delictivos contra las mujeres.

Siendo así, la República de Panamá debe actualizar su legislación y trabajar en la prevención de los delitos cibernéticos que atenten contra las mujeres, quienes son víctimas de acoso, robo de datos, de identidad, sustracción de información, estafa, bullying, captura de datos

INTRODUCCIÓN

En la República de Panamá los delitos cometidos a través de medios cibernéticos, son modalidades delictivas, que a través de los últimos años han evolución incurriendo en delitos de acoso, pornografía, extorsión, fraudes electrónicos, estafas, ataques a sistemas informáticos realizados por hackers, captura de datos bancarios (phishing, pharming), computadoras zombies (botnets), violación de los derechos de autor, pornografía infantil, pedofilia, denegación de servicios, ciberbullying, cibergrooming, violación de información confidencial y muchos otros.

En este sentido, el cibercrimen contra las mujeres es una modalidad de delito que cada vez varía más sus conductas delictivas. En este artículo haremos un enfoque sobre esta problemática con la finalidad de que las instituciones que tienen que ver con la misma, adecuen las normas existentes en relación sobre esta nueva modalidad de cibercrimen contra las mujeres en Panamá e implementen conscientemente la aplicación de los convenios internacionales ratificados por nuestro país, permitiendo ampliar el marco de expansión de conceptos necesarios para dar atención al delito.

Desde un punto de vista criminológico, existen dos enfoques, en cuanto a la naturaleza de este nuevo tipo de fenómeno criminal; el primero de ellos es que los delitos informáticos no son más que delitos convencionales que toman nueva vida a partir del uso de dispositivos informáticos y de servicios y aplicaciones en internet. El segundo afirma que las tecnologías de la información y comunicación brindan nuevas herramientas para la comisión de delitos inexistentes, como la distribución de virus o programas maliciosos a través de la red, ataques a sitios web y la piratería del software. Al respecto, consideramos que ambos enfoques son ciertos.

Existen delitos tradicionales que adquieren nuevas formas a partir de la intermediación de dispositivos automatizados como también nuevas formas delictivas que no serían posibles de cometerse si no existiese un programa de software o archivos digitales presente, como, por ejemplo, en la elaboración de programas maliciosos con el fin de dañar un servidor web para afectar el funcionamiento de la página, o aquellos para extraer información de un dispositivo -por ejemplo, los spyware o programas espías, o alterar o dañar el funcionamiento de un dispositivo a través de virus, gusanos y troyanos. **(4)**

(4)Sain, g. p.9). op. cit.

En consecuencia, el cibercrimen es entendido respecto al lugar que ocupa la tecnología para la comisión del delito más que a la naturaleza delictiva del acto mismo. “Si una persona intimida o intenta chantajear a una mujer vía correo electrónico, el dispositivo informático actúa como medio para cometer el hecho ilícito, siendo el delito de amenaza el hecho ilícito en sí. En el segundo caso, el dispositivo informático es el objeto o blanco del crimen, donde una persona puede enviar un virus a la computadora de un tercero y así dañarla a los fines de inutilizarla o alterar su funcionamiento. En este último caso la figura delictiva podría encuadrarse dentro del daño en tanto delito contra la propiedad, considerando el dispositivo informático como un bien tangible, tanto, así como la información que puede almacenar”.

3. GENERALIDADES:

De acuerdo a lo visto hasta el momento podemos decir que existen dos grandes áreas que abordan la problemática del cibercrimen en términos prácticos; el Derecho y la Seguridad Informática.

En el ámbito del área del Derecho la problemática del cibercrimen posee una perspectiva sancionatoria, interviene cuando el delito ya se ha consumado, siendo su función en términos de seguridad la conjuración y represión del delito. En materia de prevención criminal, la solución penal no resulta contra-motivacional a aquellas personas que deciden voluntariamente cometer un cibercrimen, en virtud que las altas probabilidades de una persecución penal eficaz son remotas en la mayoría de los casos en términos de identificación del responsable de estas conductas, fundamentalmente a partir del uso de identidades ficticias y lugares de conexión públicos.

Siendo así, en la actualidad existen variadas discusiones acerca de que conductas tienen que ser consideradas delito informático y cuáles no. Asimismo, lo que puede considerarse una conducta lesiva en un país no puede serlo para otro. Cada país tiene la potestad soberana para establecer su legislación penal respecto a sus realidades socioculturales predominantes, lo que no debería impedir la cooperación internacional para la persecución penal de este tipo de ilícito

Por otro lado, si bien la mayoría de los países tienen legislación relacionada con este tipo de criminalidad, existen figuras que no están tipificadas en forma uniforme. Asimismo, la uniformidad en materia de herramientas legales para investigación criminal resulta utópica, como quiera que la misma dependerá de los factores antes mencionados en cuanto a las tradiciones en término de la privacidad de las personas de un país, por un lado, y el tipo de relación que establezca la justicia de un país con las empresas proveedoras de servicio de internet multinacionales. Donde facilitan delitos contra mujeres y su relación con legislación actual en esta materia.

