INVESTIGACIÓN SOBRE EL HACKER Y SUS POSIBLES COMIENZOS EN LA COMUNIDAD ESTUDIANTIL.

CASO UNIVERSIDAD PILOTO DE COLOMBIA

Gloria Hazlady Cornejo Suarez
Sandra Lorena Manchola

Proyecto de Grado

Universidad Piloto de Colombia
Facultad de Ingeniería De Sistemas
BOGOTA D.C
2015

Investigación sobre el hacker y sus posibles comienzos en la comunidad estudiantil.

CASO UNIVERSIDAD PILOTO DE COLOMBIA

Gloria Hazlady Cornejo Suarez
Sandra Lorena Manchola

Proyecto de grado

Asesor:
Oscar Elías Herrera Bedoya

Universidad Piloto de Colombia
Facultad de Ingeniería De Sistemas
BOGOTA D.C
2015

AGRADECIMIENTOS

Los autores agradecen a la Universidad Piloto de Colombia, por ser guía en los conocimientos aprendidos y la formación académica dada durante todo el proceso de la carrera, a todos los que nos apoyaron en el transcurso y desarrollo de este proyecto en especial a el ingeniero Oscar Elías Herrera Bedoya, por la confianza, guía y contribución dadas en toda esta investigación.

Principalmente dar gracias a nuestros padres por el esfuerzo continuo y apoyo dado a lo largo de toda la carrera, por ser la primeras personas en confiar en nosotras y siempre darnos una motivación diaria para continuar en este enriquecedor camino recorrido, a nuestros profesores, compañeros de trabajo, estudio, por su colaboración en todo el proceso de formación profesional. Por ultimo a todas aquellas personas que aportaron de una u otra manera en dar una parte de su tiempo para ayudarnos a salir a delante, en especial aquellas personas que ya no están con nosotras pero que desde el cielo hacen todo para que las cosas salgan bien y nos seguirán acompañando por siempre.

Sandra Lorena Manchola, Gloria Hazlady Cornejo Suarez

El camino a la excelencia no tiene límite de velocidad.

David Johnson

Tabla de Contenido

Lista Especiales

1 GLOSARIO

- DELITOS INFORMÁTICOS: Es una acción, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

- HACKER: Es alguien que descubre las debilidades de un computador o de una red informática. también es alguien con un conocimiento avanzado de computadoras y de redes informáticas

- CRACKER: Conjunto de personas que aprovechan su conocimiento y el uso masivo de la tecnología para ingresar ilegalmente a información que es de carácter privado para cierto grupo de personas

- HACKER DE SOMBRERO GRIS: Es una clase de hacker que se dedica tanto a la obtención y explotación de vulnerabilidades como a la defensa y protección de sistemas.

- ÉTICA PROFESIONAL: Pprincipios y reglas éticas que regulan y guían una actividad profesional. Estas normas determinan los deberes mínimamente exigibles a los profesionales en el desempeño de su actividad.

- SEGURIDAD INFORMÁTICA: Es la rama de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta.

- INNOVACIONES TECNOLÓGICAS: Tecnología que permiten diseñar y crear bienes, servicios que facilitan el día a día de una comunidad, necesidades o deseos de la humanidad.

- SOFTWARE: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

- CIBERCRIMEN: Este concepto se utiliza para definir actividades delictuales realizadas con la ayuda de herramientas informáticas.

- VULNERABILIDAD INFORMÁTICA: Es una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad de sus datos y aplicaciones.

2 Resumen

Este trabajo se basa en presentar un estudio que explora la disposición de los estudiantes de los programas de Ingeniería de Sistemas, Ingeniería de Telecomunicaciones y la Especialización de Seguridad Informática de la Universidad Piloto de Colombia a participar en actividades relacionadas con delitos informáticos o una cultura hacker, teniendo en cuenta principalmente su entorno académico y la relación con los docentes. Identificando cuales cuáles pueden ser las iniciativas que tienen los estudiantes de las carreras mencionadas anteriormente para querer aprender y buscar información sobre actividades en delitos informáticos. También llegando más a fondo y observando como los docentes de la Universidad Piloto de Colombia son una guía ética adecuada para que los estudiantes no adopten actividades relacionadas con el delito informático o por el contrario el conocimiento aprendido durante la formación académica puede conllevar a estos jóvenes a que actúen y generen iniciativas hacia el delio informático. Por ultimo analizar como el profesional en seguridad informática evidencia el tema planteado en la realidad laboral del día a día.

3 INTRODUCCIÓN

En el día a día de la sociedad se generan desarrollos e innovaciones que han modificado para siempre sus hábitos y relaciones personales como es el código de barras, el cual ha cambiado el modo en que se compra, ya que permite acceder a los detalles de un producto, también están las redes sociales como lo son Facebook, WhatsApp, MySpace, etc., que han revolucionado la forma en que las personas se comunican y se ha vuelto muy útil en el campo personal, laboral, social, entre otras, además y de gran importancia es la que se conoce como la nube, que se convierte en sitios de almacenamiento de archivos, compartición de información y el cual es uno de los avances informáticos más importantes que cambiaron el mundo, al poder acceder a la información desde cualquier sitio, igualmente la www (World Wide Web) que es el sistema de distribución de información, basado en hipertexto a través de internet, que revolucionó y modificó para siempre los hábitos y relaciones entre personas, por último se nombra la tecnología GPS, la cual capta la posición exacta en cualquier lugar del planeta, se utiliza en coches, aviones y barcos, también llega a ser utilizada por científicos, estos se lo ponen a las tortugas para ver de dónde a donde migran.

En el día a día de la sociedad, se ve un manejo en la innovación y comunicación de las tecnologías, para el aprovechamiento de la misma, observando como esta se vuelve cada vez más tecnológica, llegando a un desarrollo de gran relevancia para las comunidades, y aunque en un principio a la palabra hacker[1], se le dio el significado de personas que tienen habilidades informáticas para desarrollar software, que trabajase para innovación tecnológica y desarrollo de nuevas aplicaciones, las cuales beneficiaran a la sociedad en todo aspecto, tanto tecnológico, económico, social y comunicativo, creando así el desarrollo de software, con el cual se llegó a grandes creaciones que ahora son el diario vivir, como lo es la trasmisión de la información, las redes de comunicación electrónica, que ahora se utilizan (chats, correos electrónicos, etc.).

Dentro de este popurrí de desarrollos e innovaciones aparece el término hacker[2], los llamados de forma correcta o equivocadamente, que en su mayoría son los autores de los crímenes informáticos que se benefician del desconocimiento, del avance de la tecnología y muchas veces de las vulnerabilidades que tiene la

[1] *Red Hat Enterprise, Amenazas a la Seguridad de la red {En línea}.:http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-risk.html*

información, y que en manos inadecuadas pueden llegar a generar daño social, como el acceso a sistemas informáticos de entidades, sobre todo de grandes corporaciones y que en la actualidad tiene un auge de política anti estatal y anticapitalista.

Esa graduación en la intención de los actos, clasifica a los hackers en dos principales grupos a los que se les conoce como “hacker de sombrero negro” o sinónimo de “cracker” quienes aprovechan su conocimiento y el uso masivo de la tecnología para ingresar ilegalmente a información que es de carácter privado para cierto grupo de personas, con el fin de un beneficio ya sea propio o como encargo de un tercero (valor mercantil de la información), es allí donde muchas veces se generan preguntas relacionadas con los principios éticos de estas personas, y la manera de utilizar la informática que tienen o el conocimiento informático o de telecomunicaciones para realizar un mal a un grupo social, ya que buscan el camino de menos resistencia y que tenga vulnerabilidades o que se haya cometido errores humanos para realizar un ataque o generar virus, también existe los hacker de “sombrero gris” quienes utiliza una ética ambigua, ya que penetran sistemas, hacen el daño y luego ofrecen su conocimiento para reparar dichos daños. Y por último el hacker de sombrero blanco que explotan las vulnerabilidades de los sistemas con fines académicos y con el único fin de fortalecerlo contra los otros tipos de hackers, usualmente consultores e investigadores en temas de seguridad.

Con todo ello se ve una ambigüedad en que la tecnología avanza para bien y para mal de una sociedad y es importante entonces emprender una investigación que permita detectar la disposición de los estudiantes universitarios, inicialmente de Ingeniería de Sistemas, Ingeniería de Telecomunicaciones y la Especialización de Seguridad Informática a ser parte de una comunidad hacker y si esa disposición existiera, si los conocimientos adquirido serán explotados positiva o negativamente.

Se busca entonces detectar en estudiantes universitarios, actos propios de la cultura hacker, ya sea desde el aprendizaje curricular, desde su auto-aprendizaje o como la comunidad educativa pueda influir en el que se generen estos intereses que sin la guía ética adecuada pueden culminar en actividades relacionadas con el delito informático. Así mismo se evalúa la perspectiva de expertos reconocidos en seguridad informática y que de forma habitual tienen contacto con esta cultura.

Ejemplo de ello son muchos casos entre los que se puede nombrar y ver los hacker colombianos con gran controversia en el territorio es el caso de el hacker **Andrés Sepúlveda,** que también se ha vinculado con el caso Andrómeda, al ser

un caso de espionaje e interceptaciones telefónicas ilegales, que hacia la inteligencia del ejército, el cual había montado un centro de inteligencia camuflado dentro de un centro de cómputo, en donde se hacía seguimiento a los correos electrónicos y a los chats de varios personajes de la vida pública. Se habla que el ejército recluto hackers civiles como lo es Andrés Sepúlveda, para apoyar las labores de monitoreo e interceptaciones de comunicación. Este caso es de gran importancia y aun no se ha conocido la verdad de todo, pero se ve aun expuestos personajes muy importantes como lo es el ex candidato presidencial uribista Óscar Iván Zuluaga, Gustavo Petro, y a otras personalidades de la sociedad colombiana.

Otro de los personajes, que ha sido noticia por hackeo es **Kevin Mitnick,** conocido como “El Cóndor” y calificado como el criminal informático más buscado de la historia de EEUU. Mitnick cobró fama a partir de los años 80, cuando logró penetrar sistemas ultra protegidos como los de Nokia y Motorola, robar secretos corporativos y hasta hackear a otros hackers. Tras su puesta en libertad en 2002 se dedica a la consultoría y el asesoramiento en materia de seguridad, a través de su compañía Mitnick Security. En otro de los casos se conoce al hacker **Adrián Lamo,** que es conocido en el mundo informático como “El hacker vagabundo”, por realizar todos sus ataques desde cibercafés y bibliotecas; su trabajo más famoso fue la inclusión de su nombre en la lista de expertos de New York Times y penetrar la red de Microsoft. También adquirió fama por tratar de identificar fallas de seguridad en las redes informáticas. Y por último nombraremos a dos personajes como **Jonathan Jamesq,** quien atacó las redes de del Departamento de Defensa de los Estados Unidos y la Nasa, donde robó software, evaluado en más de un millón de dólares, y a **Robert Tappan Morris,** que creó un virus informático que infectó a cerca de seis mil grandes máquinas Unix, haciéndolas tan lentas que quedaron inutilizables, causando millonarias pérdidas. Otro de los casos de gran importancia que ha sucedido en los últimos días y que no se puede dejar de mencionar, es sobre la violación de la privacidad y el estado de vulnerabilidad de la información personal, se referirse a lo sucedido con **iCloud,** el cual utilizaba un script Pyton en Github, que permitía de forma maliciosa a los usuarios usar fuerza bruta para obtener la contraseña de iCloud de una cuenta. Este script utilizaba una vulnerabilidad de Find My Phone, la aplicación que permite localizar el móvil de forma remota, que adivina contraseñas de forma repetida hasta que logra dar con la correcta. Pero la vulnerabilidad de Find My Phone hizo que se hackeara dichas cuentas y así filtrar imágenes desnudas de celebridades.

Es por ello, que este trabajo está orientado, principalmente, a una investigación de carácter teórico-exploratoria que realiza un análisis de campo en un entorno conocido, para dejar ver el valor de una cultura hacker orientada a sus aspectos

negativos, entre ellos los inicios del hacker o de delitos informáticos que se están presentando en jóvenes a temprana edad, el medio educativo en el que se desenvuelven, conociendo desde su aprendizaje propio e interés de aprender, hasta saber cómo la sociedad educativa puede llegar a manejar y detectar este tipo de situaciones en jóvenes estudiantes según el aprendizaje desarrollado. De igual forma dar a conocer la importancia de la seguridad de la información, el campo social, económico, política y de la privacidad. Observando como problema las acciones de los hackers o “piratas informáticos” también se quieren evaluar la perspectiva que tiene el experto en seguridad informática y que a diario tienen conocimiento del hacker Colombiano. La construcción social de la tecnología, para dar usos y dinámicas colectivas para el desarrollo de la sociedad de la información y el desarrollo así mismo del daño informático.

Los limites que se presentan en este proyecto, está delimitado por la documentación con veracidad eficaz, para que se pueda llevar un análisis e investigación más exhaustivas, otro de los obstáculos, es que este tipo de personas no es fácil de evidenciar o ser expuestos y consultados de forma explícita, es por ello que se debe ser cuidadoso en estructurar las encuestas con un lenguaje cercano y teniendo cuidado en no generar juicios de valor previos o segar las respuestas del encuestado y siempre garantizando confidencialidad en la información.

4 MARCO TEÓRICO

4.1 Antecedentes y contexto

Etimológicamente, "la palabra hacker deriva del vocablo inglés “hack” (cortar, golpear), el cual comenzó a adquirir su primera connotación tecnológica a principios del siglo XX, cuando pasó a formar parte de la jerga de los técnicos telefónicos de los EU, quienes en ocasiones lograban arreglar de inmediato las cajas defectuosas mediante un golpe seco, un hack”[3]

En los años 60, la palabra hacker se utilizó cuando se desarrolló sistemas eléctricos para ferrocarriles, quienes en la construcción utilizaron palabras como 'tunnel hacking', para definir a sus travesías, las cuales tenían un acceso dentro del campus; burlando puertas y barricadas.

Al principio de la masificación del término con una connotación negativa los hackers básicamente eran programadores que descubrían soluciones brillantes o que resolvían problemas de gran complejidad. “Algunas de las personas que crecieron en la cultura de los auténticos programadores permanecieron en activo hasta bien entrados los 90.

“Algunas de las personas que crecieron en la cultura de los Auténticos Programadores permanecieron en activo hasta bien entrados los 90. Seymour Cray, diseñador de la gama de supercomputadoras Cray, fue uno de los mejores. Se dice de él que, en cierta ocasión, introdujo de principio a fin un sistema operativo de su invención en una de sus computadoras, usando los conmutadores de su panel de control.”[4]

Otra parte importante de la historia de los programadores es

> “*ARPANET fue la primera red intercontinental de alta velocidad. Fue construida por el Departamento de Defensa estadounidense como un experimento de comunicaciones digitales, pero creció hasta interconectar a cientos de universidades, contratistas de defensa y centros de*

[3] *LIZAMA, Jorge Alberto. Hackers En El Contexto De La Sociedad De La Información. México. 2005. 81P.*

[4] *RAYMOND Eric S. Breve historia de la cultura hacker {En línea}. {25 septiembre de 2014}. Disponible en: (http://biblioweb.sindominio.net/telematica/historia-cultura-hacker.html).*

> *investigación. Permitió a investigadores de todas partes intercambiar información con una rapidez y flexibilidad sin precedentes, dando un gran impulso a la colaboración y aumentando enormemente el ritmo y la intensidad de los avances tecnológicos.*"[5]

Pero después de ello el código de programación dejo de ser tan exclusivo y se empezó a hablar de código abierto que es el que conocemos hoy en día. Por ello, el término hackers requiere ser revisado y vuelto a construir desde una perspectiva integral, para así rescatar los principales problemas, soluciones y significados que como comunidad atribuyen a la tecnología; esto a fin de no caer en el ejercicio sobre el cual advierte Knightmare (1994), en el sentido que la mayor parte de las personas: "mezcla realidad y fantasía para configurar distintos modelos de hackers de acuerdo a sus propios deseos."[6]

El término hacker tiene varias definiciones en donde "Jargon File (o The New Hacker's Dictionary)"[7], recoge información específica de los hacker.

Para el Jargón File, el término hacker refiere:

> "(Originalmente, alguien que hace que algo funcione mediante un golpe seco) 1. Una persona que disfruta explorando los detalles de los sistemas de programación y cómo utilizar todas sus capacidades, al contrario que la mayoría de los usuarios, que prefieren aprender sólo el mínimo indispensable. 2. Alguien que programa con entusiasmo (incluso obsesivamente) o que disfruta programando más que estudiando teoría. 3. Una persona capaz de programar rápidamente. 4. Un experto en un programa específico, o alguien que frecuentemente trabaja con él, como "un hacker de Unix". 5. Un experto o entusiasta de cualquier clase. Uno puede ser un hacker de astronomía, por ejemplo. 6. Alguien que disfruta el desafío intelectual de superar ciertas limitaciones mediante la creatividad. 7. (depreciado) Un intruso malicioso que trata de descubrir información importante explorando un sistema. Alguien que

[5] *RAYMOND Eric S., Breve historia de la cultura hacker {En línea}. {25 septiembre de 2014}. Disponible en: (http://biblioweb.sindominio.net/telematica/historia-cultura-hacker.html).*
[6] *LIZAMA, op. Cit, p.79*
[7] *RAYMOND, Eric (2003). "The New Hacker's Dictionary". {En línea}. {25 septiembre2014}. Disponible en: (http://www.tuxedo.org/~esr/jargon/jargon.html).*

> por lo tanto es un ‘password hacker’ o un ‘network hacker’. Sin embargo, el término correcto en este sentido es cracker.”[8]

Después de dar una breve descripción sobre los hacker, también se debe hablar de la primera comunidad de hackers de la historia, la cual es Old school hackers que tuvo su origen en el sistema de universidades norteamericanas dedicadas al desarrollo de la Arpanet. Sus integrantes, conocidos como old school hackers, se caracterizaban por contar con un gran respaldo de recursos tecnológicos, entre los cuales destacan:

A. Una infraestructura tecnológica de punta.
B. Un alto nivel de financiamiento destinado a la investigación y/o innovación tecnológica.
C. Acceso libre a los recursos de información-conocimiento sobre la programación y comunicación en red
D. Producción de conocimientos respaldados y prestigiados institucionalmente.

Luego de hablar en general de los hacker se debe mencionar que estos a su vez se subdividen en:

- **White hat hackers (hackers de sombrero blanco),** que no causan daño a las redes digitales y que están integrados por:
  - Samurais, los cuales practican el intrusismo informático amparados por la ley o por autorización expresa la razón, normalmente son contratados para investigar fallos de seguridad.
  - Sneakers, que practican el intrusismo informático sin contar con el amparo de la ley o una autorización expresa, su propósito es probar la seguridad de la red en cuestión sin causar daños tecnológicos o económicos.
- **Gray Hat (hacker de sombrero gris),** es una clase de hacker que “se dedica tanto a la obtención y explotación de vulnerabilidades como a la defensa y protección de sistemas, por lo tanto puede decirse que un Gray Hat, frecuentemente está catalogado como un hacker con habilidades

[8] *RAYMOND, Eric (2003). “The New Hacker’s Dictionary”. {En línea}. {25 septiembre2014}. Disponible en: (http://www.tuxedo.org/~esr/jargon/jargon.html).*

excepcionales y que sus actividades se encuentran en algún punto entre las desempeñadas por los white hackers y los black hackers."[9]

- **Black hat hackers o cracker (hackers de sobrero negro),** que buscan causar algún tipo de daño a las redes digitales y que están comandados por los:
  - Larval hackers, aprendices de internet hackers con recursos limitados y que no se apegan a la ética hacker. Practican el intrusismo informático para demostrar públicamente sus conocimientos.
  - **Lammer** "Es el que se cree Hacker y no tiene los conocimientos necesarios ni la lógica para comprender que es lo que realmente está sucediendo cuando utiliza algún programa ya hecho para hackear y romper alguna seguridad. Es el que ha bajado cientos de libros y videos de sitios donde se propaga la piratería de diversos temas de hacking."[10] Este tipo de hacker presume saber y conocer bien del tema pero casi siempre cae en actividades que no llegan a nada ni logra causar daño.

4.1.1 Hacker sombrero negro

Como se explicó anteriormente en la categoría de grupos de hackers, el más negativo es al que se le conoce como de sombrero negro o cracker, a este grupo es el que más se le teme. Este hacker utiliza su ingenio para penetrar redes "seguras" sin autorización y hacer daño a información valiosa la cual terminan siendo inutilizable. En su proceso de realizar el delito se pueden visualizar tres pasos:

- **Elección de un objetivo:** En este paso el hacker evalúa y visualiza el objetivo o red al cual va a realizar el daño ya sea por beneficio propio o interés económico o simplemente al azar." Luego, el hacker revisará los puertos de una red para determinar si es vulnerable a ataques, lo cual simplemente es probar todos los puertos de una máquina anfitrión en

[9] *Hacker en la red, Noticias y Educación sobre seguridad de la informática. {En línea} {30 septiembre de 2014}. Disponible en: (https://hackersenlared.wordpress.com/category/capacitacion/tipos-de-hackers/).*
[10] *Hacker en la red, Noticias y Educación sobre seguridad de la informática. {En línea} {30 septiembre de 2014}. Disponible en: (https://hackersenlared.wordpress.com/category/capacitacion/tipos-de-hackers/).*

busca de una respuesta. Los puertos abiertos son aquellos que respondan y que le permitirían a un hacker tener acceso al sistema."[11]

- **Recopilación de información e investigación:** En este paso el hacker busca la manera de como poder vulnerar el sistema ya sea haciendo lo que se conoce como ingeniera social, recolección urbana (buscar en un contenedor de basura).
- **Finalización del ataque:** En este paso el hacker vulnera el objetivo o red que había visualizado.

4.1.2 Hacker en la sociedad

Se empieza hablar de los hackers a partir del escenario tecnológico y social que trae consigo la sociedad de la información; el paradigma de desarrollo que mediante las nuevas tecnologías de comunicación e información y fundamentalmente a través de la internet, está transformando la dinámica de desarrollo de la economía, los servicios, la educación, la vida cotidiana e incluso la forma de relacionarse entre las personas.

Si bien históricamente el ideal de ciudadanía se ha vinculado fuertemente con la idea de contar con ciudadanos bien informados, ahora, en el contexto de la sociedad de la información, parece sumarse una nueva exigencia: "Ya no podemos decir que quien tiene la información tiene el poder (...) El problema está situado en la selección de la información más relevante para cada momento y en su procesamiento para aplicarla adecuadamente a cada situación."[12]

En este sentido, el ser humano, en virtud de que tiene que convivir con otros seres humanos, como entorno, debe aprender a vivir en convivencia, debe de ajustarse al conjunto de valores, principios y reglas que estructuran la vida en sociedad a fin de actuar correctamente.

4.1.3 Hacker Colombiano

Antes de introducirse en el tema del hacker colombiano, primero se debe entender el significado del hacker, la cual la podemos encontrar en la web como: "Hacker es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con la informática: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc. También referirse a cualquier

[11] *Wikipedia. Hacker (Seguridad Informática). {En línea} {30 septiembre de 2014}. Disponible en: (http://es.wikipedia.org/wiki/Hacker_ (seguridad_inform%C3%A1tica)).*
[12] *LIZAMA, op.cit, p.46*

profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas"[13].

Es por eso que en Colombia hay una diferencia de definición y actos de los hacker, ya que acá es llamado Hacker a criminales comunes dedicados al delito informático, también aquellas personas dedicadas hacer uso de conocimiento para afectar a los demás. En Colombia se ve al hacker como un criminal informático, realizando transferencias electrónicas de robos de tarjetas de crédito hacia diferentes cuentas en el país, afectando a personas de alto nivel u empresas que están en vulneración de un daño informático, estas son acciones de algunos delincuentes más en Colombia, delincuentes que hacen uso de herramientas informáticas para realizar sus actos criminales, es por ellos que el contexto de la palabra hacker se utilizara para este hacker criminal y también llamado hacker de sombrero negro o cracker .

Desde los principios de delitos informáticos en Colombia, se dio el caso de "Roberto Soto Prieto en 1984, por un robo millonario de 13.5 millones de dólares de la subcuenta de Colombia en el Chase Manhattan Bank y que se pensaba hacer de una cuanta del Fondo Andino de Reservas, entidad que administraba recursos de países del Grupo Animo"[14]. Roberto Soto se consideró como uno de los pioneros en operaciones fraudulentas con delitos informáticos en Colombia, ya que para ello contrato a un muy buen ingeniero de sistemas llamado Rodríguez Cristancho, quien para entonces era considerado la persona más calificada como técnico colombiano en sistemas y redes de computación, con el conocimiento de este ingeniero de sistemas el robo se realizó "a través de una red de pares aislados que cualquier técnico hubiese podido manipular y que desde Telecom permitió interceptar las líneas de télex del Banco de la República, y transferir fondos a cuentas cifradas."[15]

A través de tiempo en Colombia, los delitos informáticos hechos por hacker se volvieron un dolor de cabeza sobre todo para las entidades bancarias, ya que para esta se tienen cifras de pérdidas millonarias y se debe a problemas en los

---

[13] *Moreno David. Hacker en Colombia. Hacker {En línea}. {Agosto 10 2011}. Disponible en: (http://www.dragonjar.org/hackers-en-colombia.xhtml).*

[14] *Nullvalue, El Tiempo, Doce Secretos del Robo de US$ 13.5 Millones {En línea}. {9 enero de 2015}. Disponible en: (http://www.eltiempo.com/archivo/documento-2013/MAM-140569#).*

[15] *Ibíd.*

sistemas de seguridad de dichos bancos, el acceso a la base de datos de bancos por terceros y la clonación de tarjetas de crédito bancarias, estos son los problemas más grandes de los bancos respecto a delitos informáticos. Un ejemplo de estos delitos hechos por hackers de sombrero negro en entidades bancarias es el caso en Cali, cuando el delito se presenta por un mismo funcionario y trabajador de la entidad bancaria, ya que este hurtaba dinero a los usuarios por medios informáticos utilizando la falsedad de documento privado, "De acuerdo con la investigación, el hombre, en su calidad de ejecutivo, accedía a las cuentas de los usuarios suplantando su firma y su huella. Así, retiraba dinero que éstos poseían en sus cuentas. Desde el año 2009 hurtó a los clientes del banco $360 millones."[16] Así como este caso, en la entidad bancaria de Cali se presentan miles de denuncias al año en Colombia, por este tipo de hechos tanto que en la actualidad "se calcula que 187 denuncias mensuales son interpuestas por fraude a diferentes bancos."[17]

En los presentes estudios hechos por entidades que regulan los delitos informáticos como la Dijin, se ha confirmado que el delito informático en Colombia ha ido en aumento y también se habla de hacker, no solo en temas bancarios sino también en temas políticos, al igual que el avance de la tecnología ha dado nuevos dispositivos para hacer las acciones fraudulentas más fáciles como lo son Tablet, celulares, computadores, etc. Ya que la seguridad de estos dispositivos es casi mínima o a veces nula, siendo así un tema muy negativo en la sociedad colombiana.

El ataque cibernético en Colombia, deja perdida de los "400 millones de dólares cada año según Gonzalo, experto en seguridad de Olam ósea 45 dólares por victima"[18]. Pero esta cantidad de dinero que se da en pérdidas, se podrían ahorrar si Colombia implementa una buen plan de seguridad informática, que contenga políticas y productos, que detenga a estos delincuentes informáticos y más aún cuando en la sociedad ya es reducido la cantidad de personas que no tienen un

[16] Colprensa, El País, En Colombia las Cifras de Delitos Informáticos Van en Aumento Millones {En línea}. {9 enero de 2015}. Disponible en: (http://www.elpais.com.co/elpais/judicial/noticias/colombia-cifras-delitos-informaticos-van-aumento).
[17] Colprensa, El País, En Colombia las Cifras de Delitos Informáticos Van en Aumento Millones {En línea}. {9 enero de 2015}. Disponible en: (http://www.elpais.com.co/elpais/judicial/noticias/colombia-cifras-delitos-informaticos-van-aumento).
[18] RCN La Radio, Escuche el Informe Sobre Los Delitos Informáticos en Colombia Millones {En línea}. {9 enero de 2015}. Disponible en: (http://www.rcnradio.com/audios/escuche-el-informe-sobre-los-delitos-informaticos-en-colombia-28011).

teléfono celular o un computador en casa, en cifras del ministerio de tecnologías de la información y las comunicaciones el 72% de los hogares en Colombia tienen un computador, el 91% de las personas cuentan con un teléfono celular, el 55% posee un celular inteligente.

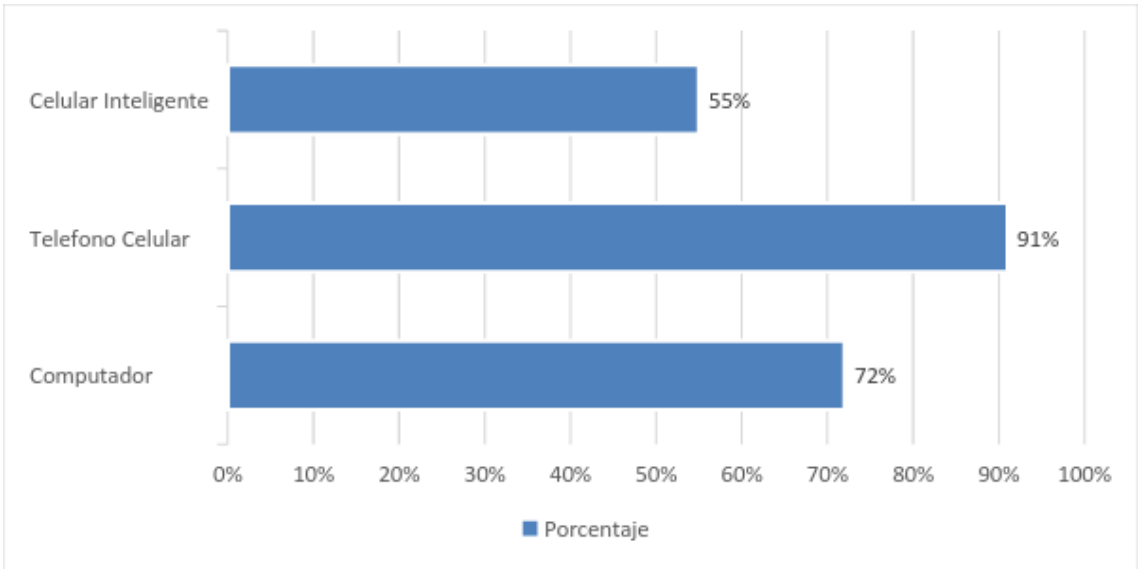


Ilustración 1 Grafica que muestra los equipos Tecnológicos que se encuentran en riesgo actualmente por el cibercrimen.

Según cifras de la Dijin indica que 8 de cada 10 colombianos está conectado a internet, lo que evalúa una gran cantidad de personas que diariamente están expuesta a riesgos de cibercrimen. La seguridad de estos dispositivos según Johan Triana, la mayoría de las personas dejan estos dispositivos como los sacaron del almacén o como se los entregaron de fábrica, pocos utilizan programas, pagan o instalan sistemas de seguridad, y aunque el computador es al que a veces las personas invierten en seguridad, muchos lo hacen de la forma inadecuada, bajando programas que son gratuitos y que no dan un sistemas de seguridad fiable ante el hacker, ahora mirando lo que son teléfonos celulares y Tablets para este tipo de productos los usuarios no dan ninguna protección a ellos.

Para darse cuenta un poco de los problemas que ahora se dan con la internet, la falta de seguridad y de conciencia que se da en Colombia, un ejemplo de ellos es

el de “Sandra Gutiérrez a la cual le robaron todos los contacto que tenían en un correo electrónico de hace 10 años lo que hicieron fue hackear su clave de ingreso al correo”[19], ahora ella misma da el testimonio de que lo que fallo, fue no tomar las recomendaciones que se hacen de cambiar la contraseña cada determinado tiempo. También un gran bum que se ha dado en Colombia, es el hackeo a personalidades reconocidas, como el hacker que se metió a la cuenta de twitter y mail del columnista de la revista semana y director de la revista Soho Daniel Samper Ospina, también un caso muy actual de septiembre de 2014 se encuentra el ataque al correo y computador de Humberto de la Calle que es el jefe negociador del Gobierno en el proceso de Paz en Colombia.

La causa de estos actos es que hay mucha desinformación sobre este tema y es por ello que hoy en día podemos encontrar anuncios como estos: necesito un “hackers” para sacarme de DataCrédito en Colombia o algo más sencillo como son los foros donde se pasan la vida debatiendo sobre quien en más el súper Cracker de la Web, aunque no se puede dejar de mencionar aquellos hackers que trabajan sin parar, para lograr de nuestra Colombia un país mejor, son aquellos que crean, investigan, desarrollan, proponen y unen esfuerzos, algunos de estos se le puede ver en grupos relacionados con la seguridad informática que se destacan en Colombia:

- •LowNoise Hacking Group
- •hackStudio
- •CUTeam
- •SinfoCOL
- •Comunidad DragonJAR

Como se puede ver ahí grupos en Colombia que ayudan a la seguridad de la información, pero también hay algunas instituciones académicas que realizan diferentes eventos relacionados con la seguridad de la información, donde se explica el modo de actuar de algunos delincuentes informáticos, se explica diferentes métodos de prevención para este tipo de ataques y las diferentes investigaciones y soluciones desarrolladas por nuestros Colombianos:

[19]RCN La Radio, Escuche el Informe Sobre Los Delitos Informáticos en Colombia Millones {En línea}. {9 enero de 2015}. Disponible en: (http://www.rcnradio.com/audios/escuche-el-informe-sobre-los-delitos-informaticos-en-colombia-28011).

- ACIS
- ACK Security Conference
- InForce Technology
- Security Zone

Gonzalo Berros, dice que hay un alto crecimiento de vulnerabilidad y registro de delitos informáticos “9 millones de personas en Colombia ha reportado ser víctima de cibercrimen, lo que quiere decir que esto va en aumento y que la penetración en internet está cerca del 50% en Colombia”[20] tanto así que Colombia es, actualmente, el tercer país en Latinoamérica donde más se cometen delitos informáticos, los más mencionados y que van en aumento son acceso a bases de datos sin permiso, sustraer archivos de computadores, ingresar a redes sociales, correos ajenos y clonar tarjetas bancarias.

Pero a causa de todo esto, no hay que olvidar que los avances tecnológicos y el oficio de este, por apropiarse ilícitamente del bien ajeno a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de información para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo.

En Colombia donde más es vulnerable la gente, es en las redes sociales, aun no se han tomado medidas preventivas para no exceder lo que se debe publicar, contar, dejar en la internet sin ninguna protección, tanto así que expertos de delitos informáticos tuvieron que ir a Puerto Asís, para investigar amenazas por red social de muerte a jóvenes y menores de edad, y aunque en principio se pensó que era broma, este tipo de amenazas en Facebook genero la movilización de autoridades locales, departamentales y nacionales. “El funcionario explicó que todo se inició el pasado 15 de agosto cuando fueron asesinados dos menores, de 16 y 17 años, cuando se movilizaban en una motocicleta entre los municipios de Caicedo y Puerto Asís.”[21] El mensaje, con una lista de nombres a los que les

[20] [20]RCN La Radio, Escuche el Informe Sobre Los Delitos Informáticos en Colombia Millones {En línea}. {9 enero de 2015}. Disponible en: (http://www.rcnradio.com/audios/escuche-el-informe-sobre-los-delitos-informaticos-en-colombia-28011)...

[21] *El Tiempo, Expertos en Delitos Informáticos Llegaron a Puerto Asis Para Investigar Amenazas por Red Social, {En línea}. {13 enero de 2015}. Disponible en: (http://www.eltiempo.com/archivo/documento-2013/CMS-7876787#).*

podía pasar lo mismo que a los dos menores de edad asesinados, empezó a ser divulgada por redes sociales, los expertos en seguridad informática llegaron hasta Puerto Asís para averiguar la procedencia de dichos mensajes.

Colombia en la actualidad también está sufriendo de los extranjeros que encuentran este país como una opción fácil para empezar sus delitos informáticos un ejemplo de esto es el de 'ciberhampa', él lo que hace es “Crear falsas cuentas gratuitas de wifi para robar claves, andan con equipos portátiles para tomar información que usuarios dejan en el ciberespacio cuando utilizan redes gratuitas en hoteles, centros comerciales y aeropuertos.”[22] La mayor parte de donde provienen estos extranjeros es de países de Europa los cuales ingresan por el caribe y así entrar al país haciéndose pasar por turistas.

La vulnerabilidad en Colombia se ha presentado más frecuentemente en edades entre los 28 años en adelante, ya que la falta de conocimiento y vacío en seguridad informática básica que se debe tener, son más vulnerables a los ataques de un hacker. De acuerdo con el más reciente Informe Global sobre Fraude de Kroll (Investigaciones internas y sobre fraude), “la mitad de las compañías se siente muy vulnerable al robo de información, y en aquellas que tienen más pérdidas por fraude, los autores más probables fueron ejecutivos de alto nivel (29%) o ejecutivos menores (8%)”[23].

[22] *El Tiempo, Así roba en Colombia el 'ciberhampa' europeo {En línea}. {18 enero de 2015}. Disponible en: (http://www.eltiempo.com/politica/justicia/delitos-informaticos-en-el-pais-habla-director-del-centro-cibernetico-de-la-dijin/14841739#).*

[23] *Caracol Radio, Tecnología, La Empresas Colombianas También son Vulnerables ante Delitos Informáticos, {En línea}. {13 enero de 2015}. Disponible en: (http://www.caracol.com.co/noticias/tecnologia/las-empresas-colombianas-tambien-son--vulnerables-ante-delitos-informaticos/20120523/nota/1693112.aspx#).*

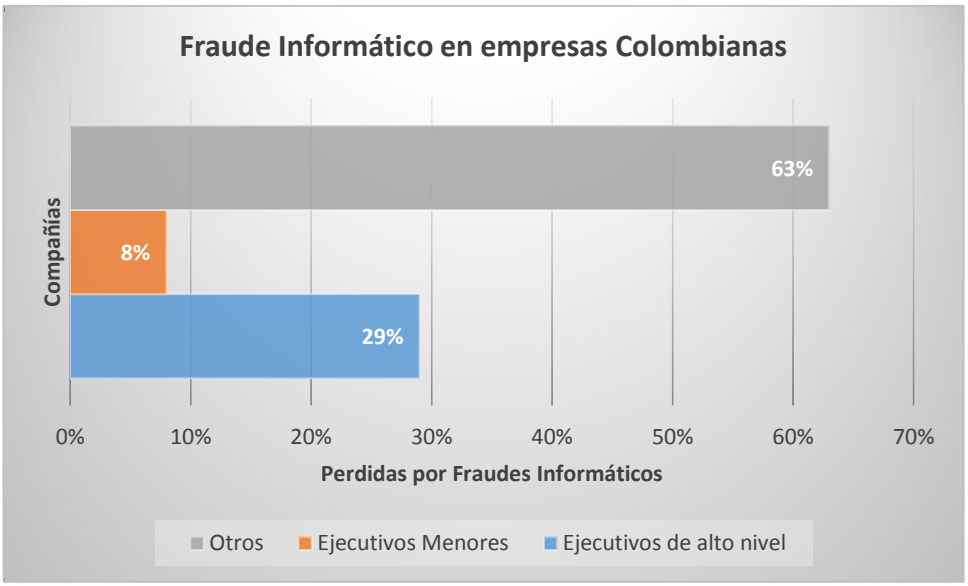


Ilustración 2. Grafica que muestra las compañías más atacadas por los hackers

También se observó los campos en los que se cometen los delitos informáticos realizados por hacker, en donde "la mayor incidencia en el robo de información y datos electrónicos, según el Informe Global sobre Fraude de Kroll 2011, ocurre en las empresas financieras (29%); de tecnología, medios y telecomunicaciones (29%); salud, farmacéuticas y biotecnología (26%); y servicios profesionales (23%). Las pérdidas por este tipo de delitos en las empresas, según el estudio, llegaron al 2.2% de sus ingresos."[24] Y se tiene conocimiento que en Colombia siete de cada 10 usuarios en internet son afectados y atacados por el delito informático, y esto también pasa porque "generalmente un 7% de la población de usuarios conectados a internet es un hacker en potencia. Cualquier persona con conocimientos de computación puede convertirse en un instante en un hacker, lo único que necesita es motivación para hacerlo."[25] Y las principales motivaciones de los hacker colombianos son. El dinero, resentimiento hacia una persona o hacia la empresa donde trabajo y por último el reconocimiento.

[24] *Caracol Radio, Tecnología, La Empresas Colombianas También son Vulnerables ante Delitos Informáticos, {En línea}. {13 enero de 2015}. Disponible en: (http://www.caracol.com.co/noticias/tecnologia/las-empresas-colombianas-tambien-son--vulnerables-ante-delitos-informaticos/20120523/nota/1693112.aspx#).*

[25] La F.M, Radio, Conozca el Perfil del Cibercriminal Colombiano *{En línea}. {13 enero de 2015}. Disponible en: (http://www.lafm.com.co/noticias/conozca-el-perfil-del-141939#).*

El perfil encontrado en Colombia tiene los siguientes conocimientos, habilidades y experiencia:

- Personas entre 18 a 40 Años de edad.
- Profesionales de ingeniería y afines.
- Conocimientos sólidos en programación, sistemas, DB, TIC.
- Conocimientos avanzados en Hacking.
- Conocimientos avanzados en metodologías de Testing de Seguridad, Pen Testing, plataformas, etc.
- Perfil de Atacante Social a través de técnicas avanzadas en ingeniería social.
- Perfil de Ciberespionaje, a través de técnicas avanzadas de espionaje en internet y a nivel empresarial.
- Conocimiento de herramientas, técnica de ataques, configuraciones, eventos, cursos relacionados con Hacking a sistemas Scada.
- Estudiantes potenciales interesados en el Hacking Underground. [Actividades Anónimas e ilícitas en el mundo de ataques informáticos].
- Personal descontento en las diferentes empresas de infraestructuras críticas, las cuales pueden suministrar información sensible de los sistemas críticos de operación.

En estadísticas en Colombia las áreas más afectadas y atacadas por los delincuentes son los cargos gerenciales, vicepresidenciales al igual que también las áreas que tienen que ver con el manejo de dinero y las que manejan la información de base de datos y automatización

El delito informático en Colombia, se observa un aumento, que se presenta muy frecuentemente por empleados que trabajan o que han trabajado para la empresa, corporación o compañía, ya que roban la información o los secretos corporativos de estos, para luego aprovecharse de ello y hacer daño, ya que cuentan con claves, muchas veces acceso que no fue cerrado al retirarse el empleado de la compañía, etc.

En la actualidad y lo analizado por parte del Grupo de Delitos Informáticos, se ha dado propuestas preventivas a los usuarios tanto de bancos, de dispositivos móviles, de la internet, etc. ya que para ellos las víctimas de estos delitos en su mayoría se da por descuidos de la misma, y es necesario que en la actualidad Colombia haga divulgación de prevención hacia estas conductas de los hacker,

además de ello, que las empresas adopten programas y personas calificadas en seguridad informática, para la protección de la información, para ellos es importante que los usuarios, empleados, etc. prevengan conductas que afectan y que llegan a ser objetivo de estos delincuentes informáticos , la seguridad en las cuentas de correos electrónicos y de redes sociales, que en la mayoría de veces, es por estos medios donde más circula la información que se necesita en una empresa o en los ciudadanos normales, los estudios hechos por la entidad de delitos informáticos de Colombia, asegura que detrás de estos delitos se encuentran grupos de criminales, que muchas veces se juntan con expertos en tecnología, el buen manejo de computadores y ahora celulares y tabletas.

Después de investigar sobre el hacker colombiano, de los grupos e instituciones que ahí en la prevención de la vulneración y daños relacionados con la información, también se debe mencionar sobre la juventud del hacker en Colombia, donde un ejemplo más claro es el del "Juan Sebastián Eljach es un bumangués de 15 años y es un 'hacker'**.** Su tío, Diego Sánchez, de 19 años, es su socio. Son de Bucaramanga, Santander, y crearon la primera 'universidad' virtual en español para aprender técnicas de ataque y defensa de sistemas informáticos. Se llama Exploiter.co y empezó a operar desde el pasado 3 de septiembre. Eljach empezó a estudiar lenguajes de programación a los 12 años y ha sido consultor de seguridad de empresas como Mejorándola y The Eagle Labs"[26].