Cibercrimen contra las mujeres

- Se observa que existen países donde el derecho a la libertad de expresión se aventaja frente al derecho de la intimidad, la pregunta que muy poco se cuestiona es ¿porque se debe aplaudir y guardar silencio cómplice a estas actividades que lesionan al avance de las mujeres, inclusivamente en la obtención de evidencias digital por parte de la justicia? El proceso en si parece denigrante y humilla a las victimas ya que deben lamentar haber puesto su confianza en una persona o bien simplemente haber querido utilizar tecnologías modernas para comunicar algo.
- En el ámbito de la seguridad informática por otro los hechos ilícitos que involucran dispositivos informáticos que llevan los tribunal son íntimos a partir de las resoluciones técnicas y administrativas que poseen estas conductas lo que representa una amplia cifra oculta en este tipo de criminalidad y de hecho muchas personas .

CIBERCRIMEN CONTRA LAS MUJERES

En segundo lugar, la obtención de evidencia digital por parte de la justicia de un país va a depender tanto de cuestiones como si la empresa posee representación legal en ese territorio o sus servidores dentro del mismo.

En el ámbito de la Seguridad Informática, por otro lado, los hechos ilícitos que involucran dispositivos informáticos que llevan los tribunales son ínfimos a partir de las resoluciones técnicas y administrativas que poseen estas conductas, lo que representa una amplia cifra oculta en este tipo de criminalidad.

En la actualidad son las empresas de seguridad informática que elaboran programas de software comerciales no contemplan una mayor intervención y poseen una mayor intervención que los propios Estados en términos de protección de datos e información y dispositivos de sus clientes. https://docplayer.es/92496152-Cibercrimen-y-delitos-informaticos.html

CIBERCRIMEN CONTRA LAS MUJERES

Uno de nuestros objetivos debería radicar en ofrecer información a las víctimas sobre las medidas tanto técnicas como jurídicas necesarias para combatir este tipo de delito. Es imposible lograr sanciones ejemplares ante estos ataques, con las leyes que tenemos en estos momentos, algunos de ellos se quedan sin pena, por no estar tipificados en el código penal; ataques que pensamos no se pueden demostrar y que, en muchos casos, no sabemos ni que son ataques**(5)**. **(5)ROIBÓN, M. P.132**

Cada día los panameños dedicamos más tiempo a las redes sociales, lo cual afecta a gran parte de la población, especialmente a las niñas y mujeres que se ven expuestas a la violencia psicológica por adultos e inclusive por menores de edad. Los daños son a través del cibera coso, sexting (envió de mensaje de sexo, visual o textual) y grooming (ganar la confianza para obtener un provecho sexual).

La forma de ver la amistad, que existía en la década de los noventa ha cambiado, porque antes era de cara a cara, la interacción era verbal y física, ahora el amigo es quienes están en el otro lado de las redes sociales. Aunadamente, el sexting es una consecuencia de los tiempos actuales, en donde la hipersexualización, la música, e incluso las nuevas tecnologías a edades tempranas, han hecho que los jóvenes vivan su sexualidad de forma distinta a lo habitual(6). **(6)Gazire (2009: 56).**

Debemos señalar que, con el uso de las redes sociales, las mujeres corren el riesgo de dañar su reputación y vida futura cuando se exponen al uso inadecuado del internet. La mensajería instantánea con la utilización de la tecnología ha generado riesgos y dinámicas ante los diversos hechos delictivos y la violencia contra la mujer.

Aunado a ello, existen mecanismos importantes para detener el cibercrimen es, principalmente, que el usuario denuncie públicamente a su acosador a través de su propio perfil. Lo que puede derivar en que cualquiera de las redes sociales como Facebook o Twitter tome la decisión de cerrar la cuenta de un cibercriminal que demuestre un comportamiento no acorde con

las reglas de uso de las redes sociales que pueden ocasionar que los delitos informáticos tiendan a aumentar en las redes sociales. Haciendo un repaso de los casos reportados en instancias policiales y publicaciones de medios locales, se evidenció que la mayoría de estos corresponde a una modalidad de cibercrimen como es la ciberextorsión.

En este caso el extorsionador se da modos para conseguir material comprometedor, muchas veces de tipo erótico, de la víctima; a quien posteriormente amenaza con publicar dicho contenido si es que ésta no le entrega una suma de dinero. Todo comienza con algo tan simple como una conversación (chat) con afanes de ligar, luego ésta empieza a tomar tintes sexuales y posteriormente se produce un intercambio de fotos o videos íntimos. La mayoría de las víctimas de este tipo delitos son adolescentes y jóvenes.