Cuando estos tipos de casos se empezaron a dar en Colombia no se tenían leyes y para ahora cabe destacar de Colombia, que es uno de los pocos países que penaliza estos delitos informáticos, desde el 2009 amparado por la Ley 1273, denominada "de la protección de la información y de los datos" y la cual menciona que: "La pena mínima es de cuatro años de cárcel. Además, la ley establece que a quien se le impute este delito no tendrá la posibilidad de modificar la medida de aseguramiento, por tal motivo no tendrían beneficios como el de prisión domiciliaria"[27]. Y si este utiliza medios electrónicos para dicho fin se puede llegar a dar doce años de prisión. Tanto es así que la ley fue tan bien hecha que fue

[26] *El tiempo. Edgar. Tecnosfera, colombiano de quince años crea escuela para aprender a 'hackear'. {En línea}. {Enero 4 2015}. Disponible en: (http://www.eltiempo.com/tecnosfera/novedades-tecnologia/como-hackear-colombiano-de-quince-anos-crea-escuela-para-aprender-a-hackear/14575255).*

[27] *Martínez John Jairo. La patria.com. Colombia, el primer país que penaliza los delitos informáticos {En línea}. {Marzo 30 2012}. Disponible en: (http://www.lapatria.com/tecnologia/colombia-el-primer-pais-que-penaliza-los-delitos-informaticos-1980).*

considerada por el Congreso de la Fiadi (Federación Iberoamericana de Asociaciones de Derecho e Informática) en Santa Cruz de la Sierra, por todos los informáticos de América asociados a este organismo, como la mejor ley de delitos informáticos del continente.

"La Fiscalía actualmente tiene 23 grupos que combaten los Delitos Informáticos en todo el país y que se divide en la parte forense e investigativa. Según dicha dependencia, en las capturas que han hecho como mínimo siempre son detenidas 15 personas."[28]. Además, estos grupos que combaten los delitos informáticos, cuentan con la asesoría jurídica de firmas privadas especializadas en nuevas tecnologías y el apoyo técnico de laboratorios de cómputo forense que cuentan con la tecnología y el capital humano necesario para hallar evidencias digitales en procesos judiciales, en el que esté vinculado cualquier dispositivo que funcione digitalmente.

Aparte de las entidades mencionadas anteriormente también encontramos el CPP (Centro cibernético policial) en donde se encuentra el laboratorio de informática forense. "El CPP también cuenta con ocho laboratorios de informática forense distribuidos a nivel nacional y 25 unidades de delitos informáticos capacitadas y especializadas en atacar el cibercriminal"[29].

"En Bogotá laboran cerca de 120 funcionarios entre peritos, investigadores y analistas que se encargan de trabajar lo relacionado con el cibercrimen, mientras que a nivel nacional 150 personas entre peritos e investigadores."[30] Además las investigaciones realizadas por el CPP de puede ver que los delincuentes cibernéticos son personas que están en contacto muchas veces entre ellos ya que ''si hay una persona que conoce una vulnerabilidad la puede ofrecer a un grupo de delincuentes, los cuales buscarán a terceros. No obedecen a una misma línea, pero se pueden conectar al momento de cometer un delito','[31] ya que estos criminales se unen o forman jerarquías dentro de esta se encuentran las que colocan el dinero, después las que desarrollan la aplicación o software, dentro

[28] *Colprensa, El Universal, Fiscalía Advierte Aumento de Delitos Informáticos en Colombia Millones {En línea}. {9 enero de 2015}. Disponible en: (http://www.eluniversal.com.co/cartagena/nacional/fiscalia-advierte-aumento-de-delitos-informaticos-en-colombia-102898#).*

[29] *Inforlaft, Lo que Debe Saber Sobre el Cibercrimen en Colombia {En línea}. {18 enero de 2015}. Disponible en: (http://www.infolaft.com/es/art%C3%ADculo/lo-que-debe-saber-sobre-el-cibercrimen-en-colombia).*

[30] *Ibíd.*

[31] *Ibíd.*

todo el grupo también se encuentran las personas que buscan a la víctimas muchas veces por internet o a lo que se le conoce como la ingeniería social, y así se conforma todo un grupo organizado al delito informático y a las organizaciones creadas por lo hacker de sombrero negro para hacer daño.

Las victimas de estas personas pueden ser diversas, puede ser alguien del común para robarle cifras mínimas, empresas , personas famosas en las cuales afectan su honra, entidades del gobierno, también es un delito instalar software malicioso para espiar a una persona. Para ellos lo que importa es encontrar una puerta abierta para poder robar la información y hacer un supuesto uso beneficioso para ellos.

Según la fiscalía en los estudios realizados y la cifras de denuncias hechas las ciudades más afectadas en delitos informáticos son: “Bogotá, Costa Caribe, Cali, Medellín, Pasto y la zona Andina, aunque ninguna parte del país se salva de este tipo de delincuentes.”[32], aunque en estas ciudades, el proceso de investigación y el de prueba legal e informática es la principal dificultad para procesar este tipo de delitos. Para Iván Darío Marrugo, abogado especialista en Derecho de Telecomunicaciones, "Solo desde hace unos años tenemos una Ley de procedimiento administrativo (Ley 1437 de 2011) y el Código General del Proceso (Ley 1564) que abrió la posibilidad de admitir pruebas electrónicas en este tipo de juicios"[33]. Cabe destacar que aparte de la sofisticación alcanzada por las autoridades para perseguir este tipo de delitos, la cultura de denuncia de los ciudadanos ha aumentado.

Sin embargo, los expertos en el tema coinciden en que la tecnología va mucho más rápido que la legislación. En ese sentido, mientras se crean normas para atacar este tipo de delitos, surgen nuevas tecnologías para burlarlas y los criminales se aprovechan de esta situación.

Colombia con respecto a Latino América

[32] *Colprensa, El Universal, Fiscalía Advierte Aumento de Delitos Informáticos en Colombia Millones {En línea}. {9 enero de 2015}. Disponible en: (http://www.eluniversal.com.co/cartagena/nacional/fiscalia-advierte-aumento-de-delitos-informaticos-en-colombia-102898#).*

[33] *Pérez Camilo, Colombia digital, En Colombia se investigan los delitos informáticos {En línea}. {1 mayo de 2013}. Disponible en: (http://colombiadigital.net/actualidad/articulos-informativos/item/4810-en-colombia-se-investigan-los-delitos-informaticos.html).*

- Trojan WinLNK.Runner.bl ” se propaga vía dispositivos USB, lo que indica que los criminales cibernéticos que atacan en América Latina utilizan este medio como el principal vector para infectar a la mayor cantidad de personas posibles”[34]

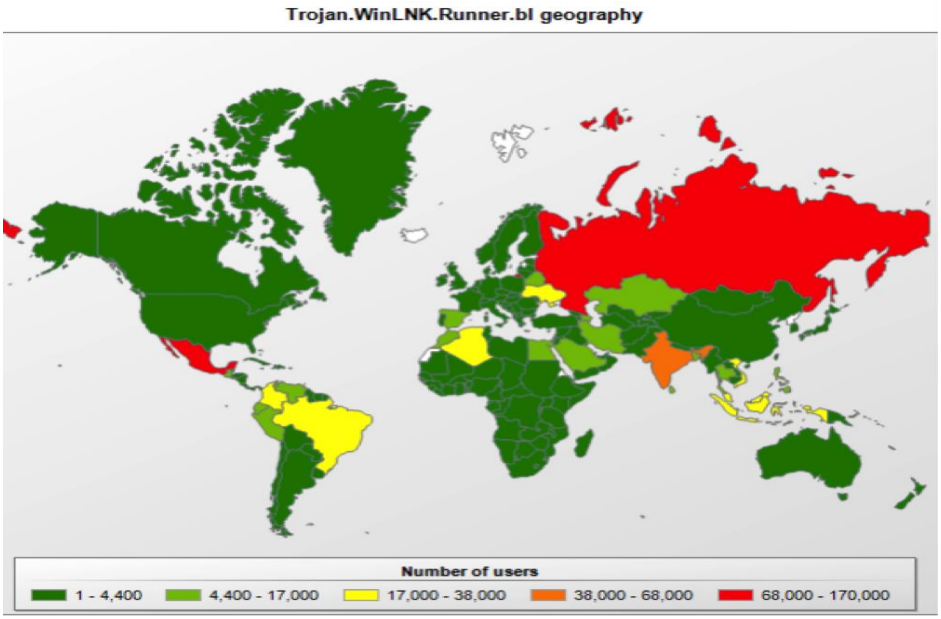


Ilustración 3. Mapa de infecciones del Trojan.WinLNK.Runner.bl a nivel global

“Las ciudades de América Latina con más riesgo online son Buenos Aires, Argentina; San Juan, Puerto Rico y Bogotá, Colombia. Las tasas más altas de infección no necesariamente se relacionan con estas ciudades, lo que revela que muchos de los usuarios toman las debidas precauciones para mantener a salvo su información.”[35] Estas estadísticas fueron tomadas en febrero de 2012 y se tuvo en cuenta equipos de escritorio y Smartphone, también lo que son actividades como el ingreso a Wi-Fi, la utilización de redes sociales y las operaciones bancarias en línea. En la actualidad como se especificó anteriormente Colombia ha incrementado sus delitos informáticos es por ello que para el 2014 Colombia se

[34] *Netmedia, Bestuzhev Dmitry, Cibercriminales, ansiosos por el crecimiento económico y Web de América Latina {En línea}. {18 enero de 2015}. Disponible en: (http://www.bsecure.com.mx/opinion/cibercriminales-ansiosos-por-el-crecimiento-economico-de-america-latina/#).*

[35] *Álvarez Ángel, Las 10 ciudades de América Latina más vulnerables al cibercrimen {En línea}. {18 enero de 2015}. Disponible en: (http://www.bsecure.com.mx/featured/las-10-ciudades-de-america-latina-mas-vulnerables-al-cibercrimen/).*

encuentra en el 3 lugar del país con más denuncias de delitos informáticos encontrándose entre los países y ciudades con el mayor riesgo.

4.1.4 Hacker internacional

4.1.4.1 Estadounidense

Después de haber introducido un poco más sobre el hacker colombiano, se hablara ahora del hacker internacional y específicamente de los más polémicos que se ha visto en los últimos tiempos los hacker estadounidenses, abordaremos los comienzos y casos que se ha visto de este, su actualidad y que leyes o normas están establecidas para controlar estos delitos.

En estados unidos se conoció el primer atentado a una computadora, el cual se registró en 1958, mientras que el primer proceso de la alteración de datos se realizó en 1966, fue realizada al banco de Minneapolis. Estos delitos dieron la primera pregunta e interrogante sobre el delito informático al cual culpaban tras la llegada de la nueva tecnología es por ellos que "el Pentágono, la OTAN, las universidades, la NASA, los laboratorios industriales y militares se convirtieron en el blanco de los intrusos."[36]

En 1976 el FBI después de empezar a detectar los casos empezó a enseñar haciendo cursos acerca de delitos informáticos y se dio lugar a la ley Federal de Protección de Sistemas en 1985 esta ley hace su mayor referencia por parte "de abuso o fraude contra casas financieras, registros médicos, computadoras de instituciones financieras o involucradas en delitos interestatales. También especifica penas para el tráfico de claves con intención de cometer fraude y declara ilegal el uso de passwords ajenas o propias en forma inadecuada."[37]Con el Acta Federal de Abuso Computacional de 1994 se complementa la ley para los abusos utilizando virus, también la de trasmitir, alterarlos, copiar, destruir, modificar datos de una computadora. Esta ley fue el comienzo de la regulación ante estos ataques, pero esto también aumento la cantidad de casos de hacking y aumento de la inseguridad los casos que muestran el cambio son "Cóndor" Kevin Mitnicky y los de "ShadowHawk" Herbert Zinn hijo.

---

[36] *Segu.Info, Legislación y Delitos Informáticos –Estados Unidos, {En línea}. {Enero 19 de 2015}. Disponible en: (http://www.segu-info.com.ar/delitos/estadosunidos.htm).*

[37] *Segu.Info, Legislación y Delitos Informáticos Estados Unidos, {En línea}. {Enero 19 de 2015}. Disponible en: (http://www.segu-info.com.ar/delitos/estadosunidos.htm).*

Kevin David Mitnick es uno de los hacker más famosos el cual nacido el 6 de agosto de 1963 a este hacker también lo llamaban el cóndor, fue arrestado y conocido por entrar en los ordenadores más seguros de estados unidos y por otros delitos informáticos realizados anteriormente, los delitos informáticos realizados por este hacker han dado lugar a libros y también a material de ficción entre estos se destaca " la novela *Takedown*, que relata su último arresto, y de la cual han sacado una película con el mismo título, Takedown, en el año 2000."[38]La carrera de este hacker estadunidense emperezo tan solo a los 16 años de edad al romper la seguridad del sistema administrativo del colegio en donde este estudiaba, pero con esto el no quiso alterar o cambiar nada lo hizo como afición y para ver si podía hacerlo. Después en 1981 "Junto a dos amigos, entró físicamente a las oficinas de COSMOS, de Pacific Bell. COSMOS (Computer System for Mainframe Operations) era una base de datos utilizada por la mayor parte de las compañías telefónicas norteamericanas para controlar el registro de llamadas."[39]Con este acto lo que quisieron obtener fueron las combinaciones de las puestas de acceso, claves y manuales que le ayudarían a entender varias cosas, a futuro la información que robo con su amigo equivale a 200.000 dólares. Kevin Davis fue accediendo a más información y agrandando sus conocimientos en los delitos informáticas tanto así que no fue suficiente lo que ya había hecho sino que quiso seguir avanzando en sus objetivos como hacker y en 1982 entro vía modem a "la computadora del North American Air Defense Command, en Colorado. Antes de entrar alteró el programa encargado de rastrear la procedencia de las llamadas y desvió el rastro de su llamada a otro lugar."[40]otro de sus delitos fue entrar ilegalmente a ARPAnet y al intentar entrar a las computadoras del pentágono, también desapareció el expediente de el mismo de la computadora de la policía local, durante meses entro al correo de los miembros del departamento de seguridad de MCI Communications y Digital Equipment Corporation y así entender como estaban protegidas dichas computadoras y con ello se apodero de 16 códigos de seguridad de MCI.

Al ser arrestado le prohibieron el uso de celular ya que se decía que él podría ingresar a computadoras desde cualquier celular después su abogado convenció al juez de que Mitnick sufría de una adicción a las computadoras, al llegar el año 1991 era considera el cracker, huyo después de salir de la cárcel y utilizo programas de teléfonos para no ser rastreado y con el conocimiento obtenido creo

[38] *Wikipedia, Kevin Mitnick {En línea}. {Enero 19 de 2015}. Disponible en: (http://es.wikipedia.org/wiki/Kevin_Mitnick).*
[39] *Wikipedia, Kevin Mitnick {En línea}. {Enero 19 de 2015}. Disponible en: (http://es.wikipedia.org/wiki/Kevin_Mitnick).*
[40] *Ibíd.*

cuentas y lanzo ataques hacia los ordenadores de Motorola, Apple y Qualcomm. Después de sumar un poco de delitos más por un tiempo el FBI empezó a rastrear sus pasos recolectaron pruebas y fue atrapado.

El otro caso mencionado anteriormente es el de Herbert Zinn, "expulsado de la educación media superior, y que operaba bajo el seudónimo de "Shadowhawk", fue el primer sentenciado bajo el cargo de Fraude Computacional y Abuso en 1986. Zinn tenía 16 y 17 años cuando violo el acceso a AT&T y los sistemas del Departamento de Defensa. Fue sentenciado el 23 de enero de 1989, por la destrucción del equivalente a US $174,000 en archivos, copias de programas, los cuales estaban evaluados en millones de dólares, además público contraseñas e instrucciones de cómo violar la seguridad de los sistemas computacionales. Zinn fue sentenciado a 9 meses de cárcel y a una fianza de US$10,000. Se estima que Zinn hubiera podido alcanzar una sentencia de 13 años de prisión y una fianza de US$800,000 si hubiera tenido 18 años en el momento del crimen"[41].

Para esta época también se conoció el caso de René David Quintana, quien llegó a territorio estadounidense el 01 de junio de 1980, y así apareciendo sus primeros registros judiciales por delitos varios, aunque menores, pero para "Quintana su delito fue cometido en el departamento de contabilidad de un negocio ubicado en el condado de Miami Dade, en el sur de La Florida, que se dedicaban a distribuir productos prepagados de telecomunicaciones, tales como tarjetas de llamadas, entre otros, Quintana utilizó los computadores de su empresa para realizar transacciones de dinero de la cuenta de esa compañía a otras abiertas y controladas por él en distintos bancos, en estos actos se apropió de 213.000 dólares y la justicia estadounidense lo procesó por los delitos de fraude por transferencia económica entre otros 14 cargos"[42].

Otro caso importante de estados unidos es el de Robert "Pimpshiz" Lyttle joven de 18 años de edad es acusado de ser miembro del grupo Deceptive Duo que robo información los servidores del sistema de la Federal Aviation Administration de los Estados Unidos , también este grupo es acusado de obtener información de los pasajeros de los aeropuertos ,ingresar a un servidor de la FAA (Federal Aviation Administration), también "Cabe mencionar que Robert Lyttle, siendo un joven

[41] *Wikipedia, Kevin Mitnick {En línea}. {Enero 19 de 2015}. Disponible en: (http://es.wikipedia.org/wiki/Kevin_Mitnick).*

[42] *Semana.com. Primer extraditado por delitos informáticos {En línea}. {Junio 19 2013}. Disponible en: (http://www.semana.com/nacion/articulo/el-primer-extraditado-delitos-informaticos/348204-3).*

adolescente, de apenas 14 años formó la corporación Sub-Seven Software, que desarrolló herramientas tales como el Troyano buscador de puertos Sub- Net, el desinstalador Uninstall it Pro y Define, entre otros."[43] "De acuerdo al libro de Bárbara Jenson "Acecho cibernético: delito, represión y responsabilidad personal en el mundo online", publicado en 1996, se calcula que unas 200.000 personas acechan a alguien cada año"[44].

En la actualidad uno de los casos recientes en el 2014 es el ataque a Sony Pictures que se ha convertido en una pelea entre Estados Unidos y Corea, convirtiéndose en un problema de seguridad informática y de política internacional ya que se responsabilizó a corea del norte por el ataque, pero este país dijo no tener hacker que hubiese hecho esto, pero el caso llego a ser tan grave que el mismo presidente "Obama fue aún más adelante en sus demandas y dijo a los coreanos que también debían indemnizar a Sony por el grave daño causado con la publicación anticipada de varias películas que constituían parte de su alta inversión anual."[45]. La respuesta de corea ante este nuevo pronunciamiento es que se exige una investigación sobre este ciberataque los autores de eso se hacen llamar "Guardians of Peace", lo que realizo esta organización fue el robo de identificación y tarjetas medicas de 3.000 empleados de la compañía, también sustrajeron mail en donde privadamente se criticaba algunos actores de la compañía, y por último robaron cinco películas. Esto causo una gran pérdida en Sony ya que tuvo que cancelar estrenos de dichas películas y la perdida millonaria por la información sustraída.

La ciberseguridad de Estados Unidos está en peligro es por ello que EE.UU. ha colocado este tema entre uno de los más importantes para este país llegando hasta debates políticos sobre esto, tanto así que el presidente Barack Obama busca sacar adelante un paquete legislativo que consolide la piratería informática y que endurezca las leyes contra los hackers. "Obama en un breve discurso en el Centro Nacional de Ciberseguridad, a las afueras de Washington. "El ataque a Sony, la cuenta de Twitter [del Ejército] pirateada , demuestran que el sector

[43] *Elhacker.net, Estos son los hackers más famosos de los últimos años,* {En línea}. {Enero 19 de 2015}. Disponible en: (http://foro.elhacker.net/foro_libre/hackers-t249680.0.html;msg1203395).
[44] Ibíd.
[45] Martínez Juan, Los Hackers no han Ganado, Estados Unidos Contraataca, {En línea}. {Enero 19 de 2015}. Disponible en: (http://www.vanguardia.com/actualidad/tecnologia/292403-los-hackers-no-han-ganado-estados-unidos-contraataca#).

público y privado tienen que hacer mucho más trabajo en fortalecer nuestra ciberseguridad”[46]

Estados Unidos Cuenta con una institución para el estudio de crímenes informáticos o asuntos de seguridad informática este instituto es el CSI quien ha realizado varios estudios a corporaciones y agencias del gobierno, también un agencia importante en estados unidos es la agencia federal de investigación el FBI que tiene la división de delitos informáticos, en el 2.000 se realizaron estadísticas donde se arrojó que las violaciones más encontradas son los virus, robo de computadoras y el abuso de empleados.

El Acta Federal de Abuso Computacional mencionada anteriormente la cual fue modificada en 1986. En esta acta se contempló la regulación de los virus, aunque no se limita a los usualmente llamados virus o gusanos, sino que contempla a otras instrucciones destinadas a contaminar otros grupos de programas, bases de datos, cuentas en banco o simplemente a una información personal.

Ahora con las nuevas tecnologías, y los casos que han sucedido en Estados Unidos ya tiene grupos que combaten estos delitos informáticos uno de ellos es “El FCIC (Federal Computers Investigation Commitee), esta es la organización más importante e influyente en lo referente a delitos computacionales, los investigadores estatales y locales, los agentes federales, abogados, auditores financieros, programadores de seguridad y policías de la calle trabajan allí comunitariamente. El FCIC es la entrenadora del resto de las fuerzas policiales en cuanto a delitos informáticos, y el primer organismo establecido en el nivel nacional”[47]. Otro grupo es la Asociación Internacional de Especialistas en Investigación Computacional (IACIS), quien investiga nuevas técnicas para dividir un delito en sus partes sin destruir las evidencias, quienes trabajan en este grupo son los forenses de las computadoras y trabajan, además de los Estados Unidos, en el Canadá, Taiwán e Irlanda.

[46] El País, Obama coloca la ciberseguridad en el centro del debate en EE UU. {En línea}. {Enero 19 de 2015}. Disponible en: (http://internacional.elpais.com/internacional/2015/01/13/actualidad/1421180628_845380.html).
[47] El País, Obama coloca la ciberseguridad en el centro del debate en EE UU. {En línea}. {Enero 19 de 2015}. Disponible en: (http://internacional.elpais.com/internacional/2015/01/13/actualidad/1421180628_845380.html).

Según el CSI de los estado unidos el ciberataque ha aumentado ya que la compra de computadoras ha aumentado y las acciones que estos realizan, son la compra de artículos, pago de cuentas , consultas de información privada , realización de negocios, para esta organización dice que a medida de que avanza la tecnología también avanza la delincuencia informática, haciendo uso indebido de herramientas que son útiles para los ciudadanos y convirtiéndolas en ataques hacia los mismo, haciendo delitos como el acceso no autorizado, el fraude, la trata de menores, sabotaje en páginas.

"Los delincuentes de la informática son tan diversos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado. Estos delincuentes pueden pasar desapercibidos a través de las fronteras, ocultarse tras incontables «enlaces» o simplemente desvanecerse sin dejar ningún documento de rastro."[48] Aparte de esto los delincuentes cibernéticos son tan avilés para ocultar a información o pruebas que puedan inculparlos.

"Según datos recientes del Servicio Secreto de los Estados Unidos, se calcula que los consumidores pierden unos 500 millones de dólares al año debido a los piratas que les roban de las cuentas online sus números de tarjeta de crédito y de llamadas"[49], Los robos que realizan estos hacker no son solo para beneficio propio sino que muchas veces también utilizan esta información para venderlas a mas organizaciones de ciberataque, también en los Estados Unidos se calcula que se generan perjuicios económicos, por los delitos informáticos, que superan los 10.000 millones de dólares y casi el 90% de los delitos informáticos que investiga el FBI en Estados Unidos tienen que ver con Internet.

Desde hace unos años según los documentos de los Estados Unidos es frecuentemente utilizada la palabra virus o gusano por los usuarios que frecuente mente tienen computadores o algún dispositivo tecnológico, estos virus son programas o software que se instalan en el computador para realizar completamente los sistemas empresariales o de personas y así también poder robar datos del disco duro. La ganancia que tienen estos delincuentes con esta clase de virus es que estos se propagan de computador a computador obteniendo muchos más datos de diferentes personas para robar sin tener que hacerlo uno por uno. Aparte de estos virus también se ponen de moda la manera de los mensajes en mails, chats en donde se llega a descargar archivos que contienen el virus.

---

[48] *Delitos Informaticos.doc {En línea}. {Enero 19 de 2015}. Disponible en: (https://docs.google.com/document/d/1shYhIUuqLCe9MiRteX1b8wsuq9WKG3kQwITiXMZGayk/edit?hl=es&pli=1).*

[49] *Ibíd.*

El impacto social que ha surgido a causa de los delitos informáticos en Estados Unidos y la especialización técnica que adquieren estos delincuentes en los delitos atentando contra la economía de las empresas o de usuarios bancarios, ya que los activos informáticos que poseen empresas son de gran importancia para las mismas y causan un decremento de aspectos importantes para la misma, y los más vulnerables a estos actos son las personas con menos conocimientos básicos sobre la protección de sus activos.

"La falta de cultura informática puede impedir de parte de la sociedad la lucha contra los delitos informáticos, por lo que el componente educacional es un factor clave en la minimización de esta problemática."[50]

La "Ley sobre el Uso Indebido de las Computadoras. Ahora son más severos los castigos impuestos a todo el que interfiera con las «computadoras protegidas» es decir, las que están conectadas con la seguridad nacional, la banca, las finanzas y los servicios públicos y de urgencia- así como a los transgresores por entrada, modificación, uso o intercepción de material computadorizado sin autorización."[51]

4.1.4.2 Alemania

Para poder observar también que pasa con los hacker en el continente europeo y con ello hacer un análisis que nos permita identificar actos similares o costumbres que también haya adoptado los hacker colombianos.

Se conoce el caso de los dos hackers alemanes, de 23 y 20 años Wau Holland y Steffen Wernery, los cuales ingresaron el 2 de mayo de 1987 sin autorización al sistema de la central de investigaciones aeroespaciales más grande del mundo. "Hacía rato que Wau Holland y Steffen Wernery permanecían sentados frente a la pantalla de una computadora, casi inmóviles, inmersos en una nube de humo cambiando ideas en susurros. Cuando la computadora comenzó a ronronear, Wau Holland y Steffen Wernery supieron que habían logrado su objetivo. Segundos más tarde la pantalla mostraba un mensaje: "Bienvenidos a las instalaciones VAX del cuartel general, de la NASA"[52].

Otro caso conocido en Alemania es la del capitán Zap o por su nombre Ian Murphy un muchacho de 23 años, el cual en julio de 1981 gana fama cuando entra a los sistemas de la Casa Blanca, el Pentágono, BellSouth Corp. TRW y así deja su

---

[50] *Delitos Informaticos.doc {En línea}. {Enero 19 de 2015}. Disponible en: (https://docs.google.com/document/d/1shYhIUuqLCe9MiRteX1b8wsuq9WKG3kQwITiXMZGayk/edit?hl=es&pli=1).*

[51] *Ibíd.*

[52] *Torres Jorge. Impacto de los delitos informáticos {En línea}. {Octubre 2000}. Disponible en: (http://www.monografias.com/trabajos6/delin/delin2.shtml).*

currículum. “Mostró la necesidad de hacer más clara la legislación cuando en compañía de un par de amigos y usando una computadora y una línea telefónica desde su hogar viola los accesos restringidos a compañías electrónicas, y tenía acceso a órdenes de mercancías, archivos y documentos del gobierno. "Nosotros usamos los a la Casa Blanca para hacer llamadas a líneas de bromas en Alemania y curiosear archivos militares clasificados" Explico Murphy”[53].

Alemania en otro caso más sobre delito informático, el ministerio de este país tuvo que pedir a las delegaciones de Estados Unidos, China y Rusia que hagan llegar la lista completa de los agentes que trabajan en territorio germano, tanto oficiales, como los que actúan bajo otra cobertura, como agentes culturales, agregados militares o de prensa, ya que uno de estos agentes-espías “pasaba información, entre otros asuntos, sobre las actividades del comité parlamentario creado precisamente para investigar las escuchas llevadas a cabo durante años por la agencia de seguridad norteamericana ”[54].y así mismo el agente vendió a la embajada de EE UU 218 documentos robados.

La noticia más importante y que generó una gran preocupación a nivel mundial es el caso de el hacker alemán Jan Krissler, conocido como "starbug", el presento presentó “una nueva técnica para vulnerar el uso de biométrica como método de identificación, al mostrar que puede obtener la huella dactilar de una persona al mirar una foto de su mano.”[55] Aunque ya antes se habían encontrado diferentes técnicas echas por delincuentes informáticos, pero estas se utilizaban cuando la persona había tomado en sus manos la foto u objeto con ellos obtenían la huella y cometían el delito. Pero con este nuevo método presentado por este hacker alemán la obtención de la huella se puede hacer de forma totalmente remota.

La demostración de esto que causó gran asombroso hizo obteniendo “La huella dactilar de la ministra de defensa de Alemania, Ursula von der Leyen, en base a

[53] *Ibíd.*
[54] *Doncel Luis. El país internacional. La captura de un agente doble enturbia las relaciones entre Berlín y Washington {En línea}. {Julio 14 2014}. Disponible en: (http://internacional.elpais.com/internacional/2014/07/04/actualidad/1404488164_311691.html).*
[55] *Emol. ciencia y tecnología. Hacker alemán muestra método para obtener huellas dactilares desde fotos, {En línea}. {Enero 27 de 2015}. Disponible en: (http://www.emol.com/noticias/tecnologia/2014/12/29/696637/hacker-aleman-muestra-metodo-para-obtener-huellas-dactilares-desde-fotos.html#).*

una serie de fotos de ella capturadas en una conferencia de prensa. La huella, indicó, puede ser usada para métodos de identificación."[56]

La más reciente medida adoptada por el ministerio de Asuntos Exteriores germano fue consensuada con otros ministerios alemanes y con la cancillería, y con ella Berlín opto por ejercer más presión para obtener las respuestas que espera desde el pasado año de Washington, uniendo ideas para contrarrestar el daño que realizan los delincuentes informáticos.

Ya para la actualidad en Alemania, a la hora de crear leyes sobre los delitos informáticos, primero se tenía que ver estos donde estaban operando o causando más daño, quienes salían perjudicados y que medios utilizaban los delincuentes para realizar sus delitos, para así introducir nuevas leyes penales para la represión de dichos hacker criminales, aunque el bien jurídico que estaba protegido primordialmente era el patrimonio, luego eran las conductas que atentara a la vida personal y la privacidad, sancionando en este el espionaje de datos, sin embargo descartan aquella información que se encuentra almacenada o que pueda ser transmitida electrónica o magnéticamente de forma accesible. En fin esta ley no protegería ningún tipo penal que estuviera referente a un espionaje de datos informatizados, es decir que la violación al derecho a la interceptación de un correo electrónico, etc. no se encuentran previstas en la Legislación alemana.

"la Organización de Cooperación y Desarrollo Económico (OCDE) inicio leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales"[57], por ello dio a notar 4 principios importantes:

- "No es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir.
- No es la computadora la que afecta nuestra vida privada, sino el aprovechamiento que hacen ciertos individuos de los datos que ellas contienen.
- La humanidad no está frente al peligro de la informática sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que

[56] *Ibíd.*
[57] *Segu-info. Legislación y Delitos Informáticos - La Información y el Delito, {En línea}. {Enero 27 de 2015}. Disponible en: (https://www.segu-info.com.ar/legislacion/)*

significa el conocimiento.

- Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas."[58]

Con lo descrito anterior y de acuerdo a lo que, la sociedad alemana tomo en cuenta y describió los aspectos más importantes para tomar en su ley como lo son: espionaje e datos, estafa informática, falsificación de datos probatorios, alteración de datos, sabotaje informático, utilización abusiva de cheques o tarjetas de crédito. Además dentro de la ley adopto aspectos como los datos personales que fueran almacenados en registros informatizados, y que con la obtención de los registros o información fueran modificados, divulgados sin autorización.

4.1.5 Daño social de hacker colombiano

El gran incremento de los delitos informáticos en Colombia, ha hecho que nuestra sociedad sea cada vez más desconfiada al uso de las tecnologías de la información, ya que estos delitos o daños que se observan, pueden retardar el desarrollo de nuevas formas de hacer negocios, como lo es el comercio electrónico, que puede verse afectado por la falta de apoyo de la sociedad.

Con el gran avance de Internet en los últimos años, la información privada y la vida social de los gobiernos, las empresas y las personas han aumentado en un mayor riesgo, ya que los hackers, profesionales y aficionados a causar daños, se han convertido en una amenaza constante para la seguridad de la información y si estos personajes no son detenidos, las consecuencias para la sociedad en general son delicados, es mucha la cantidad de personas que operan el lado malicioso u oscuro de la internet, que llega a atentar, hacer daño sobre estas tecnologías que fueron creadas para el bien útil de la sociedad, es por ellos que "Colombia es un blanco fácil para que las personas inescrupulosas que se aprovechan de la tecnología y lleven a cabo acciones tales como; hurto de datos personales, hurto de información confidencial, estafas, envío de virus o spam."[59], entre otras, con esto se puede analizar las conductas que se presentan allí y que pueden vulnerar o atentar contra los derechos y la integridad de las personas y organizaciones que interactúan constantemente con internet, o sencillamente harán que las empresas que poseen informaciones importantes, sean cada vez más celosas y exigentes en

[58] *Ibíd.*

[59] *Rodríguez Arbeláez Juan David. Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación {03 febrero 2015} {En línea} Disponible en: http://bdigital.ces.edu.co:8080/repositorio/bitstream/10946/1334/2/Delitos%20en%20las%20Redes%20Sociales.pdf*

la contratación de personal para trabajar en éstas áreas, pudiendo afectar en forma negativa a la sociedad laboral de nuestros tiempos.

Unos de los daños sociales más común que se ve por los hacker, es la libertad de la información, ya que los hacker tienen "el grado de especialización técnica que adquieren los delincuentes para cometer éste tipo de delitos, por lo que personas con conductas maliciosas cada vez más están ideando planes y proyectos para la realización de actos delictivos, tanto a nivel empresarial como a nivel global."[60], es por esto que un caso sobresaliente sobre este daño es en la política, ya que estos tienen la capacidad de hablar libremente sin preocuparse por la opinión pública, dado que es un componente vital de cualquier Estado democrático, pero adverso a esto, los hackers alientan a las personas poderosas para discutir temas sólo en persona, para alentarlos a causar daños a los demás contrincantes, cambiando sus informaciones en todos los sentidos y en consecuencia de estos actos lo que hace es que reduce la eficiencia, la eficacia y la honestidad del gobierno Colombiano, estos nos lleva a la conclusión como lo menciona la abogada Odelia Tijerina en el documental sobre cuidado con los datos , la web nos vigila, no estamos solos ,que nos dice: "no existe la privacidad absoluta, ni siquiera existe el derecho absoluto a la privacidad de las leyes"[61].

Un ejemplo de daño social a un estado y uno de los primeros en ser realizados, fue en abril de 2007 en Estonia, el cual fue un ataque cibernético de envergadura hacia un estado, que se realizó para desorientar a la población y sembrar confusión en la misma y así revelando una nueva forma de hacer la guerra[62]

Otros daños o consecuencias que deja los delitos informáticos en nuestra sociedad y que son muy conocidos tanto en lo niños como ya en las personas adultas y causa un gran daño social son:

- "Ciber Bullying o bullying cibernético: Este delito que se produce ya en las redes sociales y en las tecnologías de información y comunicación en Colombia día a día es la prolongación del acoso escolar (bullying) a través

[60] *Landaverde Contreras Melvin Leonardo. Delitos informáticos, Impacto de los delitos informáticos {Octubre de 2000} {En línea} Disponible en: http://www.monografias.com/trabajos6/delin/delin2.shtml#impa*

[61] *Black hack mx. Documental. Tijerina Ofelia, Cuidado con los datos, la web nos vigila, no estamos solos. {18 febrero 2014} {En línea}. Disponible en: https://www.youtube.com/watch?v=qJFjSAaTnMU*

[62] *AnonymousMexico2. Anonymous Ciberguerilla {01 junio 2013} {En línea}. Disponible en: https://www.youtube.com/watch?v=BhJfaKAycNs*

de internet, video juegos, celular, telefonía móvil, en general todas las redes sociales. Cuando se comete este delito se atenta contra la moral y la integridad de la persona por parte los agresores y muchas más personas, inclusive desconocidas. Se prolonga entonces el maltrato y acoso. Los medios más comunes son: Messenger, Hotmail, Facebook, foros, redes P2P, entre otros.

- Perfiles Falsos: Estos actos ilícitos consisten en la creación de perfiles simulados con datos reales de personas o empresas para obtener o manipulara los usuarios. También este delito tiene la finalidad de menoscabar muchas veces la dignidad y la integridad de las personas realizando actividades con su identidad en las redes sociales que denigren sus derechos y sus libertades utilizando información de todas clase, como videos, fotos, comentarios, escritos, grabaciones de sonido, entre otras.
- Pornografía Infantil: Los números casos de pornografía infantil online que han ocurrido y están ocurriendo en el mundo y en el país, demuestran que Internet se ha convertido en el medio principal para que pedófilos intercambien archivos y fotografías de menores, superando fronteras con su accionar, planteando un grave problema de protección para los mismos.

Este daño social de la pornografía infantil, que afecta a gran mayoría de los que ahora navegan en internet está cobrando vida en los últimos años y del cual "se estima que hay más de 20 millones de páginas web que proporcionan este delito, dentro de las cuales se encuentran en cada una de estas, 9 millones de imágenes y videos individuales, el cual el 39% de los niños tienen menos de 5 años y el 19% tienen menos de 3 años"[63].

- Fraude Informático: Este acción ilícita consiste en realizar estafas mediante técnicas específicas utilizadas por los delincuentes. Entre los más importantes se encuentra el Phising y el robo de identidad.
- El Phising es una modalidad defraudadora que consiste en remitir un correo electrónico engañoso a clientes para que revelen información personal a través de sitos Web simulados en una respuesta de correo electrónico. Los daños causados por el phising oscilan entre la pérdida del acceso al correo electrónico a pérdidas económicas sustánciales. Desde hace tiempo han aumentado considerablemente las modalidades delictivas

[63] *The Eternauta666. Documental. Atrapados en la red Delitos informáticos. {15 febrero 2012} {En línea}. Disponible en: https://www.youtube.com/watch?feature=player_embedded&v=t75Zrhhe5a0*

relacionadas con los datos personas, la cual afecta a diversos bienes jurídicos: propiedad, privacidad, honra y honor.

- Robo de Información: Es uno de los delitos cibernéticos más populares y olvidados por los usuarios de las redes, quienes han descuidado la forma en que publican información personal en lugares como blog, foros o redes sociales, que colocan en sus correos electrónicos o simplemente datos que ofrecen desconocidos a través de la mensajería instantánea o chats.
- Daño Informático: Las redes sociales son propicias para este tipo de acciones, dado que el intercambio de archivos o descarga de material pueden involucrar casos de virus informáticos."[64]

Sin embargo, con estos actos delictivos se sigue dando información incorrectamente, sin mirar causas ni consecuencias, aun conociendo de que no hay garantía de que internet sea segura y así siguen 6 millones de usuarios conectados a red las 24 horas y se estima que hay 2 millones de usuarios en internet, 34% de la población mundial conectada y dando así que cada día hay 247.000 millones de correos en todo el mundo"[65] y aun estando atento de todos los males que ahí, seguimos en la red más grande que nos encierra cada día a un mundo esclavo de la tecnología.

En la actualidad y como algo cotidiano de la sociedad es normal tener Facebook, Twitter, Instagram, entre otras redes sociales, estas se han convertido en una puerta abierta socialmente, no solo para las personas adultas sino para niños, es una brecha en donde no se sabe quién es en verdad el verdadero personaje que aparece detrás de un perfil falso, la interacción que dan este tipo de redes con gente que muchas veces ni siquiera conoces, lo que se convierte en un contacto repetitivo con nuevas personas, que en dado caso pueden ser delincuentes que solo quieren ganar la confianza de la persona y aprovecharse de dicho espacio para hacer daño, este daño se ha convertido en un volumen grande de personas que diariamente denuncian este tipo de actos cuando se dan cuenta, pero para las autoridades es tan difícil rastrear estos delitos ya que son miles de cuentas creadas falsas creadas diariamente . En muchos casos el contacto de las personas sobrepasa el espacio virtual y llega a un encuentro físico.

---

[64] *Landaverde Contreras Melvin Leonardo. Delitos informáticos, Impacto de los delitos informáticos {Octubre de 2000} {En línea} Disponible en: http://www.monografias.com/trabajos6/delin/delin2.shtml#impa*

[65] *Rec reporteroscuatro. Documental. Estamos desnudos en internet? {11 noviembre 2012} {En línea}. Disponible en: https://www.youtube.com/watch?v=H20OPj7FBaw*

Estos daños que afectan nuestra dignidad o simplemente nuestra vida social y a quien más afecta, son aquellas personas que no poseen los conocimientos informáticos básicos, ya que son más vulnerables a ser víctimas de un delito, que aquellos que si los poseen. Estas personas que no conocen sobre información básica de hacker son por lo general personas de escasos recursos económicos y que pueden ser engañadas si en un momento dado poseen acceso a recursos tecnológicos y no han sido asesoradas adecuadamente para la utilización de tecnologías como la Internet, correo electrónico, etc., pero a pesar de que estemos en capacidad de entender o no entender, de tener información necesaria sobre estos delitos el 70% de las personas están preocupadas porque sienten que han perdido el control sobre sus datos[66].

"La falta de cultura informática puede impedir de parte de la sociedad la lucha contra los delitos informáticos, por lo que el componente educacional es un factor clave en la minimización de esta problemática"[67].O se debería hacer como unos años anteriores, en donde los científicos después de la segunda guerra mundial, se les tuvo del lado bueno, para así ganar influencia sobre estos, hoy en día seria tener a los hacker de nuestro lado para tener conocimiento de sus técnicas y así tener prevenciones sobre estas.

El gran problema que enfrenta no solo Colombia sino todos los países, sobre la afectación social, ya que este tipo de criminalidad es difícil de combatir por el nivel de internacionalidad ,dichos personales están distribuidos por todo el mundo y su víctima igualmente puede estar en cualquier lugar, lo que también dificulta los procesos legales al enfrentarse a leyes.

La tecnología y los sistemas informáticos son ahora para la sociedad Colombia y para el mundo una forma de poder social, que se puede encontrar en todo lo que nos rodea. En la actualidad hasta entidades del gobierno utilizan sistemas informáticos, presidentes, ministros, etc. con redes sociales como twitter para expresar o dejar ver información. En la actualidad ninguna persona se salva de no tener un contacto tecnológico social con el mundo.

La importancia de los sistemas tecnológicos para la sociedad es de gran importancia por la rapidez, ahorro de tiempo, facilidad de comunicación,

[66] *Black hack mx. Documental, Cuidado con los datos, la web nos vigila, no estamos solos. {18 febrero 2014} {En línea}. Disponible en: https://www.youtube.com/watch?v=qJFjSAaTnMU*

[67] *Landaverde Contreras Melvin Leonardo. Delitos informáticos, Impacto de los delitos informáticos {Octubre de 2000} {En línea} Disponible en: http://www.monografias.com/trabajos6/delin/delin2.shtml#impa*

interacción con otras personas entre otras, que facilitan que la gente no se pueda desprender en estos momentos de la tecnología, pero así como es de imposible que la sociedad no utilice más la tecnología, es difícil conocer o creer la buena fe de todos los que se encuentran en la red.

La desconfianza que existe en la sociedad por el que está al lado del computador, debería ser igual de preocupante por quien está al otro lado del computador, el sistema social de desconfianza siempre por quienes nos rodean, familiares, amigos, etc. ahora se debe tener en cuenta que mucho menos se debe dejar atrás la desconfianza por el que está detrás de un computador, por creer que no se está viendo, desconfiar siempre de todo aquello que pueda producir daño o un impacto social grande y dañino. No se puede dejar atrás el avance de la tecnología, por lo tanto se debe saber que tampoco se debe descuidar la seguridad al acceder a todo tipo de tecnología en la cual no se sabe quién puede estar espiando.

"El grado de especialización técnica que adquieren los delincuentes para cometer éste tipo de delitos, por lo que personas con conductas maliciosas cada vez más están ideando planes y proyectos para la realización de actos delictivos, tanto a nivel empresarial como a nivel global."[68]

Un gran problema para contrarrestar el daño social producido por un hacker es que todo esto depende la cultura informática que tenga la sociedad, por lo tanto "la falta de cultura informática puede impedir de parte de la sociedad la lucha contra los delitos informáticos, por lo que el componente educacional es un factor clave en la minimización de esta problemática."[69]

"Los informes de las compañías antivirus sobre el descubrimiento de una nueva botnet o un nuevo refinado ejemplar de malware que roba datos aparecen con regularidad. Con cada vez más frecuencia las compañías comerciales se convierten en víctimas potenciales de los ataques informáticos. Según los resultados de una encuesta realizada por Kaspersky Lab y la compañía analítica B2B International, el 91% de las empresas encuestadas en todo el mundo fueron

[68] *Reyes Sánchez Yuridia Elena, Fernández Aramburo Ever Alfonso, delitos informáticos proyecto final (2 de febrero de 2015) {En línea}.http://www.scribd.com/doc/24068494/DELITOS-INFORMATICOS-PROYECTO-FINAL#scribd.*
[69] *Ibíd.*

víctimas de por lo menos un ataque al año y el 9% de las compañías fueron víctimas de ataques selectivos."[70]

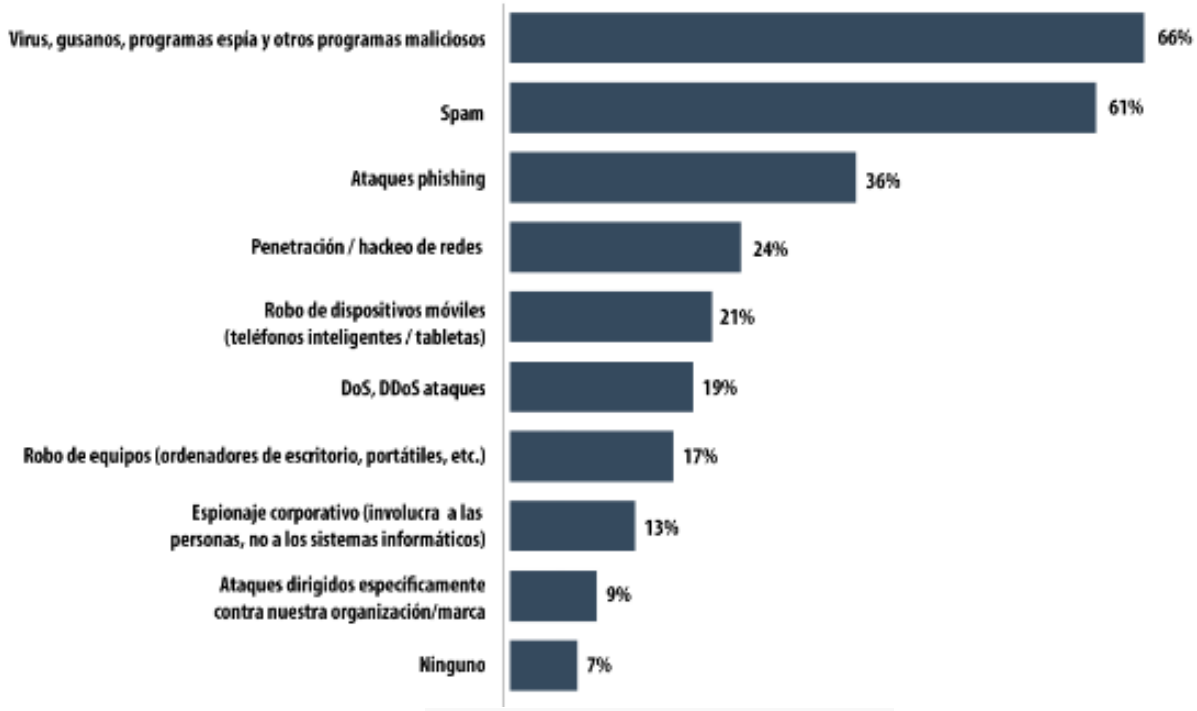


Ilustración 4. Ataques que presentan las Compañías

4.1.6 Herramientas utilizadas por los hacker para hacer daño

En la actualidad se encuentran programas que son legales y que los delincuentes tecnológicos los utilizan para hacer daño, la mayoría de estos programas legales son utilizados para acceder a los ordenadores. Es lógico que la mayoría de estos programas sean instalados en los equipos sin consentimiento del usuario, tomando el control absoluto del sistema al que está accediendo, los programas legales que son utilizados ilegalmente es de gran frecuencia utilizado por los hacker y esto hace aún más difícil la detección del mismo.

Algunos de estas herramientas se agrupan en diferentes grupos como:

- **Marcadores (dialers):** "Estos programas no causan daño al equipo en que son instalados. Sin embargo, si no son detectados y eliminados, pueden

[70] *Viruslist.com todo sobre seguridad en internet. Amenazas Corporativas(2 de febrero de 2015) {En línea}.http://www.viruslist.com/sp/analysis?pubid=207271238#00*

causar serias consecuencias financieras. Los propietarios de sitios web usan estos programas para hacer que los equipos infectados efectúen llamadas a sitios (teléfonos) de pago. Con gran frecuencia son sitios pornográficos. Aunque no se causan daños al ordenador, una gran factura de teléfono hace que estos programas no sean del agrado de los propietarios de ordenadores y redes."[71]

Estos dialers son utilizados de dos formas como marcadores troyanos o como marcadores maliciosos. Estos dos son instalados sin conocimiento de los usuarios y aunque la diferencia es que el troyano realiza las llamadas en forma automática en cambio el malicioso avisa sobre la llamada que se está haciendo.

- **Descargadores (downloaders):** Estos son programados "para funcionar en segundo plano, sin la intervención directa del usuario. Para un hacker es fácil sustituir los enlaces para dirigir al programa hacia recursos infectados, haciendo que los programas maliciosos sean descargados al equipo víctima sin que el usuario se dé cuenta."[72]
- **Servidores FTP:** "Son utilidades que se pueden usar para obtener acceso a archivos remotos. Una vez que un hacker las instala en un sistema, hace posible que los usuarios remotos descarguen cualquier archivo del equipo víctima y monitoreen las actividades en el ordenador infectado."[73]
- **Servidores proxy:** "Estas utilidades en un principio se diseñaron para proteger las redes internas, separando las direcciones internas de los usuarios externos. No obstante, los hackers las usan para conectarse a Internet de forma anónima. La dirección real del hacker se sustituye por la dirección del servidor proxy."[74]
- **Servidores Telnet:** "Estas utilidades se diseñaron para proporcionar acceso remoto a los recursos ubicados en otros equipos. Los hackers las usan para obtener acceso total a los equipos víctimas."[75]
- **Servidores Web:** "Los servidores web proporcionan acceso a las páginas web ubicadas en un área determinada del sistema de archivos. Los hackers

[71] *Viruslist.com, todo sobre seguridad en internet. Programas afines a los programas maliciosos(9 de febrero de 2015) {En línea}.http://www.viruslist.com/sp/virusesdescribed?chapter=152540533*
[72] *Ibíd.*
[73] *Ibíd.*
[74] *Viruslist.com, todo sobre seguridad en internet. Programas afines a los programas maliciosos(9 de febrero de 2015) {En línea}.http://www.viruslist.com/sp/virusesdescribed?chapter=152540533*
[75] *Ibíd.*

las usan para obtener acceso irrestricto al sistema de archivos del equipo de la víctima."[76]

- **Clientes de IRC:** "Estas utilidades proporcionan acceso a los canales de IRC. Esta prestación se puede explotar para escribir troyanos y gusanos de IRC. Mientras instalan un troyano IRC en un equipo víctima, los hackers con frecuencia también instalan un cliente IRC."[77]
- **Monitor:** "Son utilidades legales que monitorean las actividades del ordenador y del usuario. En el mercado existen versiones comerciales de este tipo de utilidad. Normalmente, la información de las actividades se guarda en el disco duro o se envía a las direcciones de correo electrónico especificadas. Los programas de monitoreo se diferencian de los troyanos espías sólo en que éstos no disimulan su presencia en el sistema y es posible desinstalarlos."[78]
- **Herramientas de recuperación de contraseñas (PSWTool**): "Sirven para recuperar contraseñas perdidas u olvidadas. Por lo general, muestran información sobre la contraseña en la pantalla, o la guardan en el disco duro. Cuando se realiza un ataque, esta información es enviada al atacante remoto."[79]
- **Herramientas de administración remota (RemoteAdmin):** "Estas herramientas de administración remota proporcionan a los hackers un control completo sobre el equipo víctima."[80]
- **Crackers:** "Estos programas no son virus ni troyanos, sino herramientas que usan los hackers para "piratear" diferentes tipos de software. Por lo general no representan peligro para los programas instalados y su función se reduce a eliminar la protección contra copia o introducir una clave "pirateada" en los programas."[81]
- **Bromas pesadas y mensajes falsos (Hoaxes):** "Este grupo incluye programas que no causan ningún daño directo a los equipos que infectan. No obstante, muestran advertencias falsas sobre supuestos daños ocurridos o por ocurrir. Pueden ser mensajes advirtiendo a los usuarios de que los discos se han formateado, que se ha encontrado un virus o se han

[76] *Ibíd.*
[77] *Ibíd.*
[78] *Viruslist.com, todo sobre seguridad en internet. Programas afines a los programas maliciosos(9 de febrero de 2015) {En línea}.http://www.viruslist.com/sp/virusesdescribed?chapter=152540533*
[79] *Ibíd.*
[80] *Ibíd.*
[81] *Ibíd.*

detectado síntomas de infección. Las posibilidades son limitadas sólo por el sentido del humor del autor del virus."[82]

Tipos de malware:

- **Trojan-SMS:** Se suscribe a la víctima a números de mensajería Premium sin su consentimiento, conocido como *Android/TrojanSMS.Boxer.AA*.
- **RiskTool: "**Es cualquier programa que automáticamente muestra publicidad web al usuario durante su instalación o durante su uso para generar lucro a sus autores"[83]
- **Adware: "**Es aquel que difunde publicidad a través de banners, ventanas emergentes, etc. mientras está funcionando. Gracias a esta publicidad se subvenciona la aplicación. A veces, estos programas incluyen un código de seguimiento, que recoge información sobre los hábitos de navegación del usuario, funcionando como programa espías o spyware."[84]
- **Trojan:** "Se denomina 'caballo de Troya' a un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado."[85]
- **Exploit:** "Es un fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo."[86]
- **Backdoor:** "En un sistema informático es una secuencia especial dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo (autentificación) para acceder al sistema."[87]
- **HackTool:** conjunto de herramientas que facilitan el ataque de los sistemas.
- **Atmer:** Diseñada para robar dinero a cajeros automáticos

---

[82] *Viruslist.com, todo sobre seguridad en internet. Programas afines a los programas maliciosos(9 de febrero de 2015) {En línea}.http://www.viruslist.com/sp/virusesdescribed?chapter=152540533*

[83] *Wikipedia, Adware. (9 de febrero de 2015) {En línea}.http://es.wikipedia.org/wiki/Adware*

[84] *Cimputer forensi, GLOSARIO. (9 de febrero de 2015) {En línea}http://www.delitosinformaticos.info/delitos_informaticos/glosario.html*

[85] *Wikipedia, Troyano (informática) (9 de febrero de 2015) {En línea}http://es.wikipedia.org/wiki/Troyano_%28inform%C3%A1tica%29*

[86] *Wikipedia, Exploit. (9 de febrero de 2015) {En línea}.http://es.wikipedia.org/wiki/Exploit*

[87] *Wikipedia Puerta trasera. . (9 de febrero de 2015) {En línea . http://es.wikipedia.org/wiki/Puerta_trasera*

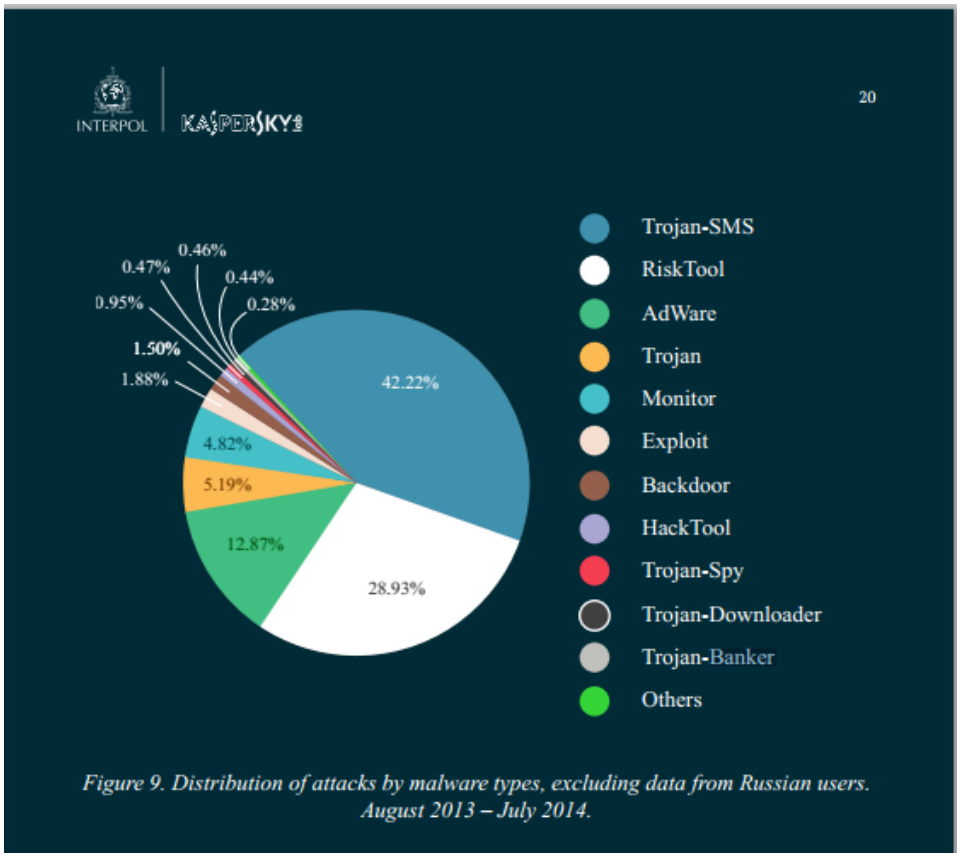


Ilustración 5 Virus más utilizaos por los hackers

En el 2012 se descubrieron vulnerabilidades que fueron aprovechadas por los hacker en done detectaron que los protocolos de código abierto como Heartbleed "(es un agujero de seguridad (*bug*) de software en la biblioteca de código abierto Open SSL)"[88]. Heartbleed es usado para comunicaciones por medio de internet, entre estas comunicación se incluye lo que son los coreos, Privadas Virtuales (VPN), esto lo hicieron mediante Shellshock, también conocida como 'Bash'. "La falla le permite al atacante adjuntar de forma remota un fichero malicioso a una variable que se ejecuta cuando se llama el intérprete de comando Bash (Bash es el Shell predeterminado en sistemas Linux y Mac OS X)". [89]

Por estas y otras razones, es seguro decir que la mayoría de las ciberamenazas móviles están apuntando Android.

[88] *Wikipedia, Heartbleed. (9 de febrero de 2015) {En línea}.http://es.wikipedia.org/wiki/Heartbleed*
[89] *Viruslist.com, todo sobre seguridad en internet., Kaspersky Security Bulletin 2014. Evolución del malware(9 de febrero de 2015) {En línea}.http://www.viruslist.com/sp/analysis?pubid=207271276*

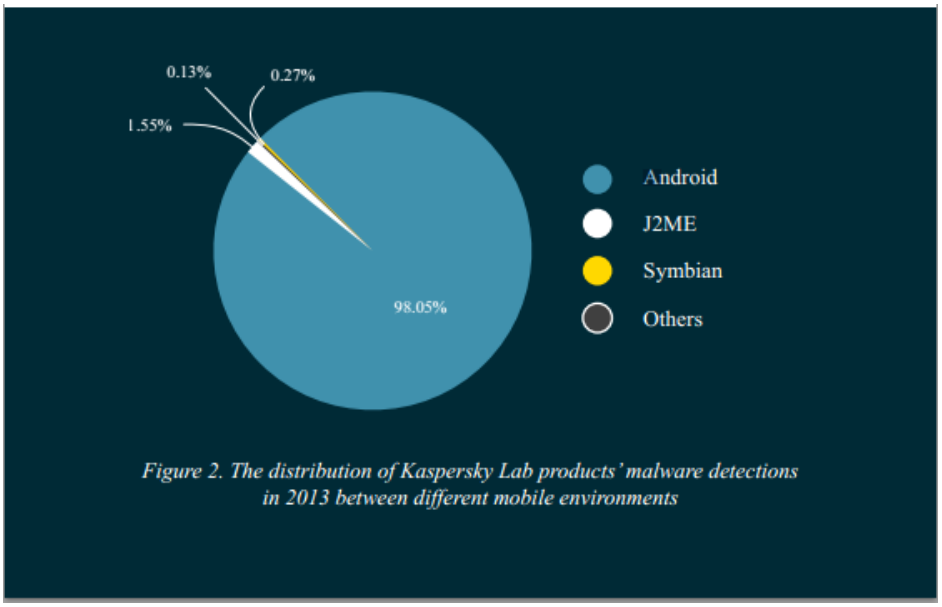


Ilustración 6 Sistemas operativos más atacados

"Es fácil entender por qué los ciberdelincuentes crean tantos programas maliciosos focalización dispositivos Android: estos días, los teléfonos inteligentes son cada vez más a menudo utilizados como una herramienta para pagar en línea para mercancías y servicios."[90] Los hacker utilizan el tipo de herramientas de virus móviles ya que el usuario muchas veces descarga e instalan aplicaciones de terceros no confiables al descargar estas aplicaciones o paquetes se está descargando con ellos un malware que se quedara instalado en el dispositivo por debajo del software corriendo.

Los ataques generados de la forma anteriormente explicada se ven en la gráfica siguiente por países:

[90] *Kaspersky Lab & Interpol Joint Report. Mobile Cyber Threats. (9 de febrero de 2015) {En línea}.http://media.kaspersky.com/pdf/Kaspersky-Lab-KSN-Report-mobile-cyberthreats-web.pdf*

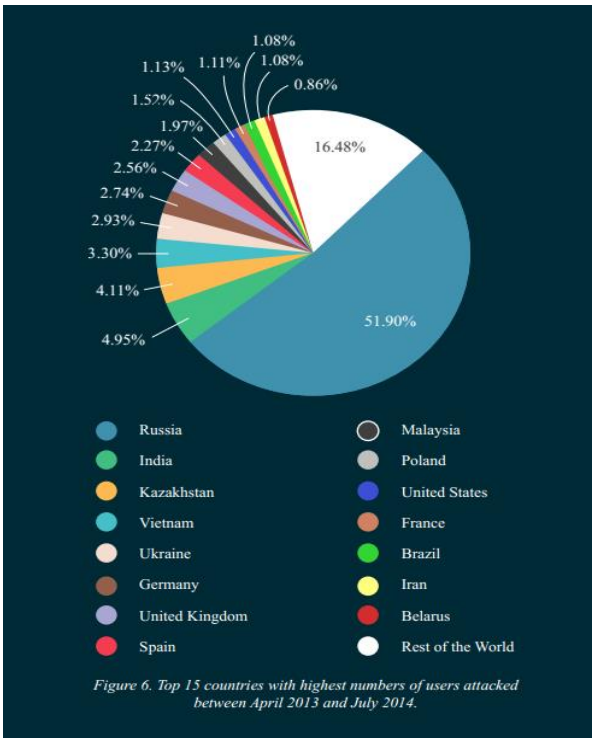


Ilustración 7. Países más Atacados

Otra de las herramientas muy utilizadas por los hacker es la nueva táctica que pasa en Facebook, Twitter, Instagram y Skype, este programa malicioso lo que hace es crear un perfil falso en cualquiera de estas redes, cuando la persona acepta la invitación, dicha persona recibe un mensaje y cuando el usuario lo responde se instala un programa que tiene como función instalarse en el ordenador y robar la información que esta guardada en este.

Luego de hablar de los grupos de herramientas utilizadas por lo hacker para vulnerar cualquier sistema o persona, ahora se explicara una de ellas las cuales son herramientas de seguridad y hacking que son extremadamente útiles en la obtención y explotación de redes y sistemas de información. Estas herramientas fueron diseñadas de tal manera que se puede recopilar la información necesaria para asegurar o explotar un computador o una red completa, esto depende de la persona que esté haciendo uso de la herramienta, es decir, todas estos programas son muy utilizados por los piratas informáticos y analistas de seguridad.

Las herramientas que se describirán a continuación son herramientas como anteriormente se mencionó de seguridad y hacking, estas fueron diseñadas para fines tanto legales como ilegales, aunque la mayoría de las personas piensan que estas herramientas son más útiles para los hacker que para aquellas personas

que son responsables de la seguridad y cuando en realidad están diseñadas para ayudar a los administradores y profesionales de seguridad a asegurar las redes y los sistemas de información, estas son las más utilizadas:

- **Nmap:** "Nmap ("Network Mapper") es una herramienta gratuita de código abierto para la exploración de la red o la auditoría de seguridad. Fue diseñado para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales"[91].
- Esta herramienta determina que hosts están disponibles en la red, qué servicios estos equipos ofrecen, qué sistemas operativos se están ejecutando y con estos docenas de otras características, todo esto para la seguridad de un sistema o contrario a ello para hackear aquellas empresas u organizaciones con mucha información valiosa, ya que esta se ejecuta en la mayoría de los ordenadores y consola y es utilizada porque es libre y de código abierto.
- **Nessus: "**Es el escáner de vulnerabilidades más popular y es utilizado en más de 75.000 organizaciones en todo el mundo. Muchas organizaciones alrededor del mundo están dando cuenta de los importantes ahorros de costes que estas reciben mediante el uso de Nessus como herramienta de auditoría de sistemas de información para la búsqueda de fallas críticas de seguridad"[92].
- **John the Ripper**: "Es esencialmente una herramienta de descifrado de contraseñas que se desarrolló para sistemas tipo UNIX. También sus desarrolladores han extendido su apoyo a los sistemas Windows y MAC[93].

Esta herramienta o software es comúnmente utilizado por usuarios para probar el nivel de seguridad de una contraseña elegida, pero también esta herramienta también puede ser usada para descifrar las contraseñas y entrar en un sistema o si se habla de un individuo para poder ingresar a sus correos o redes sociales.

Ripper "es compatible tanto con ataque de diccionario (probando todas las palabras en el diccionario, de ahí que nunca se debe elegir una palabra que se ha encontrado en el diccionario) y ataque de fuerza bruta (en este caso todas las posibles combinaciones son juzgados por lo tanto, si usted elige una contraseña que es alfanumérico y largo plazo, será difícil romperlo)"[94].

---

[91] Duarte Eugenio. Seguridad Informática, hacking seguridad informática. {11 julio2012} {En línea}. Disponible en: http://blog.capacityacademy.com/2012/07/11/las-8-mejores-herramientas-de-seguridad-y-hacking/

[92] Ibíd.

[93] Ibíd.

[94] *Duarte Eugenio. Seguridad Informática, hacking seguridad informática. {11 julio2012} {En línea}. Disponible en: http://blog.capacityacademy.com/2012/07/11/las-8-mejores-herramientas-de-seguridad-y-hacking/*

- **Nikto:** “Es un software de código abierto (GPL) para escanear vulnerabilidades en los servidores web. Esta herramienta tiene el potencial de detectar más de 3200 archivos potencialmente peligrosos CGIs, versiones sobre más de 625 servidores, y los problemas específicos de la versión de más de 230 servidores. Los elementos de exploración y plugins pueden ser actualizado automáticamente (si se desea)”[95].
- **Wireshark: “**Es un programa analizador de protocolos de red o sniffer, que le permite capturar y navegar de forma interactiva por los contenidos de los paquetes capturados en la red. El objetivo del proyecto fue crear un analizador de calidad comercial para Unix. Funciona muy bien en Linux y Windows (con una interfaz gráfica de usuario), fácil de utilizar y puede reconstruir flujos TCP / IP y VoIP!”[96].
- **NetStumbler:** “Es una herramienta de detección de redes inalámbricas para Windows. NetStumbler es una herramienta para Windows que permite detectar redes de área local (WLAN), usando 802.11b, 802.11ay 802.11g”[97].
- El uso de esta herramienta está basado para verificar que una red está configurada de la manera segura para cualquier usuario, ayuda a detectar otras redes que puedan estar causando interferencias en la red, también sirve para detectar AP no autorizados “rogue” en su lugar de trabajo.
- **Metasploit:** “Es un proyecto de seguridad informática que proporciona información sobre las vulnerabilidades, ayuda en las pruebas de penetración y en la ejecución de la explotación de vulnerabilidades de seguridad”[98].
- Metasploit es un conjunto de herramientas que ayuda a los profesionales de seguridad y hacker a llevar a cabo ataques informáticos de manera sistematizada y automatizada.
- **Eraser:** “Es una herramienta avanzada de seguridad (para Windows), que le permite eliminar completamente los archivos de tu disco duro, sobre escribiendo varias veces con patrones cuidadosamente seleccionados”[99].

Esta herramienta es útil para los hacker ya que es una excelente herramienta para mantener los datos realmente seguro, si se ha eliminado, es decir cuando estos efectúen algún daño o vulnerabilidad no dejaran rastro alguno y es útil ya que es

[95] *Ibíd.*
[96] *Ibíd.*
[97] *Ibíd.*
[98] *Ibíd.*
[99] *Taringa. Las Herramientas Hacking/Seguridad más usadas. {Junio 2011} {En línea}. Disponible en: http://www.taringa.net/posts/apuntes-y-monografias/11561390/Las-Herramientas-Hacking-Seguridad-mas-usadas.html*

un software libre y su código fuente se distribuye bajo licencia GNU General Public License.

- **Yersinia:** "Es una herramienta de red diseñada para tomar ventaja de algunas debilidades en los diferentes protocolos de capa 2, es decir capa de enlace. Pretende ser un marco sólido para analizar y probar redes y sistemas"[100].

Un poco más adentro de estas herramientas el hacker tiene una anatomía de como hackear la cual está dividida por el objetivo a hackear, en el cual se centran en lo que van o a quien van a vulnerar, a clave en esta fase es no perderse de ningún detalle, la metodología, es aquella que van hacer, como lo es el rastreo, el robo, la obtención de acceso, etc., la técnica que es lo que ejecutan para realizar el objetivo y por último la herramienta a utilizar, que es aquella que hacen uso para realizar las técnicas, un ejemplo de este seria:

- Objetivo: Conseguir el espacio de nombres y los rangos de direcciones del sistema objetivo, así como reunir toda la información posible sobre el sistema a atacar, son actividades esenciales para realizar ataques quirúrgicos.
- Metodología: Rastreo
- Técnica: Búsquedas en las fuentes abiertas Whois, Interfaz web a whois, ARIN who is, Transferencia de zona DNS
- Herramientas: USE Net, motores de búsqueda, Cualquier cliente UNIX"[101].

Es por ello, que los hacker si comprende por completo como funciona cierto software de aplicaciones y de sistemas así como sus debilidades, para estos las debilidades estructurales del software es la llave de la tierra prometida, por que dichas debilidades son los objetos de explotación"[102].

4.1.7 Imagen de la sociedad sobre el hacker

Para tener contexto y verlo con un poco de historia sobre la imagen de los hacker, se sabe que desde "la introducción del ordenador personal a finales de los 70, la inspiración por el hacking ha crecido no solo en amplitud y miembros, sino que

[100] *Taringa. Las Herramientas Hacking/Seguridad más usadas. {Junio 2011} {En línea}. Disponible en: http://www.taringa.net/posts/apuntes-y-monografias/11561390/Las-Herramientas-Hacking-Seguridad-mas-usadas.html*
[101] *Google Sites. Hacker piratas informáticos, anatomía de una acción de hacker. {En línea}. Disponible en: https://sites.google.com/site/hackerspiratasinformaticos/anatomia-de-una-accion-de-hacker*
[102] *Ibíd.*

también ha cambiado la dinámica de la institución, como resultado del cambio del papel de la tecnología en la sociedad. Por tanto, la imagen pública del "típico" hacker se ha transformado de novato inocuo a techno-criminal maligno"[103].

Es por esto que la imagen que se tienen de los hacker varían de acuerdo con la posición socio-política del grupo o individuo que lo defina, una de estas es que son definidos como entusiastas de la informática que tienen un interés apasionado en aprender acerca de los sistemas informáticos y cómo usarlos de formas innovadoras y por otro lado es que la mayoría de los estudios realizados siempre se han enfocado en dos perspectivas: una, es aquella que se tiene como una figura criminal, es por esto que se emplea teorías derivadas para explicar la formación y organización de la comunidad hacker; y la segunda imagen o teoría que se ha dado es que se enfoca en las actuales leyes de crimen-informático y como los hackers son privados de sus derechos Constitucionales, no pueden hacer nada al respecto con sus actos buenos.

A pesar de todas las imágenes o significados que se tienen de estos personajes, estos pequeños o grandes grupos juegan actualmente un papel vital en la progresión de la tecnología, ya que realizan funciones reguladoras para el control social, protestando, burlando, e ingeniosamente abriendo el control estatal y corporativo por medio de los ordenadores y tecnologías relacionadas con los mismos"[104].

Es por ello que aún si los hacker son buenos para la sociedad, la envidia de los medios y los celos colectivos, están inculcando a la sociedad que sus actividades son criminalizadas y ahora los hackers están siendo perseguidos por la ley a una escala desproporcionada a la amenaza actual que plantean. Los hackers quieren que sus motivaciones y éticas sean vistas como legítimas, o al menos entendidas, en vez de ser simplemente descritos como tortuosos adolescentes que no tienen nada mejor que hacer que molestar cada uno de los ordenadores disponibles"[105].

Ejemplo de la forma de protestar de los hacker en contra de la imagen que se tiene de ellos, es que estos realizan actividades relativamente inofensivas que son partes de dicha protesta, por ser considerados ilegal, como ocurre con cualquier subcultura revolucionaria, el movimiento hacker es estigmatizado, desacreditado, y perseguido por los medios de comunicación y la cultura

---

[103] *Borghello Cristian. Amenazas Humanas - Hackers: Rebeldes con Causa. {2009} {En línea}. Disponible en: https://www.segu-info.com.ar/amenazashumanas/hackers_rebeldes.htm*

[104] *Ibíd.*

[105] *Ibíd.*

corporativa como juvenil, trastornador, y criminal. Y, todo el tiempo, es generalmente malinterpretado.

Para ver un contexto fuera de Colombia, en España para “Javier Garaloces, presidente de la Asociación para la Información de Hackers (AIH), el problema es que no se distingue entre las varias comunidades que hay”[106].

“En contra de lo que muestran los medios de comunicación -explica Garaloces- los hackers nos consideramos útiles. El presidente de la AIH cree que «el hacking es una actitud ante la vida». El hacker tiene un compromiso social y uno de sus principios es «el conocimiento libre». «Creemos que la información debe circular libremente y que no debe prohibirse el acceso a ella», asegura. Respecto al objetivo que persigue el hacker con su actividad, Garaloces afirma que se trata de «conseguir el reconocimiento de la comunidad y sentirse útil»”[107].

Es por ello que Garaloces en Madrid, conforma esta asociación de hacker primero, para fomentar la buena imagen de estos y por otra parte, desde abril del año pasado conforman una campaña contra la pornografía infantil en Internet. Los hackers de esta asociación trabajan en la destrucción de este tipo de páginas web otra actividad de esta organización de hacker es que estos realizan actividades en la detección de fallos de seguridad en los sistemas, es decir si detecta un fallo de seguridad, el hacker avisa al administrador del sistema, su intención nunca es la de dañar a la empresa o persona de dicha vulneración.

Un ejemplo claro de la visión de la sociedad, se puede ver en el tan mencionado grupo anonymous de hackers, a quien muchos de nuestra sociedad denominan terroristas y otros libertadores y protectores de la libertad, es por ello que este grupo de personas se ha estado gente en todo el mundo día a día más y más gente que se une a la causa de este grupo de hackers, a la vez la popularidad de estos personajes y sus de imágenes aumentaba, la idea de Anonymous como un colectivo de individuos sin nombre se convirtió en un meme o fenómeno de Internet.

Para ver a fondo en nuestro universo de estudio, en este caso la comunidad estudiantes de pregrado y postgrado, más los docentes de la universidad piloto de Colombia, de cómo estos tienen muchas imágenes, creencias o significados de los hacker dependiendo en el estado en que se encuentra o simplemente en el

[106] *Hemeroteca. Los hacker españoles quieren rehabilitar su imagen ante la sociedad. {08 octubre 2103} {En línea}.disponible en: http://www.abc.es/hemeroteca/historico-08-10-2003/abc/Internet/los-hackers-espa%C3%B1oles-quieren-rehabilitar-su-imagen-ante-la-sociedad_212503.html#*

[107] *Ibíd.*

momento en que le hacen la pregunta en qué piensa usted cuando escucha la palabra hacker?, es allí donde se empieza a indagar por la imagen de hacker en nuestra sociedad, casi todo el mundo debe tener una idea, aunque sea muy equivocada, sobre cómo es y qué hace un hacker, por ejemplo una imagen de este puede ser aquella persona genio de la informática que con una computadora y conexión a internet es capaz de hacer cualquier cosa que se proponga o también aquella persona que por una cantidad de dinero, no tiene inconvenientes en guardar cualquier respeto en el bolsillo.

Otra imagen que las personas ven sobre este personaje, es que lo imaginan como un soñador, que es aquel que lucha por la libertad de información y la protección de la privacidad en internet, un ejemplo de este es el de "Edward Snowden, el ex empleado de la CIA que hizo pública una serie de documentos clasificados como alto secreto, que destaparon uno de los mayores escándalos de espionaje en la historia de Estados Unidos, y que desde entonces vive en un exilio forzoso"[108].

Con lo anterior mencionado se ve que hay significados infinitos sobre la figura de un hacker en la sociedad, en su gran parte de estas imágenes pueden ser mitos creados por películas, libros o periodistas.

4.1.8 Jóvenes estudiantes reconocidos por cometer delito informático

En la actualidad se ven jóvenes hacker que utilizan este conocimiento para beneficio propio como fue la noticia de Alejandro Robayo (Estudiante de último semestre de la Universidad de los Andes), condenado a tres años de prisión, "cuando violó la plataforma de notas de su universidad y modificó algunas de sus calificaciones"[109]. Inicialmente con el objeto de modificar sus propias notas para mantener una beca y posteriormente como servicio ofrecido a terceros. Para el caso de Robayo este fue Según la Unidad de Delitos Informáticos de la DIJÍN, que realizó la investigación, más de 20 estudiantes pudieron haberle pagado a Robayo por cambiar notas y planillas de asistencia a clases."[110]. La Unidad de Delitos Informáticos de la DIJÍN al ver lo ocurrido con este estudiante adelanta investigaciones de denuncias realizadas por otras universidades en Bogotá, Pasto

[108] *Laurencena Víctor. Hackers: ¿héroes o piratas? {Marzo 2014} {En línea}. Disponible en: http://www.rumbosdigital.com/secciones/notas/hackers-heroes-o-piratas.*

[109] El Espectador, Valentina Obando Jaramillo {En línea} {2015, Mayo 15}.Disponible en: http://www.elespectador.com/noticias/judicial/universidades-victimas-de-hackers-articulo-560884.

[110] El Espectador, Valentina Obando Jaramillo {En línea}{2015, Mayo 15}.Disponible en: http://www.elespectador.com/noticias/judicial/universidades-victimas-de-hackers-articulo-560884

y Barranquilla en donde no solo se investiga casos realizados por los estudiantes sino también en otro tipo de empleados como los de admisiones y registro entre otro.

Otro de los casos Colombianos muy sonados es el de "un joven estudiante de ingeniería de sistemas que logró acceder a la cuenta del periodista y director de la revista SOHO Daniel Samper Ospina. Así como el bloqueo de la página de la Registradora en las elecciones parlamentarias de 2010."[111]

4.1.9 Grupos de Jóvenes Que Realizan Delito Informático

Actualmente existen las nuevas conformaciones de grupos de Hacker que se unen para realizar delitos informáticos, este es el caso de Gerson Daniel Peña Mejía que hacia parte de la banda los Troyanos, que tiene 20 miembros y se dedicaba a delitos informáticos. Este grupo se dedicaba a "reclutar jóvenes estudiantes de ingeniería de sistemas con la idea de instruirlos sobre los delitos informáticos, trabajar con ellos y hacer los fraudes"[112]. Así como este personaje se encuentran miles de organizaciones en el mundo que ahora se dedican al reclutamiento de jóvenes con conocimientos en sistemas y con la capacidad de querer aprender sobre cómo realizar ataques a diferentes organizaciones. Muchas veces se vende la idea de una ganancia económica fácil y de la poca posibilidad de ser descubiertos y judicializados por lo que muchos jóvenes estudiantes se inclinan a formar parte de estos grupos y comenzar a ser Hacker para estas organizaciones. En las que podemos encontrar reconocidos nombres como: Anonymous, Legion of Doom (LOD), Milw0rm, LulzSec entre otros.

Es importante resaltar que también existe aquellos grupos y comunidades positivas como BSidesCO que es un espacio que busca desarrollar y compartir conocimiento en seguridad de la información, teniendo de la mano aquellos hacker de sombrero blando expertos en seguridad informática tomando este conocimiento como innovador y positivo más que un aprendizaje negativo y contrarrestar la problemática que a diario sufre Colombia y diferentes organizaciones. Estos grupos son orientados en su mayoría por jóvenes con grandes conocimientos del

[111] El Espectador, María Camila Rincón Ortega, Santiago La Rotta {En línea} {2014, Febrero 8}.Disponible en: http://www.elespectador.com/noticias/actualidad/el-oscuro-mundo-de-los-hackers-articulo-473752.

[112]El Heraldo, Cayó hacker que presuntamente reclutaba estudiantes. {En línea}{2015, Junio 25}.Disponible en: http://www.elheraldo.co/region/cayo-hacker-que-presuntamente-reclutaba-estudiantes-201632

mundo informático que presentan cursos, charlas, entrenamientos, etc. para capacitar sobre los riesgos y a su vez el intercambio de conocimiento en diferentes ámbitos de la asegurar informática.

La lucha contra los hacker no solo lleva a grupos Colombianos como el mencionado anteriormente sino también organizaciones a nivel mundial como: GEANC (Grupo de Expertos de Alto Nivel sobre Ciberseguridad, que elabora recomendaciones que ayudarán a coordinar en todo el mundo la lucha contra la constante evolución de la ciberdelincuencia y las amenazas a las redes.

En el delito informático en Colombia se observa un aumento que se presenta muy frecuentemente por empleados que trabajan o que han trabajado para la empresa, corporación o compañía, ya que roban la información o los secretos corporativos de estos, para luego aprovecharse de ello y hacer daño, contando con credenciales que muchas veces no fueron eliminadas o desactivadas al retirarse el empleado de la compañía.

4.1.10 Delito informático del hacker

Para encajar en el tema se muestra como las innovaciones en nuestra vida son buenas o por el contrario malas, dependiendo el uso que le demos un ejemplo claro de esta proposición es “Recordando un poco la historia, al ser humano actual le ha sucedido lo mismo que a nuestros antepasados prehistóricos cuando fabricaron el primer cuchillo. Tuvo un gran alivio en sus labores diarias, se sintió feliz, porque ya contaba con una herramienta que le ayudaría en sus tareas cotidianas de supervivencia. Pero no faltó quien usara esta herramienta con otras intenciones en contra de sus congéneres y terminara cometiendo delitos que, seguramente, en su momento no se llamaron así, aunque sí se entendían como actos en contra de la supervivencia de los demás”[113].

Así mismo observando la historia, se ve que en nuestra actualidad ocurre algo similar con los sistemas informáticos y la tecnología, las personas están cada día más interesadas por descubrir algo más allá de estas mismas, debido a su vertiginoso desarrollo y a la enorme influencia que ha alcanzado en muchas de las actividades diarias de las personas y las organizaciones.

“Así como la tecnología y su desarrollo han incidido en prácticamente todas las actividades del ser humano a lo largo de su historia, en la actualidad, la

[113] *Ojeda-Pérez, Jorge Eliécer; Rincón-Rodríguez, Fernando; Arias-Flórez, Miguel Eugenio & Daza-Martínez, Libardo Alberto. Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad. {En Línea} {febrero 2010}. Disponible en: http://www.scielo.org.co/scielo.php?pid=S0123-14722010000200003&script=sci_arttext*

dependencia tecnológica ha venido concentrándose cada vez más en el fenómeno de la tecnología informática, la información y la comunicación. Con efecto retardado, se descubrió luego que ese desarrollo venía acompañado de distintos y también novedosos riesgos"[114].

Observando lo anterior con la historia y el presente de nuestros sistemas informáticos, se ve como día tras día, los sistemas atraen riesgos muchos de ellos realizados por hacker esos riesgos se representa por los delitos informáticos, los cuales existen muchos tipos de delitos, la diversidad de comportamientos constitutivos de esta clase de ilícitos es inimaginable, a decir de "Camacho Losa, el único límite existente viene dado por la conjugación de tres factores: la imaginación del autor, su capacidad técnica y las deficiencias de control existentes en las instalaciones informáticas"[115]. Los siguientes ítems son algunos de los delitos informáticos de la actualidad:

- Los fraudes: En este tipo de delito se ven los datos falsos o engañosos, las falsificaciones informáticas, la manipulación de los datos, entre otros cuantos delitos más.
- El sabotaje informático: En el sabotaje se ve los gusanos, los virus informáticos y malware, el ciberterrorismo, los ataques de denegación de servicios, etc.
- El espionaje informático y el robo o hurto de software: en este delito se puede ver la fuga de datos, la reproducción no autorizada de programas informáticos de protección legal entre otros cuantos.
- El robo de servicios: En el robo se entiende cuando hay hurto del tiempo del computador, la apropiación de informaciones residuales (Scavenging), robo de datos de personas o empresas, etc.
- El acceso no autorizado a servicios informáticos: en este delito se ve las puertas falsas, la llave maestra entre otros accesos no autorizados.

Por otro lado se observa el indiscutible crecimiento de delitos en la Internet, ya que los ámbitos de la actividad humana son cada vez mayor en este medio, es decir a estos ambientes de personas se le suma los millones de transacciones

[114] *Ojeda-Pérez, Jorge Eliécer; Rincón-Rodríguez, Fernando; Arias-Flórez, Miguel Eugenio & Daza-Martínez, Libardo Alberto. Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad. {En Línea} {febrero 2010}. Disponible en: http://www.scielo.org.co/scielo.php?pid=S0123-14722010000200003&script=sci_arttext*

[115] *Ojeda-Pérez, Jorge Eliécer; Rincón-Rodríguez, Fernando; Arias-Flórez, Miguel Eugenio & Daza-Martínez, Libardo Alberto. Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad. {En Línea} {febrero 2010}. Disponible en: http://www.scielo.org.co/scielo.php?pid=S0123-14722010000200003&script=sci_arttext*

comerciales que se dan en la red, el intercambio de información entre las diferentes empresas y los millones de contactos sociales de todo tipo que se ofrecen en la red, por eso mismo la mayor parte de los usuarios ven en la Internet una posibilidad maravillosa de realizar estos intercambios encontrándose con situaciones muy positivas, pero también al margen de todo eso, hay muchas personas en todo el mundo que también exploran el lado oscuro que tiene Internet, como toda creación humana, hay este otro lado oscuro, que atenta contra todas estas sanas intenciones; el fraude, el abuso de confianza, el robo, la estafa electrónica, falsas loterías, el engaño, piratería, extorsiones, amenazas, calumnias, injurias, pornografía, explotación sexual infantil son algunos de los delitos que más frecuentemente que se ha encontrado en la red"[116].

Uno de los primeros ejemplos que se ve de delitos informáticos fue en 1980, en donde "la ArpaNet (Advanced Research Projects Agency Network) del Departamento de Defensa de Estados Unidos, creadora de la internet, documentó que en su red se emitieron extraños mensajes que aparecían y desaparecían en forma aleatoria, y que algunos códigos ejecutables de los programas usados sufrían una mutación; en ese momento, los hechos inesperados no pudieron comprenderse pero se les buscó solución"[117], otro caso que se ve fue el que ocurrió con el famoso gusano de Internet que lanzó Robert Morris Jr. en noviembre de 1988 y que acabó bloqueando más de 6 000 ordenadores, aunque en Estados Unidos se calcula que se generan perjuicios económicos, por los delitos informáticos, que superan los 10.000 millones de dólares o más de 5.000 millones de libras esterlinas en el Reino Unido. También hay que recordar que hasta la propia Dirección General de Policía en España, al igual que muchos otros países, ha tenido que crear un Grupo dedicado en exclusiva a los delitos informáticos. Casi el 90% de los delitos informáticos que investiga el FBI en Estados Unidos tienen que ver con Internet"[118].

Es por esto, que se tiene que hacer como dice "PHIL WILLIAMS Profesor de Estudios de Seguridad Internacional, Universidad de Pittsbugh45, Es necesario contar no solo con leyes e instrumentos eficaces y compatibles que permitan una cooperación idónea entre los estados para luchar contra la Delincuencia

[116] *Wordpress, myprofetecnologia. Delios informáticos. {En línea} {Octubre 2011}. Disponible en: https://myprofetecnologia.wordpress.com/2011/01/30/delitos-informaticos/*

[117] *Ojeda-Pérez, Jorge Eliécer; Rincón-Rodríguez, Fernando; Arias-Flórez, Miguel Eugenio & Daza-Martínez, Libardo Alberto. Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad. {En Línea} {febrero 2010}. Disponible en: http://www.scielo.org.co/scielo.php?pid=S0123-14722010000200003&script=sci_arttext*

[118] *Ramírez Emilio. Los Delitos Informáticos. Tratamiento Internacional. {En Línea} {Mayo 2009}. Disponible en: http://www.eumed.net/rev/cccss/04/rbar2.htm*

Informática, sino también con la infraestructura tanto técnica como con el recurso humano calificado para hacerle frente a este nuevo tipo de delitos transnacionales"[119].