La tipificación de estos delitos no se contempla en la legislación nacional, es así que hasta el momento sólo se tiene una sola ley al respecto que está relacionada con el feminicidio. Asimismo, las pruebas contra delitos que se encuentren en redes sociales deben cumplir con lo establecido en la Ley No.63 de 2008. Por otro lado, se puede evidenciar que redes sociales como Facebook, Snapchat, WhatsApp, Instagram y Twitter, son usadas en muchos casos como instrumentos para ejercer violencia contra la mujer.

Por otra parte, las mujeres pueden sufrir violencia verbal o física en el noviazgo y una de las formas en que los jóvenes controlan a sus novias ahora es el WhatsApp; porque presenta una serie de modalidades por las que se puede vigilar a una persona constantemente (se encuentra en línea, último chat, última publicación en su estado).

El ciberacoso es un tipo de violencia que afecta específicamente a las mujeres, tal como fue el caso de la persona que mantenía fotografía de cientos de mujeres panameñas en redes sociales.

5. EL CIBERCRIMEN CONTRA LAS MUJERES EN PANAMÁ

Las agresiones contra las mujeres continúan a pesar de los avances legales y la implementación y ratificación de los Convenios Internacionales. Sin embargo, es necesario llevar a cabo acciones, como la creación de un refugio para mujeres que sufren violencia doméstica.

Aunado al hecho es imperativo una campaña de prevención a nivel masivo, creando un banco de datos que recopile los casos de delitos cibernéticos contra las mujeres reportados ante las autoridades competentes en aras de garantizarles una vida libre

de violencia. Este tipo de delitos muchas veces son tomados con morbo, incluso por la prensa.

Creando más que datos, un lado más humano de la tragedia. Toda aquella acción que mediante medios digitales acose, amenace o extorsione a cualquier individuo se conoce como Violencia Digital.

En violencia de género podemos definir el término violencia de género digital como toda aquella agresión psicológica que realiza una persona través de las nuevas tecnologías como el correo electrónico, sistemas de mensajería como WhatsApp o redes sociales, contra su pareja o ex pareja de forma sostenida y repetida en el tiempo, con la única finalidad de discriminación, dominación e intromisión sin consentimiento a la privacidad de la víctima.

Es imprescindible disponer de la información y ayuda necesaria para detectar cualquier caso de ciberacoso en internet, redes sociales y dispositivos tecnológicos, puesto que la vulneración de nuestros derechos básicos constitucionales y el derecho a la intimidad en las telecomunicaciones es materia tipificada y penada por nuestro actual código penal.

La persona que sufre el ciberacoso, en la mayoría de los casos ignora la forma de enfrentarse a la situación que está sufriendo, igual que ignora sus derechos, porque nadie le proporciona información legal que le indique los recursos de los que puede disponer, y los medios de protección adecuados que existen a cada tipo de ataque; que en la mayoría de los casos incluye la violencia basada en el sexo, cuyas imágenes afectan de manera desproporcionada, ya que incluyen daños o sufrimiento de índole física, mental o sexual, ciberamenaza, coacción y otras formas de privación de libertad digital.

5.1. Violencia de Género Digital:

La doctora Nora Cherñavsky sostiene que cuando las consultas son sobre extorsiones, acosos y publicaciones de imágenes íntimas no autorizadas. La especialista relaciona esas conductas con la porno venganza, producto de una ruptura de pareja. Agrega que la tecnología es el medio elegido para humillar a la víctima

En los Estados Unidos, la Universidad de Michigan determinó que en el 90% de los casos de “pornovenganza” el

agresor es un hombre y que cinco de cada diez víctimas admiten haber recibido fuertes insultos en las redes sociales. Más de 40 Estados americanos sancionaron leyes que penan éste tipo de delitos **(7).**

(7)"Las mujeres y la ciberseguridad". Boletín N° 35 **Centro de Ciberseguridad de CABA**

La vicepresidenta de Cyber Civil Rights Initiative, la abogada Mary A. Franks, impulsó desde la organización sin fines de lucro el reclamo para combatir los abusos online. La profesora de Derecho Penal de la Universidad de Miami sostiene que existen 3.000 sitios web que publican pornografía de venganza, la cual es redistribuida a través de los medios digitales.

Entre las políticas de Estado que garanticen a las mujeres la protección contra estos delitos tenemos:

- Que la víctima tenga a quien acudir ante un caso de ciberacaso, un lugar donde la víctima se sienta protegida y le entiendan por lo que está pasando.
- Proporcionar las herramientas necesarias para combatir y protegerse de cualquier ataque informático.
- Ayudar a la víctima a superar sus miedos tecnológicos tras haber sufrido un ciberdelito.
- Impartir cursos formativos para su inserción laboral en caso de necesitarlo.
- Impartir charlas formativas en centro educativos desde temprana edad para concienciar a los menores sobre los peligros a los que están expuestos en internet.
- Impartir talleres a las víctimas para el uso correcto de las nuevas tecnologías.
- Formar profesionales para el tratamiento adecuado a víctimas de violencia digital.