Ya para nuestro país los delitos informáticos va en aumento, esto se puede ver que nuestro país es actualmente, el tercer país en Latinoamérica donde más se cometen estos delitos informáticos, ya que mensualmente se calcula que 187 denuncias son interpuestas por fraude a diferentes bancos, así lo reveló en los últimos días "el Colegio Colombiano de Juristas, que explicó que la lista de esta modalidad de delito la encabezan Brasil y México. Algunos de los delitos electrónicos que más se presentan en el país y que, según expertos de la Fiscalía, van en aumento son acceder a bases de datos de bancos u otras entidades sin permiso, sustraer archivos de computadores, ingresar a redes sociales y correos ajenos y clonar tarjetas bancarias".

Ya para nuestro país se puede ver un ejemplo, ocurrido en Cali, "cuando un exejecutivo bancario que hurtaba dinero a los clientes de la entidad financiera en la que trabajaba fue capturado por el CTI sindicado del delito de hurto por medios informáticos y falsedad en documento privado. De acuerdo con la investigación, el hombre, en su calidad de ejecutivo, accedía a las cuentas de los usuarios suplantando su firma y su huella. Así, retiraba dinero que éstos poseían en sus cuentas. Desde el año 2009 hurtó a los clientes del banco $360 millones"[120].

"Hoy en día un computador, un celular, cámaras de video, un televisor de alta gama o una consola de video juegos, son aparatos que permiten guardar todo tipo de información que muchas veces es considerada valiosa para los investigadores del lado oscuro, lo que hace que el seguimiento a delitos informativos se convierta en un desafío para la los del CTI de la Fiscalía colombiana. Así lo afirma "Fabio Herrera, ingeniero del Grupo de Delitos Informáticos, dependencia adscrita al CTI de la Fiscalía General de la Nación"[121].

Otro ejemplo que se ve en la sociedad colombiana por delitos informáticos y que relaciona la cita anterior, fue un allanamiento que se encontró en un Smart Tv, un televisor de última gama, que tenía un disco duro con evidencias valiosas de información.

En conclusión se puede ver que las modalidades de delitos informáticos que se presentan en el país no solo están ligadas a la clonación de tarjetas bancarias, el acceso a bases de datos sin permiso, la sustracción de archivos de computadores,

---

[119] *Acurio Santiago. Delitos informáticos: Generalidades. {En línea} {2009}. Disponible en: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf*

[120] *Elpais.com. En Colombia las cifras de delitos informáticos van en aumento. {En línea}{Diciembre 2012}. Disponible en: http://www.elpais.com.co/elpais/judicial/noticias/colombia-cifras-delitos-informaticos-van-aumento*

[121] *El Universal. El delito informático es muy joven en Colombia. {En línea}{09 marzo 2014}. Disponible en: http://www.eluniversal.com.co/tecnologia/el-delito-informatico-es-muy-joven-en-colombia-fiscalia-153299*

sino también a los insultos a través de redes sociales o correos electrónicos, la suplantación de personas, los ataques de tipo cibernético y hasta las amenazas de muerte a través de la web, cada día los delincuentes aprovechan las nuevas tecnologías para crear nuevas formas de robo u ocultamiento de la información, lo que muchas veces resulta en delitos que atentan con el buen nombre o perjudican el bolsillo de las personas.

Un grupo en Colombia el cual es conocido como el "Grupo de Delitos Informáticos del CTI de la Fiscalía ha tenido a su cargo varios casos de connotación nacional, entre los que se destaca la violación de información encontrada en los computadores de los fallecidos guerrilleros de las Farc, Raúl Reyes y Alfonso Cano y del extraditado Rodrigo Tovar Pupo conocido como Jorge 40, además también tuvieron en sus oficinas el caso de las conocidas 'chuzadas del DAS' en donde se analizó toda la evidencia encontrada en interceptaciones telefónicas y seguimientos ilegales realizados por la agencia de inteligencia colombiana, durante el gobierno del presidente Álvaro Uribe"[122].

Es por esto que para Colombia, con algunos antecedentes de carácter jurídico (sobre la base de los derechos de autor) y alguna normatividad complementaria (Código Penal y circulares de la Superintendencia Financiera), en 2009 se logró expedir la Ley 1273, con la cual pudo acceder al grupo de países que se han preparado con herramientas más eficaces para contrarrestar las acciones delictivas del cibercrimen, en sectores claves de la sociedad como el financiero, cuyas condiciones de vulnerabilidad son las más estudiadas e investigadas por los delincuentes informáticos.

La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes"[123].

A continuación se dará una de las últimas noticias conocidas por delitos informáticos en tres las cuales se destaca:

- Detienen a tres ciberdelincuentes por defraudar un millón de euros: Engañaron a varios bancos tras robar los correos electrónicos de sus víctimas y ordenar transferencias de más de 600.000 euros. La Unidad Central de Delitos Informáticos de los Mossos d'Esquadra detuvieron el

[122] *I El Universal. El delito informático es muy joven en Colombia. {En línea}{09 marzo 2014}. Disponible en: http://www.eluniversal.com.co/tecnologia/el-delito-informatico-es-muy-joven-en-colombia-fiscalia-153299.*

[123] *Gandini isabella. Ley de Delitos Informáticos en Colombia. {En línea} {Abril 2014}. Disponible en: http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia*

pasado 4 de febrero a tres personas de 36, 37 y 38 años, nacionalidad española y vecinos del municipio madrileño de Ciempozuelos acusados de un delito de estafa continuada. http://ccaa.elpais.com/ccaa/2015/02/18/catalunya/1424247738_506080.html

- Un mundo en supe alerta: Ataques recientes como el sufrido por Sony por la película 'La entrevista' anuncian una época de inseguridad prolongada e intensa debido a las amenazas informáticas. La división de Sony en Estados Unidos sufrió un ataque informático de dimensiones históricas. Toda la infraestructura de datos y comunicaciones de la compañía fue víctima de piratas despiadados que dejaron al descubierto un tesoro de contratos confidenciales, contenido creativo, correos electrónicos embarazosos, información económica reservada, acuerdos de compensación, documentos legales secretos y mucho más. Se calcula que los daños totales sobrepasaron los 100 millones de dólares (88.320.000, en euros). El propósito del ataque no era el robo de secretos profesionales ni el espionaje industrial convencional. El objetivo aparente era crear el caos y la destrucción en venganza por la intención de Sony de distribuir The Interview, una comedia de humor grosero (estrenada el viernes en España) en la que se ridiculizaba al líder supremo de Corea del Norte, Kim Jong-un. http://internacional.elpais.com/internacional/2015/02/06/actualidad/1423251886_196084.html

- Madonna, 'hackeada': Hace dos meses un pirata informático israelí fue detenido como presunto autor de las filtraciones de varios temas de *Rebel Heart,* el último trabajo discográfico de la reina del pop, al haber accedido a su ordenador personal. http://elpais.com/elpais/2015/02/06/opinion/1423247749_434323.html

- La policía arresta a 12 personas por entrar en ordenadores del Santander en Londres: Los arrestados lograron presuntamente controlar todos los ordenadores de una sucursal en Londres. Las fuerzas del orden detuvieron el jueves a once hombres, de edades comprendidas entre los 23 y los 50 años, en Hounslow, al suroeste de Londres, mientras que otro, de 34 años, fue arrestado en el puente de Vauxhall, en el suroeste de la ciudad. Doce personas han sido detenidas en Londres en relación con un supuesto complot para acceder a los ordenadores del Banco Santander con el objetivo de robar, informó este viernes la Policía. http://economia.elpais.com/economia/2013/09/13/actualidad/1379064512_059825.html
- Ciberespías chinos logran sortear a EE UU y robar secretos militares vitales: La Casa Blanca se dispone a pedir cuentas al país asiático por la tecnología robada gracias a la piratería informática. los ciberespías

chinos la engañaran. Durante tres años, unos piratas informáticos vinculados al ejército chino se infiltraron en los ordenadores de QinetiQ y pusieron en peligro la mayor parte de su labor investigadora, por no decir toda. En un momento dado, se introdujeron en la red interna de la compañía aprovechando un fallo de seguridad que se había descubierto meses antes y nunca se había reparado. http://internacional.elpais.com/internacional/2013/05/04/actualidad/1367700469_570919.html

- La Policía Nacional detuvo a 270 personas en 2012 por delitos de piratería: Las falsificaciones de 'software' superan a las copias ilícitas de material audiovisual Las plantillas territoriales arrestaron a un 50% menos de infractores que en 2011. El año pasado 270 personas fueron detenidas por delitos contra la propiedad intelectual por las distintas unidades de la Policía Nacional que investigan las copias y falsificaciones de obras audiovisuales, literarias o informáticas. Los dos grupos especializados en este tipo de infracciones detuvieron en 2012 a algo más de un centenar de personas en 57 operaciones desarrolladas durante el año. A esta cifra hay que sumar los 164 arrestos de las plantillas territoriales, casi un 50% menos que en 2011, año en el que 317 personas fueron detenidas, según cifras que la Policía Nacional ha adelantado hoy, Día Mundial de la Propiedad Intelectual
http://cultura.elpais.com/cultura/2013/04/26/actualidad/1366972119_24577.html

4.1.11 Vulnerabilidades que aprovechan los hacker

Para hablar de aquellas vulnerabilidades que aprovechan los hacker, se define q es vulnerabilidad “según lo señalado por la Comisión Económica para América Latina (CEPAL), la vulnerabilidad es el resultado de la exposición a riesgos, aunado a la incapacidad para enfrentarlos y la inhabilidad para adaptarse activamente”[124].

Luego de conocer que es vulnerabilidad y ver cómo se puede acceder a esta la siguiente grafica muestra los abusos y ataques informáticos.

[124] *Caro Elizabeth. La Vulnerabilidad Social Como Enfoque De Análisis De La Política De Asistencia Social. {julio 2003} {En línea}. Disponible en: http://www.cepal.org/celade/noticias/paginas/9/12939/eps9_ecaro.pdf*

Analizando la gráfica se ve algunos de los abusos más aprovechados por hacker en cuanto a el pishing, como lo es la penetración al sistema exterior, abusos por parte del empleado y virus de la computadora, aunque entre otros esta es el software obsoleto, el código erróneo, los activos digitales abandonados o errores de los usuarios, estas son algunas de las principales amenazas que acechan a las empresas en lo que a su seguridad se refiere, estas vulnerabilidades los hacker la explotan mediante diversos métodos, como lo son las peticiones DNS, exploit kits, ataques de amplificación que muchas veces son mucho más sencillas de explotar de lo que muchos piensan, al estar basadas en vulnerabilidades conocidas.

Un ejemplo de estas vulnerabilidades se ve los ataques DdoS, los cuales aumentaron un 90% en el último trimestre de 2014 "Akamai Technologies ha presentado un informe sobre la cantidad de ataques DDoS (denegación de servicio) producidos durante el último trimestre de 2014**,** según el informe, los ataques DDoS en el último trimestre de 2014 se hann incrementado un 90% con respecto al mismo periodo de 2013, y un 57% con respecto al tercer trimestre de 2014**.** También se ha detectado el uso de un mayor ancho de banda medio por parte de los que utilizan esta forma de atacar servidores, con un incremento del 52%"[125]**.** Ya para Colombia se ve como estas vulnerabilidades van en aumento un ejemplo de esto es la siguiente tabla sobre casos de vulnerabilidades registrados en cada país

Se ve que Colombia es el segundo país con el 19,44% con más registros de vulnerabilidades, después de Argentina que es el primero con 33,33% de registros de vulnerabilidades y en tercer lugar se encuentra dos países que es Brasil con el 11,11% de los registros y España con los mismos registros.

[125] *Medina Eduardo. Los ataques DDoS aumentaron un 90% en el último trimestre de 2014. {30 enero 2015} {En línea}. Disponible en: http://www.muycomputer.com/2015/01/30/ataques-ddos-aumentaron-90-2014*

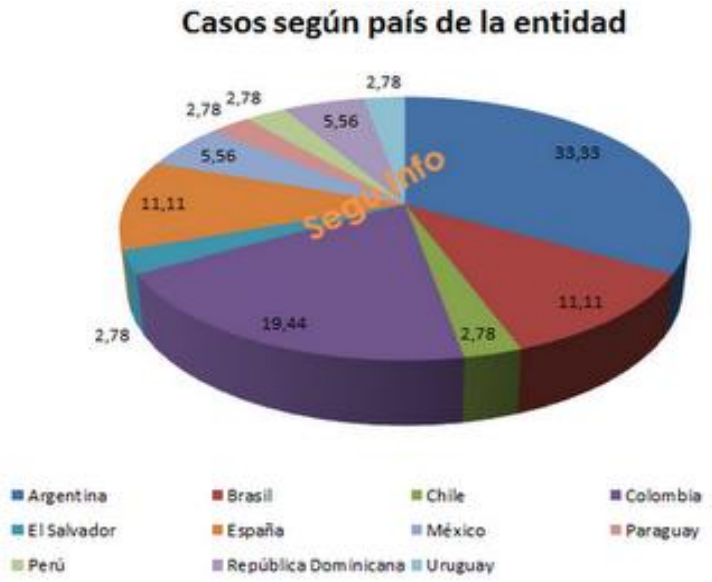


Ilustración 8. Porcentaje de se da por país

Por ello luego de observar las actividades de vulneración más comunes y más peligrosas, conociendo como están afectan a cada país, las empresas dan por hecho que solo esas son las que existen, olvidándose de las más comunes, que muchas veces son las más sencillas de explotar y comprometen la seguridad de las empresas como en otros casos.

"Los ataques 'Man-in-the-Browser' (MiTB) constituyen un riesgo para las empresas donde en casi el 94% de las redes corporativas analizadas en 2014 contienen tráfico que dirige hacia sitios web que albergan malware"[126].

Luego de conocer las vulnerabilidades más conocidas o las de que más se habla, se dará a conocer vulnerabilidades en cuanto a redes(internet), vulnerabilidades de usuarios y puestos de trabajo comunes pero algunas no tan sonadas, para así dar consejos de cómo evitar estas vulnerabilidades:

- "Arquitecturas inseguras: Una red mal configurada es un punto de entrada principal para usuarios no autorizados. Al dejar una red local abierta, confiable, vulnerable a la Internet que es altamente insegura, es casi como que dejar una puerta abierta en un vecindario con alta criminalidad, puede

[126] *Pymes autónomos. Software obsoleto, código erróneo o errores de los usuarios principales amenazas de seguridad .{En línea} {6 agosto 2014}Disponible en: http://www.pymesyautonomos.com/tecnologia/software-obsoleto-codigo-erroneo-o-los-propios-de-los-usuarios-principales-amenazas-de-seguridad-para-las-empresas*

que no ocurra nada durante un cierto tiempo, pero eventualmente alguien intentará aprovecharse de la oportunidad.

- Servidores centralizados: Otra falla potencial de redes es el uso de computación centralizada. Esto puede ser conveniente porque es fácil de manejar y cuesta considerablemente menos que una configuración de múltiples servidores. Sin embargo, un servidor centralizado introduce un punto único de falla en la red. Si el servidor central está comprometido, puede dejar la red totalmente inútil o peor aún, sensible a la manipulación o robo de datos. En estas situaciones un servidor central se convierte en una puerta abierta, permitiendo el acceso a la red completa.

- Amenazas a la seguridad de servidores: La seguridad de servidores es tan importante como la seguridad de la red debido a que los servidores usualmente contienen una gran cantidad de información vital de la organización. Si un servidor está comprometido, todos sus contenidos pueden estar disponibles para que un pirata los manipule o robe a su gusto. Las siguientes secciones detallan algunos de los problemas más importantes.
- Servicios sin sus parches: La mayoría de las aplicaciones de servidores incluidas en la instalación por defecto, son piezas de software robustas y sólidas que ya han sido probadas. Estas han sido usadas en ambientes de producción por varios años y su código ha sido refinado en detalle y muchos de los errores han sido encontrados y reparados. Una buena administración de sistemas requiere vigilancia, seguimiento constante de errores y un mantenimiento de sistemas apropiado para asegurar un ambiente computacional seguro.

- Administración desatendida: Una de las amenazas más grandes a la seguridad de los servidores son los administradores distraídos que olvidan remendar sus sistemas, la causa primaria de la vulnerabilidad de seguridad de los sistemas es «asignar personal poco entrenado para mantener la seguridad y no proporcionar ni el entrenamiento ni el tiempo para permitir que ejecuten su trabajo.

Unos ejemplos de estas vulnerabilidades son la falla en emparchar sus servidores y estaciones de trabajo, leer los mensajes del registro de eventos del kernel del sistema o tráfico de la red, otro error común es dejar las contraseñas o llaves a servicios sin modificar.

- Servicios intrínsecamente inseguros: Aún hasta la organización más atenta y vigilante puede ser víctima de vulnerabilidades si los servicios de red que seleccionen son intrínsecamente inseguros. Una categoría de servicios de red inseguros son aquellos que requieren nombres y contraseñas de usuario sin encriptar para la autenticación. Telnet y FTP son dos de estos servicios.
- Amenazas a la seguridad de estaciones de trabajo y PCs del hogar: Las estaciones de trabajo y PCs del hogar a menudo no son tan susceptibles a ataques como las redes o servidores, pero puesto que a menudo estas contienen información confidencial, tales como información de tarjetas de crédito, pueden ser blancos para los crackers de sistemas.
- Malas contraseñas: Las malas contraseñas son una de las formas más fáciles para que un atacante obtenga el acceso a un sistema.
- Aplicaciones cliente vulnerable: A pesar de que un administrador puede tener un servidor completamente actualizado y seguro, eso no significa que un usuario remoto esté seguro cuando accede al mismo. Aun cuando se utilicen protocolos seguros, tales como SSH, un usuario remoto puede ser vulnerable a ciertos ataques si no mantienen sus aplicaciones cliente actualizadas"[127].

Luego de nombrar algunas vulnerabilidades, como se mencionó anteriormente, ahí unos "consejos de seguridad, como lo son:

- Mantener actualizados los programas Java y de Adobe.
- Usar contraseñas que incluyan números, y letras en mayúscula y minúscula.
- Nunca usar las mismas contraseñas para sitios sensibles que para otros de bajo riesgo.
- Utilizar antivirus, firewalls y filtros de correo no deseado; y mantenerlos actualizados.
- Recibir con sospecha mensajes no deseados, aun cuando vienen de conocidos"[128].

[127] *Red Hat, Inc. Ataques y vulnerabilidades {En línea} {2003}. Disponible en: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-risk-net.html*

[128] *Finanzas personales. Hackers éticos: copiando a los criminales. {En línea} {Noviembre 2014}. Disponible en: http://www.finanzaspersonales.com.co/consumo-inteligente/articulo/hackers-eticos-copiando-criminales/50089*

5 METODOLOGÍA

5.1 Estudio Descriptivo:

Este trabajo gira en torno a la incertidumbre relacionada a si el estudiante universitario, inicialmente de Ingeniería de Sistemas, Ingeniería de Telecomunicaciones y la Especialización de Seguridad Informática de la Universidad Piloto de Colombia, tendría la opción de ser parte de una comunidad hacker y si esta iniciativa existiera; si los conocimientos adquirido serían explotados positiva o negativamente, así mismo indagar como la comunidad educativa, los docentes, puede influir en el que se generen estos intereses, que sin la guía ética adecuada pueden culminar en actividades relacionadas con el delito informático.

Para ello el desarrollo de la investigación se apoya en el enfoque académico de estudiantes y docentes de los programas de Ingeniería de Sistemas, Ingeniería de Telecomunicaciones y la Especialización de Seguridad Informática de la UPC a

través de un “muestreo simplificado o azaraficado”[129], así como el análisis de expertos de seguridad informática. Inicialmente se toma como primer panorama a los jóvenes que están más expuesto en aprender técnicas propias de la cultura hacker, estudiantes entre los 17 a 30 años de edad de ambos géneros, por otro lado el grupo que también dejaría ver si es enseñado dicho conocimiento sería el de profesores o docentes del pregrado de Ingeniería de Telecomunicaciones, Ingeniería de Sistemas e incluso los docentes del posgrado de Seguridad informática que son aquellos que más enseñarían este tipo de conocimiento pero inclinando las preguntas para conocer si en la forma en la que lo enseñan la ética es protagonista para utilizar el conocimiento de forma apropiada.

Con los estudios realizados a través de encuestas y entrevistas se busca obtener el nivel de conocimiento que dichas personas dicen tener, la clase de actos que han llegado a realizar y en algunos casos el semestre desde el cual llegan a entender y tener conocimientos en temas relacionados con la cultura Hacker. También poder observar si existe un grupo de jóvenes que han llevado su interés a un nivel o daño, como por ejemplo (haber realizado una vulnerabilidad con fines distintos al académico o de aprendizaje), para ello las preguntas de las encuesta estaban agrupadas, para así tener un mayor entendimiento de las respuestas y análisis de integridad de las mismas.

Para el estudio con los estudiantes se desarrollaron 4 grupos, el primer grupo de preguntas pretendía determinar si existe una tendencia de los jóvenes para obtener beneficios económicos realizando vulneración a sistemas informáticos, el Segundo grupo de preguntas quería identificar aquellos jóvenes que tienen conocimientos para vulnerar sistemas, los cuales conocen e identifican programas para realizar actividades de hacking con fines distintos al académico o de aprendizaje o que muchas veces ya han realizado cierto tipo de ataques, el tercer grupo de preguntas quería identificar los jóvenes que quizás acudirían a un profesional con conocimiento en técnicas de hackeo de sistemas o aprenderían a través del conocimiento de otras personas para realizar actividades de hacking con fines distintos al académico o de aprendizaje y el último grupo de preguntas realizadas quería identificar las personas que consumen software pirata pero que no representarían ningún peligro.

Así mismo para la encuesta de los docentes se dividieron en dos grupos las preguntas, el primer grupo de preguntas pretendían determinar la influencia de los profesores para que un estudiante tenga iniciativas en participar en actividades

[129] *Ignacio Hernández Molina, La formulación de proyectos en ciencias e ingenierías. Editorial. Universidad Piloto de Colombia. ISBN 978-958-8537-33-7*

relacionadas con la cultura hacker, aunque este influencia no sea evidente y el segundo grupo de preguntas quería identificar aquellos profesores que estimulan a los estudiantes para que utilicen sus habilidades de forma positiva y no influyen de forma negativa.

La dinámica utilizada para realizar el estudio, teniendo orden y llevando la contabilidad de los estudiantes y docentes que responden a la encuesta, se realizó con la herramienta de Gmail, Google Drive “formularios de google”, en donde se realizaron dos formularios, el primero “Encuesta de estudiantes” y el segundo formulario “Encuesta de profesores”, cada una de estas con sus respectivas hojas de respuestas, las encuesta realizadas se observa en la Imagen 1.

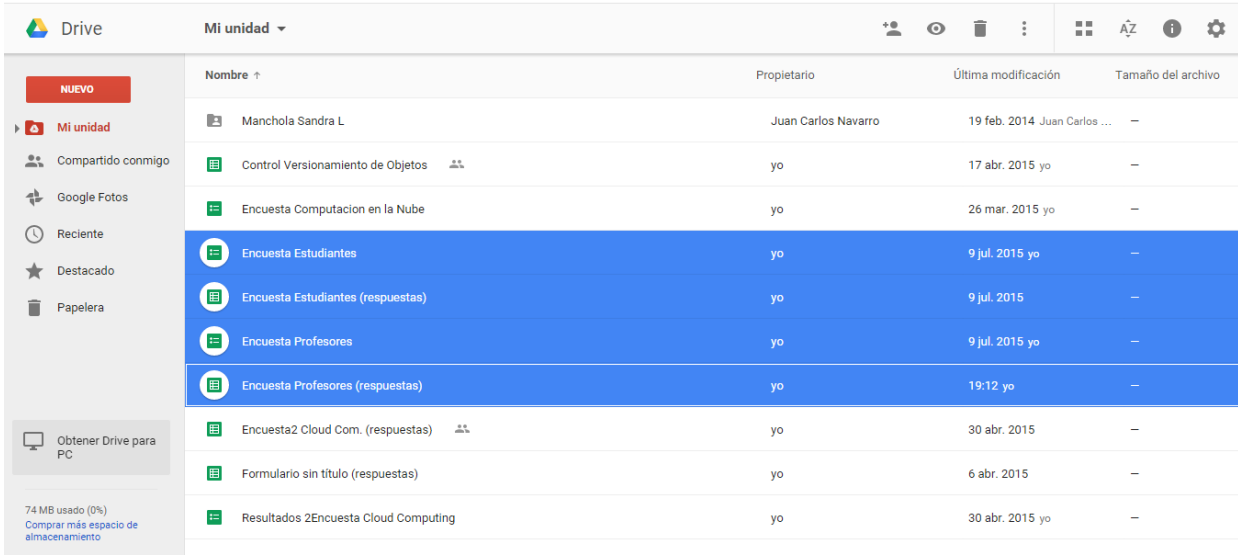
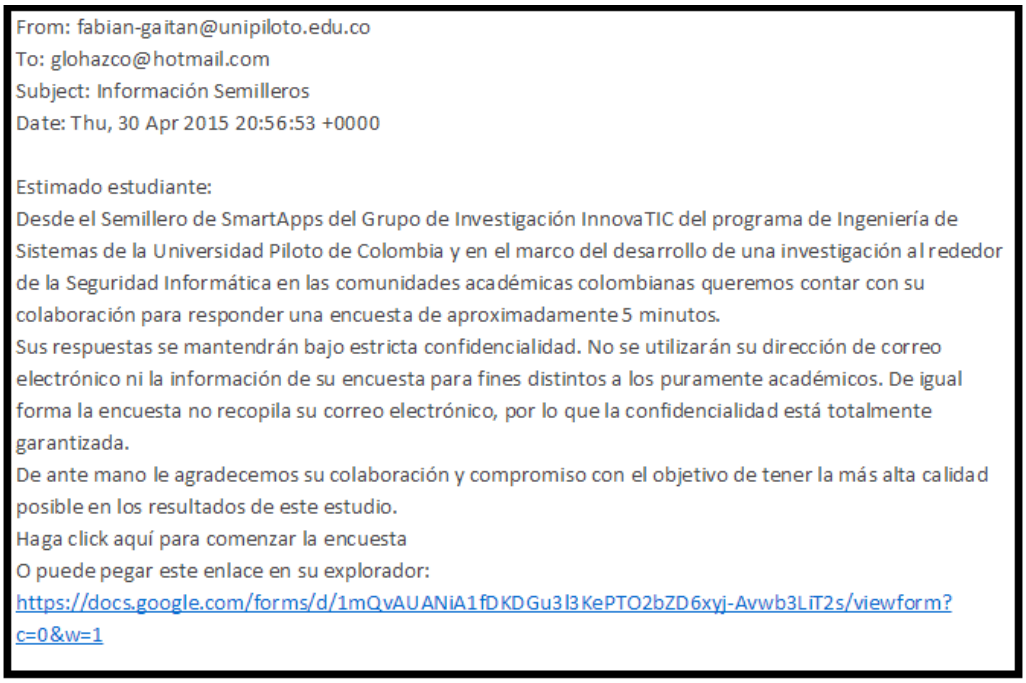


Imagen1

La distribución de estas encuestas se realizó a través de los Coordinadores de los programas analizados y a todo el universo de docentes y estudiantes para el 2015.El cuestionario fue enviado mediante un link a los estudiantes como lo muestra la Imagen2.



From: fabian-gaitan@unipiloto.edu.co
To: glohazco@hotmail.com
Subject: Información Semilleros
Date: Thu, 30 Apr 2015 20:56:53 +0000

Estimado estudiante:
Desde el Semillero de SmartApps del Grupo de Investigación InnovaTIC del programa de Ingeniería de Sistemas de la Universidad Piloto de Colombia y en el marco del desarrollo de una investigación al rededor de la Seguridad Informática en las comunidades académicas colombianas queremos contar con su colaboración para responder una encuesta de aproximadamente 5 minutos.
Sus respuestas se mantendrán bajo estricta confidencialidad. No se utilizarán su dirección de correo electrónico ni la información de su encuesta para fines distintos a los puramente académicos. De igual forma la encuesta no recopila su correo electrónico, por lo que la confidencialidad está totalmente garantizada.
De ante mano le agradecemos su colaboración y compromiso con el objetivo de tener la más alta calidad posible en los resultados de este estudio.
Haga click aquí para comenzar la encuesta
O puede pegar este enlace en su explorador:
https://docs.google.com/forms/d/1mQvAUANiA1fDKDGu3l3KePTO2bZD6xyj-Avwb3LiT2s/viewform?c=0&w=1

Imagen 2

Al dirigirse al link en este caso los estudiantes se encontraban con la encuesta que estaba diseñada de la siguiente forma.

Encuesta Seguridad Informatica

*Obligatorio

ÁREA ITIC

INGENIERÍA DE SISTEMAS
INGENIERÍA DE TELECOMUNICACIONES
FACULTAD DE INGENIERÍA
UNIVERSIDAD PILOTO DE COLOMBIA

Universidad *

Facultad *

Semestre *

1. Accedería a vulnerar un sistema con el objetivo de facilitar su vida laboral? *

Responda de 0 a 5 siendo 0 el más bajo y 5 el más alto

0 1 2 3 4 5

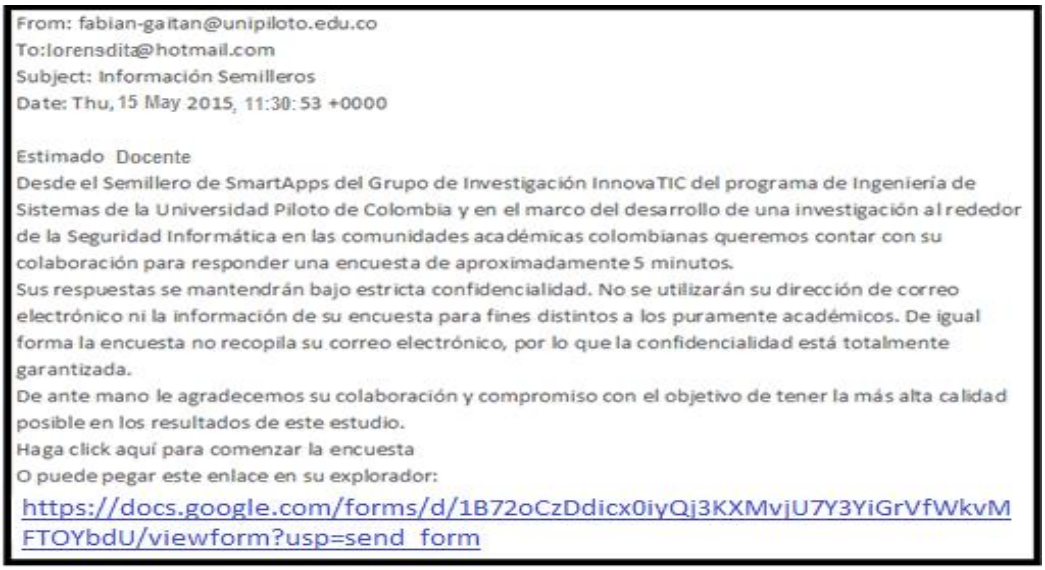
2. Está preparado o tiene alternativas, de cómo evitar un ataque informático si le llegara a suceder? *

- Ninguna
- Poco conocimiento
- Algo de conocimiento
- Si se evitar una ataque

3. Si alguien le propone acceder a un sistema informático, una página o programa indebido con una buena recompensa económica lo haría? *

- Nunca
- Quizás lo haría
- Si lo haría

Para ver la encuesta de estudiantes completa Anexo1 Igualmente él envió del cuestionario a los docentes se realizó de la misma manera, enviando el link a todos los docentes de las carreras mencionadas como lo evidencia la Imagen3

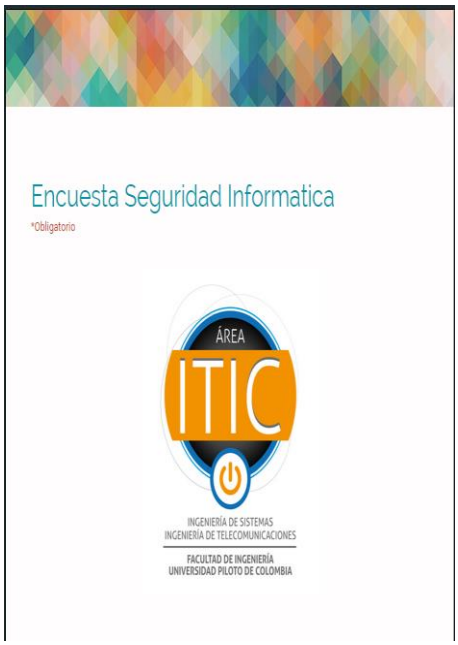


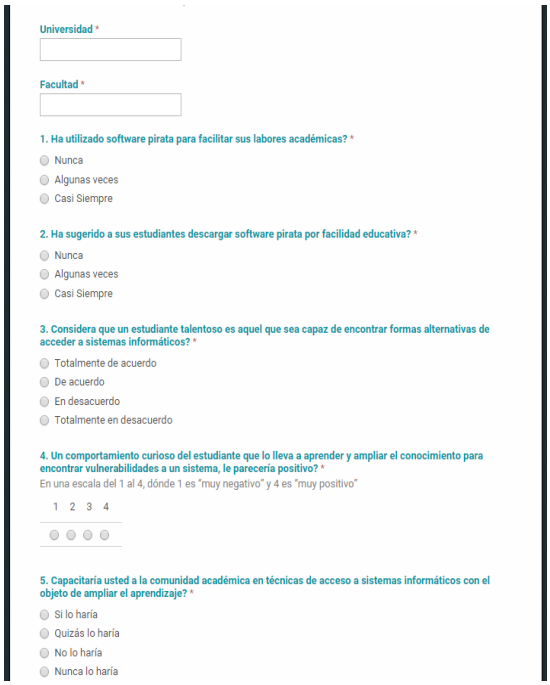
From: fabian-gaitan@unipiloto.edu.co
To:lorensdita@hotmail.com
Subject: Información Semilleros
Date: Thu, 15 May 2015, 11:30:53 +0000

Estimado Docente
Desde el Semillero de SmartApps del Grupo de Investigación InnovaTIC del programa de Ingeniería de Sistemas de la Universidad Piloto de Colombia y en el marco del desarrollo de una investigación alrededor de la Seguridad Informática en las comunidades académicas colombianas queremos contar con su colaboración para responder una encuesta de aproximadamente 5 minutos.
Sus respuestas se mantendrán bajo estricta confidencialidad. No se utilizarán su dirección de correo electrónico ni la información de su encuesta para fines distintos a los puramente académicos. De igual forma la encuesta no recopila su correo electrónico, por lo que la confidencialidad está totalmente garantizada.
De ante mano le agradecemos su colaboración y compromiso con el objetivo de tener la más alta calidad posible en los resultados de este estudio.
Haga click aquí para comenzar la encuesta
O puede pegar este enlace en su explorador:
https://docs.google.com/forms/d/1B72oCzDdicx0iyQj3KXMvjU7Y3YiGrVfWkvMFTOYbdU/viewform?usp=send_form

Imagen 3

Al dirigirse al link los docentes se encontraban con la encuesta que estaba diseñada de la siguiente forma.





Para ver la encuesta completa de los docentes anexo 3

Después de realizar las encuestas y para completar el estudio, se realizaron entrevistas a expertos en lo relacionado con la Seguridad Informática y si perciben

la existencia de jóvenes que se están inclinando por el camino de la delincuencia informática, igualmente conocer sus puntos de vista en relación a la investigación adelantada.

Por ello se realizó entrevista a 2 profesionales en seguridad informática, uno de ellos fue el ingeniero Álvaro Escobar Director de la Especialización de Seguridad Informática y Cesar Rodríguez Ingeniero de Seguridad, docente en la especialización de seguridad y consultor de seguridad para diversas empresas a nivel nacional. Estas entrevistas se realizaron para tener un concepto más amplio del tema planteado durante la investigación y como actualmente se evidencia en la realidad. Esta entrevista se basó en 12 preguntas, con 2 de ellas (16.66%) se quería validar si los entrevistados están de acuerdo con que los delitos informáticos empiezan desde muy temprana edad, con otras 6 (50%) de las preguntas se quería validar cómo ve y analiza el estado del delitos informáticos en Colombia, con las 4 restantes preguntas (33.33%), validar porque los delitos van en aumento en el país.

5.2 Estudio Teórico

En este tipo de estudio utilizara el estado del arte en donde se recolectara y analizara la información meticulosamente de textos, artículos, ensayos, tesis que traten del tema, para así crear las temáticas o subgrupos en los que se va a enfatizar como :

- Hacker colombiano
- Hacker de otros países
- Daño social del hacker
- Daño social del hacker colombiano
- Herramientas utilizadas por los hacker
- Imagen de la sociedad sobre el hacker
- Delito informático echo por el hacker
- Estados de vulnerabilidad que aprovechan los hacker

Para todas estas temáticas se investigó las tendencias metodológicas y paradigmas que fueron de ayuda para construir la base teórica de la investigación. En la segunda fase del estado del arte se utilizó la parte descriptiva para generar los datos pertinentes y de gran importancia que se identificaron

Después se interpretó y analizaron las temáticas que se escogieron para poder empezar la documentación específica y por último con todo lo anterior se pudo

construir e identificar la hipótesis dada en el documento y si la sociedad educativa, el ambiente y la influencia en el desarrollo de jóvenes, que sin la guía ética adecuada pueden culminar en actividades relacionadas con el delito informático. Además de ello observar el manejo de otros países con este delito, ampliar el conocimiento de actos de gran importancia para observar el conocimiento heredado.

Toda esta parte investigativa se encuentra en el marco teórico del presente documento.

6 Desarrollo final

El estudio desde el enfoque de los estudiantes fue realizado con las respuestas de 10 estudiantes del programa de Ingeniería de Telecomunicaciones, 37 del programa de Ingeniería de Sistemas y 8 del posgrado de seguridad Informática, se observó en los resultados que para los programas de pregrado las respuestas se dieron más entre los estudiantes de semestre de noveno, decimo semestre y egresados, que equivalen a un total de 33 estudiantes que están en los últimos semestres de la carrera o ya se encuentran graduados.

Respecto a esto, la encuesta realizada se basó en 15 preguntas, estas respuestas se pueden ver en "Respuestas estudiantes", se realizó un grupo de preguntas en donde se quería determinar si existe una tendencia de los jóvenes para adoptar iniciativas de trabajar o buscar medios económicos realizando acciones a sistemas informáticos. Para el cual se obtuvo el siguiente resultado como se puede ver en la Ilustración 9. **¡Error! No se encuentra el origen de la eferencia.**

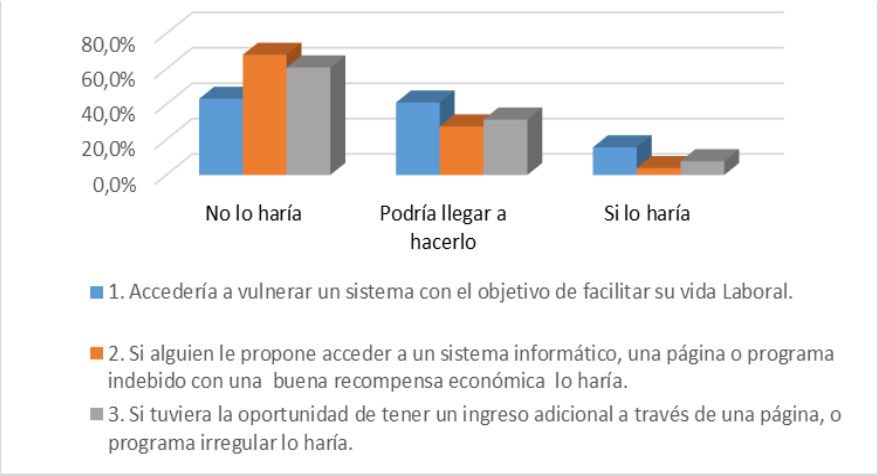


Ilustración 9. Resultado Encuesta de Estudiantes para validar iniciativas de trabajar o realizar acciones a sistemas informáticos.

Para este caso se encontró una fuerte inclinación en las respuesta que podrían llegar a hacerlo y en un cierto número aquellas personas que lo harían, con respecto a ello se encontró un 41 % de los encuestados podrían llegar a realizar vulneración a sistemas con retribución económica y un porcentaje muy considerable del 15.7 % considera que si lo haría, por ultimo un 43,1% no lo harían. Como se observa en la Imagen 3,el análisis de estas respuestas podemos dar una observación primaria de cómo hay una atracción entre los jóvenes, ya que lo ven como una forma de ganar dinero, esto se puede observar ya en anuncios de internet donde abiertamente publican anuncios de “busco hacker para obtener contraseña de Facebook y es trabajo por dinero.

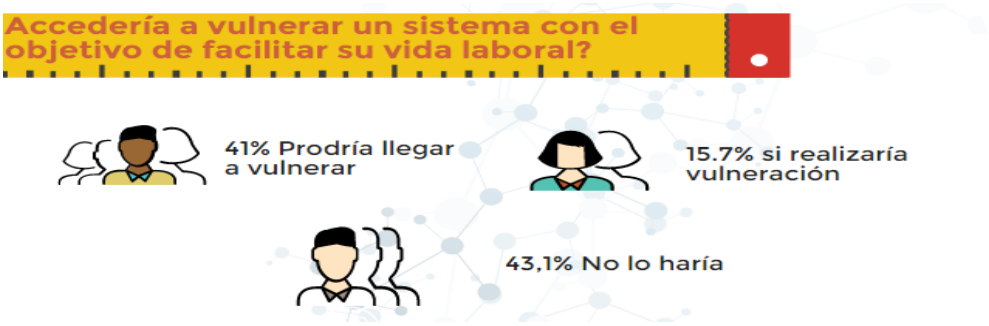


Imagen 3

Teniendo en cuenta lo anterior se realizó la pregunta ¿si alguien le propone acceder a un sistemas informático, una página o programa indebido con una

buena recompensa económica lo haría? Para lo cual se obtuvo un resultado del 27.5% podría llegar acceder a páginas o programas indebidos teniendo como recompensa una buena oferta en dinero, el 3.9% opino que si lo haría rotundamente y el 27.5% nunca lo haría, como se observa en la Imagen 4. La publicación de el diario el Dinero: "De ataques 'clásicos', como robo de identidad y datos de tarjetas de crédito, se ha pasado a los grupos que ofrecen sus servicios profesionales en este campo para quien los quiera contratar", le dice a BBC Mundo Raoul Chiesa, presidente de Security Brokers, una organización especializada en la investigación de seguridad en internet."[130] Y es así que un número de compañías buscan personas con conocimiento de hackers para que se vinculen, están personas tendrán obtención y ganancia en dinero, ya que cada vez el pedido de robar cuantas tan comunes como redes sociales o tan difícil como las cuentas de bancos es más grande y el mercado cada vez es más amplio.

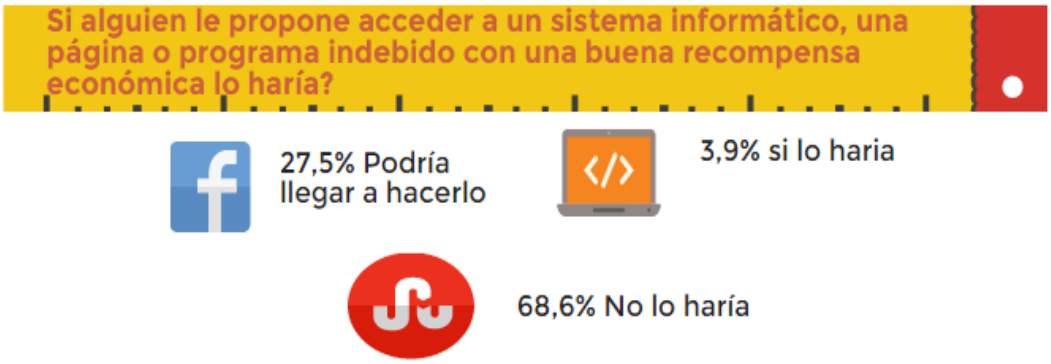


Imagen 4

Jóvenes Colombianos que crean sus propias empresas de hackers o que se vinculan a ellas es lo que se está viendo en la actualidad. Es el caso de "Juan Sebastián Eljach es un bumangués de 15 años y es un 'hacker'. Su tío, Diego Sánchez, de 19 años, es su socio. Son de Bucaramanga, Santander, y crearon la primera 'universidad' virtual en español para aprender técnicas de ataque y defensa de sistemas informáticos. Se llama Exploiter.co y empezó a operar desde el pasado 3 de septiembre."[131] .Es así que empresas como estas que son creadas por jóvenes que desde temprano aprendieron a programar y se interesaron cada vez más por obtener este tipo de conocimiento, lo que se ve ahora es que los

[130] *Dinero, La amenaza hacker. {12 Abril de 2013} {En línea} Disponible en: http://www.dinero.com/empresas/articulo/empresas-hacker-cobran-datos/189128*

[131] Medina Édgar, Colombiano de quince años crea escuela para aprender a 'hackear'. {23 septiembre 2014} {En línea} Disponible en: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/como-hackear-colombiano-de-quince-anos-crea-escuela-para-aprender-a hackear/14575255.

jóvenes son los dueños de la Web, tanto en su navegación, como en la obtención de conocimientos. “Eljach forma parte de esa camada de jóvenes prodigios que se han empezado a convertir en los orfebres de esta era de la web. Empezó a estudiar lenguajes de programación a los 12 años y ha sido consultor de seguridad de empresas mejorándola y The Eagle Labs. Él y su tío han dictado conferencias en instituciones académicas de Bucaramanga como la Universidad Autónoma, la Universidad Santo Tomás y el colegio San Sebastián.”[132] Esta enseñanza que realizan muchos jóvenes vía internet, muchas veces es aprovechada por jóvenes igual que ellos que aprenden, miran los tutoriales, las clases y utilizan este aprendizaje como forma de daño y creación de empresas para vulneración de sistemas, ya que no se desempeña un nivel ético para el conocimiento adquirido.

Se buscó indagar si una persona tuviera la oportunidad de tener ingreso adicional yo no atreves de una persona que le ayude sino a traes de una página o un programa irregular lo haría. Se encontró que el 31.4% de los encuestados son estudiantes que quizás buscarían este tipo de programas o personas, el 7.8 lo buscaría y el 60.8% no lo haría como se ve en la Imagen 5.

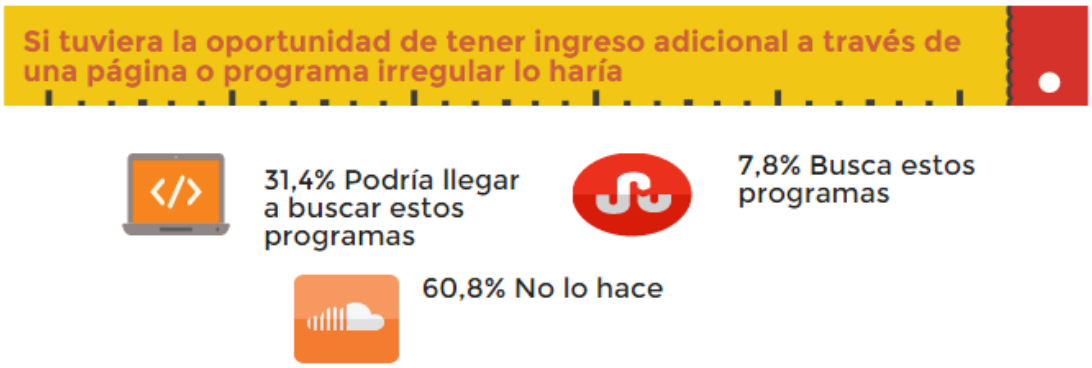


Imagen 5

El análisis presentado con este tipo de tendencia que se quiso evidenciar con las respuestas obtenidas era que cierta cantidad de estudiantes que estudian este tipo de carreras y que tienen un grado de conocimiento sobre el tema están dispuestas o podrían tener motivación de realizar dichos actos, si tienen un ingreso económico o que quizás contratarían por comodidad personas para acceder por medio de ayuda a información a lo que ellos no pueden. Es por ello que el mercado de hackers en la web ya que es el sitio en donde más se encuentra todo

[132] Medina Édgar, Colombiano de quince años crea escuela para aprender a 'hackear'. {23 septiembre 2014} {En línea} Disponible en: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/como-hackear-colombiano-de-quince-anos-crea-escuela-para-aprender-a hackear/14575255.

tipo de empresas o personas que realizan trabajo de vulneración a sistemas, el hackeo a todo tipo de sistema a cambio de dinero ya no es difícil de encontrar, pero el costo muchas veces si es grande. Es por ello que “Un programa troyano que bloquea dispositivos móviles cuesta alrededor de mil dólares, pero con este tipo de programas maliciosos los piratas podrían ganar mucho más, afirman los expertos. “Los 'hackers' piden entre 10 y 200 dólares para liberación de móviles, lo que significa que así pueden ganar hasta 20.000 dólares.”[133] O también se pueden encontrar con “los piratas informáticos pagan cerca de 2.000 dólares para obtener un programa cifrado de datos y piden 100 dólares al usuario para su desbloqueo.”[134].Aunque se dice que el que más dinero les da a este tipo de personajes son los troyanos que acceden a cuentas bancarias.

Ilustración 10. Imagen de como gana dinero un hacker.

[133] *SEPA MÁS, ¿Cuánto ganan los 'hackers'? Kaspersky explica el lucro de la piratería. . {30 Agosto de 2014} {En línea} Disponible en: http://actualidad.rt.com/actualidad/view/138751-ganan-hackers-expertos-kaspersky-explican*

[134] *Ibíd.*

La atracción de los hackers o crackers es muchas veces impulsada por el nivel lucrativo que lleva a hacer estos actos, y como se pudo observar en los resultados de las preguntas anteriormente mencionadas, existe una porcentaje de jóvenes que podían o pueden actualmente inclinarse a este tipo de delito por iniciativa del dinero que podrían obtener o con la ayuda de profesionales que los ayuden a conseguir sus objetivos.

Luego de analizar aquellos jóvenes que por dinero podrían ser capaces de inclinarse hacia el lado hacker o cracker, con otro de los grupos de preguntas realizadas se buscó identificar los jóvenes que quizás acudirían a un profesional con conocimiento en técnicas de hackeo de sistemas o aprenderían a través del conocimiento de otras personas para realizar delitos informáticos. Los resultados obtenidos para este tipo de preguntas realizadas se pueden ver en la lustración 11

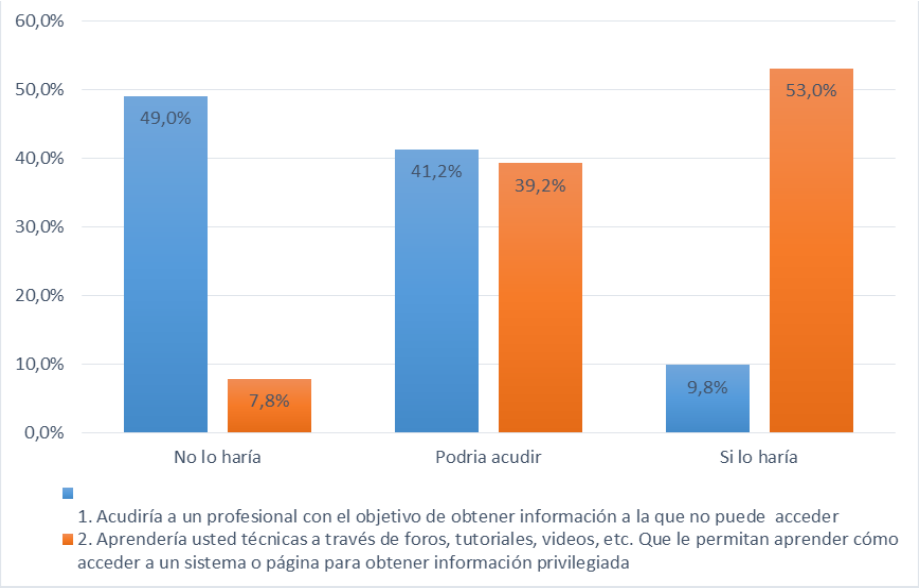


Ilustración 12 Resultado Encuesta Estudiantes Preguntas para identificar jóvenes que aprenderían del conocimiento

[135] *SEPA MÁS, ¿Cuánto ganan los 'hackers'? Kaspersky explica el lucro de la piratería. . {30 Agosto de 2014} {En línea} Disponible en: http://actualidad.rt.com/actualidad/view/138751-ganan-hackers-expertos-kaspersky-explican*

En la cual en una de ella se indaga si los jóvenes tienen conocimiento de vulneración y que aun con ello no han realizado ningún acto delictivo pero que en algún momento podrían tomar esta decisión, en este caso se observa que muchos jóvenes con el 41,2% de los resultados podrían optar en alguno momento a tomar este conocimiento para llegar a vulnerar información en la cual no tienen acceso, para un muestra un poco representante se observa que el 9.8 % utilizaría este conocimiento y el 49% nunca acudiría a un profesional como lo muestra la Imagen 6. Se observa que la mayoría de jóvenes si tiene tendencias a indagar más allá de sus sensatez y en muchos casos realizar delitos informáticos, es por ellos que con esta pregunta se da la visión que los jóvenes aun estando en la pubertad del conocimiento, se están inclinado por estar un paso más allá de las cosas y que en muchos casos tomarían cualquier medio para llegar a tal punto de saber todo, un ejemplo claro de que el conocimiento se puede llevar más allá es el caso de "Luis Iván Luende, un joven asturiano que se ha convertido en el hacker más reconocido de Europa. Admite que en el instituto no era muy buen estudiante, pero con 12 años inició su primer proyecto y con 15 montó su primera empresa. Ahora, con 19 años, varias empresas le han hecho propuestas para que se incorpore a sus plantillas."[136]

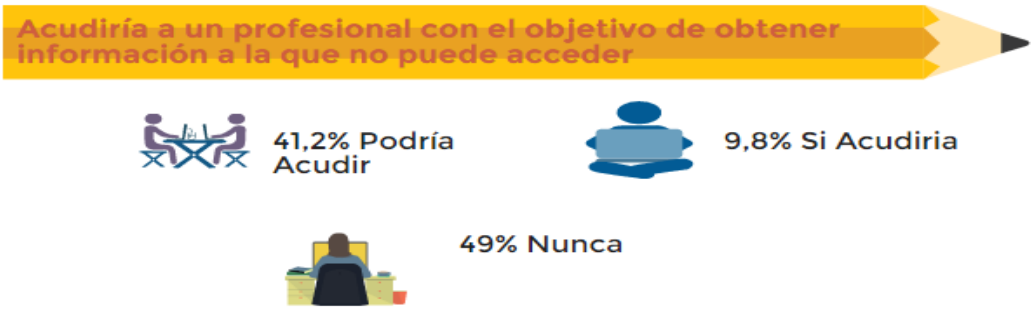


Imagen 6

Otra pregunta que hace referencia a la tendencia anterior de aquellos jóvenes que aún están en los inicios de conocimiento para llegar a vulneraciones y un poco más adelante llamarse hacker, se preguntó si aprendería técnicas a través de foros, tutoriales, videos, etc. Que le permitan aprender cómo acceder a un sistema o página para obtener información privilegiada en las cual encontramos una tendencia del 39,2% tienen la iniciativa de aprender por estos medios el 53% aprenderían o se podría decir que están aprendiendo por esta clase de medios y

[136] Antena3.com .Un hacker español, entre los jóvenes más brillantes del mundo: "No estudiaba pero monté mi primera empresa con 15 años". {01 Enero de 2015} {En línea} Disponible en: http://www.antena3.com/noticias/tecnologia/hacker-espanol-jovenes-mas-brillantes-mundo-estudiaba-pero-monte-primera-empresa-anos_2015013000119.html

el 7,8 de los encuestados no aprendería ni le interesa aprender. Como se puede observar en la Imagen 7.

El caso del ejemplo anterior del joven australiano que “de acuerdo a los reportes, el estudiante halló un foro de hackers que otorgaba puntos a sus miembros, muy parecido al sistema de millas de viaje o una tarjeta de club, por cada ataque exitoso, y en tres meses ya estaba ubicado entre los 50 principales hackers de aproximadamente unos 2,000 usuarios registrados en el foro”[137],

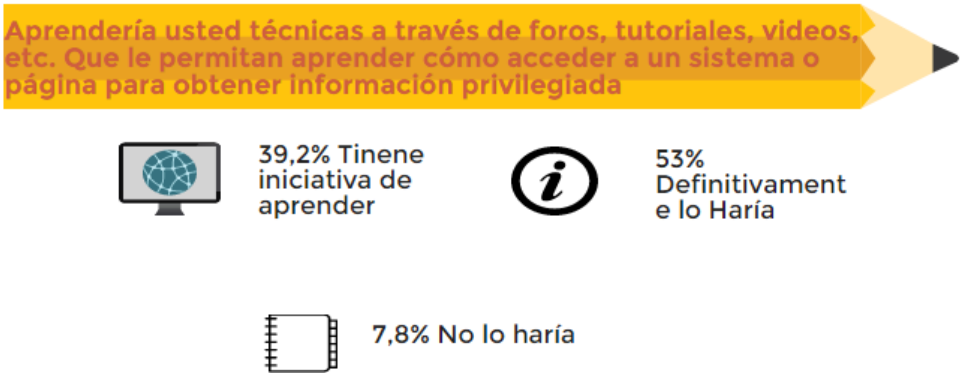


Imagen 7

Se observa que la tendencia del hacker se puede ver con inicios en casos tan pequeños como lo es ingresando a foros, mirando videos o en casos apartados buscando a personas un poco más especializadas para que expresen un poco de conocimiento con ellos y así ir aprendiendo, conociendo herramientas, métodos para vulnerar sistemas y así en su recorrido y con mayor experiencia en el campo llegar a convertirse en hacker.

Un caso particular de como el nicho utilizado para el estudio, la comunidad estudiantes de pregrado y postgrado, teniendo en cuenta los docentes de la universidad piloto de Colombia, se indaga con “la hacker HighSchool, una iniciativa del Instituto por la Seguridad y las Metodologías Abiertas (ISECOM) que quiere enseñar a los adolescentes a ser hackers. La Hacker HighSchool no es propiamente una escuela sino un seminario de dos horas en el que auténticos hackers enseñan a jóvenes de entre 13 y 17 años los fundamentos para vivir de

[137] Mundo contact. Jóvenes emulan a ciberdelincuentes buscando fama y elogios. {29 Julio de 2014} {En línea} Disponible en: http://mundocontact.com/jovenes-emulan-a-ciberdelincuentes-buscando-fama-y-elogios/

forma segura y privada en Internet."[138], este seminario enseña a jóvenes poco hacking ofensivo y mucho defensivo, es decir ayuda en un mejor propósito para que aquellas personas tengan más seguridad en el correo electrónico, sepan identificar tipos de virus, otro énfasis que tienen es el uso del comando "netstat" para mostrar las conexiones abiertas en el ordenador, rastreo de un intruso mediante la lectura de los ficheros "log", esto aunque el seminario sea un curso de hacking defensivo, en muchos casos jóvenes con estos conocimientos, no solo se va a centrar en cuidar su entorno, si no que querrán vulnerar puertos, hacer conexiones que no tienen acceso, etc., no solo se quedaran con un hacking defensivo si no que lo utilizaran como un hacking ofensivo o con un poco más de palabras sabia como lo dice la frese de Linda Sandvik, cofundadora de Code Club "Lo mismo puede decirse de la tecnología digital. Para alfabetizarnos no sólo importa aprender a leer, también hace falta escribir. En este caso pasa lo mismo. Ya no es suficiente aprender a utilizar programas de computadoras, si no estar a la defensas de ellas"[139].

Ya para otra tendencia de como la sociedad está junto a la iniciativa de jóvenes hacia el hackeo, a disposiciones de jóvenes que aun con algo de interés por el mundo hacking no representa ningún peligro ni en el presente ni a futuro y solo representa una tendencia a descarga y consumismo de software pirata, se realizó una pregunta que pretendía evaluar aquellos jóvenes que solo consumen software pitara. Para esto se obtuvo el porcentaje de respuesta presentado en la Ilustración 13.

[138] *El mundo. Lecciones de 'hacking' para adolescentes. {08 Diciembre de 2013} {En línea} Disponible en: http://www.elmundo.es/tecnologia/2013/12/08/52a3801e63fd3d043f8b456d.html*
[139] *BBC Mundo. Los hackers de hoy, cada vez más jóvenes. {11 Febrero de 2013} {En línea} Disponible en: http://www.bbc.co.uk/mundo/noticias/2013/02/130210_tecnologia_ninos_hackers_en*

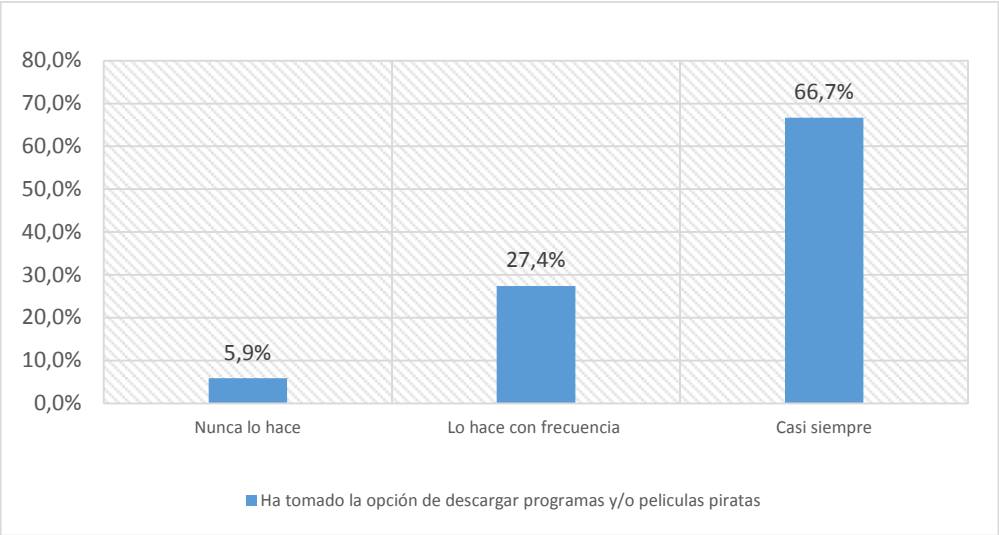


Ilustración 14 Respuesta Estudiantes que consumen Software Pirata

En la cual se obtuvo respuestas de que el 5.9% de las personas nunca lo hacen. El 27,4% lo hace frecuentemente y el 66,7% lo hacen todo el tiempo. Esto se puede observar en la Imagen 8. "Tenemos a millones de jóvenes cuya salida de escape ya sea entretenimiento o forma de aprender y emprender es el internet y los contenidos gratis. Un ejemplo de esto se ve Estoy en paro pero quiero aprender mandarín, descargo "Rosseta Stone". Estoy en paro no tengo dinero ni siquiera para ir a Francia, pero quiero practicar mi francés, descargo películas en ese idioma. O simplemente estoy aburrido y quiero jugar en la computadora. Entonces no es de extrañar que estas edades sean quienes más consumen piratería"[140].

[140] *Gfierro, Rankia. Analizando la Piratería desde sus Causas, No desde sus Efectos. {01 Febrero de 2012} {En línea} Disponible en: http://www.rankia.com/blog/etfs-pm/1082304-analizando-pirateria-sus-causas-no-efectos*

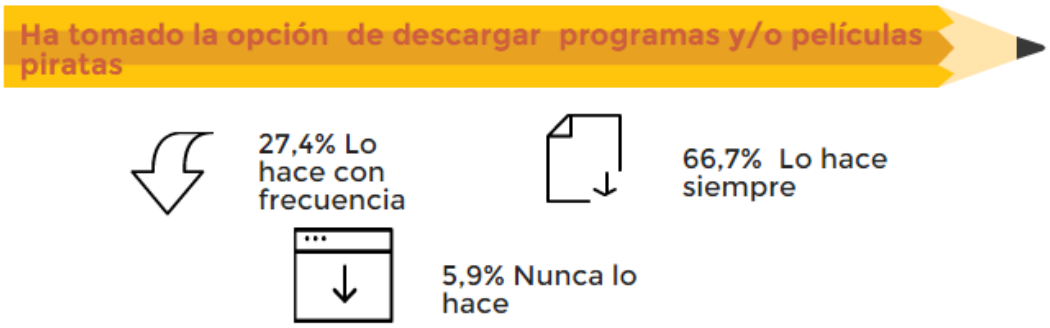


Imagen 8

Ya para entrar un poco más en el tema como la piratería está cada vez más propensa a ser realizada se analiza los sitios donde más se concentran las descargas de piratería por parte de jóvenes se puede observar la siguiente imagen donde ilustra cada aplicación de descarga

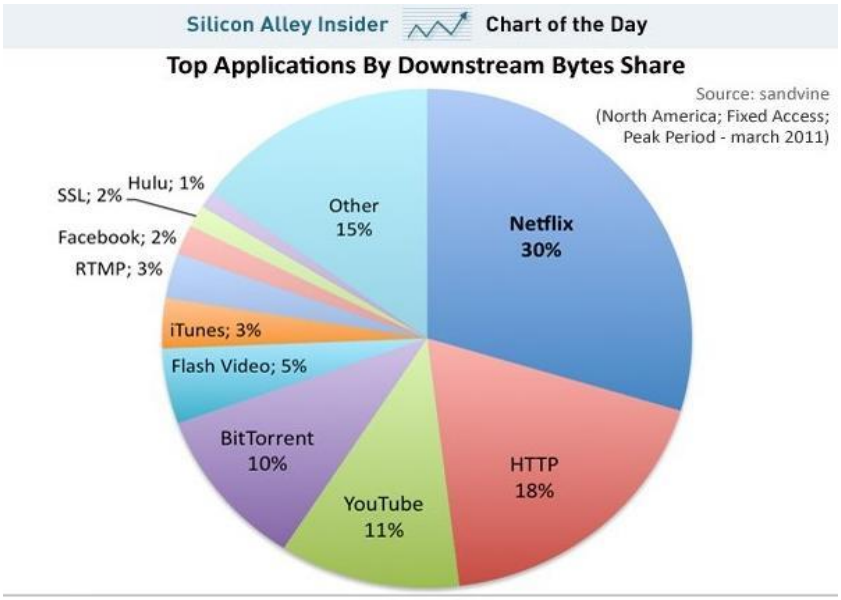


Ilustración 15 Sitios de piratería

Donde se observa que la mayoría de jóvenes se enfocan por la aplicación Netflix muchas veces para descargas de películas, otro medio es HTTP para diversos programas, seguido de YouTube para descargas de música entre otros.

Aun viendo estos porcentajes tan altos de jóvenes que se inclinan por descargas programas, películas músicas entre otras cosas, también se observa como Colombia está haciendo un gran esfuerzo por minimizar estas hazañas de piratería y se ubica en la 5 posición entre países suramericanos contra la piratería.

Argentina	69%
Bolivia	79%
Brasil	50%
Chile	59%
Colombia	52%
Costa Rica	59%
Ecuador	68%
El Salvador	80%
Guatemala	79%
Honduras	74%
México	54%
Nicaragua	82%
Panamá	72%
Paraguay	84%
Perú	65%
República Dominicana	75%
Uruguay	68%
Venezuela	88%
Otros LA	84%
TOTAL AL	59%

Ilustración 16 Países mayor concentración de piratería

El índice promedio de América Latina es de 59 por ciento. “Colombia ha avanzado de forma notable contra la piratería, en gran medida gracias al accionar de entidades del Gobierno. Un punto porcentual menos notable, la piratería es un fenómeno difícil de controlar, mantener los mismos índices ya puede considerarse como un éxito. Este es solo el comienzo, va seguir bajando”, indica Rodger Correa, director de Marketing de BSA para Latinoamérica”[141].

Aunque esta última validación no representa un riesgo de los jóvenes Colombianos en convertirse en hacker o en estar aprendiendo técnicas, nos muestra como si hay mucho consumismo de software indebido. Lo que se quería observar con esta pregunta era ver quienes podían convertirse o son potenciales jóvenes hacker a aquellos que solo utilizan o son consumidores de software pirata.

Por último se realizó otro grupo de preguntas donde quería identificar aquellos jóvenes que tienen conocimientos para realizar actos indebidos en sistemas informáticos, También identificas aquellos que conocen e identifican programas

[141] *Calderón Cardona. En Colombia la piratería se redujo 1% en los últimos 720 días* On {27 junio 2014} *{En línea} Disponible en: https://www.calderoncardona.com/archivos/4087*

para realizar un delito informático o que en ocasiones ya han realizado cierto tipo de ataques. Este resultado se puede ver en las Ilustración 17 E Ilustración 18.

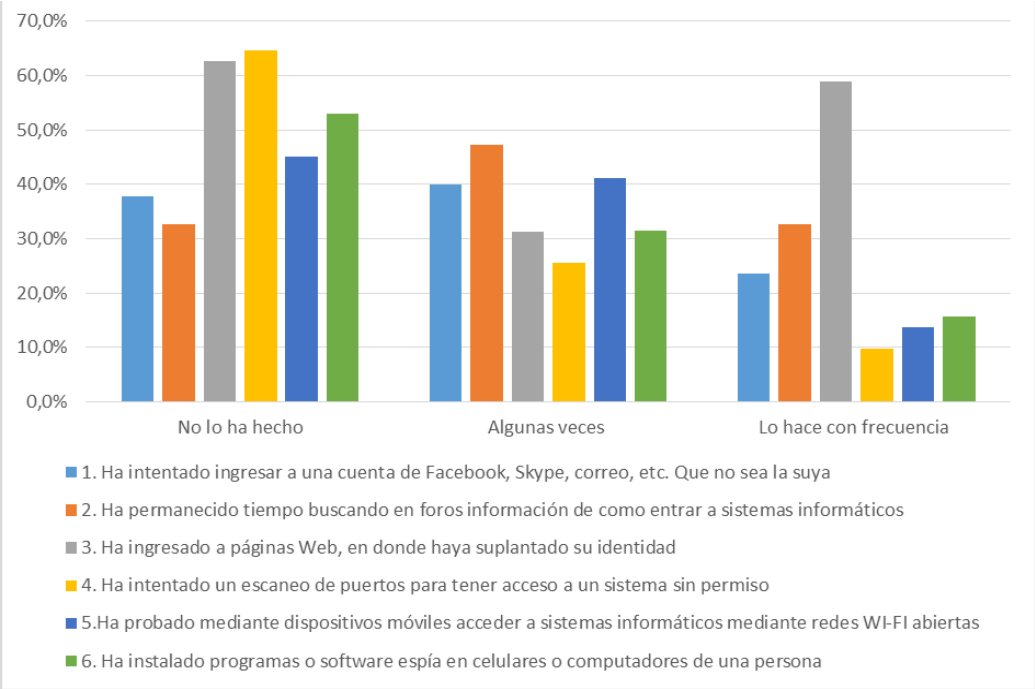


Ilustración 18. Resultado Encuesta Estudiantes con conocimiento en realizar actos a sistemas informativos.

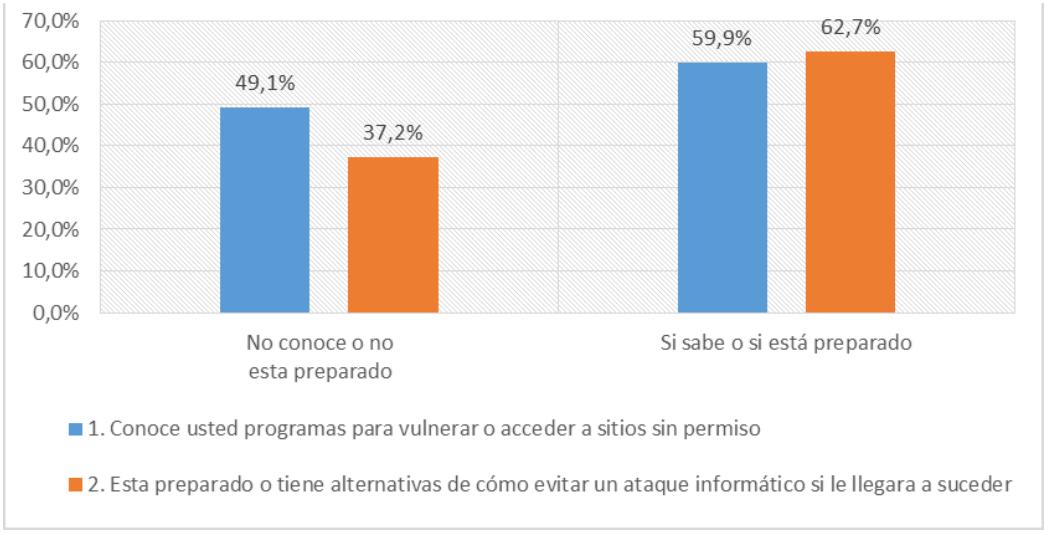


Ilustración 19 Resultado Encuesta Estudiantes con conocimiento de programas para acceder a sitios sin permiso.

Analizando los resultados de este grupo de preguntas se validó si los estudiantes están preparado o tiene alternativas de cómo evitar un ataque informático, si le llegara a suceder lo cual saco como resultado que el 62.7% de los encuestados tiene conocimiento, están preparados o tiene alternativas de cómo evitar ataques informáticos, mientras el 37.2% de los encuestados no sabrían cómo evitar un suceso de vulneración si en algún momento le llegara a sucederse o no estarían preparadas para dichos acontecimientos como se observa en la Imagen 9.

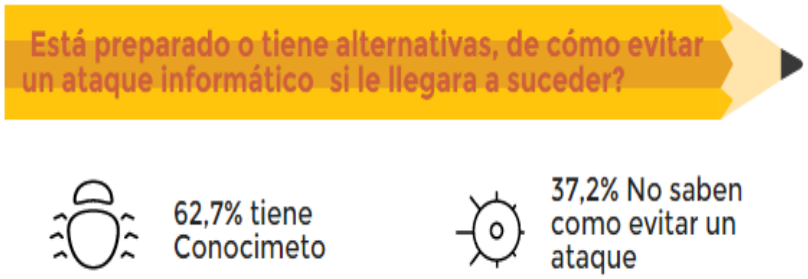


Imagen 9

Una de las preguntas que nos dejaría evidenciar si el estudiante tiene conocimientos claves en este tipo de irregularidades y además de poseer información y realizaría este tipo de actividades como el de vulnerar sistemas .Otra pregunta muy similar pero que dejaría evidenciar más conocimiento de los encuestados y perder desviar la curva de error que pueda tener la encuesta, en la que se preguntó ¿si ha intentado ingresar a una cuenta de Facebook, correo, Skype, etc. que no sea la suya? Con esta pregunta se identificaría si estos estudiantes a los que se les pregunto tiene conocimientos e iniciativas de hackeo mucho más fortalecidas que con solo haber leído o ver tutoriales, y que con estos conocimientos podrían llegar a realizar delitos en algún momento que podrían ser, hurtos por medios informáticos, suplantación de sitios web, transferencias no consentidas de activos, el acceso no autorizado a sistemas informáticos, el daño informático, violación de datos personales y uso de software malicioso."[142], ya que con estos delitos si se requiere realizar la violación de datos personales o la suplantación para esto buscando ingresar a cuentas que no sean la suyas, es por ello que tendría el aprendiz podría llegar a tener más incentivos de realizar dichos actos Los resultados obtenidos con esta indagación muestra es que el 37,7% no han tenido la iniciativa de acceder a estas cuentas con identidad falsa, el 39,2% lo

[142] *El Tiempo. Hurtos y suplantación de sitios web son las prácticas más comunes de los delincuentes virtuales. {18 mayo 2012}{En línea}.*

ha intentado y ha buscado como hacerlo, y el 23.5% lo hacen con mayor frecuencia como se observa en la Imagen 10.

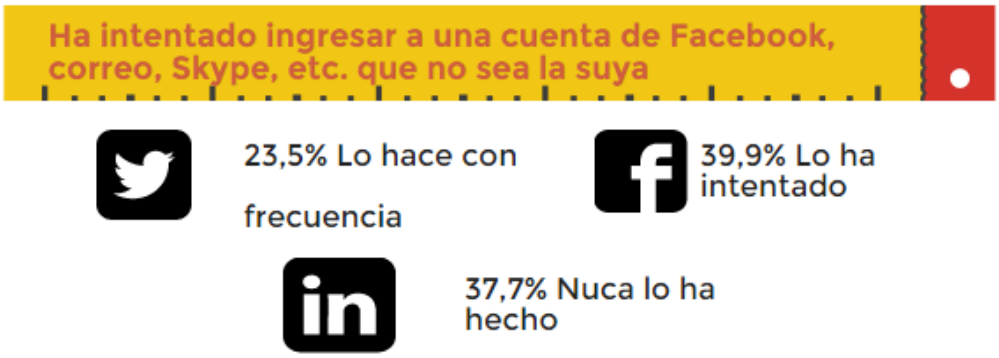


Imagen 10

Es por ello que se ve el caso donde situaciones comunes en las personas que pierden el control de sus correos y acceso a las redes sociales por personas que los suplantan y acceden a sus claves, siendo esto suplantación, que en muchos casos es realizado a través de la conocida técnica llamada pichinga, en los cuales los delincuentes capturan los datos personales de sus víctimas enviando un mensaje donde supuestamente informan que las tarjetas bancarias de los usuarios están bloqueadas o en otros casos como se ve en las ofertas que el señalado hacker Andrés Sepúlveda brindaba "Si usted quiere denigrar o posicionar a una persona o marca en la red, vale 160 millones de pesos (...). Podemos convertir un tema en 'tendencia' en 24 horas a nivel nacional y conseguirle miles de seguidores en Facebook en menos de una hora" u otro caso "También tenemos una aplicación para identificar palabras o frases que puedan afectar su imagen, y filtrarlas y atacarlas, desapareciéndolas de las redes o haciéndolas imperceptibles para sus miembros""[143], siendo esto ejemplo para muchos jóvenes a seguir y en muchos casos una guía para llegar a realizarlos y suplantar cosas tan básicas como Facebook, en los cuales se han detectado páginas y perfiles en Facebook creados para deshonrar a personas o empresas. "Diálogosavoces.com, por ejemplo, se montó para bombardear el proceso de paz con mentiras que hicieron carrera"[144], así como esto los jóvenes pueden empezar y llegar a suplantar cosas

[143] *Unidad Investigativa, El Tiempo. Así opera el negocio sucio de los trinos. {27 Mayo 2014}{En línea} Disponible en: http://www.eltiempo.com/politica/justicia/el-negocio-de-hackear-y-delinquir-por-redes-sociales/14044778*

[144] *Unidad Investigativa, El Tiempo. Así opera el negocio sucio de los trinos. {27 Mayo 2014}{En línea} Disponible en: http://www.eltiempo.com/politica/justicia/el-negocio-de-hackear-y-delinquir-por-redes-sociales/14044778*

básicas hasta identidades más grandes como podrían ser entidades bancarias y validando así con los delitos más realizados por jóvenes como se puede observar en la siguiente imagen:

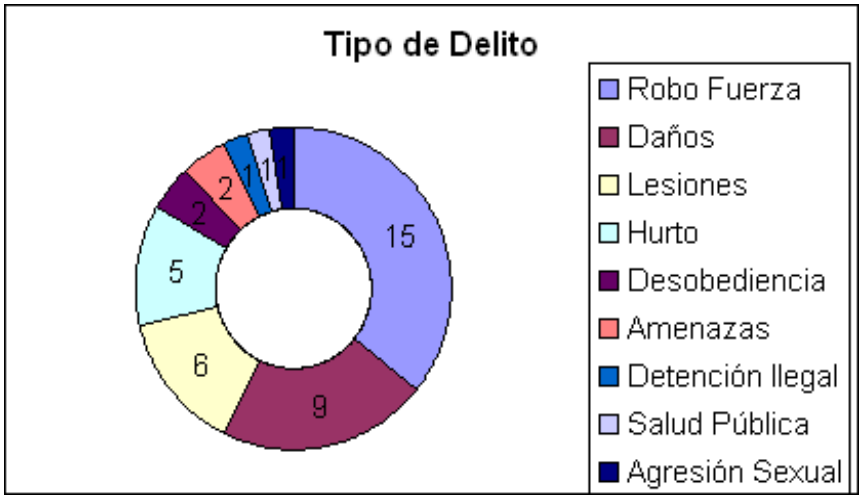


Ilustración 20 Tipo de delitos

En esta ilustración se observa que el principal delito es el de robo a fuerza que en los casos la gran mayoría es realizada con identidades falsas en diferentes sitios.

Con la investigación y realización de la encuesta de identifico aquellas personas que han permanecido tiempo buscando en foros información de cómo entrar a sistemas informáticos, esta pregunta realizada nos indicaría si un estudiante se podría convertir o tiene iniciativas en empezar a explorar su lado hacker, donde los resultados arrojan que el 32.7% de los encuestados afirman no haber buscado nada de este tipo de información, el 47.3% lo ha hecho pero con menos ocurrencia de veces y el 20% se puede decir que busca constantemente y permanece en estos sitios como lo muestra la Imagen 11.

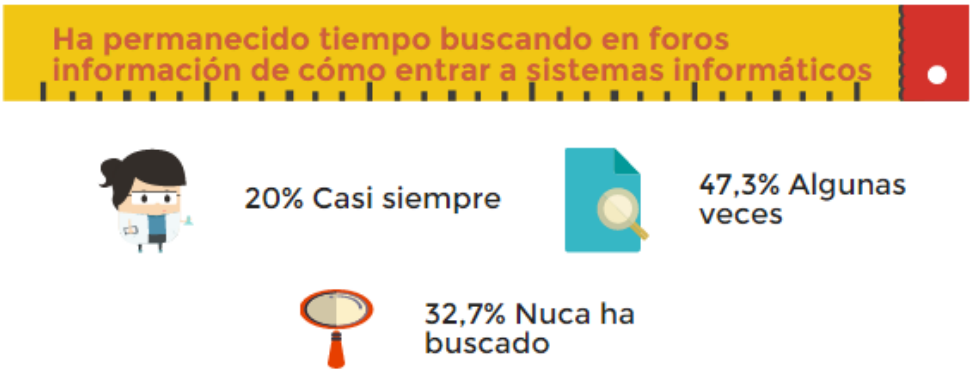


Imagen 11

En Colombia y Latinoamérica cada vez son más los adolescentes que transforman sus innovadores conocimientos de informática en potenciales empresas o por el contrario convirtiéndose en peligroso delincuentes, que lo único que buscan es hacer daño a personas o empresas y que lo van logrando buscando y accediendo a medios en casos desde muy temprana de edad, para validar estos resultados se ve el caso del joven colombiano "Juan Eljach que empezó su aventura dentro del mundo de las computadoras cuando tenía tan sólo 12 años. El tiempo que dedicó al estudio de lenguajes de programación le permitió ser consultor de seguridad y difundir técnicas de hackeo ético"[145], se observa con esta pregunta que los jóvenes colombianos en promedio si tiene tendencias a convertirse en hacker y desde muy temprana edad buscando información para irse preparándose, ya sea para robar información que beneficie a sí mismo o en casos haciéndolo por hobby, que tiempo después se convertirá en algo más usual y en momentos por remuneración, convirtiéndose este acto no en hobby si no trabajo diario.

Otra de las preguntas de este grupo era indagar si el encuestado conocía programas para vulnerar o acceder a sitios sin permiso, con lo cual se quiso observar el conocimiento sobre herramientas de vulneración, los resultados arrojan que el 50.9% afirma no tener ningún conocimiento sobre programas para vulnerar sistemas y el 49.1% de los estudiantes encuestados tienen algo de conocimiento o si saben de muchos de los temas de herramientas y programas para el hackeo, como lo muestra la Imagen 12.

[145] *Pulsosocial. Joven latinoamericano crea escuela para aprender a hackear{06 Octubre 2014}{En línea} Disponible en: http://pulsosocial.com/2014/10/06/joven-latinoamericano-crea-escuela-para-aprender-hackear/*

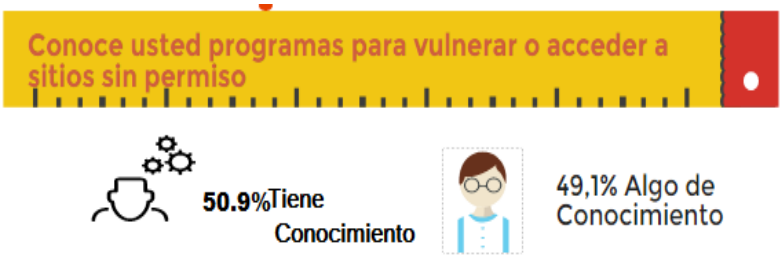


Imagen 12

Según lo observado y muchas veces cuando empieza a buscar o se tiene conocimiento de las herramientas de vulneración de la información, es porque se empieza a indagar lo que se quiere hacer y porque sabe dónde atacar, ya sea para obtener datos personales, robar cuentas, ingresara medios ocultando su identidad entre otros delitos y es allí donde conocen todo sobre cada sistema operativo para mandar ataques preparados para cada uno y así verificar cada herramienta diseñada por un hacker que es capaz de encontrar la vulnerabilidad necesaria para comprometer el sistema y robar la información que se quería obtener de dichos sistemas, como es el caso de “Faber Orlando Restrepo, quien por dos años trabajó en Bancolombia y luego en una reconocida firma que prestaba soporte técnico y de seguridad al banco. Además, Restrepo era experto en arquitectura de virtualización de la banca. Peritos del Centro Cibernético de la Policía explicaron que a través de Restrepo, a quien llamaban 'Repo', la red logró acceder a los usuarios y contraseñas de gerentes y subgerentes del banco que estaban en vacaciones o con días de permiso y así "insuflar" cuentas, es decir, mover sumas de dineros a las cuentas reclutadas”[146].

Aunque con esta validación se observa que la mitad de los jóvenes no conoce ni busca herramientas para vulnerar, se ve gran representación de jóvenes que si lo está haciendo y que con esto se podrían convertir no en hacker pero si en personas que en casos se les tendrían respecto, que aunque no realicen delitos informáticos en su vida diaria en caso alguno podrían llegar hacer un daño informático de gran impacto.

Otro caso en el que se puede observar si un joven ya está más afianzado y tiene mayor conocimiento sobre hackeo o piratas informáticos fue con la siguiente pregunta. Al crear sus contraseñas en correos, computador, etc. se fija en, en este caso se dio opciones de respuesta que dejaran ver si una persona es muy

[146] *Justicia El Tiempo. Así planearon los hackers el robo de $ 160.000 millones. {18 Diciembre 2014}{En línea} Disponible en: http://www.eltiempo.com/politica/justicia/hackers-movieron-160000-millones-de-pesos/14991075*

protectora y tienes claves diferentes para cada cuenta, o se fija mucho en utilizar símbolos y caracteres alfanumérico, etc. Ya que en el momento de realizar cuentas y crear sus contraseñas ya previene ataques siendo seguros un poco más seguro, también se podría observar si tiene los tips que da el primero joven Colombiano de realizar una escuela de hackeo, el cual nombra "que las contraseñas no son seguras, es importante definir frases de paso, en lugar de claves convencionales, no usar la misma clave para todo , es importante tener el mismo patrón anterior modificado para cada servicio en internet, siempre usar conexiones seguras , sus datos viajan encriptados, no se conecte a redes Wifi abiertas en lugares públicos que no sean legítimas, la descarga del software pirata, cracks y todo tipo de programas no legales están acompañados de gusanos que pueden infectar el computador y convertirlo en un zombie esclavo de otros atacantes"[147], por ello analizando las respuesta a esta pregunta se puede observar que el 74.5% de los encuestados si tiene precauciones con sus contraseñas, mientras que un 20% son más propensos a ataques ya que no tienen en cuenta de su vulneración y el 5.5% de los estudiantes no aseguran sus datos, como se puede ver en la Imagen 13.

Imagen 13

Con la imagen anterior se puede evidenciar que los jóvenes si están seguros con sus cuentas y están precavidos con una situación de vulneración y no están en peligro que sus datos sean descifrados fácilmente con algún software. Como lo menciono "el coronel Bautista como un delito informático puro, consiste en ingresar a cuentas de terceros, suplantarlos o divulgar información privada. En la oficina de Sepúlveda se halló un software para descifrar y violar contraseñas. Esos servicios ilegales –que derivan en delitos más graves como la extorsión–, se

[147] *Ramírez Galvis. La primera escuela para aprender a hackear. {28 Septiembre 2014 }{En línea} Disponible en: http://www.vanguardia.com/actualidad/tecnologia/280521-la-primera-escuela-para-aprender-a-hackear.*

ofrecen por sumas que van desde los 100.000 a los 500.000 pesos"[148]. Aunque la respuesta no indica que saben protegerse, también indica que este tipo de personas podrían llegar a tener conocimiento no solo de cómo protegerse sino, también de como atacar.

Al ser los sistemas, la información, el internet medios que facilitan el aprendizaje se realizó preguntas dentro de la encuesta que se acercaron más a indagar estos puntos, un nivel quizás más avanzado de conocimiento del tema en estos jóvenes ¿ha ingresado a páginas web en donde haya suplantado su identidad las respuestas indicaron que de estas personas el 62,7% no lo habían intentado, el 31,3% de los encuestados algunas veces lo han intentado con una intensidad más baja, mientras que el 5,9% de los encuestados son personas que realizan esta acción con más frecuencia, para observar esto podemos visualizarlos en la Imagen 14.