5.2. Modalidades más frecuentes

- Hacking: Vulneran cuentas de correo electrónico. Procedimiento ilegal involucrado con el robo de cuentas de correo electrónico o similares para cometer hechos ilícitos.
- Phishing: Obtienen contraseña e información privada. El delincuente informático suplanta la identidad de un contacto de la víctima con el fin de obtener contraseñas o información bancaria privada.

CIBERCRIMEN CONTRA LAS MUJERES

- Pharming: La suplantación de una página web. Es como el anterior, pero en este caso se suplanta una dirección de correo electrónico o página web con los mismos fines. Por otra parte, el pharming como una nueva modalidad de fraude en línea consiste en suplantar el sistema de resolución de nombres de dominio (DNS) para conducir al usuario a una página web bancaria falsa y apoderarse de sus claves. Cuando un usuario teclea una dirección en su navegador, esta debe ser convertida a una dirección IP numérica. Este proceso es lo que se llama resolución de nombres, y de ello se encargan los servidores DNS. El pharming implica acceder al sistema de un usuario y modificar ese sistema de resolución de nombres, de manera que cuando el usuario crea que está accediendo a su banco en Internet, realmente está accediendo a la IP de una página web falsa.
- Ciber Extorsión: La extorsión, el delito más denunciado en la República de Panamá. Se extorsiona a la víctima, amenazando con publicar fotos,

  videos o cualquier otro contenido comprometedor.
- CiberaCiber bullying: El acoso a través de las redes sociales. Bullying a través de redes sociales. Muchas veces promueven el suicidio de la víctima.
- coso: El hostigamiento hacia personas por Facebook y otras redes. Hostigamiento de una persona a través de medios electrónicos y/o redes sociales.
- Sexting: La pornografía y envío de material para adultos. Envío de contenidos sexuales o eróticos. Es ilegal cuando involucra a menores de edad.
- Cracking: quebrantación de la seguridad de contraseña.

https://docplayer.es/92496152-Cibercrimen-y-delitos-informaticos.html

6. CONCLUSIONES

Combatir el cibercrimen en contra de la mujer o de cualquier otro género es una tarea difícil y complicada, en donde se han de combatir temas tan complejos como relaciones, menores, cultura, conocimiento de las nuevas resulta gratuita, el precio a pagar es la renuncia a la privacidad, porque al momento de aceptar las condiciones de servicio de estas

redes, les estás otorgando pleno derecho a usar toda la información que publicas y a tener acceso a las galerías de fotografías, videos, ubicación y otros elementos que se encuentren en el equipo de telefonía móvil personal.

Siendo así, es evidente que el llamado, hackeo, como tal no es tan común, a nuestro criterio, el acceso a las cuentas, se da por dejar las cuentas abiertas en lugares públicos y es ahí donde otros pueden acceder a fotografías, videos e información guardada. Todo esto sucede porque al tener acceso internet, no se hace con conciencia plena de los actos y omisiones; se actúa por inercia y con comportamiento de consumidores.

- **RECOMENDACIONES**
- Establecer campañas de prevención en temas de ciberseguridad orientada a evitar la violencia de género.
- Crear un plan de apoyo para las mujeres que han sido víctima de delitos cibernéticos.
- Implementar reformas a la legislación penal orientada a sancionar las nuevas conductas delictivas que se efectúan mediante el uso de las redes tecnológicas.

- **GLOSARIO:**
- Acecho sexual. Perseguir, atisbar, observar a escondidas, aguardar cautelosamente a una mujer, con propósitos sexuales.
- Acoso sexual. Todo acto o conducta de carácter sexual no deseada que interfiere en el trabajo, en los estudios o en el entorno social, que se establece como condición de empleo o crea un entorno intimidatorio o que ocasiona a la víctima efectos nocivos en su bienestar físico o psicológico.
- Ámbito privado. Aquel donde tengan lugar las relaciones interpersonales, domésticas, familiares, de pareja o de confianza, dentro de las cuales se cometan hechos de violencia contra una mujer.
- Ámbito público. Aquel donde tengan lugar las relaciones interpersonales en el ámbito social, laboral, comunitario, educativo, religioso o cualquier otro tipo de relación que no esté comprendido en el ámbito privado. **(9)**

(9)**Fernández, Horacio. P. 204**.