Revisando estos porcentajes y para entender mejor la suplantación de la identidad esta puede "realizarse a los dispositivos informáticos, pasando desde tu dispositivo de red, llegando a tu ordenador y visitando tu teléfono móvil. La suplantación de identidad a dispositivos informáticos se denomina spoofing y consisten en utilizar técnicas que permitan engañar de alguna forma la tecnología"[149]. Desde esta denominación se deriva diferentes clases de spoofing como lo es la Ip Spoofing, Mail Spofing, Phone Spofing, etc. En la pregunta nombrada anteriormente al suplantar la identidad en la web podemos estar hablando de Ip Spoofing ya que este ataque funciona suplantando la identidad "de otro ordenador con una IP determinada de tal forma que todo el tráfico que este genere, parezca legítimo de la IP suplantada. Para efectuar el ataque se deben de generar paquetes IP con una IP de origen falsa."[150]

[148] *Unidad Investigativa, El Tiempo. Hay tarifas para posicionar candidatos, difamar y crear falsas tendencias. El tema pasó a lo penal. {27 Mayo 2014 }{En línea} Disponible en: http://www.eltiempo.com/politica/justicia/el-negocio-de-hackear-y-delinquir-por-redes-sociales/14044778*

[149] *Undercode, Spoofing, suplantando tu identidad. {24 Diciembre de 2014 }{En línea} Disponible en: https://underc0de.org/foro/seguridad/spoofing-suplantando-tu-identidad/*

[150] *Ibíd.*

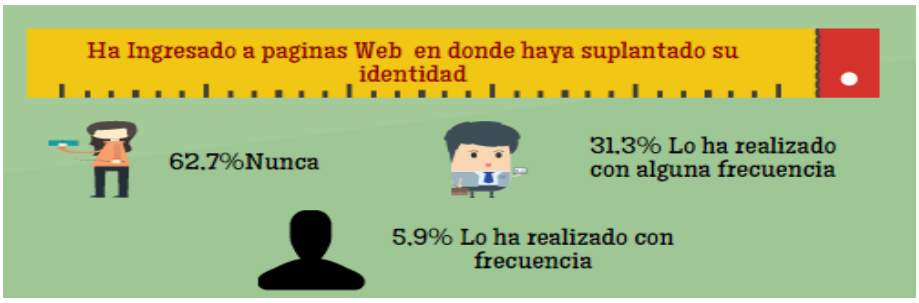


Imagen 14

Otras de las preguntas que dejaba ver si estos jóvenes conocen diferentes métodos que muchas veces utilizan los ¿ha intentado un escaneo de puertos para tener acceso a un sistema sin permiso?, el resultado de esta pregunta dejo evidenciar como el 64,7% de los encuestados nunca han realizado este tipo de actividad, el 25,5% de los encuestados en algunas ocasiones lo han realizado y el 9,8% de las personas si lo hacen, esto se puede ver en la Imagen 15.

Uno de los programas más conocidos para este tipo de actividad de detección de puertos abiertos encontramos "Nmap es un programa muy conocido, y puedes encontrarlo en versiones tanto para Windows como para Linux."[151]. Este programa escanea un equipo, detectando los puertos abiertos, cerrados hay páginas en donde se puede llegar a descargar este equipo de forma gratuita y otros mejorando el programa de forma pagada, se dice que es un programa muy difícil de detectar por los antivirus o por el usuario del equipo, este programa deja ver al hacker la mejor forma de acceder y penetrar el equipo. El funcionamiento del programa depende de: "velocidad de la computadora de quien escanea (hacker), latencia en la red (si la red es lenta o rápida), y velocidad de respuesta y medidas de seguridad de la computadora escaneada (victima)"[152]

Para visualizar las cifras anteriormente dichas y evidenciar lo dicho se dieron los resultados a la pregunta formulada anteriormente de la siguiente forma:

[151] *V. Jorge, Herramientas básicas para Hacking (escaneo). {3 julio 2015 }{En línea} Disponible en: http://codigoprogramacion.com/articulos/hacking/97-herramientas-basicas-para-hacking.html#.VbUY0_l_Oko*
[152] *Ibíd.*

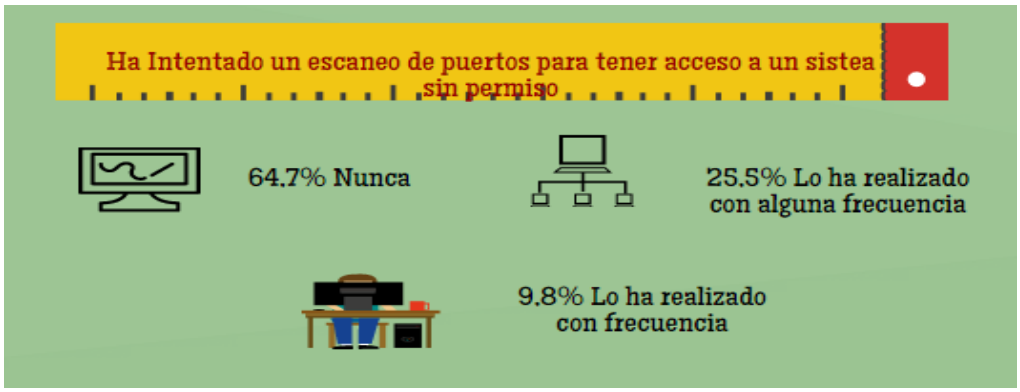


Imagen 15

Haciendo una búsqueda en internet sobre programar para encontrar puertos abiertos para hacker se encontró el siguiente resultado:

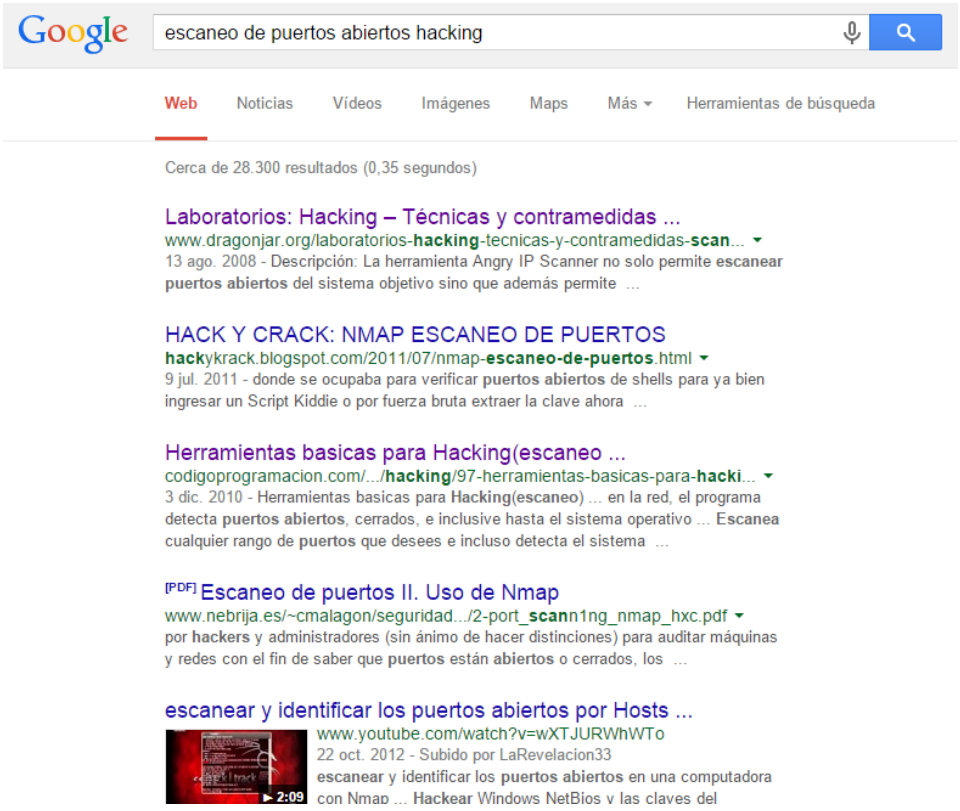


Ilustración 21.Información que se encuentra con tan solo colocar palabras claves en el explorador

Para este caso se encontró 28.300 resultados, después se procedió a buscar programas para escaneo de puertos en esta búsqueda se encontró 44.800 resultados de estos resultados la mayoría de páginas dice cómo funcionan algunos programas para el escaneo de puertos, diciendo el paso a paso de cómo utilizarlos los diferentes métodos y en algunos de estos tienen un link para descarga del programa, otros para tutoriales con video de cómo realizarlo. Con esto se pudo comprender como el internet es el mayor mecanismo de flujo para encontrar información para hackers, muchas de estas páginas son realizadas por grupos de hackers que enseñan a otros como ingresar y realizar las cosas, foros de jóvenes donde se reúnen expertos y jóvenes que quieren empezar a conocer y aprender sobre los métodos. El internet deja evidenciar un flujo importante de información para principiantes, expertos, y empresas formadas para este tipo de delitos.

Continuando con la investigación en jóvenes colombianos se realizó la siguiente pregunta: ¿Ha probado mediante dispositivos móviles acceder a información mediante redes wi-fi abiertas? La indagación a esta pregunta fue formulada ya que mediante todo el estudio del estado del arte del tema del hacking se encontró un gran grupo de personas que estaban realizando este tipo de métodos en centros comerciales, empresas, etc. en donde encontraban esta metodología como una oportunidad muy buena para el hackeo.

El resultado de esta pregunta para los jóvenes encuestados de la Universidad Piloto de Colombia nos arrojó las siguientes respuestas: el 45,1% de los encuestados nunca ha realizado esta actividad por este método, el 41,1% de los encuestados respondió que lo ha realizado con una frecuencia irregular, y el 13,7 de los encuestados lo ha realizado con más frecuencia y conocen plenamente del tema, para evidenciar mejor estos resultados se pueden ver en la siguiente Imagen 16.

[153] *Google.com, escaneo de puertos abiertos hacking. {26 julio de 2015 }{En línea} Disponible en: https://www.google.com.co/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=escaneo+de+puertos+abiertos+hacking*

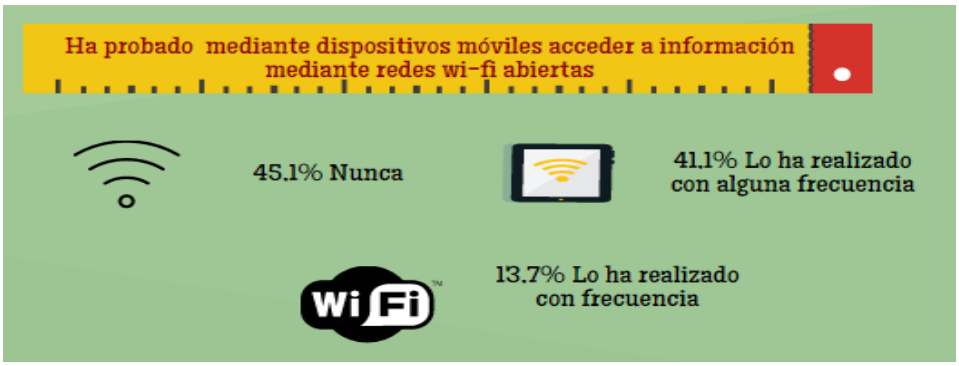


Imagen 16

El acceso a el dispositivo de alguien no solo de realiza muchas veces por medio de redes Wifi abiertas, existen programas en donde nos puede obtener la contraseña de la red, aunque lo primero que muchas veces realiza el hacker es buscar información o usuarios, empresas, etc. claves con redes abiertas, si este no es el plus que le da el acceso a una potencial víctima, utiliza los programas que les ayudan a hackear la clave de acceso a la red. También es muy utilizado este método ya que "una ventaja para el hacker de navegar con wifi ajenas es que si comete algún delito informático, queda registro de la IP de la red hackeada, y no de la del hacker"[154]

Una de las noticias importantes de este método que utilizan los hackers es "el sistema creado por Hacking Team, empresa considerada por la organización Reporteros Sin Fronteras como un enemigo del Internet, funciona a través de un troyano, que es un software computacional "maligno" que permite realizar una serie de acciones dentro de un dispositivo"[155], lo bueno de la aplicación es que "la implantación del troyano no es complicada, aunque requiere acceso directo al dispositivo. Según la misma empresa detalla, la infección se puede realizar vía WiFi (por la misma red de internet del aparato), cable USB, a través del proveedor de internet e, incluso, mediante aplicaciones diseñadas especialmente para engañar al usuario. Esto último tiene un precio adicional (US$175 mil)"[156]

---

[154] *Gonzales Antonio, Cómo hackear wifi o robar wifi al vecino? 10 programas para robar contraseñas y acceder. {26 julio de 2015 }{En línea} Disponible en: http://antoniogonzalezm.es/como-robar-la-wifi-de-un-vecino-10-programas-para-hackear-contrasena-y-acceder/*

[155] *Ciper, Los correos que alertaron sobre la compra del poderoso programa espía de la PDI. {10 julio de 2015 }{En línea} Disponible en: http://ciperchile.cl/2015/07/10/los-correos-que-alertaron-sobre-la-compra-del-poderoso-programa-espia-de-la-pdi/*

[156] *Ibíd.*

Con toda esta información surgió la pregunta que también tenía mucho que ver con el mundo actual y la utilización masiva de la comunicación portable como lo es las Tablet, y los dispositivos móviles como los celulares ya que por este medio es por donde también se ha incrementado el delito informático y la utilización de estos medios para robar información, que ahora los usuarios guardan y que puede dar valiosa información para un hacker, desde las noticias como el robo de fotografías a personajes importante o robo de claves bancarias y acceso a múltiples programas y páginas personales o conversaciones importantes. Dado este Bum e importancia generado últimamente se realizó la última pregunta para los estudiantes la cual se basó en cuestionar si ha intentado instalar programas o software espía en celulares, Tablet o computadores personales.

El resultado arrojado observo que el 52,9% de los encuestados no ha realizado nunca este tipo de actividad, el 31,4 lo ha hecho y el 15,6% lo hace con gran frecuencia esto se puede observar en la siguiente Imagen 17.

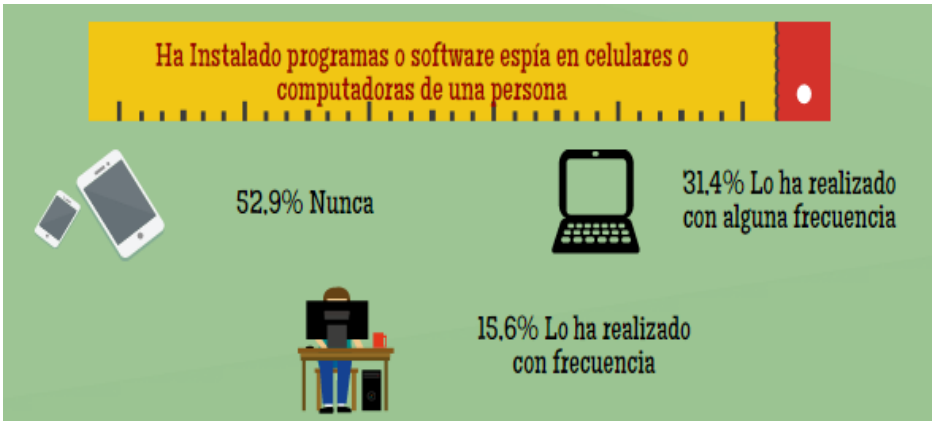


Imagen 17

Estas respuestas dejaron ver como entre el porcentaje de las personas que algunas veces lo han realizado y aquellas que lo realizan con frecuencia es un número de estudiantes alto, que deja ver como el conocimiento en cierto punto es interés mismo, que deja la carrera y la atracción de algunos temas hacia la misma. Hace que estos jóvenes intenten métodos escuchados, aprendidos y reforzados muchas veces por lo que ahora deja el internet y los foros, estos jóvenes se inclinan en gran medida a realizar, probar o investigar sobre el tema.

Si bien las encuestas realizadas a estudiantes, en su mayoría fue respondida por estudiantes de pregrado tanto de Ingeniería de Sistemas como de Telecomunicaciones, de igual forma algunos del posgrado de seguridad informática pero en menor cantidad, por lo cual deja ver que la mayoría de los estudiantes que contestaron la encuesta, no son personas que estarían trabajando

en el tema, o ya con conocimiento más estructurado para este tipo de actividades, se puede decir que estas personas han buscado conocimiento más allá del aprendido en las carreras y que han intentado un camino de delito informático que aún no se puede denominar como alto, pero si un porcentaje muy importante y evidenciable para determinar que existe un grupo de estudiantes inclinados por este tipo de actos.

La mayoría de la encuesta fue respondida por 37 estudiantes de Ingeniería de sistemas, 10 de Telecomunicaciones y 8 del Posgrado de Seguridad informática, en su mayoría ellos están en último semestre de ingeniería de Sistemas, encontramos resultados entre los semestres de 7, 8 y 9 que equivalen al 13% y encontramos una cantidad muy considerable e importante de evaluar entre los semestre de 1 a 5 los cuales ya han realizado y conocen varias técnicas de vulnerabilidad, ya sea indagando sobre software pirata para llegar a una meta propuesta o simplemente empezando a practicar sobre vulnerabilidad como claves de wifi o redes sociales Facebook, intentando ingresar con credenciales falsas, estos actos relevantes son realizado en algunos casos por estudiantes de primeros semestres, , sin saber el daño que pueden causar o por el contrario pueden causarse si se meten en un acto delictivo, ya para estudiantes de ingeniería de sistemas con semestre más avanzados empiezan son a descargar programas piratas, ya sea para ver una película pirata por Netflix vulnerándolo o simplemente ya en casos más exactos han realizado episodios donde han ejecutado sus conocimientos para realizar vulneración en beneficio propio o en trabajo para terceros, ya para estudiantes de ingeniería de telecomunicaciones se encontró resultados entre los semestres de 7, 8, 9 y 10, que para el grupo de telecomunicaciones equivalen al 15.68%, igualmente se evidencio un 1.96% de los encuestados de semestre 2, se pudo observar con los resultados de la encuesta para este grupo que la mayoría tiene un conocimiento claro de cómo evitar vulneraciones, saben técnicas para hacerlo, pero en su momento no se atreverían a realizar ya un acto de hackeo o vulnerabilidad a un sistema, ya sea para beneficio propio o si alguien les llegara a proponer hacerlo por dinero no estarían dispuestos a realizarlo, también se observa que no están en la capacidad de buscar a un tercero para realizar delitos informáticos sus conocimientos los aprendes por intuición misma, o en otro caso para el semestre inferior este se ve que tiene toda la disponibilidad de aprender sobre las técnicas, programas, etc., que existen para vulnerar sistemas, así se para tener este conocimiento y en su momento utilizarlos como los estudiantes de sistemas, para vulnerar cosas básicas e ingresar a redes con identidad falsa, todos estos resultados como se evidencia en las Ilustración 21 e Ilustración 22

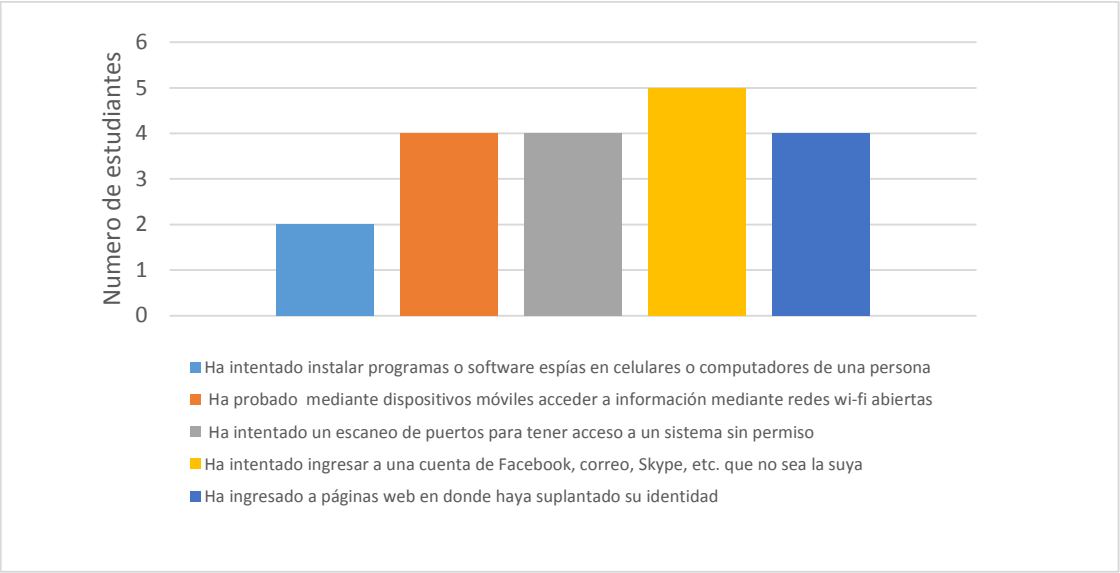


Ilustración 22 Número de estudiantes que han realizo dichas actividades planteadas en las preguntas

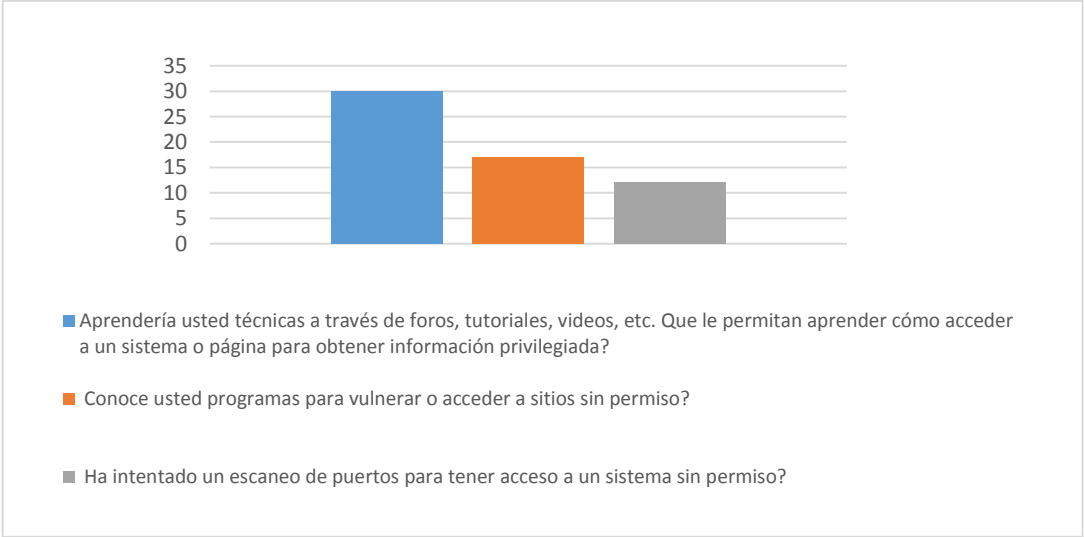


Ilustración 23. Respuesta dadas por estudiantes de semestres entre 9, 10 y egresados.

Los estudiantes manifiestan que es más habitual consumir contenido de forma ilegal o en casos más extremos dicen haber accedido a aprender técnicas de ataque a sistemas informáticos, conocen programas e intentado ejecutar escaneo de puertos para acceder a sistemas sin permiso.

Para la encuesta realizada a los docentes de las carreras mencionadas anteriormente se realizaron dos validaciones en el primer grupo se buscaba

identificar si existe una influencia de los profesores desde los conocimientos transmitidos en las actividades académicas o con actos de enseñanza, para que un estudiante tenga iniciativas en participar en actividades relacionadas con la cultura hacker. Para el cual se obtuvo el siguiente resultado como se puede observar en la lustración 23 y lustración 24

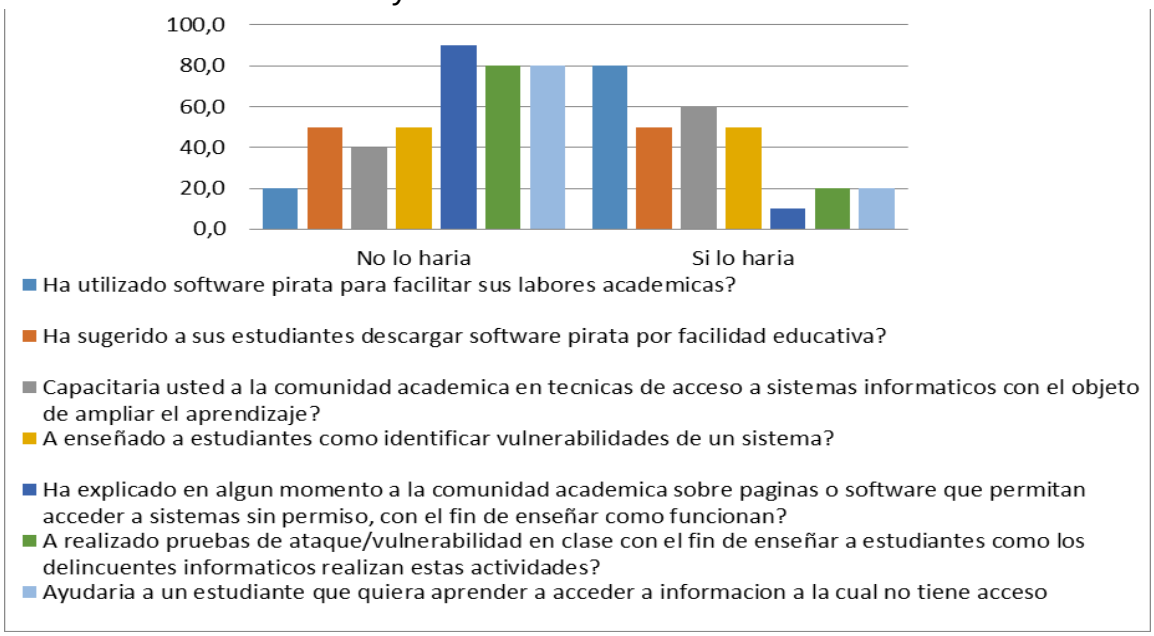


Ilustración 24 Resultado Encuesta de Docentes para validar la influencia en estudiantes, para que realicen actividades relacionadas con la cultura hacker

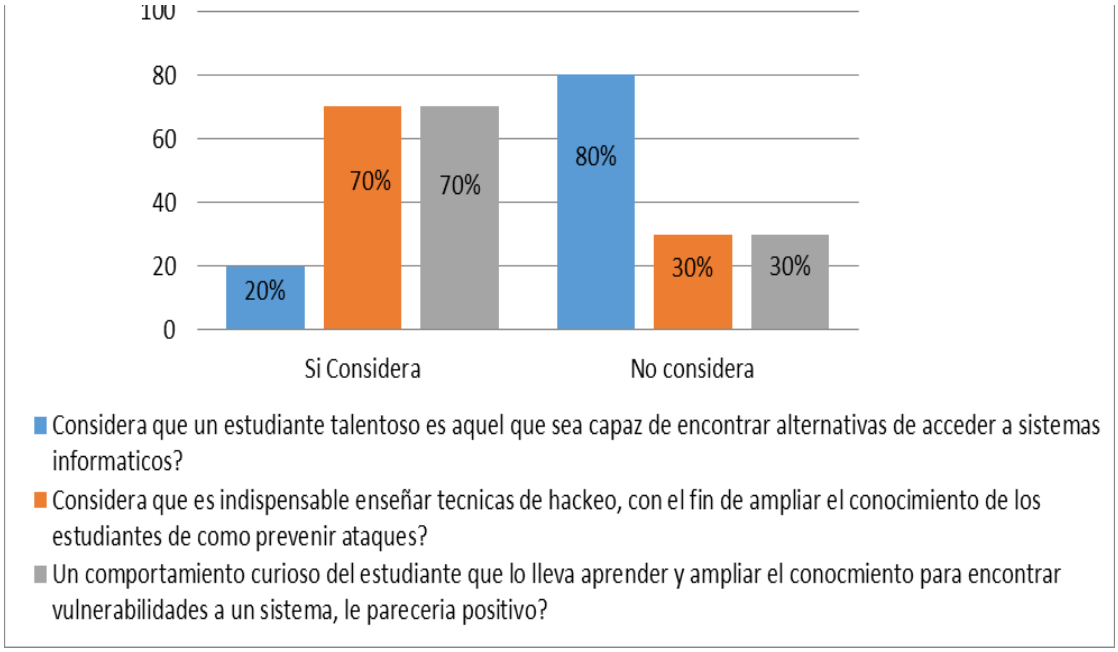


Ilustración 25 Resultado Encuesta de Docentes para validar la influencia en estudiantes para que realicen actividades relacionadas con la cultura hacker

Con relación a lo anterior, la encuesta realizada a los profesores se basó en 12 preguntas, que se puede tener acceso al anexo de este documento "Respuesta Profesores".

Basándose en la primera validación que se quería encontrar, una de las preguntas del primer grupo, era identificar aquellos profesores que influyen para que un estudiante tenga iniciativas en participar en actividades relacionadas con la cultura hacker, por lo cual han utilizado software pirata para facilitar sus labores académicas. Para este caso se encontró una fuerte inclinación en las respuesta que podrían llegar hacerlo y en un cierto número aquellas personas que lo harían, con respecto a ello se encontró que el 20 % de los encuestados nunca utilizaría software pirata para desarrollar sus labores académicas, mientras el 80% realizaría este acto de utilizar software pirata para sus labores académicas con estudiantes como se observa en la Imagen 18, con el análisis de la primera pregunta podemos observar como los profesores tienen una atracción de utilizar software pirata, ya que lo ven como una forma de facilitar sus labores académicas sin necesidad de dar a sus estudiantes un gasto económico.

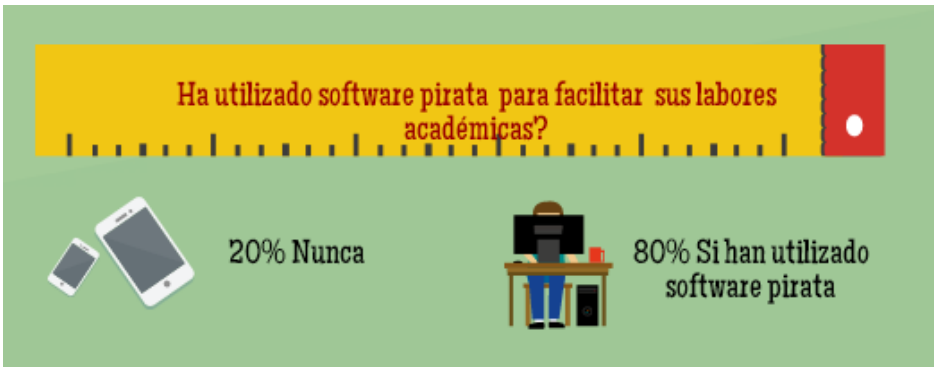


Imagen 18

Un artículo que nos habla de porque usar software pirata no es una buena práctica. Se dice que es más caro el precio del software que viene incluido en el computador que el precio del computador en sí y se realiza las siguientes preguntas "¿El trabajo de los desarrolladores de Microsoft Office es menos valioso que el de los desarrolladores de procesadores? ¿Les costó menos trabajo desarrollar una aplicación que desarrollar un procesador?"[157] Razones dadas por muchas personas es que comprar los productos en este ejemplo de Microsoft Office es muy costoso y la mayoría de personas no tiene el dinero suficiente para comprarlo, el artículo no hace una reflexión diciendo:" ¿Por qué, entonces, mejor no se roba el computador y compra el software? ¿Cuál es la diferencia? ¿Si robar un computador fuera tan fácil como copiar un programa, lo robaría? probablemente no, ¿cierto?"[158] .

Las razones numerables de porque no se debe utilizar el software pirata es porque dentro de esto vienen lo que llamamos los virus de los delincuentes informáticos así, que si un profesor usa un software pirata está dando inicio el mismo a la no protección de su información, y peor aún si este indica a sus estudiantes a descargar software estará haciendo que los delincuentes informáticos tengan una puerta abierta y así dejando brechas de seguridad mucho más altas para los hacker informáticos.

No alejándose mucho de la piratería, que muchas veces se hace por desconocimiento dejando una puerta abierta se realizó la pregunta queriendo ver

[157] *Alvarado Noguera Ernesto, Universidad Segio Arboleda, No use software pirata. - Alternativas para no ser ilegal, {26 julio de 2015} {En línea} Disponible en: http://www.usergioarboleda.edu.co/altus/software-pirata-alternativas.htm.*

[158] *Alvarado Noguera Ernesto, Universidad Sergio Arboleda, No use software pirata. - Alternativas para no ser ilegal,{ 26 julio de 2015 }{En línea} Disponible en: http://www.usergioarboleda.edu.co/altus/software-pirata-alternativas.htm*

si los profesores incitan a los estudiantes a descargar software pirata para muchas veces por facilidad educativa. En este caso encontramos una balanza semejante ya que el 50% nunca lo hacen y el otro 50% de los profesores si incitan a los estudiantes a descargar programas piratas, como se observa en la Imagen 19.

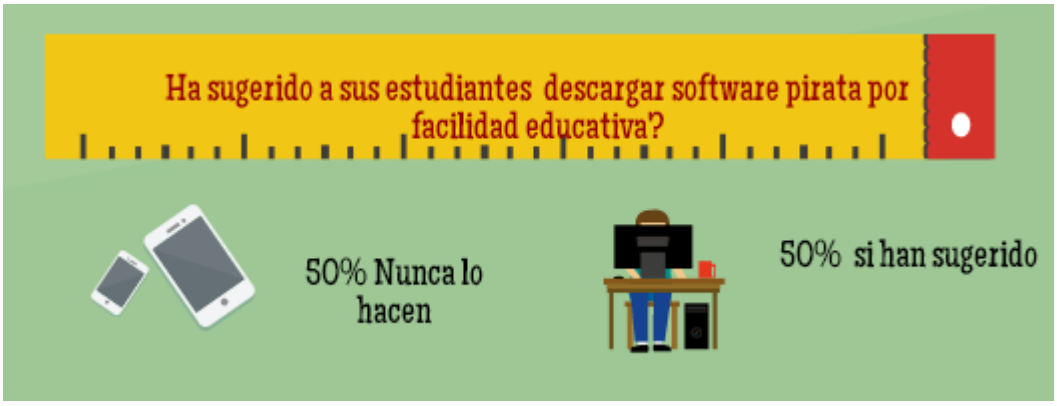


Imagen19

El periódico portafolio indica como "uno de cada tres consumidores y tres de cada diez empresas en el mundo es 'pirata'."[159] "La investigación muestra que los consumidores gastan 1,5 millones de horas y 22.000 millones de dólares en la identificación, reparación y recuperación de los efectos de malware, mientras que en las empresas globales superan los 114.000 millones de dólares para enfrentar el impacto de un malware inducido por los ciberdelincuentes"[160]

Otra de las preguntas realizadas en la encuesta para identificar aquellos profesores que podrían influir para que un estudiante tenga iniciativas e indagaciones en estos temas. Se preguntó si considera que un estudiante talentoso es aquel que sea capaz de encontrar formas alternativas de acceder a sistemas informáticos. Para esta pregunta se obtuvo respuestas en las que el 20% de los encuestados están de acuerdo y consideran que un estudiante que tenga capacidades de vulnerar sistemas o realizar actos delictivos es un estudiante talentoso, mientras el 80% cree que esto no es un estudiante talentoso, considerando que es totalmente al contrario, es una persona que ya no ve el conocimiento en buena forma si no que lo lleva a otro camino siendo esto de poca ética estudiantil.

[159] *Portafolio, Empresas pierden US$114.000 millones por software ilegal. ,{ 8 2013 }{En línea} Disponible en: http://www.portafolio.co/negocios/software-pirata*
[160] *Ibíd.*

Imagen 20

Se identificó una noticia que identificaba como “Gerson Daniel Peña Mejía, en la foto, conocido con el alias del Ministro, se dedica a reclutar jóvenes estudiantes de ingeniería de sistemas con la idea de instruirlos sobre los delitos informáticos, trabajar con ellos y hacer los fraudes”[161]. Esto se hace mediante archivos en internet que estimulan a jóvenes estudiantes que tienen conocimiento en programación a que se estimules a través de dinero a ingresar a este tipo de grupos a aprender mediante foros y llevarlos a que comiencen a cometer delitos informáticos. Las personas ven como grandes potencias los jóvenes que están en constante aprendizaje y que están más cercanos a temas de hackeo ya que son personas conocimiento de aportar.

Para validar la tendencia en que si los profesores podrían llegar a incitar a sus estudiantes a irse por el camino de la vulnerabilidad, sin que sea una iniciativa a que lo hagan, sino como forma de aprendizaje que podría llevar a jóvenes a inclinarse a utilizar este conocimiento aprendido para encaminarse por el lado de la vulnerabilidad de los sistemas, una de las preguntas que se planteó y de la cual se tendría un acercamiento sobre este tema, es que si los profesores estarían dispuestos a capacitar a sus estudiantes en técnicas de acceso a sistemas informáticos, donde se observó en los resultados de la pregunta que el 60% de los profesores si estarían dispuestos a enseñar a sus estudiantes técnicas de hackeo para que este amplié su conocimiento sobre el tema, mientras el 40%, tiene claro que no lo haría y que si influyen en este conocimiento de técnicas verían a sus estudiantes haciendo el mal en un futuro, como se evidencia en la Imagen 21.

[161] *EL HERALDO.COM, Cayó hacker que presuntamente reclutaba estudiantes. , {25 junio de 2015 }{En línea} Disponible en: http://www.elheraldo.co/region/cayo-hacker-que-presuntamente-reclutaba-estudiantes-201632*

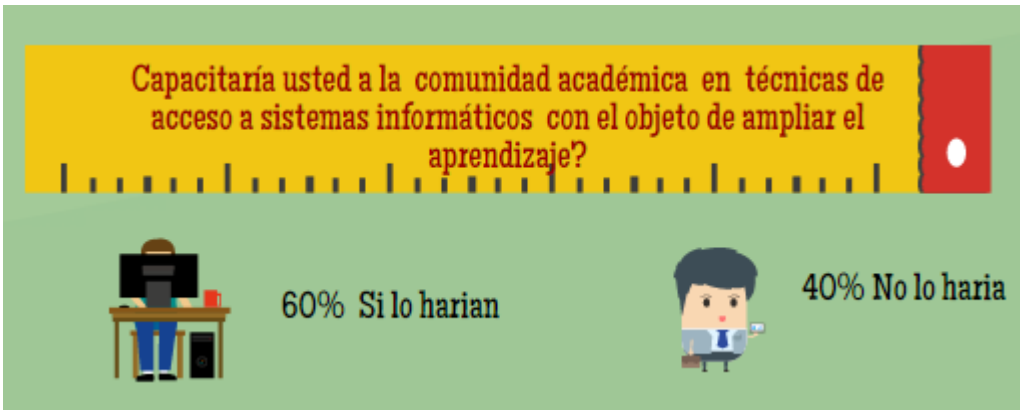


Imagen 21

Analizando los resultados se observa que los profesores se van más por el lado de la libertad de aprendizaje, en donde sus estudiantes estén en el abismo de nuevos conocimientos, como se explica en un blog de conektioblog sobre cuatro metáforas para representar el rol del profesor en las nuevas tendencias de aprendizaje, “Obviamente no nos referimos a un delincuente informático, sino a la palabra hacker en su sentido más amplio: alguien con pasión y entusiasmo por lo que hace. Los hackers son innovadores y desafían al sistema para que cambie y funcione mejor. Es una mentalidad y una actitud, y como se explica en esta charla TED, nuestro mundo necesita más gente con mentalidad de hacker. De igual forma, la educación necesita más profesores con mentalidad hacker para que se cuestionen el sistema y lo transformen, idea que ha desarrollado Alejandro Piscitelli”[162]. Y aun así si esta metodología no se llegara a implementar se tendría que ver la opción como dice John Hawkes, consultor privado de seguridad., “Los chicos son infinitamente inquisitivos, así que siempre será un reto mantenerlos alejados de las cosas que quieren husmear, pero no debería estar fuera de nuestra capacidad.”[163].

Respecto al tendencia que se quiso validar en lo antes mencionado, otra pregunta en donde se observaba si un profesor sería una influencia en el conocimiento de vulnerabilidad en los estudiantes, es que si los profesores piensan que enseñarle técnicas de hackeo es indispensable en su vida académica para que los

[162] *Marlopduar. Los nuevos roles del profesor: hacker, DJ, coach y Community Manager. { 20 febrero 2014} {En línea}. Disponible en: http://conektioblog.com/2014/01/30/LOS-NUEVOS-ROLES-DEL-PROFESOR-HACKER-DJ-COACH-Y-COMMUNITY-MANAGER/*

[163] *Jiménez Roberto. Expulsan a alumnos californianos por hackear PC de profesores y cambiar calificaciones. {04 febrero 2014}{En línea}. Disponible en: http://www.qore.com/noticias/15819/Expulsan-a-alumnos-californianos-por-hackear-PC-de-profesores-y-cambiar-calificaciones*

estudiantes sepan cómo prevenir si en algún momento les llegara a suceder un episodio de hackeo, donde para esta pregunta las respuestas de los encuestados se centró en que un 70% está de acuerdo en la enseñanza de técnicas para prevenir ataques ya sean por personas diferentes a ellos o en algún momento como en la preguntan anterior ellos mismos capacitarlos, para que así los estudiantes tengan en su carrera académica todos los posibles conocimientos como lo es las técnicas básicas o de expertos sobre hackeo y el 30% de los encuestados respondieron que están en desacuerdo en la enseñanzas de técnicas, como se ve en la Imagen 22.

Imagen 22

Además de estas respuestas dadas por los profesores se puede observar que esta idea no está muy lejos de ser implementada en diferentes universidades, ya que están permitiendo a los estudiantes experimentar el modo de pensar de un hacker mediante cursos que enseñan cómo escribir o codificar virus de computadoras y otros programas maliciosos, para así en un futuro estos estén a la defensa de cualquier vulnerabilidad y que estas prácticas le sirvan para su vida personal, aunque muchas empresas se cuestionan de que si verdaderamente los estudiantes toman estos conocimientos en bien común ayudando a las empresas a prevenir, o por el contrario realizar diferentes actos delictivos perjudicando a una persona u organización, como se evidencia en un anuncio publicado por wordpress.com, “ Un instructor asegura que si los estudiantes pueden evadir fácilmente un programa de antivirus, entonces eso demuestra que el producto es deficiente. ¿Existe algún beneficio al enseñar a los estudiantes cómo hacer “hacking”?. Los que proponen tales cursos reclaman que estas destrezas de “hacking” permitirán a la próxima generación de expertos en seguridad a pensar como hackers maliciosos, ayudando así a detener la propagación de

“malware”.”[164], además de estas preguntas generadas se puede despejar muchas más como en el mismo anuncio lo específica “¿Deberían las universidades enseñar sobre hacking? Sí o No y porqué. ¿Deberían las compañías contratar personas adiestradas en la creación de malware y en hacking? Sí o No y porqué. ¿Qué precauciones deben tomar estas instituciones educativas si planifican ofrecer dichos cursos? ¿Quién debería ser el responsable en el caso de un estudiante que propague malware? ¿Por qué?”[165].

Se preguntó ¿si los profesores en su vida laboral o de consejo de amigo ha explicado en algún momento a la comunidad académica sobre paginas o software que permitan acceder a sistemas sin permiso, con el fin de enseñar cómo funcionan, para esta pregunta se obtuvo respuestas que el 90% de los encuestados respondió que no lo haría y el 10% de los profesores respondió que quizás enseñaría estas técnicas a sus estudiantes sobre software pirata o paginas para que estos vulneraran un sistema, como se ve en la Imagen 23.

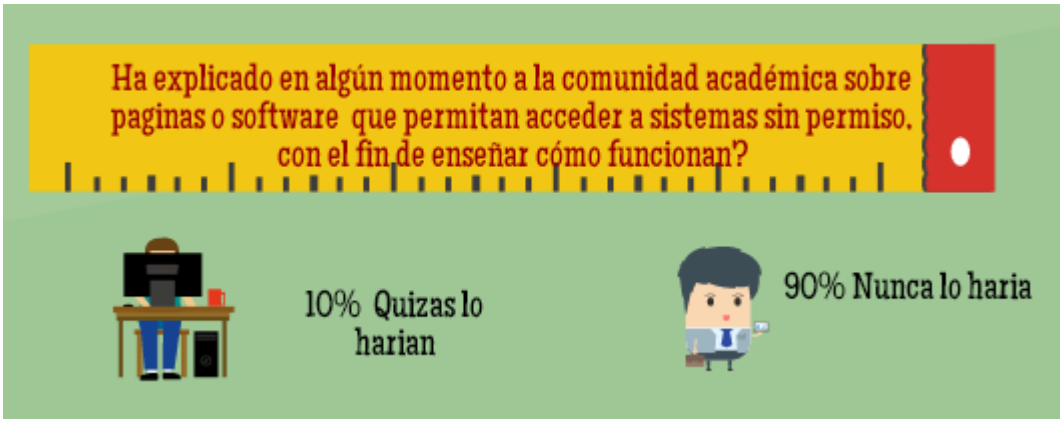


Imagen 23

Aun así se ve casos en donde los profesores por ayudar a los estudiantes comenten actos piratas, sin tener en cuenta que esto puede ser una iniciativa para que los estudiantes siga ese camino, un caso particular ocurrió a un profesor de matemática, que “por beneficio a sus estudiantes enlazo a través de su web personal a copias "piratas" de respuestas que facilitaran el estudio a sus alumnos. Hay que aclarar que la página personal del profesor no tiene ningún fin comercial y tan sólo trata de ayudar a sus estudiantes en los estudios. El maestro fue

[164] *Mlarracuente. ¿Deberían Las Universidades E Instituciones Educativas Enseñar Sobre “Hacking”? {24 abril 2014 }{En línea}. Disponible en: https://mlarracuente.wordpress.com/2014/04/24/25-deberian-las-universidades-e-instituciones-educativas-ensenar-sobre-hacking/*

[165] *Ibíd.*

encontrado culpable de facilitar la infracción del copyright"[166], u otro caso, en donde los profesores son los causantes de piratería dentro de una institución académica alentando a los alumnos a seguir sus pasos, es cuando estos alteran los programas o es peor "cuando "profesores" de institutos o centros educativos en cualquier parte del mundo, cogen ordenadores que vienen con software libre, los borra o directamente hace un arranque dual, e instala software privativo pirata. Pues ya no solo está haciendo que la administración para la que trabaja sea responsable de piratería, sino que además, está condenado a futuros profesionales al yugo tecnológico y la ilegalidad, o lo que es peor, a pasar toda la vida por caja para pagar una licencia o derecho de uso de un programa que tiene su alternativa en software libre"[167], se ve como con cosas tan mínimas se puede llegar a influir en la vida profesional de una persona, que ya en un futuro por estar ahorrando dinero y por otro lado ganando hace instalaciones piratas, ocasionando vulnerabilidades y jugando con la seguridad de una empresa con sus datos o la seguridad de una persona del común.

Otra pregunta que se formulo es que si ha enseñado a los estudiantes a encontrar vulnerabilidades en un sistema, donde los resultados se observó, que los profesores en sus actividades académicas si lo han hecho, han dado sus conocimientos a los estudiantes para que encuentren vulnerabilidades, ya sean en casos reales o en un taller realizado durante la clase, esto se valida con el 50% de las respuestas, mientras el 50% de los profesores aseguran que nunca lo han hecho. Como se ve Imagen 24.

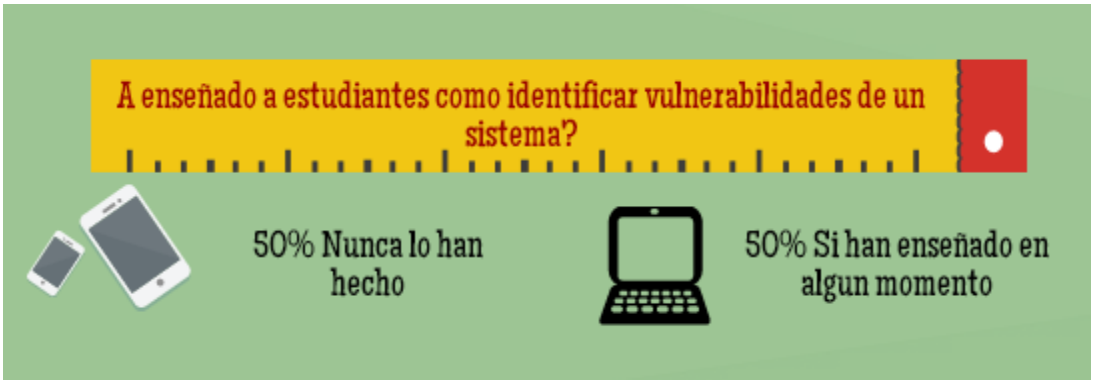


Imagen 24

[166] *Miguel Jorge. 20 minutos. Profesor de matemáticas condenado por enlazar a respuestas "piratas". {17 Enero 2013}{En línea}. Disponible en: http://www.20minutos.es/noticia/231176/0/multa/profesor/piratear/*

[167] *WordPress. Ramón. Software pirata en administraciones públicas, una completa irresponsabilidad. {30 enero 2014}{En línea}. Disponible en: http://ramonramon.org/blog/2014/01/30/software-pirata-instituciones-publicas/*

Existen artículos sobre el tema de aprender a hackear se puede ver este que solo con el título nos referencia todo “YouTube se enfrenta a los videos que enseñan a hackear”[168] El articulo nos habla de cómo YouTube se enfrenta a los videos subidos por personas con conocimiento de hacker para enseñar a los demás a cómo hacerlo. Dice que ahora es tan sencillo saber cómo hackear nos habla de un grupo específico, el cual sus videos fueron estudiados y comprobados que si enseñaban a los usuarios al hacking, en este caso los videos enseñaban a entrar a cámaras web y a computadoras ajenas. El artículo nos especifica que “tuvo 37,000 vistas antes de ser eliminados. Este tipo de contenido, frecuentemente acompañado por música, muestra paso a paso las instrucciones para lo que se conoce como "esclavizar" a las víctimas. Ellos toman sus computadoras, encienden sus cámaras y en algunas ocasiones interactúan con ellos.”[169]

Esto se realiza entrando a los computadores de las personas de forma remota, instalando un virus, enseñan desde como descargar el programa, como ser instalado y cómo manejarlo. Es por ello que estos sitios vuelven cada vez más fácil la forma de aprender a jóvenes que quieren entender y vivir más de cerca el delito informático. Muchos de estos tutoriales son colocados por personas que han aprendido del tema que hacen de esto una forma lucrativa.

Otro de los cuestionamientos que se quiso validar fue si un profesor en sus clases por enseñar a sus estudiantes ha realizado algún tipo de vulneración o de ataques a sistemas, como lo podría ejecutar un delincuente informático, con esta pregunta se validó que el 80% de los profesores no han realizado estas pruebas durante sus clases o delante de sus estudiantes y un 20% de los encuestados si han realizado estos actos durante su clase, muchos de ellos por mostrarle como es que los hacker vulneran sistemas tan fáciles , ya que si un docente puede realizar estos actos, una persona que se enfoca hacer daño, puede realizarlo sin ningún inconveniente realizando muchas vulnerabilidades en poco tiempo y si ya es de gran magnitud lo pueden hacer sin ningún problema o muchos docentes lo hacen como se menciona en el blog de conektioblog sobre cuatro metáforas para representar el rol del profesor en las nuevas tendencias de aprendizaje “El nuevo rol del educador consiste en empoderar al grupo y a cada uno de los alumnos para que ellos sean los protagonista de su propio proceso de aprendizaje. El coaching

[168] *Segall Laurie, YouTube se enfrenta a los videos que enseñan a hackear. {31 Julio 2015}{En línea}. Disponible en: http://www.cnnexpansion.com/tecnologia/2015/07/30/youtube-se-enfrenta-a-los-videos-que-ensenan-a-hackear*
[169] *Ibíd.*

aporta habilidades y herramientas para fomentar la motivación, la comunicación y la colaboración"[170], en la Imagen 25, se muestra las respuestas a esta pregunta:

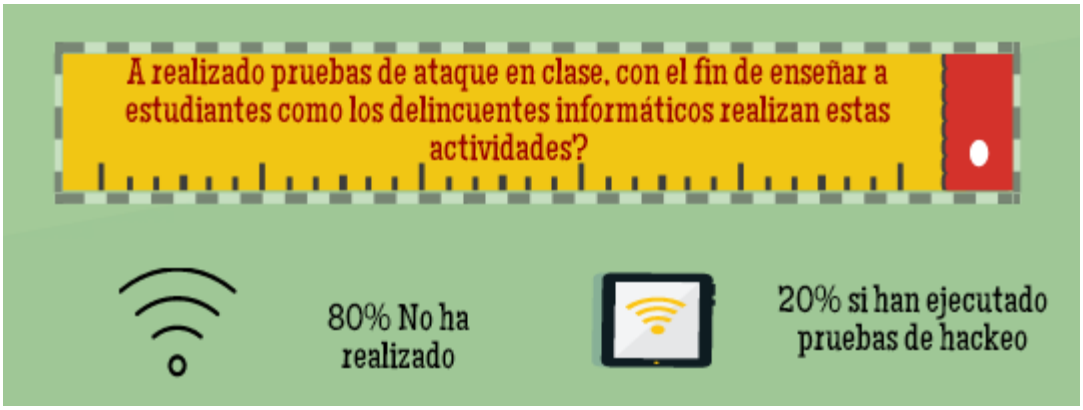


Imagen 25

Con toda la información obtenida para realizar la validación si los docentes influyen para que un estudiante tenga iniciativas en participar en actividades relacionadas con la cultura hacker sin muchas veces darse cuenta, una de las preguntas formuladas para esta tendencia fue, que si los profesores ayudarían a un estudiante que quiera aprender a acceder a información a la cual él no tiene acceso, para esta pregunta se observó que el 80% de los encuestados respondieron que no lo harían y el 20% delos encuestados quizás lo harían o en su momento lo han realizado, se analiza que los profesores no estarían dispuestos a ayudar a los estudiantes para que se vallan por el lado de la delincuencia informática, como se ve en la ilustración 24.

[170] *Marlopduar. Los nuevos roles del profesor: hacker, DJ, coach y Community Manager. { 20 febrero 2014} {En línea}. Disponible en: http://conektioblog.com/2014/01/30/LOS-NUEVOS-ROLES-DEL-PROFESOR-HACKER-DJ-COACH-Y-COMMUNITY-MANAGER/*

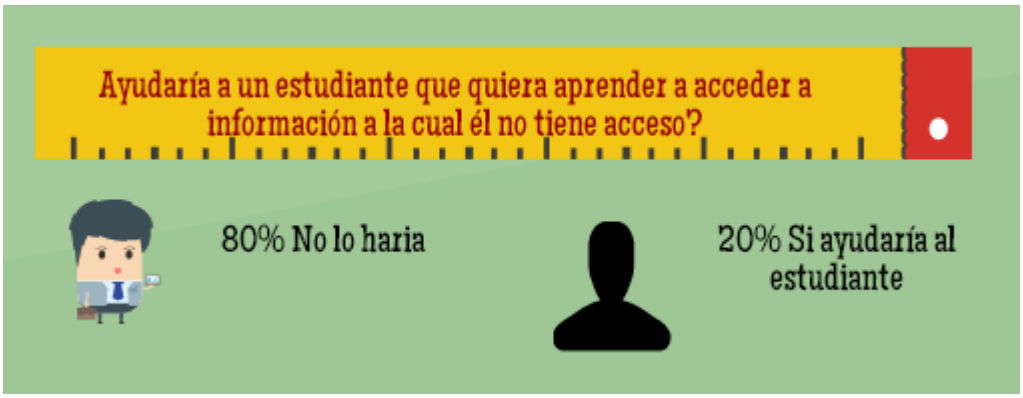


Ilustración 24

Para ilustrar mejor esta hipótesis que se quería validar al mirar si muchas veces los profesores o docentes de carreras como la Ingeniería de Sistema o afines realizan cátedras pensando en dar un conocimiento positivo a los estudiantes e imaginando que este conocimiento va a ser utilizado de la mejor forma. Pueden llegar a insistir o enseñar a estudiantes como aprender habilidades que no son bien utilizadas por dichos jóvenes.

Es por ello que el siguiente artículo nos habla como un evento que se realizó en ciudades de Colombia como Bogotá, Barranquilla y Medellín. Estas conferencias tienen el título de "Explotando vulnerabilidades con Metasploit Framework" (Federico Gacharná), "Wireless Hacking" (Nicolás Marciales), "Ingeniería Social" (Jeffrey Borbón), "Calling Mom and 5 more VoIP attacks" (Daniel Rodríguez y Giovanni Cruz) y la exposición de David Pereira, al cierre de la jornada"[171]

El artículo contaba como muchos de los conferencistas mostrabas los programas servían para vulnerar equipos remotos, programas que descifraban contraseñas, se realizó un laboratorio en donde se pudo observar como atacar las plataformas VoIP, suplantación y herramientas para detectar vulnerabilidades de inyección SQL, etc.

Es acá donde la pregunta que se quiso realizar con esta encuesta viene a la luz, que tan bueno es enseñar esto, si bien hablamos de una ética al tomar estos cursos, cuántos de los que asisten salen con buenas intenciones de lo aprendido.

Se observaron muchas noticias sobre el tema una de ellas y que causo mucha observación ya que un chico que se hacía llamar @R4lph_is_here y que tenía la autoría de ser el autor de más de 100 ataques a páginas web colombianas, el

[171] *Hotfixed. Hack x Colombia 2011. . { 12 Octubre 2011} {En línea}. Disponible en: http://hotfixed.net/hack-x-colombia-2011/*

error que cometió fue al atacar “la página con el objetivo de extorsionar por una boleta para poder asistir al evento y quizás para demostrar que era capaz de atacar incluso a los de su propia comunidad.”[172] Como lo dice el artículo muchas de las personas aprenden por su propio interés en la Internet que es capaz de enseñar y dar a conocer información de esta en. Es por ello que con todo esto se puedo observar como el conocimiento daño muchas veces es utilizado de mala formas.

Ya para la última pregunta de este grupo de validación, era indagar como el docente ve a aquellos estudiantes que amplían su conocimientos para encontrar vulnerabilidades en un sistema en donde el 30% no cree que este comportamiento sea algo positivo, mientras que el 70% de los docentes cree que esto si es un comportamiento positivo esto se puede observar en la Imagen 26.

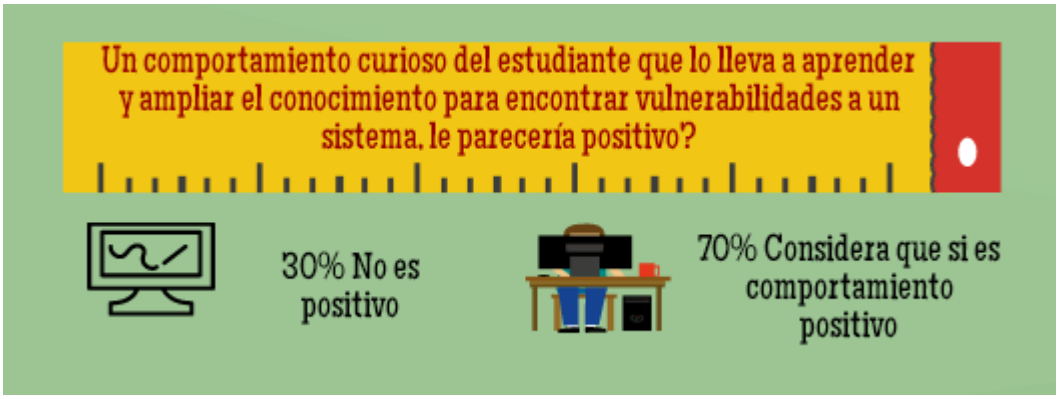


Imagen 26

La premisa para estos casos de hackeo es que para saber defenderse de los ataques de los criminales hay que saber también como ataquen dichos hacker. “Eduardo Arriols, fundador y uno de los responsables de HighSec, la plataforma creada por ellos para, según el propio creador, “que cualquier usuario sea capaz de aprender a atacar y a defenderse virtualmente”.[173] Estos jóvenes indagaron en las páginas de internet y se dieron cuenta que estos tutoriales empezaban de forma avanzada, lo que quisieron hacer es enseñar desde tutoriales básicos. Crearon “Un blog dentro de la web detalla lo que el usuario puede aprender mientras juega: desde hackear la wifi del vecino hasta cómo avanzar más rápido

[172] *Muchohacker.Tras la captura de un hacker Colombiano. { 13 Octubre 2014} {En línea}. Disponible en: http://muchohacker.com/tras-la-captura-de-un-hacker-colombiano/*

[173] Villa Marta. Seis universitarios de la Autónoma enseñan a hackear wifi mediante un juego. { 12 Febrero 2014} {En línea}:http://noticias.lainformacion.com/economia-negocios-y-finanzas/redes/seis-universitarios-de-la-autonoma-ensenan-a-hackear-wifi-mediante-un-juego_VxPGsaGZIFcedfRe1mpoj7/

en el juego de Facebook Farm Héroes, elaborado por los creadores del Candy Crush"[174]

Hay numeroso libros de hacker muy reconocidos que han enseñado sus técnicas de hackeo ético. Estos libros pueden ser comprados por internet y son distribuidos con mucha frecuencia, Muchos de ellos también para usuarios que quieren protegerse de los delincuentes informáticos

Y por último con el segundo grupo de preguntas se quería identificar aquellos profesores que estimulan a los estudiantes para que utilicen las habilidades de forma positiva, ver si se aclara que lo enseñado es para hacer un bien y no un mal a la comunidad, establecer parámetros de hasta donde le enseño a un estudiantes para que ese conocimiento enseñado no se vea utilizado de mala forma, para ello se indago ¿si los docentes han intentado guiar a los estudiantes que tienen habilidades para el ataque a sistemas informáticos, para que utilicen este conocimiento de forma positiva y no negativa?, el 40% de los docentes nunca ha intentado guiar a aquellos estudiantes de forma positiva, muestras que el 60% de los docentes si ha guiado a los estudiantes que ve con este potencial de conocimiento para que se inclinen de forma positiva y no utilicen esta habilidad negativamente esto se puede observar en la Imagen 27.

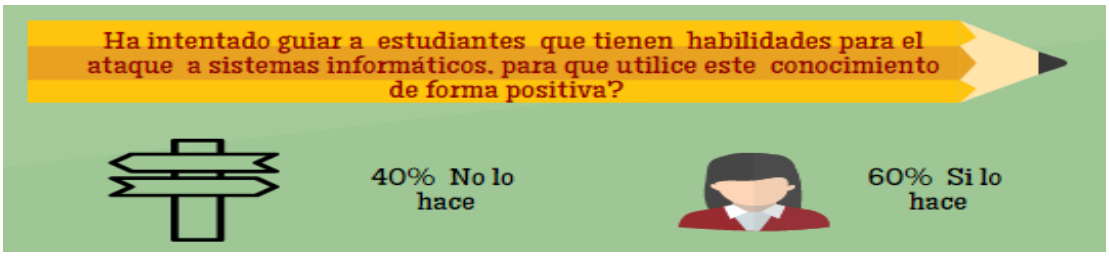


Imagen 27

Es así como muchos de los artículos también encontrados en internet nos hablan sobre el lado positivo del hacker ético y la importancia de ellos para las empresas ya que como lo dice el siguiente articulo el "El hacking ético es una herramienta de prevención y protección de datos. Lo que se pretende es estar constantemente adelante de aquellos que nos intentan agredir haciendo pruebas y ataques propios con la ayuda de los expertos informáticos, los cuales han sido entrenados en la

[174] Ibíd.

mentalidad delictiva de los piratas informáticos así como en las diferentes técnicas de ataque digital."[175]

Los hackers éticos realizan pruebas a los sistemas buscando vulnerabilidades de penetración del sistema, encontrar errores o configuraciones mal realizadas previamente, con todo esto buscar contrarrestar aquellos problemas encontrados y tomar medidas de protección al respecto.

El hacking negativo realizado por delincuentes informáticos cada día toma más importancia, es indispensable que la comunidad tanto los usuarios como las empresas, que manejan sus activos tengan presente que nadie esta excepto de esto y más cuando las empresas tienen atractivos vistos para los hacker, es por ello que es necesario la concientización y la responsabilidad de protección a los sistemas informáticos.

Por último se preguntó si los docentes toman como prevención con lo que enseñan y tratan de guiar por el buen camino del hacking ético se preguntó. Si el comportamiento de una comunidad o de un grupo de personas que tiende a vulnerar sistemas informáticos, con un beneficio propio, el docente lo considera como un grupo que tiene conocimientos que en alguna ocasión podrían ayudar para algún fin positivo. Con esta pregunta se quiso ver si aquellos docentes que se den cuenta de un grupo que se está desviando del hacker ético y está tomando unas actividades más dadas a un hacker negativo, en alguna ocasiones pueden ser educados éticamente para que este conocimiento se vuelva positivamente de manera legal y si el docente al detectar este grupo actuaria a enseñar los métodos positivos La respuesta de los docentes dejo evidenciar que el 40% está de acuerdo en que este grupo de personas podrían cambiar su pensamiento y guiarlos a que utilicen el conocimiento de forma positiva y ellos sean docentes que ayudarían a que esto pasara, mientras que el 60% respondió que este grupo de personas no tienen nada positivo que entregarle a la sociedad y creen que no van a cambiar el pensamiento de hacer daños a sistemas informáticos esto se puede ver en la Imagen 28.

[175] *Enter.co. EL HACKING ÉTICO Y SU IMPORTANCIA PARA LAS EMPRESAS. { 28 Febrero 2014} {En línea}:http://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/*

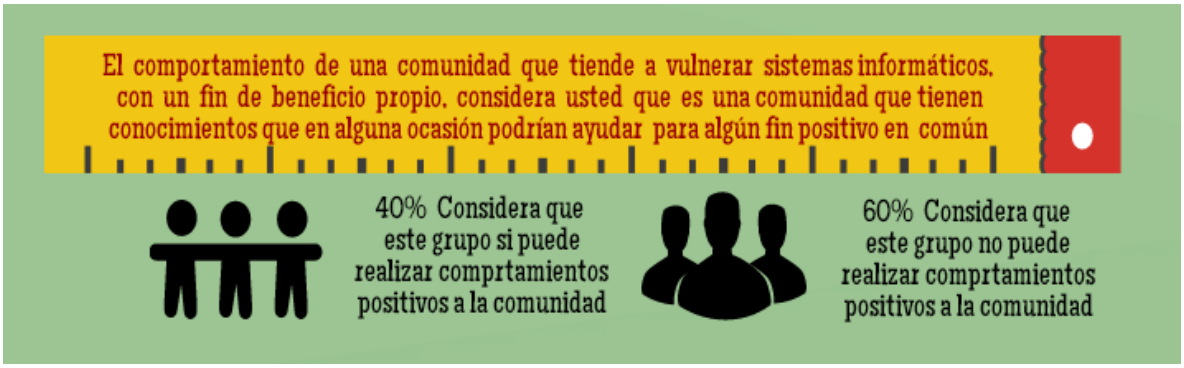


Imagen 28

Muchos de los hacker más famosos del mundo y que por mucho tiempo realizaron daños a empresas o personas, después de cumplir sus condenas con la ley, han sido contratados por multinacionales para que se vuelvan el agente de seguridad informática dentro de la organización, es así como el conocimiento que utilizaron de forma negativa por mucho tiempo ahora es utilizado de forma positiva.

Un ejemplo de ello es el hacker canario Deepak Daswani como lo dice este anuncio en el que el mismo expreso "Aunque puede quebrar la seguridad de sistemas informáticos, y pudo haber perjudicado a sus vecinos gorrones, Daswani utiliza sus conocimientos para hacer el bien. Es lo que se conoce como un 'hacker ético', un experto en ciberseguridad que pone su destreza al servicio de organismos públicos y empresas para descubrir puntos débiles en sus defensas digitales y desarrollar soluciones de seguridad "[176]

Otro caso encontrados fue el de "Alonso es un reputado hacker ético que capitanea un equipo de más de 100 informáticos, desarrollando productos de seguridad para empresas y particulares, como la aplicación gratuita Latch, que permite echar un pestillo extra a cuentas y servicios en línea, tales como la banca personal, por ejemplo."[177]

El hacker más famoso del mundo Kevin Mitnick, conocido por penetras sistemas muy protegidos como Nokia y Motorola en esas épocas y que hasta fue acusado de haber hackeando a otros hackers con éxito, Después de haber pagado la condena ahora se dedica como consultor y asesor de seguridad para diferentes compañías a través de la propia compañía que el creo llamada dedica a la

[176] *Mayo Cerqueiro Pablo, El confidencial, Hackers con principios. { 20 Junio 2015} {En línea}:http://www.elconfidencial.com/tecnologia/2015-06-20/hackers-eticos-ciberseguridad-hacking_893699/*
[177] *Ibíd.*

consultoría y el asesoramiento en materia de seguridad, a través de su compañía Mitnick Security.

Leonard Rose fue acusado de robar código fuente de empresas, se le acuso de distribuir programas de malware, trojan, etc. En la actualidad este hombre creo la lista de correo Full Disclousure utilizado en empresas para detallar vulnerabilidades, además de ello trabaja como expertos de seguridad en empresas.

Luego de analizar las encuestas realizadas a estudiantes e igualmente a docentes, se evidencio como el ámbito estudiantil en el que actualmente se desenvuelve el joven Colombiano, necesita un refuerzo más, para así guiar a estos jóvenes que en su vida diaria están en la navegación y búsqueda de información valiosa para su conocimiento, al dejarlos solos e indagar en la internet en donde pueden llegar a encontrar múltiples de respuesta muchas veces negativas deja un hueco en el que se puede llegar a inclinar por el lado negativo, por ello se debería tener un acompañamiento más para así que no se desvíen del buen actuar.

Se encontró dentro de la encuesta de profesores, respuestas que donde se evidencia que algunas veces el conocimiento se centra en darlo, sin en ocasiones verificar si es la forma correcta de enseñarlo, ya que ese conocimiento llega a jóvenes ansiosos de buscar y aprender cada vez más.

También dentro de la investigación se quiero validar como personas expertas en el tema ven estos conceptos en la vida real, si en verdad existen jóvenes que se están inclinando por el camino de la delincuencia informática, igualmente analizar si en verdad la sociedad afecta en estos casos sobre los estudiantes y como los profesionales ven el tema en Colombia referente a los casos de delitos informáticos mencionados durante la investigación y analizados en las encuestas realizadas.

Por ello se quiso realizar una entrevista a 2 profesionales en seguridad informática, uno de ellos es el ingeniero Álvaro Escobar docente en postgrado en la especialización de seguridad informática y Cesar Rodríguez ingeniero de seguridad, docente en la especialización de seguridad y trabaja como consultor de seguridad para las diversas empresas a nivel nacional, estas entrevistas se realizaron para tener un concepto más amplio del tema planteado durante la investigación, la cual se basó en 12 preguntas. Con un primer grupo de preguntas se quiso validar si los entrevistados están de acuerdo con que los delitos informáticos empiezan desde muy temprana edad, otro grupo de preguntas quería validar como estos expertos ve y analiza el estado de los delitos informáticos en

Colombia, para ver como los jóvenes se ven más afectados con dichos surgimientos y el último grupo de preguntas que se realizaron a los expertos validaban porque los delitos informáticos van en aumento en el país. Para ver las dos entrevistas completas: Entrevista Cesar Rodríguez (https://www.youtube.com/watch?v=A1itj1vjxfc&feature=youtu.be) Entrevista Álvaro Escobar (https://youtu.be/Ngidx2IWonk)

Una de las preguntas de las validaciones que se quería analizar con el conocimiento de los entrevistados al preguntar si consideran que los delitos informáticos son cometidos por jóvenes entre 12 y 18 años y si lo hacen para tener beneficios económicos, se evidencio que los profesionales están de acuerdo y opinan que una persona que pueda leer y escribir puede cometer estos actos, ya que todo se encuentra descrito en algún lado y es muy fácil de acceder a estas informaciones y por ello es que se comenten delitos, igualmente expresaron que muchas veces los jóvenes sin querer hacer daño alguno con sus conocimientos terminan haciéndolo, empiezan por explorar conocimiento, por jugar por quitar borrar y a lo último se dan cuenta que cometieron un delito y que perjudicaron alguna empresa, persona, etc., pero lo realizan sin conocer el que hicieron y que eso era un delito, además se concluyeron los entrevistados que los jóvenes muy poco lo hacen por dinero a sus edades lo que quieren es aprender y obtener reconocimiento, además también es importante para ellos ser admirados de las hazañas cometidas por medio de anónimos. Como se menciona en la página de delitos informáticos de como “Las TICs (tecnologías de la información y la comunicación) fueron un salto fundamental para que esta generación de jóvenes con claras tendencias narcisistas encontraran el amparo necesario para lograr difusión. Más que nunca aquello de los 15 minutos de fama estuvo tan cerca de ser real. YouTube, MySpace, Facebook, Tuenti. Fotologs, blogs. Cualquier red social es buena para comenzar a lograr la fama y el reconocimiento de los pares sin la filosofía del esfuerzo y con tal de obtener reconocimiento son capaces de realizar cualquier cosa, incluso delitos”[178], mientras el otro entrevistador piensa que está en otro rango de edades, desde los 16 a los 25 años para la actualidad, el considera que los hacker jóvenes eran de antes o de unos años más atrás, ya que hoy en día los que existe son grupos delictivos, son profesionales y que si un joven a temprana edad, hoy en día realiza estos actos de delincuencia informática, es porque es un joven solo y tiene demasiado tiempo para investigar y tomar el conocimiento para realizar un delito informático, otro aspecto para el entrevistador era que las influencias familiar afectan en las actuaciones de estos jóvenes

[178] *Cabezas López Carlos. Delitos informáticos. Neópatas, de la mitomanía al crimen. {10 noviembre 2008} {En línea}. Disponible en: http://www.delitosinformaticos.com/11/2008/noticias/neopatas-de-la-mitologia-al-crimen#*

igualmente que las malas influencias, se puede concluir con este entrevistador que en ocasiones las influencias sociales si están a cargo para que un joven estudiante se esté inclinando por el lado del hacker.

Los dos entrevistados concluyen que los jóvenes muy poco lo hacen por dinero a sus edades lo que quieren es aprender y obtener reconocimiento, además también es importante para ellos ser admirados de las hazañas y reconocidos por cada vez ser mejores en los grupos de cultura del Hacker.

Los entrevistados también opinaron que en la actualidad también se vive una tendencia a formar grupos delictivos de hackers, el rango de edad de estos grupos puede llegar a comenzar desde los 16 años a los 25 años de edad estos jóvenes ya, son profesionales, otro aspecto para el entrevistador era que las influencias familiar afectan en las actuaciones de estos jóvenes igualmente que las malas influencias, la independencias de las familias y el problema social que se vive ahora hace que pasen más tiempo en redes buscando dicho tipo de información es por ellos que dejaron evidenciar con esta respuesta que muchas veces las influencias sociales si están a cargo para que un joven estudiante se esté inclinando por el lado del hacker de sombrero negro o gris.

Otra de las preguntas de la misma validación anterior, era saber cuál era el delito informático más realizado en el país y si así mismo también era realizado por los jóvenes, buscando analizar si en verdad los delitos informáticos cada vez son más realizados por los jóvenes colombianos que atacan a empresas que se encuentran en el país o también se convierten en hackers internacionales, como fue encontrado en la investigación en la que no existen fronteras para estos delincuentes informáticos experimentados y cada vez buscan realizar actos de más dificultad y/o de mayor impacto; el problema de las leyes entre países y penalización de este tipo de delito deja que no sean muchas veces condenados si realizan sus actos dirigidos hacia fuera del país. Los entrevistaron concordaron estar de acuerdo y el delito más cometido en el país es la suplantación, ya que como se mencionó en la primera pregunta la facilidad de acceso que se tiene para ejecutar cualquier crimen es muy fácil, además por los medios los cuales se puede realizar este delito que a comparación de otros como la vulneración, son más complejos y la dificultad que se tiene para realizar es más alta, es así que es el delito cometido por los jóvenes como lo revelo el periódico el Tiempo en un artículo llamado “Aumentan casos de ciberdelitos contra menores en el país “Están disparados los robos de identidad digital (cuando le roban el perfil de Facebook, o una cuenta de correo, etc.), las amenazas, injurias y el 'grooming', en donde acosadores se hacen pasar por un niño o niña para engañar a menores de edad, a quienes luego invitan a intercambiar fotografías eróticas con las que

después los extorsionan", explica el coronel Freddy Bautista, director del Centro Cibernético de la Policía Nacional"[179].

Se analizó con este grupo de preguntas que los profesionales con sus conocimientos y experiencias en el tema, están de acuerdo que la gran mayoría los delitos informáticos son cometidos por jóvenes y que desde hace tiempo se viene con este acontecimiento y que cada día crece más, como también se evidencio con las encuestas realizadas a los docentes y estudiantes, los cuales se observaron que estos desde temprana edad realizan actos y que cada día quieren aprender más sobre el tema.

En la entrevista realizada a estos expertos que trabajan y se desempeñan la gran mayoría de su trabajo en el fortalecimiento del hacker ético en el país, como lo menciona Álvaro Escobar, para él "la comunidad hacker ética es la que ha tenido mayor aumento en la sociedad colombiana, y que el desarrollo de la política de seguridad de la información ha ido más encaminada a formar aquel profesional que cuente con conocimientos para detener ataques y detectar esos posibles huecos de seguridad, para él la formación actual está encaminada a fortalecer el hacker ético. De igual forma nos comenta como el hacker ético no existiría si no existe el delincuente informático. Observando este tema en comunicados y documentos analizados por expertos en el tema por ejemplo Gustavo Caraballo en su artículo nos menciona que "Colombia es blanco de delincuentes informáticos: el sector financiero, el comercio electrónico y la tecnología siguen presentando incrementos porcentuales en el número de víctimas."[180] El problema que muestra este articulo nos evidencia que no está muchas veces en la eficiencia de sistemas tecnológicos sino en la concientización de los funcionarios en las empresas o de las personas en su vida diaria, es por ellos que dice: "Los ladrones no sólo se valen de herramientas tecnológicas para robar claves y datos. Una de sus armas más usadas es el descuido, que se ha vuelto incontrolable para los responsables de seguridad informática de las entidades financieras."[181] Es por ello que nos explica que no solo es proteger una entidad con sistemas tecnológicos muy grandes ya que, los delincuentes tecnológicos en su mayoría ahora utilizan es la inocencia de sus víctimas.

---

[179] *García R José Carlos. Aumentan casos de ciberdelitos contra menores en el país. {10 Agosto 2015} {En línea}. Disponible en: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/internet-es-cada-vez-mas-peligroso-para-los-ninos/16207955*

[180] *Gustavo Caraballo. Descuido de los usuarios, el mayor aliado de los hackers. . {30 Agosto 2015} {En línea}. Disponible en: http://www.kienyke.com/economia/descuido-de-los-usuarios-el-mayor-aliado-de-los-hackers/*

[181] *Ibíd.*

No solo es importante tener expertos en seguridad informática que nos encuentren estos huecos en las empresas, sino la capacitación y concientización a los usuarios sobre la seguridad de la información y la importancia de ellos en todo el sistema de seguridad. Se estima que "42% de usuarios de Internet en Colombia han sido víctimas de delitos informáticos"[182].De igual manera para el ingeniero Cesar Rodríguez la comunidad colombiana es muy sana aun en estos temas y aun no considera que haya un número considerable de perdonas que se estén encaminando a ser delincuentes informáticos. El considera que ni siquiera los casos más sonados en Colombia sobre delincuencia hacker sean personas que se vean con mucho conocimiento del tema. Para el igual que la opinión del Ingeniero Álvaro estos delincuentes informáticos colombianos aún son muy inocentes a diferencia de los hacker de otros países. Aun en Colombia se ve más al delincuente informático realizando ataques solo a bancos y al sistema financiero con toda la clonación de tarjetas. Aunque es el sector más atacado en todo el mundo en Colombia la mayoría de ataques solo están inclinados a este sector y no se ve mucho la amplitud de conocimiento para atacar otro tipo de sectores.

Durante toda la investigación se ha hecho mucho énfasis en que la seguridad informática y la seguridad de la información son aspectos que se han vuelto muy importantes en la vida diaria, ya sea por el avance de la tecnología que es cada vez más grande, y que en todo el aspecto lo principal así se tengan todas las herramientas tecnológicas de protección es que las personas, empresas de den cuenta que todo comienza por la conciencia y de darse cuenta que es ahora importe proteger la información, si en la actualidad no se toma esa conciencia siguen habiendo empresas y personas que en la vida diaria no creen que esto es algo importante.

Álvaro Escobar en la entrevista planteaba como en la actualidad gran cantidad de empresas aun no dedican ni el 10% de dinero a la seguridad informática, el considera que aún falta mucha concientización del daño tan grande que se pueden sufrir. Un artículo que nos habla sobre las Pymes (microempresas Colombianas) en el sector de la seguridad informática nos explica como aun la seguridad de la información estaba basada en las grandes empresas y gobiernos, pero explica como "las Pymes se están convirtiendo en un blanco muy atractivo para los ladrones digitales, que están aprovechando la poca seguridad de estas empresas para adquirir secretos industriales y demorar los planes de la

[182] *Gustavo Caraballo. Descuido de los usuarios, el mayor aliado de los hackers. . {30 Agosto 2015} {En línea}. Disponible en: http://www.kienyke.com/economia/descuido-de-los-usuarios-el-mayor-aliado-de-los-hackers/*

competencia."[183]Las empresas en la actualidad aun no ven razones de invertir en seguridad informática, hasta que tienen que reaccionar ante un ataque. En Colombia las empresas prefieren reaccionar después de lo sucedido antes que prevenir, este estudio nos muestra que hasta la fecha "el 73% de las Pymes Colombianas sufrieron por lo menos un ataque informático"[184].El problema de estas empresas es que sus recursos son limitados, pero son el blanco más fácil de ataques informáticos para los delincuentes. En todo este estudio se evidencio como los jóvenes hacker que en la actualidad están comenzando a temprana edad y que lo que quieren es coger experiencia y métodos en los cuales no sean descubiertos, estas empresas por la poca seguridad que manejan son un punto focal fácil para estas persona que pueden cometer el delito informático de manera muy fácil, que es muy posible que no sean descubiertos así aun no tengan la experiencia para ocultar el delito de forma adecuada. Como lo indico el Ingeniero Cesar Rodríguez la concientización de la seguridad informática esta sectorizada en Colombia más a empresas financieras, y a nivel de personas esta conciencia e información sobre la seguridad informática es muy baja con tan solo tomar un ejemplo de la utilización de claves en la vida diaria, ya sea para cuentas, redes sociales, correo o documentación importante que ahora se aloja en la nube.

Para evaluar la perspectiva de estas dos personas entrevistadas y que además de trabajar en seguridad informática y han desempeñado actividades como docentes de especializaciones y que tienen contacto muy a menudo con jóvenes que a diario indagan sobre estos temas, se preguntó si quizás han tenido el caso en el que un estudiante tanto de pregrado como de la especialización de seguridad informática haya utilizado el conocimiento aprendido para quizás utilizarlo de una forma inadecuada. Los dos expertos en el tema concuerda en el que hasta el momento no han conocido un caso en concreto, pero si muchas veces son personas que a nivel personal utilizan ese conocimiento para obtener información que requieren en su vida personal, no consideran que sean personas que lo utilicen para realizar daño a empresas muy grandes, opinan que este conocimiento aprendido si lo utilizan como consultores a empresas de seguridad y en la vida laborar tienen un carácter muy ético. Pero que dado el conocimiento adquirido en ámbitos que no les parece tan graves utilizan para tener información lo cual también se considera un delito informático.

---

[183] Santos Mateo. LOS RETOS DE SEGURIDAD PARA LAS PYMES. {13 Julio 2013} {En línea}. http://www.enter.co/especiales/enterprise/los-retos-de-seguridad-para-las-pymes/

[184] Santos Mateo. LOS RETOS DE SEGURIDAD PARA LAS PYMES. {13 Julio 2013} {En línea}. http://www.enter.co/especiales/enterprise/los-retos-de-seguridad-para-las-pymes/

Se ve en jóvenes de pregrado mucho la inquietud y el preguntar por aspectos que ya son más avanzados, o el querer saber cómo funciona dicha herramienta o como usarla. Esto concuerda con muchos artículos y con la encuesta realizada a los jóvenes que si el morbo por saber es grande, que muchos de ellos si han tratado de entrar de forma inadecuada a las cuentas personales de otras personas y que si han dedicado tiempo a buscar cómo realizar actos que aunque no consideran delito informático, porque es muy difícil de judicializar o que la persona reporte la animalidad si es un delito informático.

Para el segundo grupo de peguntas con el cual se quería validar como va los delitos informáticos en Colombia, para ver como los jóvenes se ven más afectados con dichos surgimientos, para esto se realizó una pregunta si se creía que en la sociedad colombiana ha aumentado la conciencia de seguridad informática y si los entrevistados nos podían dar un porcentaje de cómo cree que ha aumentado, se observó referente a la pregunta, que si se ha aumentado la conciencia respecto a la seguridad informática, ya que cada día se ve como los ataques por los hacker son más dañinos, ya que estos evolucionan por las nuevas tecnologías que se crean, llevando esto a que la gente sea más consiente al momento de crear una cuenta con su respectiva contraseña, con correos extraños o simplemente con la conversación por medio de una red social con un desconocido, llevando esto que la conciencia de la seguridad informática evolucione para crear antivirus o programas que bloquen dichos ataques, aunque para ello como se menciona en un artículo de nakedsecurity “Así que parece que la conciencia está aumentando, pero todavía tenemos un largo camino por recorrer antes de que podamos reclamar ningún tipo de victoria decisiva”[185]. Para poder generar conciencia en las personas, empresas u organizaciones lo importante es comenzar a crear conciencia en las personas que desarrollan las nuevas tecnologías que crean innovación igualmente en los estamentos de decisión, acerca de la necesidad de formalizar acciones de contención y gestión de la información, que hagan que las tecnologías de la información y la comunicación cumplan con el rol fundamental que hoy tienen en la empresa, en ser más veraz y confiable y que cumplan con la alineación de cada negocio, o como se observó en un artículo de política digital donde mencionan una encuesta realizada por “Joint Future Systems llevó a cabo el tercer Estudio de Percepción sobre Seguridad en Informática, que muestra las principales medidas para enfrentar los retos de seguridad en informática que son

[185] *Mark Stockley. Acaso la seguridad informática conseguir mejor o peor en el 2014? Usted tiene la palabra. {18 diciembre 14} {En línea}. Disponible en: https://nakedsecurity.sophos.com/es/2014/12/18/did-computer-security-get-better-or-worse-in-2014-have-your-say/*

los antivirus, firewalls y medidas de identificación de usuarios, como se visualiza en la imagen

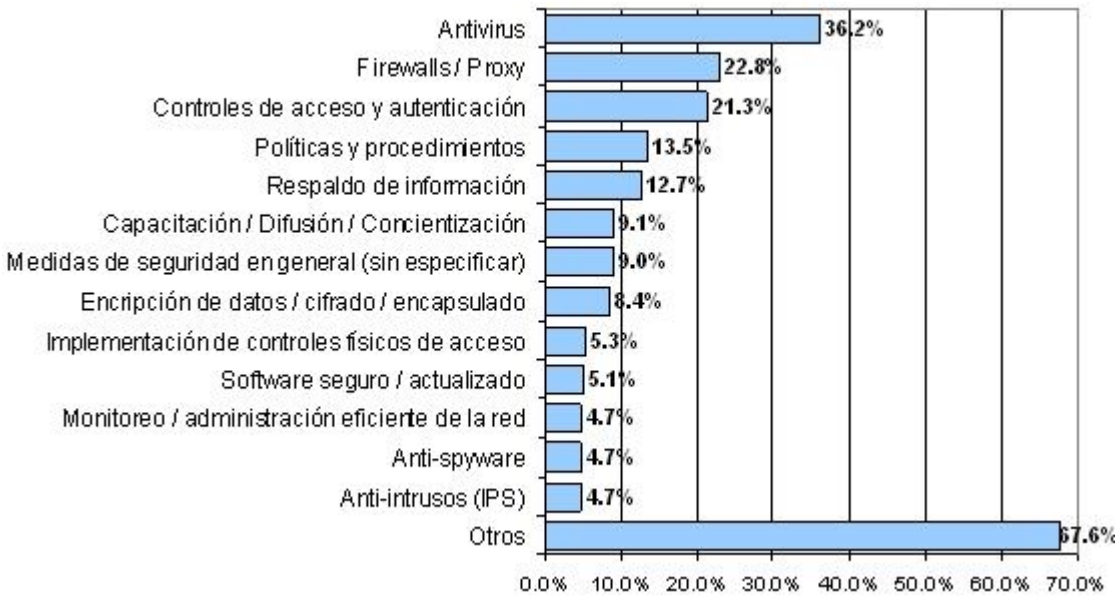


Ilustración 26 principales medidas para enfrentar los retos de seguridad en informática que son los antivirus, firewalls y medidas de identificación de usuarios,

Otras de las preguntas realizada durante la entrevista, en donde se quería validar como los delitos informáticos se desarrollan en Colombia y como estos delitos y sus surgimientos afectan en los jóvenes, era identificar si los delitos informáticos en Colombia son perseguidos por la ley como debería ser o por el contrario cada día se ven mejores castigos para estos crímenes, para ellos se observó que las respuestas de los entrevistados fueron similares en afirmar que el estado tiene la preocupación de enfrentar a los hacker, que existen leyes que persiguen a los delitos informáticos y que hay muy buenas herramientas tanto nivel fiscalía como policía para enfrentar los delitos, pero actualmente no son perseguidos como debería ser, aunque existen leyes, están van muy atrás de lo que debería, como se mencionó en la pregunta anterior falta de conciencia en las personas en que puede denunciar y que hay formas de hacerlo, que aunque no son procesos rápidos de solucionarlos pero que aun así se pueden denunciar, de acuerdo a las respuestas de los entrevistados se puede afirmar con un artículo de la patria.com donde destaca que Colombia es el primer país que penaliza los delitos con la Ley 1237 de 2009, pero que aun así los jueces no saben cómo penalizarlo y se evidencia en lo escrito del artículo “Lo raro es que a mis talleres no asistieron abogados, jueces o personas que deben conocer cómo funciona la Ley en estos

casos, pues aún en nuestro país muchos no saben cómo juzgar un delito de estas características"[186].