REFERENCIAS BIBLIOGRÁFICAS

1. Asamblea Nacional. Código Penal de la República de Panamá, Ley No. 14 de 18 de mayo de 2007.
2. Asamblea Nacional. Código Procesal Penal de la República de Panamá, Ley No. 63 de 28 de agosto de 2008.
3. Asamblea Nacional. Constitución Política de la República de Panamá.
4. Asamblea Nacional. Proyecto Asamblea Nacional. Proyecto de Ley 463, de Protección de Datos de Carácter Personal. Disponible: http://www.asamblea.gob.pa/proyley/2017_P_463.pdf Asamblea Nacional. Proyecto de Ley 558, que modifica y adiciona artículos al Código Penal, relacionados al Cibercrimen. Disponible en: http://www.asamblea.gob.pa/proyley/2017_P_558.pdf Consejo de
5. Europa. Convenio sobre la Ciberdelincuencia.
6. Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas.
7. Código Judicial.
8. Ley 63 de 2008.
9. Comprensión del Ciberdelito: Fenómenos Dificultades y Respuesta Jurídica. Sector de Desarrollo de Telecomunicaciones.
10. CATÁ DEL PALACIO, ARTURO. Ciberdelincuencia Desarrollo Y Persecución Tecnológica. Universidad Politécnica de Madrid. 2014

VULNERABILIDADES EN LOS SISTEMAS DE INFORMACIÓN VITALES ECONÓMICAS, CIUDADANAS Y ESTATALES DE PANAMÁ

INTRODUCCIÓN

En el presente artículo abordaremos de manera breve y concisa el tema de la vulnerabilidad en los sistemas informáticos, riesgos, amenazas y su contraste con la prevención y protección a nivel estatal, financiero económico y el rol de los usuarios. Consideramos que todos los elementos que integran un sistema informático deben ser igualmente considerados dentro de este análisis como; la capacidad, las condiciones y características del sistema mismo incluyendo la entidad o persona que los manejan o administran.

Dichos factores propician susceptibilidades y constantes amenazas en los sistemas de datos, no obstante, los Gobiernos del mundo están conscientes que las innovaciones y nuevas modalidades en materia de delitos informáticos, razón por la cual se hace necesario el redoblar esfuerzo para tener la capacidad de responder o reaccionar ante una amenaza y de igual forma aplicar técnicas que coadyuven a la recuperación de los posibles daños o secuela que pueden emerger de estos ataques.

En este orden de ideas y dándole un sentido lógico, la vulnerabilidad esta correlacionada directamente con los riesgos, las amenazas y los daños que se puedan presentar en los sistemas, lo que indica que para que un elemento del sistema sea vulnerable, debe estar presente una amenaza de inicio, lo que pueda traer como consecuencia un daño como fin. De tal manera que, este artículo tendrá como objetivos principales informar y generar conocimiento básico sobre las posibles vulnerabilidades del sistema informático y demás acciones o reacciones a nivel general.

QUE ES LA VULNERABILIDAD EN LOS SISTEMA DE INFORMACION

Básicamente, una vulnerabilidad en los sistemas de internet o informático es una debilidad presente en un sistema operativo, software o sistema que le permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

MARCO JURIDICO Y REGLAMENTACION DE LA ACCION DEL DELITO CIBERNETICO

El marco jurídico de este hecho punible está tipificados bajo la Ley 14 de 2007, y en el código penal panameño en el Título VIII nominada Delitos contra la Seguridad Jurídica de los Medios Electrónicos Capítulo I "Delitos contra la Seguridad Informática" que abarca los artículos 289 que dice: "quien indebidamente ingrese o utilice una base de datos, red o sistema informático" el artículo 290 que dice: "se apodere, copie, utilice o modifique los datos en tránsito o contenidos en una base de datos o sistema informático, o interfiera, intercepte, obstaculice o impida su transmisión" son dos modalidades y en los artículos 291 y 292 "están establecidas que la sanción se agravará entre una sexta y una tercera parte"

Desde que, en 2007 el delito informático fue incluido en el Código Penal panameño se han reportado 359 investigaciones relacionadas a este hecho, sin embargo, solo ha habido tres condenas.

Aunque el código Penal incluye el Delito Informático, hay aspectos sobre el tema que no están contemplados. Por ejemplo, la usurpación de identidad en redes sociales como Facebook, Twitter o Instagram, modalidad delictiva que se presenta con mucha frecuencia en el país.

En Panamá, el **Equipo de Respuesta a Incidentes de Seguridad de la Información** (**CSIRT PANAMA**) es entidades gubernamentales encargada de la prevención, detección, manejo y recopilación de información sobre incidentes de seguridad, creado mediante Decreto Ejecutivo No.709 en septiembre 2011, y adscrito a la **Autoridad Nacional para la Innovación Gubernamental** (**AIG**), son los entes que conforman el equipo Nacional de respuesta a incidentes de seguridad de la información de Panamá.

Entre sus objetivos están la prevención, tratamiento, identificación y resolución de ataques a incidentes de seguridad sobre los sistemas informáticos que conforman la

infraestructura crítica del país y el acceso a la información de parte de los ciudadanos de Panamá.

En la publicación del diario La Prensa del 16 de septiembre de 2019, se informó que el CSIRT PANAMA realizó un análisis de los sistemas gubernamentales sobre una alerta del 13 de mayo del mismo año. Informaron que “Hasta ese momento no se habían reportado ni detectado ninguna brecha de inseguridad en las plataformas que conforman los sistemas informáticos estatales. Una vez culminen las investigaciones acordes, los protocolos requeridos para este tipo de incidentes, se le informará a la ciudadanía sobre sus resultados”.

Este equipo se propone fortalecer la difusión, el conocimiento y atención de suceso de Seguridad Informática del Estado con la coordinación y colaboración de los estamentos para la resolución de incidentes de seguridad de la información y comunicación, según la Autoridad.

No obstante, el Índice Nacional de Seguridad Cibernética (NCSI), a reportado que Panamá se encuentra entre los diez líderes de Latinoamérica que miden la capacidad de los países para evitar las principales ciberamenazas y la preparación para gestionar incidentes cibernéticos, crímenes y crisis cibernéticas a gran escala.

El estudio detalla que en Latinoamérica se analizaron veintidós (22) países y Panamá se ubicó en la posición número siete, liderado por Estados Unidos, Canadá y Chile.

Esa investigación analizó la situación de seguridad cibernética de las naciones a través de 12 capacidades estratégicas y 46 indicadores, así como una base de datos global que proporciona enlaces y documentos sobre seguridad cibernética nacional.

Sin embargo, aunque el 61% de los Gerentes Generales de las compañías más importantes del país hayan señalado que les preocupa la ciberseguridad, solo el 37% de las organizaciones declaran que cuentan con un plan de acción. En Panamá lamentablemente debemos aceptar que estamos muy mal preparados para enfrentar el ciberdelito.

Los delitos en Internet se sitúan en dos categorías generales, la primera abarca ataques monetizables, como el robo de identidad o tarjetas de pago. La segunda, el ciberespionaje el robo de secretos comerciales, estrategias de negociación e información sobre productos.

En nuestro país desde el 2013, existe una póliza de cobertura de riesgos cibernéticos que abarca las afectaciones o daños producidos por los Delitos Informáticos de la corredora de Seguros Ducruet/Unity. Louis Ducruet Jr., presidente de la

compañía, dijo que “la póliza está orientada a la responsabilidad civiles que tienes que asumir por todo el tema moral”.

¿QUÉ HACER ANTE CONSTANTES AMENAZAS LOS SISTEMAS?

Los expertos concuerdan con que Panamá es un país vulnerable al ataque cibernético. Pero aplicando las medidas de protección necesarias, como la instalación y actualización de antivirus, firewall, y otros programas como anti-melaware se pueden prevenir.

En este sentido, en Panamá ya muchas empresas han sido víctimas de RANSOMWARES (un programa malicioso que bloquea el ordenador y exige un pago por recuperar los equipos y la información), por querer ahorrar y utilizar programas gratuitos de antivirus o pirateados.

Según el Ingeniero y Abogado Guillermo Donadío Velarde, Presidente de la Comisión de Derecho Informático y Nuevas Tecnologías del Colegio de Abogados de Panamá, dicha entidad fue víctima de este tipo de ataques cibernéticos en donde no hubo posibilidad de recobrar la información y se tuvo que formatear los equipo.

Por lo que los expertos recomiendan desconectar los Routers (direccionador) inalámbricos cuando no se usen, así como leer todas las cláusulas a la hora de momento de bajar aplicaciones a computadoras y dispositivos electrónicos. Es importante no distribuir información confidencial en redes sociales

https://www.prensa.com/politica/Acechan-delitos-informaticos-Panama_0_4220578020.html

Los mecanismos o políticas de seguridad para mitigar la posible vulneración más utilizados incluyen herramientas de protección como antivirus y firewalls, pero sobre todo nuestra atención debe estar enfocada en lo que estamos haciendo para mitigar este delito que debe llevarse desde el control hasta la recuperación en caso de que se haya perpetrado un ataque, entre las políticas básicas de seguridad tenemos las siguientes:

Prevención: Poner especial atención en la actualización de antivirus, estar atentos a los enlaces que aparecen en correos electrónicos, Evitar cualquier circunstancia en la que podamos entrar en peligro.

Detección: Estar seguros que contamos con las herramientas adecuadas para la detección de ataques. En este sentido, lo mejor es utilizar una herramienta antivirus que también nos ofrezca la posibilidad detectar intrusiones en la red.

Recuperación: Este ítem implica la creación de copias de seguridad de todos nuestros documentos, así como el inmediato cambio de todas las contraseñas que utilizamos para los servicios de Internet y demás. Lamentablemente, lo más probable cuando se detecte una violación, es que tengamos que tomar medidas drásticas, y es por ello que las mencionadas copias de seguridad son esenciales para recuperar el buen funcionamiento de nuestras actividades. https://www.tecnologia-informatica.com/vulnerabilidades-informaticas/

Ciertamente, de las tres recomendaciones mencionadas, la prevención y la detección son a las que debemos prestar más atención ya que, la recuperación de los datos puede ser una tarea desagradable y que nos demande mucho tiempo en realizar, y no siempre podremos volver exactamente al lugar en que nos encontrábamos.

PANAMÁ COMO CENTRO FINANCIERO INTERNACIONAL Y LA VULNERABILIDAD ANTE FRAUDES FINANCIERO

La tradicional condición de Panamá como un país de paso, **"un hub" (centro de conexiones)** aérea, , comercial, logístico, financiero y marítimo con alcance global, y una de las economías de mayor crecimiento en los últimos años en América Latina, le exponen más que otras naciones al impacto del fraude financiero y de los ciberataques, reconocieron hoy en expertos en el tema.

En panamá existe **la Comisión de Seguridad Informática de la Asociación Bancaria de Panamá (ABP),** expertos explican que la exposición al fraude financiero afecta a Panamá por ser un país de tránsito y por la migración que existe en este tipo de delitos.

Dentro del grupo de instituciones financieros, los bancos son los más sensibles a los ciberataques, según lo señalado los expertos en ciberseguridad de la Organización Internacional Crime Stoppers, ahora con presencia en Panamá, que buscan capacitar al sector financiero sobre la lucha en contra del blanqueo de capitales y de la protección de datos sobre finanzas y comercio, quienes le recomendaron a las empresas e instituciones a invertir más en seguridad y que la misma podría ser garantizada a través de la cultura de la prevención.

La Autoridad de la Innovación Gubernamental (AIG) de Panamá ha sido relevante para ayudar a los bancos a detener los ataques, al hacerse una especie de filtrado al pasar la fibra óptica por Panamá, y a fin que no sea afectado el país. Detalló que han intentado emplear esta modalidad de fraude no sólo con entidades bancarias, sino también del gobierno.

Panamá por su posición necesita de una protección especial al tener un sistema financiero en el que hay cerca de 80 bancos con licencia General e Internacional radicados, lo que lo convierte en un sector interesante para el ataque por parte de los ciberdelincuentes. Por lo que es muy importante para nosotros contar con esta legislación, y al ser Panamá un **"Hub financiero"** (centro financiero) de América, ya que el fraude cada año se está duplicando y es importante que el presupuesto en materia de seguridad se incremente para contar con las herramientas adecuadas que permitan cumplir con esta tarea.

CAUSAS DE LAS VULNERABILIDADES DE LOS SISTEMAS INFORMÁTICOS

- Debilidad en el diseño de los protocolos utilizados en las redes.
- Errores de programación.
- Configuración inadecuada de sistemas informáticos.
- Políticas de seguridad deficientes o inexistentes.
- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
- Disponibilidad de herramientas que facilitan los ataques.
- Limitación gubernamental al tamaño de las claves criptográficas y a la utilización de este tipo de tecnologías.
- Existencia de "puertas traseras" en los sistemas.
- Descuido de los fabricantes.

DIFERENCIA ENTRE VULNERABILIDAD, RIESGOS Y AMENAZAS EN LOS SISTEMAS INFORMÁTICOS

El riesgo es la posibilidad de que la amenaza se accione, lo que expone una relación directa entre vulnerabilidad, amenaza y riesgo, sin que ello signifique lo mismo, ni tampoco que las mismas se generen de manera inmediata.

Una amenaza a un sistema informático es una circunstancia que tiene el potencial de causar un daño o una pérdida de datos. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo. sin embargo, el desarrollo de una amenaza (virus) conduciría a un daño determinado, aunque existen daños que pueden ser subsanados.

Sin embargo, el hecho de que la vulnerabilidad exista, no quiere decir que el sistema este dañado, sino de que posee un punto determinado donde se puede accionar una amenaza y la misma ocasione un daño.

La compañía ESET, líder en detección proactiva de estas amenazas, experto en ventas antivirus, soporte técnico y Protección avanzada de sistema de internet reveló que Panamá mantiene una tendencia al alza en vulnerabilidad de sistemas informáticos.

El ingeniero Luis Lubeck, (Security Researcher) especialista en seguridad informática de la compañía ESET, señaló que en 2018, en Panamá se detectó un 80% de amenazas a sistemas, asegurando que este 2019, continúa esta vulnerabilidad, por tal razón se mantienen desarrollando productos de seguridad informática, con enfoque en la detección de amenazas informáticas, para diversas plataformas.

DELITO DE ESTAFA CIBERNÉTICA Y SUS CARACTERÍSTICAS

Uno de los hechos más relevantes del delito cibernético en el continente se dio a conocer en julio del 2016, cuando dos delincuentes nigerianos se declararon culpables del DELITO DE ESTAFA, por medios de transferencia electrónica en diciembre del mismo año, por un Juez Federal de los Estados Unidos que los condenó a 36 meses de prisión.

Este delito o crimen comenzó cuando esta organización criminal de sudafricanos inician una relación por medio de las redes sociales con una mujer de unos 50 años, de nacionalidad norteamericana, de la ciudad de Texas, la cual se encontraba infeliz en su matrimonio y buscaba con quien conversar por los traumas emocionalmente que había sufrido por más de 10 años, elemento que fue aprovechado por los delincuentes, quienes al tiempo comenzaron a mandarse fotos y a conversar con frecuencia de tema tanto personales como financieros, los cuales les sirvieron a los sudafricanos para estudiar más a fondo a la su víctima, al punto que la solitaria mujer llego a enamorarse, sin embargo con la promesa de verse pronto pero en medio de esas conversaciones el hombre le dijo que estaba desarrollando un proyecto de construcción y que para terminarlo necesitaba $30 mil dólares lo cual fue enviado por la víctima por medio de un giro bancario, con la promesa que se los pagaría a las semanas siguientes, lo cual nunca hizo por supuestamente estar en aprietos razón por la cual le volvió a pedir otra cantidad de dinero esa vez superior y cada vez mucho más, teniendo como excusa que apenas resolviera eso inconveniente de encontrarían,

dándose esta situación por dos años, y siendo esta situación alertada por el asesor financiero de la víctima por sospechas fraude, quien analizó el comportamiento y alentó a su cliente a que lo denunciara a las autoridades. Esta modalidad de estafa se le conoce como estafadores románticos, quienes operan de la misma manera, con los mismos argumentos y sus victima tiene el mismo perfil. Desde el 2016 se dio un aumento de denuncias clasificadas como estafas románticas, lo cual se ha incrementado en especial en los Estados Unidos.

Las pérdidas asociadas con esta actividad delictiva han superado los $230 millones de dólares y el mayor número de víctimas son en los Estados de: California, Texas, Florida, Nueva York y Pensilvania. El año pasado en Texas, el Internet Crime Complaint Center (IC3) adscripto al F.B.I. recibió más de 1,000 quejas de víctimas que reportaron más de $16 millones en pérdidas relacionadas con estafas románticas.

Los elementos típicos que integran el delito de estafa informática son:

- La manipulación informática y artificio semejante,
- transferencia patrimonial no consentida por el titular del mismo,
- ánimo de lucro y perjuicio en tercero.

El ánimo de lucro es elemento subjetivo del injusto que consiste en el propósito o intención del delincuente de conseguir un beneficio o ventaja económica.

El concepto de manipulación informática puede definirse como la introducción, alteración o supresión indebida de datos informáticos, especialmente datos de identidad, y la interferencia ilegítima en el funcionamiento de un programa o sistemas informáticos, cuyo resultado sea la transferencia no consentida de un activo patrimonial en perjuicio de tercero. Por tanto, queda incluido en el término la introducción de datos falsos, la introducción indebida de datos reales, la manipulación de los datos contenidos en el sistema, así como las interferencias que afectan al propio sistema.

La transferencia de un activo patrimonial consiste en el traspaso fáctico de un activo; esto es, una operación de transferencia de un elemento patrimonial valorable económicamente que pasa del patrimonio originario a otro, no teniendo necesariamente que producirse por medios electrónicos o telemáticos.

CONCLUSIÓN

Luego de lo expuesto, podemos concluir que la vulnerabilidad de los sistemas informáticos corresponde a una debilidad que ocurre por la exista una amenaza, lo que implica que se debe condicionar el sistema integral de tal manera que no se viole ninguno de sus aspectos, tales como confidencialidad, disponibilidad de la información, integridad, control de accesos a la base de datos u otros apartados del sistema.

Dentro del análisis, es preciso que tanto las entidades gubernamentales, el sector financiero y los usuarios tenga claro las terminologías de vulnerabilidad, amenaza y riesgo, pues son diferentes y además el hecho de su existencia condiciona la operatividad efectiva de los sistemas, principalmente porque la vulnerabilidad casi siempre son el resultado de fallos existentes en el diseño creado del sistema, sin embargo, también pueden ser originarias de la inexistencia de un sistema seguridad con base en la inversión en prevención.

Por su parte, una amenaza en los sistemas tiene que ver más con el entorno permisible que da lugar a que se produzca o genere una violación del sistema, ya sea por modificación, intercepción, fabricación e interrupción, entre otras circunstancias. Y por otro parte el riesgo, es la probabilidad de que la amenaza ocurra.

Por lo tanto, el hecho de que exista una vulnerabilidad determinada, no condiciona el hecho de un daño, sin embargo, podría generar o propicia inseguridad representativa tras su uso, lo que puede dar paso a las amenazas y además riesgos contraproducentes de daños tangibles e intangibles de los sistemas de información.