Otra de las preguntas de como los delitos van en aumento en nuestros país, otra de las preguntas que se realizo era saber si los medios de comunicación no dan relevancia a los delitos informáticos más allá de los que son más conocidos como Andrómeda o el caso Sepúlveda, para ello se observó en las respuestas de los entrevistados que uno de ellos considera que si dan más relevancia a los casos que le den más rating al medio comunicativo, como el caso Andrómeda, las clonaciones de tarjetas o redes sociales de los hijos de los expresidentes, a las divulgaciones de información de los famosos, entre otras vulneraciones realizadas a los altos mandatarios, mientras otra respuesta considera que no se debe dar mucha divulgación a estos delitos, que existe muchos problemas en el país para que todos los días divulguen que se arrestó a un hacker y que eso será darles reconocimientos a estos personajes y que muchos quieran seguir este camino dándoles un impulso más a personas jóvenes. Como se observa en la imagen los medios que más relevancia le dan a los delitos informáticos "son los medios impresos.

Ilustración 27 Figuran 11 medios que más relevancia le dan a los delitos informáticos

"[187]

[186] Martínez John Jairo. Colombia, el primer país que penaliza los delitos informáticos. {30 marzo 2012} {En línea}. Disponible en: http://www.lapatria.com/tecnologia/colombia-el-primer-pais-que-penaliza-los-delitos-informaticos-1980?qt-lo_m_s10=0

[187] Veloza Carolina. Conozca las dos nuevas modalidades de delitos informáticos. {01 octubre 2013} {En línea}. Disponible en: http://colombia.mmi-e.com/blog/category/sector/tic/c%C3%B3nozca-las-dos-nuevas-modalidades-de-d%C3%A9litos-inform%C3%A1ticos

Como se observa la república es el medio que más ha registrados noticias sobre el delito informático en el país.

Para concluir con la entrevista realizada a los 2 profesionales, y el último grupo de preguntas que se realizaron a los expertos se quiso validar porque los delitos informáticos van en aumento en el país, para esto se realizó una pregunta muy básica, la cual se basó en saber cuál es la razón por la cual los delitos informáticos en Colombia han ido en aumento durante los últimos años, donde se observó que los entrevistados tenían puntos semejantes en la respuesta, concluyendo, que hoy en día hay más gente conectada tantos en las redes sociales como en los medios tecnológicos, existe más información publicada, la reducción de procesos con apoyo de sistemas automatizados, existen más direcciones IP, transacciones electrónicas y la facilidad de acceso a las herramientas para cometer estos delitos informáticos, ya que cualquier persona puede leerlas, conocerlas y practicarlas y así realizar más actos que causan daño y así existen otras muchas causas por las cual los delitos van en aumento y es así mismo que los delitos informáticos van pasando en mayor aumento y con mayor facilidad a este mundo, ya que los delincuentes ven más oportunidades de accesibilidad a las miles de vulnerabilidades que existen por medios de todos los actos que las personas comenten día a día, además se puede contribuir con la respuesta que dan en el periódico el universal, donde expresan “Acceder a bases de datos de bancos o diferentes entidades, sin permiso, sustraer archivos de computadores, ingresar a redes sociales y correos ajenos y clonar tarjetas bancarias, son algunas de las modalidades de delitos informáticos que se presentan en el país y que según expertos de la Fiscalía van en aumento”[188], por esto que el mayor problema para que los delitos informáticos vayan en aumento es que todo parte de descuidos de las víctimas, ya que toman precauciones en sus actos y el mayor problema son las grandes estructuras delincuenciales que hay alrededor de este tipo de hechos.

Otra de las preguntas realizadas durante la entrevista, para validar porque los delitos informáticos van en aumento en nuestro país, era saber si el mayor problema que se encuentra en las víctimas de delitos informática es la no denuncia de los mismos y esto hace que aumente los delitos informáticos o si caso contrario a este, cual creía que era la causa, para esta pregunta las respuestas de los entrevistados fueron similares, y se concluyó que si es la falta de la no denuncia de los actos delictivos que como persona le cometen, la única manera de hacer la denuncia o que tome importancia el asunto es cuando un delitos se vuelve escándalo nacional, es allí cuando se toma conciencia, pero

[188] *Colprensa. El Universal. Fiscalía advierte aumento de delitos informáticos en Colombia. {23 diciembre 2013} {en línea}. Disponible en: http://www.eluniversal.com.co/cartagena/nacional/fiscalia-advierte-aumento-de-delitos-informaticos-en-colombia-102898*

cuando se clonan una tarjeta la persona solo hace el denuncio a la entidad bancaria sin llevar el proceso más lejos, en algunos casos no vuelven a preguntar o indagarse que paso con el caso, además no realizan una denuncia en la fiscalía para así tener el control de todos los actos delictivos y que lleven un seguimiento de los proceso denunciados, otro de los temas para que los delitos no sean denunciados y así mismo vallan en aumento, es la falta de campañas de todos los medios y grupos que ahí ante los delitos informáticos, solo re realizan en grupos cerrados y así mismo en sitios cerrados, mucha gente no tiene conocimiento que en la sijin, fiscalía se cuenta con personas especializados en estos temas y que se crean grupos para hacer seguimiento a los delincuentes, además de la gente no conocer, en Colombia no existen fiscales que tengan conocimiento sobre estos temas como lo dice Andrés Guzmán en un artículo de Colombia digital :"En Colombia no existen fiscales ni jueces especializados en delitos informáticos. Si a un ciudadano le roban el carro puede dirigirse a una Fiscalía especializada en Automotores, pero si a esa misma persona la roban en Internet debe dirigirse a un fiscal que en la mañana, por ejemplo, llevó un caso por inasistencia alimentaria"[189], se evidencio con las respuestas de los entrevistados que la no denuncia es el mayor problema que se tiene referente a los delitos informáticos y es por ellos que estos cada vez van en aumento en nuestro país, sin embargo, como se menciona en el mismo artículo de Colombia digital " los expertos en el tema coinciden en que la tecnología va mucho más rápido que la legislación. En ese sentido, mientras se crean normas para atacar este tipo de delitos, surgen nuevas tecnologías para burlarlas y los criminales se aprovechan de esta situación"[190]

También para este último grupo de preguntas de porque los delitos informáticos van en aumento, una pregunta que se realizó a los expertos durante la entrevista se basó en saber que comparaciones tendrían ante el daño que realiza los hackers de otros países a los daños que realizan los hackers Colombianos, los delincuentes informáticos en Colombia son muy principiantes, hasta hora están empezando en el tema, es por ello que la gran mayoría se ha llegado al paradero de estas personas, además todos los sistemas, virus, etc., que utilizan los hacker que están en Colombia son de otros países, aunque las técnicas que se realizan para vulnerar son las mismas a nivel mundial, la mayoría de sistemas son creados por hacker extranjeros, no se ha escuchado de colombianos que innoven en este tema, por ello se observa que las comparaciones de estos dos hacker colombiano y extranjero es muy grande, en cuanto a conocimiento y agilidad para realizar

[189] *Garcia Pérez Camilo. ¿En Colombia se investigan los delitos informáticos? {01 mayo 2013} {En línea}. Disponible en: http://colombiadigital.net/actualidad/articulos-informativos/item/4810-en-colombia-se-investigan-los-delitos-informaticos.html*

[190] *Garcia Pérez Camilo. ¿En Colombia se investigan los delitos informáticos? {01 mayo 2013} {En línea}. Disponible en: http://colombiadigital.net/actualidad/articulos-informativos/item/4810-en-colombia-se-investigan-los-delitos-informaticos.html*

delitos informáticos, el extranjero está por encima del colombiano ya que son creadores propios de sistemas mientras que los colombianos lo que hacen es utilizar estos medios para lograr sus metas.

A la culminación de la entrevista realizada a los dos profesionales, se realizó una pregunta para validar porque los delitos van en aumento en Colombia, la cual se basó en saber cuál es el manejo para los delitos informáticos que son realizados por delincuentes informáticos que provienen de otros países, pero que sus actos están apuntando a entidades Colombianas, se evidencio en las respuestas que los entrevistados llegaban al punto que aunque los derechos informáticos a nivel internacional son los mismos, no hay acuerdos internacionales para judicializar a los perpetradores, a menos que el delito cometido por estas personas halla perjudicado a grandes empresas, varias naciones o cuando la información vulnerada perjudique a un personaje de alto nivel, es allí cuando se toman las casos enserio y cuando existen penas para estas personas haciendo convenios diferentes países para llegar a las personas que cometen estos delitos informáticos, de lo contrario en muchos países existen paraísos fiscales, en donde si una persona llega a cometer un delito a un país, pero esta se encuentra en un territorio donde no existe estas penas, ni judicializaciones simplemente no realiza ningún acto contra el hacker.

Con esto se validó porque los delitos informáticos van en aumento en el país, se observó que es la falta de conciencia en la gente referente a los problemas que estos trae, la falta de divulgación de los medios que hay para denunciar, la falta de conocimiento que tienen los jueces y abogados para tratar los procesos de delitos, también se observó la influencia que tienen los hacker de otros países para tomar enseñanza de eso y seguir cometiendo las vulneraciones y por último se concluyó con los entrevistados que cualquier persona que pueda leer y escribir puede ejecutar un ataque informático siendo estos cada vez más fácil y al mismo tiempo difícil para las personas que controlan estos procesos, así que si las leyes en el país avanzan para controlar los ataques, las tecnologías y los hacker avanzan el doble para burlarlas

7 Conclusiones:

Luego de realizar la investigación, con sus respectivas entrevistas, las encuestas realizadas tanto a los docentes como a los estudiantes de las diferentes carreras, con las entrevistas realizadas a los profesionales, se obtuvo un conocimiento más profundo sobre el tema a investigar, se conocieron muchos casos en Colombia, que la mayoría de personas en el país no saben que existen o por el contrario no saben que estos tipos de delitos se comenten en el país, además de la falta de conciencia que hay a nivel nacional para tomar estos casos de delitos informáticos y la preparación de personas de la fiscalía para que penalicen estos actos, ya que en la mayoría lo toman como delitos informáticos en general sin saber, que hay unos que pesan más que otro.

Se encontró dentro de las encuesta de profesores respuestas que permiten evidenciar que algunas veces el conocimiento además de transmitirlo debe dar importancia al finalidad de ese aprendizaje, en especial para aquellos que pueden utilizarse para fines negativos o delictivos. También se observó que las respuestas obtenidas por algunos profesores resultaron ambiguas y aunque se pudo establecer una inclinación a la enseñanza o conocimiento que trasmiten, se pudo observar una contradicción en las afirmaciones dadas. Por Ejemplo aceptaron que utilizaban “software pirata” en sus clases o que daban ejemplos para explotar vulnerabilidades a sistemas informáticos no necesariamente con fines académicos y así mismo consideraban que conocer técnicas de vulneración no debía ser considerado como un talento académico, al menos que fueran empleados al servicio de la seguridad informática.

Otro de los temas que se pudo observar durante la investigación es que los estudiantes si tienen una gran inclinación a vulnerar sistemas, especialmente en los primeros semestres donde se concentran las mayores intensiones de experimentar, estos casos de hackeo, ya sea desde lo más mínimo para así llegar en un futuro a realizar a gran magnitud daños informáticos y ya en casos de semestres superiores, los estudiantes vulneran sistemas para un fin personal, para terceros, para poner en prueba su conocimiento y demostrar que puede realizar actos delictivos sobre vulneración o ya en casos extremos por dinero, dando esto así que los jóvenes colombianos si tienen un pensamiento de hacker, dado desde el universo en estudio, en este caso la comunidad estudiantes de pregrado y postgrado, más los docentes de la universidad piloto de Colombia que los incitan y los llevan a irse por este camino, tanto por docentes que les enseñan o por personas exteriores que los contratan para efectuar delitos informáticos, desde la universidad.

Las respuestas dejaron observar como muchos de los jóvenes que estudian éstas carreras ya entran con conocimiento propios de la cultura del hacking, muchas veces este conocimiento es fortalecido por el entorno de aprendizaje, de forma indirecta o directa. También se pudo concluir como el mundo en el que la tecnología cada vez avanza más, estos jóvenes son capaces de obtener conocimientos de distintas fuentes sin un control adecuado en su utilización por parte del entorno académico.

Además se evidencio con las entrevistas como en actualidad gran cantidad de empresas aun no dedican ni el 10% de dinero a la seguridad informática, se concluye que aún falta mucha concientización del gran daño grande que se pueden sufrir si no se toma medidas para garantizar la seguridad, y como el delito más cometido en el país es la suplantación, por la facilidad de acceso que se tiene para ejecutar cualquier crimen, además por los medios los cuales se pueden realizar este delito que a comparación de otros como la vulneración, son más complejos y la dificultad que se tiene para realizar es más alta. Las respuestas de los expertos, también se puso evidenciar en las encuestas realizadas a los estudiantes donde jóvenes de edades tempranas respondieron positivamente a preguntas de buscar, realizar o haber suplantado su identidad en algunas páginas.

De igual forma se observó que muchos jóvenes de pregrado indagan en gran medida por aspectos avanzados de la cultura hacker no necesariamente con la finalidad explícita de cometer delitos informáticos, pero muchas veces realizándolos por el desconocimiento de aspectos jurídicos, nacionales o internacionales.

8 Trabajos futuros:

Como trabajos futuros se puede contemplar este estudio ampliando el universo a otras universidades que validen el resultado que se dio en los jóvenes encuestados de la Universidad Piloto de Colombia y así mismo validar si los niveles socio-económicos de las universidades influyan en los estudiantes en aprender las actividades de la cultura hacker. Igualmente se podrían realizar encuestas virtuales en donde puedan contestar jóvenes que se encuentran en otros países de la región y que pertenecen al mismo rango de edades, pudiendo realizar una comparación internacional generando una visión más amplia de este tema que cada vez se hace más importante

9 Bibliografía

- *LIZAMA, Jorge Alberto. Hackers En El Contexto De La Sociedad De La Información. México. 2005. 81P.*
- *RAYMOND Eric S. Breve historia de la cultura hacker {En línea}. {25 septiembre de 2014}. Disponible en: (http://biblioweb.sindominio.net/telematica/historia-cultura-hacker.html).*
- *LIZAMA, op. Cit, p.79*
- *Hacker en la red, Noticias y Educación sobre seguridad de la informática. {En línea} {30 septiembre de 2014}. Disponible en: (https://hackersenlared.wordpress.com/category/capacitacion/tipos-de-hackers/).*
- *Wikipedia. Hacker (Seguridad Informática). {En línea} {30 septiembre de 2014}. Disponible en: (http://es.wikipedia.org/wiki/Hacker_(seguridad_inform%C3%A1tica)*
- *Moreno David. Hacker en Colombia. Hacker {En línea}. {Agosto 10 2011}. Disponible en: (http://www.dragonjar.org/hackers-en-colombia.xhtml).*
- *Nullvalue, El Tiempo, Doce Secretos del Robo de US$ 13.5 Millones {En línea}. {9 enero de 2015}. Disponible en: (http://www.eltiempo.com/archivo/documento-2013/MAM-140569#).*
- *Colprensa, El País, En Colombia las Cifras de Delitos Informáticos Van en Aumento Millones {En línea}. {9 enero de 2015}. Disponible en: (http://www.elpais.com.co/elpais/judicial/noticias/colombia-cifras-delitos-informaticos-van-aumento).*
- *RCN La Radio, Escuche el Informe Sobre Los Delitos Informáticos en Colombia Millones {En línea}. {9 enero de 2015}. Disponible en: (http://www.rcnradio.com/audios/escuche-el-informe-sobre-los-delitos-informaticos-en-colombia-28011).*
- *El Tiempo, Expertos en Delitos Informáticos Llegaron a Puerto Asis Para Investigar Amenazas por Red Social, {En línea}. {13 enero de 2015}. Disponible en: (http://www.eltiempo.com/archivo/documento-2013/CMS-7876787#).*
- *El Tiempo, Así roba en Colombia el 'ciberhampa' europeo {En línea}. {18 enero de 2015}. Disponible en: (http://www.eltiempo.com/politica/justicia/delitos-informaticos-en-el-pais-habla-director-del-centro-cibernetico-de-la-dijin/14841739#).*
- *Caracol Radio, Tecnología, La Empresas Colombianas También son Vulnerables ante Delitos Informáticos, {En línea}. {13 enero de 2015}. Disponible en: (http://www.caracol.com.co/noticias/tecnologia/las-empresas-*

colombianas-tambien-son--vulnerables-ante-delitos-informaticos/20120523/nota/1693112.aspx#).

- La F.M, Radio, Conozca el Perfil del Cibercriminal Colombiano *{En línea}. {13 enero de 2015}. Disponible en: (http://www.lafm.com.co/noticias/conozca-el-perfil-del-141939#).*
- *El tiempo. Edgar. Tecnosfera, colombiano de quince años crea escuela para aprender a 'hackear'. {En línea}. {Enero 4 2015}. Disponible en: (http://www.eltiempo.com/tecnosfera/novedades-tecnologia/como-hackear-colombiano-de-quince-anos-crea-escuela-para-aprender-a-hackear/14575255).*
- *Martínez John Jairo. La patria.com. Colombia, el primer país que penaliza los delitos informáticos {En línea}. {Marzo 30 2012}. Disponible en: (http://www.lapatria.com/tecnologia/colombia-el-primer-pais-que-penaliza-los-delitos-informaticos-1980).*
- *Colprensa, El Universal, Fiscalía Advierte Aumento de Delitos Informáticos en Colombia Millones {En línea}. {9 enero de 2015}. Disponible en: (http://www.eluniversal.com.co/cartagena/nacional/fiscalia-advierte-aumento-de-delitos-informaticos-en-colombia-102898#).*
- *Inforlaft, Lo que Debe Saber Sobre el Cibercrimen en Colombia {En línea}. {18 enero de 2015}. Disponible en: (http://www.infolaft.com/es/art%C3%ADculo/lo-que-debe-saber-sobre-el-cibercrimen-en-colombia).*
- *Pérez Camilo, Colombia digital, En Colombia se investigan los delitos informáticos {En línea}. {1 mayo de 2013}. Disponible en: (http://colombiadigital.net/actualidad/articulos-informativos/item/4810-en-colombia-se-investigan-los-delitos-informaticos.html).*
- *Netmedia, Bestuzhev Dmitry, Cibercriminales, ansiosos por el crecimiento económico y Web de América Latina {En línea}. {18 enero de 2015}. Disponible en: (http://www.bsecure.com.mx/opinion/cibercriminales-ansiosos-por-el-crecimiento-economico-de-america-latina/#).*
- *Álvarez Ángel, Las 10 ciudades de América Latina más vulnerables al cibercrimen {En línea}. {18 enero de 2015}. Disponible en: (http://www.bsecure.com.mx/featured/las-10-ciudades-de-america-latina-mas-vulnerables-al-cibercrimen/).*
- *Segu.Info, Legislación y Delitos Informáticos –Estados Unidos, {En línea}. {Enero 19 de 2015}. Disponible en: (http://www.segu-info.com.ar/delitos/estadosunidos.htm).*

- *Wikipedia, Kevin Mitnick {En línea}. {Enero 19 de 2015}. Disponible en: (http://es.wikipedia.org/wiki/Kevin_Mitnick).*
- *Semana.com. Primer extraditado por delitos informáticos {En línea}. {Junio 19 2013}. Disponible en: (http://www.semana.com/nacion/articulo/el-primer-extraditado-delitos-informaticos/348204-3).*
- *Elhacker.net, Estos son los hackers más famosos de los últimos años,* {En línea}. {Enero 19 de 2015}. Disponible en: (http://foro.elhacker.net/foro_libre/hackers-t249680.0.html;msg1203395).
- Martínez Juan, Los Hackers no han Ganado, Estados Unidos Contraataca, {En línea}. {Enero 19 de 2015}. Disponible en: (http://www.vanguardia.com/actualidad/tecnologia/292403-los-hackers-no-han-ganado-estados-unidos-contraataca#).
- El País, Obama coloca la ciberseguridad en el centro del debate en EE UU. {En línea}. {Enero 19 de 2015}. Disponible en: (http://internacional.elpais.com/internacional/2015/01/13/actualidad/1421180628_845380.html).
- *Delitos Informaticos.doc {En línea}. {Enero 19 de 2015}. Disponible en: (https://docs.google.com/document/d/1shYhIUuqLCe9MiRteX1b8wsuq9WKG3kQwITiXMZGayk/edit?hl=es&pli=1).*
- *Torres Jorge. Impacto de los delitos informáticos {En línea}. {Octubre 2000}. Disponible en: (http://www.monografias.com/trabajos6/delin/delin2.shtml).*
- *Doncel Luis. El país internacional. La captura de un agente doble enturbia las relaciones entre Berlín y Washington {En línea}. {Julio 14 2014}. Disponible en: (http://internacional.elpais.com/internacional/2014/07/04/actualidad/1404488164_311691.html).*
- *Emol. ciencia y tecnología. Hacker alemán muestra método para obtener huellas dactilares desde fotos, {En línea}. {Enero 27 de 2015}. Disponible en: (http://www.emol.com/noticias/tecnologia/2014/12/29/696637/hacker-aleman-muestra-metodo-para-obtener-huellas-dactilares-desde-fotos.html#).*
- *Segu-info. Legislación y Delitos Informáticos - La Información y el Delito, {En línea}. {Enero 27 de 2015}. Disponible en: (https://www.segu-info.com.ar/legislacion/)*
- *Rodríguez Arbeláez Juan David. Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación {03 febrero 2015} {En línea} Disponible en:*
    - *http://bdigital.ces.edu.co:8080/repositorio/bitstream/10946/1334/2/Delitos%20en%20las%20Redes%20Sociales.pdf*

- *Landaverde Contreras Melvin Leonardo. Delitos informáticos, Impacto de los delitos informáticos {Octubre de 2000} {En línea} Disponible en: http://www.monografias.com/trabajos6/delin/delin2.shtml#impa*
- *Black hack mx. Documental. Tijerina Ofelia, Cuidado con los datos, la web nos vigila, no estamos solos. {18 febrero 2014} {En línea}. Disponible en: https://www.youtube.com/watch?v=qJFjSAaTnMU*
- *AnonymousMexico2. Anonymous Ciberguerilla {01 junio 2013} {En línea}. Disponible en: https://www.youtube.com/watch?v=BhJfaKAycNs*
- *The Eternauta666. Documental. Atrapados en la red Delitos informáticos. {15 febrero 2012} {En línea}. Disponible en: https://www.youtube.com/watch?feature=player_embedded&v=t75Zrhhe5a0*
- *Landaverde Contreras Melvin Leonardo. Delitos informáticos, Impacto de los delitos informáticos {Octubre de 2000} {En línea} Disponible en: http://www.monografias.com/trabajos6/delin/delin2.shtml#impa*
- *Rec reporteroscuatro. Documental. Estamos desnudos en internet? {11 noviembre 2012} {En línea}. Disponible en: https://www.youtube.com/watch?v=H20OPj7FBaw*
- *Reyes Sánchez Yuridia Elena, Fernández Aramburo Ever Alfonso, delitos informáticos proyecto final (2 de febrero de 2015) {En línea}.http://www.scribd.com/doc/24068494/DELITOS-INFORMATICOS-PROYECTO-FINAL#scribd.*
- *Viruslist.com todo sobre seguridad en internet. Amenazas Corporativas(2 de febrero de 2015) {En línea}.http://www.viruslist.com/sp/analysis?pubid=207271238#00*
- *Wikipedia, Adware. (9 de febrero de 2015) {En línea}.http://es.wikipedia.org/wiki/Adware*
- *Cimputer forensi, GLOSARIO. (9 de febrero de 2015) {En línea}http://www.delitosinformaticos.info/delitos_informaticos/glosario.html*
- *Wikipedia, Troyano (informática) (9 de febrero de 2015) {En línea}http://es.wikipedia.org/wiki/Troyano_%28inform%C3%A1tica%29*
- *Wikipedia, Exploit. (9 de febrero de 2015) {En línea}.http://es.wikipedia.org/wiki/Exploit*
- *Wikipedia Puerta trasera. . (9 de febrero de 2015) {En línea . http://es.wikipedia.org/wiki/Puerta_trasera*
- *Wikipedia, Heartbleed. (9 de febrero de 2015) {En línea}.* http://es.wikipedia.org/wiki/Heartbleed
- *Viruslist.com, todo sobre seguridad en internet., Kaspersky Security Bulletin 2014. Evolución del malware(9 de febrero de 2015) {En línea}.http://www.viruslist.com/sp/analysis?pubid=207271276*

- *Kaspersky Lab & Interpol Joint Report. Mobile Cyber Threats. (9 de febrero de 2015) {En línea}.http://media.kaspersky.com/pdf/Kaspersky-Lab-KSN-Report-mobile-cyberthreats-web.pdf*
- Duarte Eugenio. Seguridad Informática, hacking seguridad informática. {11 julio2012} {En línea}. Disponible en: http://blog.capacityacademy.com/2012/07/11/las-8-mejores-herramientas-de-seguridad-y-hacking/
- *Taringa. Las Herramientas Hacking/Seguridad más usadas. {Junio 2011} {En línea}. Disponible en: http://www.taringa.net/posts/apuntes-y-monografias/11561390/Las-Herramientas-Hacking-Seguridad-mas-usadas.html*
- *Google Sites. Hacker piratas informáticos, anatomía de una acción de hacker. {En línea}. Disponible en: https://sites.google.com/site/hackerspiratasinformaticos/anatomia-de-una-accion-de-hacker*
- *Borghello Cristian. Amenazas Humanas - Hackers: Rebeldes con Causa. {2009} {En línea}. Disponible en: https://www.segu-info.com.ar/amenazashumanas/hackers_rebeldes.htm*
- *Hemeroteca. Los hacker españoles quieren rehabilitar su imagen ante la sociedad. {08 octubre 2103} {En línea}.disponible en: http://www.abc.es/hemeroteca/historico-08-10-2003/abc/Internet/los-hackers-espa%C3%B1oles-quieren-rehabilitar-su-imagen-ante-la-sociedad_212503.html#*
- *Laurencena Víctor. Hackers: ¿héroes o piratas? {Marzo 2014} {En línea}. Disponible en: http://www.rumbosdigital.com/secciones/notas/hackers-heroes-o-piratas.*
- *Ojeda-Pérez, Jorge Eliécer; Rincón-Rodríguez, Fernando; Arias-Flórez, Miguel Eugenio & Daza-Martínez, Libardo Alberto. Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad. {En Línea} {febrero 2010}. Disponible en: http://www.scielo.org.co/scielo.php?pid=S0123-14722010000200003&script=sci_arttext*
- *Wordpress, myprofetecnologia. Delios informáticos. {En línea} {Octubre 2011}. Disponible en: https://myprofetecnologia.wordpress.com/2011/01/30/delitos-informaticos/*
- *Jeda-Pérez, Jorge Eliécer; Rincón-Rodríguez, Fernando; Arias-Flórez, Miguel Eugenio & Daza-Martínez, Libardo Alberto. Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad. {En Línea} {febrero 2010}. Disponible en: http://www.scielo.org.co/scielo.php?pid=S0123-14722010000200003&script=sci_arttext*

- *Ramírez Emilio. Los Delitos Informáticos. Tratamiento Internacional. {En Línea} {Mayo 2009}. Disponible en: http://www.eumed.net/rev/cccss/04/rbar2.htm*
- *Acurio Santiago. Delitos informáticos: Generalidades. {En línea} {2009}. Disponible en: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf*
- *Elpais.com. En Colombia las cifras de delitos informáticos van en aumento. {En línea}{Diciembre 2012}. Disponible en: http://www.elpais.com.co/elpais/judicial/noticias/colombia-cifras-delitos-informaticos-van-aumento*
- *El Universal. El delito informático es muy joven en Colombia. {En línea}{09 marzo 2014}. Disponible en: http://www.eluniversal.com.co/tecnologia/el-delito-informatico-es-muy-joven-en-colombia-fiscalia-153299*
- *Gandini isabella. Ley de Delitos Informáticos en Colombia. {En línea} {Abril 2014}. Disponible en: http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia*
- *Caro Elizabeth. La Vulnerabilidad Social Como Enfoque De Análisis De La Política De Asistencia Social. {julio 2003} {En línea}. Disponible en: http://www.cepal.org/celade/noticias/paginas/9/12939/eps9_ecaro.pdf*
- *Medina Eduardo. Los ataques DDoS aumentaron un 90% en el último trimestre de 2014. {30 enero 2015} {En línea}. Disponible en: http://www.muycomputer.com/2015/01/30/ataques-ddos-aumentaron-90-2014*
- *Pymes autónomos. Software obsoleto, código erróneo o errores de los usuarios principales amenazas de seguridad .{En línea} {6 agosto 2014}Disponible en: http://www.pymesyautonomos.com/tecnologia/software-obsoleto-codigo-erroneo-o-los-propios-de-los-usuarios-principales-amenazas-de-seguridad-para-las-empresas*
- *Red Hat, Inc. Ataques y vulnerabilidades {En línea} {2003}. Disponible en: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-risk-net.html*
- *Finanzas personales. Hackers éticos: copiando a los criminales. {En línea} {Noviembre 2014}. Disponible en: http://www.finanzaspersonales.com.co/consumo-inteligente/articulo/hackers-eticos-copiando-criminales/50089*
- *Dinero, La amenaza hacker. {12 Abril de 2013} {En línea} Disponible en: http://www.dinero.com/empresas/articulo/empresas-hacker-cobran-datos/189128*
- Medina Édgar, Colombiano de quince años crea escuela para aprender a 'hackear'. {23 septiembre 2014} {En línea} Disponible en: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/como-hackear-

colombiano-de-quince-anos-crea-escuela-para-aprender-a-hackear/14575255.

- Antena3.com .Un hacker español, entre los jóvenes más brillantes del mundo: "No estudiaba pero monté mi primera empresa con 15 años". {01 Enero de 2015} {En línea} Disponible en: http://www.antena3.com/noticias/tecnologia/hacker-espanol-jovenes-mas-brillantes-mundo-estudiaba-pero-monte-primera-empresa-anos_2015013000119.html
- Mundo contact. Jóvenes emulan a ciberdelincuentes buscando fama y elogios. {29 Julio de 2014} {En línea} Disponible en: http://mundocontact.com/jovenes-emulan-a-ciberdelincuentes-buscando-fama-y-elogios/
- *El mundo. Lecciones de 'hacking' para adolescentes. {08 Diciembre de 2013} {En línea} Disponible en: http://www.elmundo.es/tecnologia/2013/12/08/52a3801e63fd3d043f8b456d.html*
- *BBC Mundo. Los hackers de hoy, cada vez más jóvenes. {11 Febrero de 2013} {En línea} Disponible en: http://www.bbc.co.uk/mundo/noticias/2013/02/130210_tecnologia_ninos_hackers_en*
- *Gfierro, Rankia. Analizando la Piratería desde sus Causas, No desde sus Efectos. {01 Febrero de 2012} {En línea} Disponible en: http://www.rankia.com/blog/etfs-pm/1082304-analizando-pirateria-sus-causas-no-efectos*
- *Calderón Cardona. En Colombia la piratería se redujo 1% en los últimos 720 días* On {27 junio 2014} *{En línea} Disponible en: https://www.calderoncardona.com/archivos/4087*
- *El Tiempo. Hurtos y suplantación de sitios web son las prácticas más comunes de los delincuentes virtuales. {18 mayo 2012}{En línea}.*
- *Unidad Investigativa, El Tiempo. Así opera el negocio sucio de los trinos. {27 Mayo 2014}{En línea} Disponible en: http://www.eltiempo.com/politica/justicia/el-negocio-de-hackear-y-delinquir-por-redes-sociales/14044778*
- *Pulsosocial. Joven latinoamericano crea escuela para aprender a hackear{06 Octubre 2014}{En línea} Disponible en: http://pulsosocial.com/2014/10/06/joven-latinoamericano-crea-escuela-para-aprender-hackear/*
- *Justicia El Tiempo. Así planearon los hackers el robo de $ 160.000 millones. {18 Diciembre 2014}{En línea} Disponible en: http://www.eltiempo.com/politica/justicia/hackers-movieron-160000-millones-de-pesos/14991075*

- *Ramírez Galvis. La primera escuela para aprender a hackear. {28 Septiembre 2014 }{En línea} Disponible en: http://www.vanguardia.com/actualidad/tecnologia/280521-la-primera-escuela-para-aprender-a-hackear.*

- *Undercode, Spoofing, suplantando tu identidad. {24 Diciembre de 2014 }{En línea} Disponible en: https://underc0de.org/foro/seguridad/spoofing-suplantando-tu-identidad/*
- *V. Jorge, Herramientas básicas para Hacking (escaneo). {3 julio 2015 }{En línea} Disponible en: http://codigoprogramacion.com/articulos/hacking/97-herramientas-basicas-para-hacking.html#.VbUY0_l_Oko*
- *Google.com, escaneo de puertos abiertos hacking. {26 julio de 2015 }{En línea} Disponible en: https://www.google.com.co/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=escaneo+de+puertos+abiertos+hacking*
- *Gonzales Antonio, Cómo hackear wifi o robar wifi al vecino? 10 programas para robar contraseñas y acceder. {26 julio de 2015 }{En línea} Disponible en: http://antoniogonzalezm.es/como-robar-la-wifi-de-un-vecino-10-programas-para-hackear-contrasena-y-acceder/*
- *Ciper, Los correos que alertaron sobre la compra del poderoso programa espía de la PDI. {10 julio de 2015 }{En línea} Disponible en: http://ciperchile.cl/2015/07/10/los-correos-que-alertaron-sobre-la-compra-del-poderoso-programa-espia-de-la-pdi/*
- *Alvarado Noguera Ernesto, Universidad Segio Arboleda, No use software pirata. - Alternativas para no ser ilegal, {26 julio de 2015} {En línea} Disponible en: http://www.usergioarboleda.edu.co/altus/software-pirata-alternativas.htm.*
- Portafolio, Empresas pierden US$114.000 millones por software ilegal. ,{ 8 2013 }{En línea} Disponible en: http://www.portafolio.co/negocios/software-pirata
- *Marlopduar. Los nuevos roles del profesor: hacker, DJ, coach y Community Manager. { 20 febrero 2014} {En línea}. Disponible en: http://conektioblog.com/2014/01/30/LOS-NUEVOS-ROLES-DEL-PROFESOR-HACKER-DJ-COACH-Y-COMMUNITY-MANAGER/*
- *Jiménez Roberto. Expulsan a alumnos californianos por hackear PC de profesores y cambiar calificaciones. {04 febrero 2014}{En línea}. Disponible en: http://www.qore.com/noticias/15819/Expulsan-a-alumnos-californianos-por-hackear-PC-de-profesores-y-cambiar-calificaciones*
- *Mlarracuente. ¿Deberían Las Universidades E Instituciones Educativas Enseñar Sobre "Hacking"? {24 abril 2014 }{En línea}. Disponible en: https://mlarracuente.wordpress.com/2014/04/24/25-deberian-las-universidades-e-instituciones-educativas-ensenar-sobre-hacking/*

- *Miguel Jorge. 20 minutos. Profesor de matemáticas condenado por enlazar a respuestas "piratas". {17 Enero 2013}{En línea}. Disponible en: http://www.20minutos.es/noticia/231176/0/multa/profesor/piratear/*

- *WordPress. Ramón. Software pirata en administraciones públicas, una completa irresponsabilidad. {30 enero 2014}{En línea}. Disponible en: http://ramonramon.org/blog/2014/01/30/software-pirata-instituciones-publicas/*
- *Segall Laurie, YouTube se enfrenta a los videos que enseñan a hackear. {31 Julio 2015}{En línea}. Disponible en: http://www.cnnexpansion.com/tecnologia/2015/07/30/youtube-se-enfrenta-a-los-videos-que-ensenan-a-hackear*
- *Marlopduar. Los nuevos roles del profesor: hacker, DJ, coach y Community Manager. { 20 febrero 2014} {En línea}. Disponible en: http://conektioblog.com/2014/01/30/LOS-NUEVOS-ROLES-DEL-PROFESOR-HACKER-DJ-COACH-Y-COMMUNITY-MANAGER/*
- *Hotfixed. Hack x Colombia 2011. . { 12 Octubre 2011} {En línea}. Disponible en: http://hotfixed.net/hack-x-colombia-2011/*
- *Muchohacker.Tras la captura de un hacker Colombiano. { 13 Octubre 2014} {En línea}. Disponible en: http://muchohacker.com/tras-la-captura-de-un-hacker-colombiano/*
- Villa Marta. Seis universitarios de la Autónoma enseñan a hackear wifi mediante un juego. { 12 Febrero 2014} {En línea}:http://noticias.lainformacion.com/economia-negocios-y-finanzas/redes/seis-universitarios-de-la-autonoma-ensenan-a-hackear-wifi-mediante-un-juego_VxPGsaGZIFcedfRe1mpoj7/
- *Enter.co. EL HACKING ÉTICO Y SU IMPORTANCIA PARA LAS EMPRESAS. { 28 Febrero 2014} {En línea}:http://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/*
- *Mayo Cerqueiro Pablo, El confidencial, Hackers con principios. { 20 Junio 2015} {En línea}:http://www.elconfidencial.com/tecnologia/2015-06-20/hackers-eticos-ciberseguridad-hacking_893699/*
- Cabezas López Carlos. Delitos informáticos. Neópatas, de la mitomanía al crimen. {10 noviembre 2008} {En línea}. Disponible en: http://www.delitosinformaticos.com/11/2008/noticias/neopatas-de-la-mitologia-al-crimen#
- García R José Carlos. Aumentan casos de ciberdelitos contra menores en el país. {10 Agosto 2015} {En línea}. Disponible en: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/internet-es-cada-vez-mas-peligroso-para-los-ninos/16207955

- Gustavo Caraballo. Descuido de los usuarios, el mayor aliado de los hackers. . {30 Agosto 2015} {En línea}. Disponible en: http://www.kienyke.com/economia/descuido-de-los-usuarios-el-mayor-aliado-de-los-hackers/
- Santos Mateo. LOS RETOS DE SEGURIDAD PARA LAS PYMES. {13 Julio 2013} {En línea}. http://www.enter.co/especiales/enterprise/los-retos-de-seguridad-para-las-pymes/
- Mark Stockley. Acaso la seguridad informática conseguir mejor o peor en el 2014? Usted tiene la palabra. {18 diciembre 14} {En línea}. Disponible en: https://nakedsecurity.sophos.com/es/2014/12/18/did-computer-security-get-better-or-worse-in-2014-have-your-say/
- PoliticaDigital. La seguridad informática se vuelve cotidiana. {01 febrero 2014} {En línea}. Disponible en: http://www.politicadigital.com.mx/?P=leernoticiaprint&Article=820
- Martínez John Jairo. Colombia, el primer país que penaliza los delitos informáticos. {30 marzo 2012} {En línea}. Disponible en: http://www.lapatria.com/tecnologia/colombia-el-primer-pais-que-penaliza-los-delitos-informaticos-1980?qt-lo_m_s10=0
- Veloza Carolina. Conozca las dos nuevas modalidades de delitos informáticos. {01 octubre 2013} {En línea}. Disponible en: http://colombia.mmi-e.com/blog/category/sector/tic/c%C3%B3nozca-las-dos-nuevas-modalidades-de-d%C3%A9litos-inform%C3%A1ticos
- Colprensa. El Universal. Fiscalía advierte aumento de delitos informáticos en Colombia. {23 diciembre 2013} {en línea}. Disponible en: http://www.eluniversal.com.co/cartagena/nacional/fiscalia-advierte-aumento-de-delitos-informaticos-en-colombia-102898
- Garcia Pérez Camilo. ¿En Colombia se investigan los delitos informáticos? {01 mayo 2013} {En línea}. Disponible en: http://colombiadigital.net/actualidad/articulos-informativos/item/4810-en-colombia-se-investigan-los-delitos-informaticos.html
- YouTube. Enero 5 del 2015. Crónicas RCN- hacker o violación de la intimidad. [Archivo de Video]. Obtenido de https://www.youtube.com/watch?v=aXukkwfuvQc
- YouTube. Hace 4 años. Tecnología forence: CTI. [Archivo de Video]. Obtenido de https://www.youtube.com/watch?v=5CmM9K_FCqc
- YouTube. Hace 5 años. Delitos informáticos en Colombia. [Archivo de Video]. Obtenido de https://www.youtube.com/watch?v=E18e5SiX0zc
- YouTube. Hace 2 años. Anonymous Ciberguerrilla '08 Documental completo. [Archivo de Video]. Obtenido de https://www.youtube.com/watch?v=BhJfaKAycNs

- YouTube. Hace 1 año. Cuidado con tus datos la web nos vigila? no estamos solos seguridad informática documental. [Archivo de Video]. Obtenido de https://www.youtube.com/watch?v=qJFjSAaTnMU
- YouTube. Hace 3 años. Atrapados en la red - (documental) delitos informáticos. [Archivo de Video]. Obtenido de https://www.youtube.com/watch?v=t75Zrhhe5a0

10 Anexos

10.1 Anexo 1 Encuesta Realizada a Estudiantes:

1. Accedería a vulnerar un sistema con el objetivo de facilitar su vida laboral? *

Responda de 0 a 5 siendo 0 el más bajo y 5 el más alto

0 1 2 3 4 5

2. Está preparado o tiene alternativas, de cómo evitar un ataque informático si le llegara a suceder? *

- Ninguna
- Poco conocimiento
- Algo de conocimiento
- Si se evitar una ataque

3. Si alguien le propone acceder a un sistema informático, una página o programa indebido con una buena recompensa económica lo haría? *

- Nunca
- Quizás lo haría
- Si lo haría

4. Acudiría a un profesional con el objetivo de obtener información a la que no puede acceder? *

- Nunca
- Quizás lo haría
- Si lo haría

5. Ha tomado la opción de descargar programas y/o películas piratas? *

Responda del 0 al 4 siento 0 el menos frecuente y 4 el más frecuente

1 2 3 4 5

6. Si tuviera la oportunidad de tener ingreso adicional a través de una página o programa irregular lo haría? *

- Nunca
- Algunas veces
- La mayoría de las veces

7. Aprendería usted técnicas a través de foros, tutoriales, videos, etc. Que le permitan aprender cómo acceder a un sistema o página para obtener información privilegiada? *

Responda del 0 a 5 siendo 0 el más bajo y 5 el más alto

0 1 2 3 4 5

8. Ha intentado ingresar a una cuenta de Facebook, correo, Skype, etc. que no sea la suya? *

Responda del 0 a 5 siendo 0 nunca y 5 muchas veces

0 1 2 3 4 5

9. Ha permanecido tiempo buscando en foros información de cómo entrar a sistemas informáticos? *

Responda del 0 a 5 siendo 0 el menos frecuente y 5 el más frecuente

0 1 2 3 4 5

10. Conoce usted programas para vulnerar o acceder a sitios sin permiso? *

- Ninguno
- Alguno
- Muchos

11. Al crear sus contraseñas en correos, computador , etc. se fija en : *

- Utilizar la misma para todos o para la mayoría de estos medios.
- Siempre son diferentes, además que sea alfanumérica y con mayúscula
- Solo utiliza números
- Solo Utiliza Letras
- No tiene en cuenta nada al momento de crearla.

12. Ha ingresado a páginas web en donde haya suplantado su identidad? *

Responda de 0 a 5 siendo 0 el más bajo y 5 el más alto

0 1 2 3 4 5

13. Ha intentado un escaneo de puertos para tener acceso a un sistema sin permiso? *

Responda del 0 a 5 siento 0 el menos frecuente y 5 el más frecuente

0 1 2 3 4 5

14. Ha probado mediante dispositivos móviles acceder a información mediante redes wi-fi abiertas? *

Responda del 0 a 5 siento 0 el menos frecuente y 5 el más frecuente

0 1 2 3 4 5

15. Ha intentado instalar programas o software espías en celulares o computadores de una persona? *

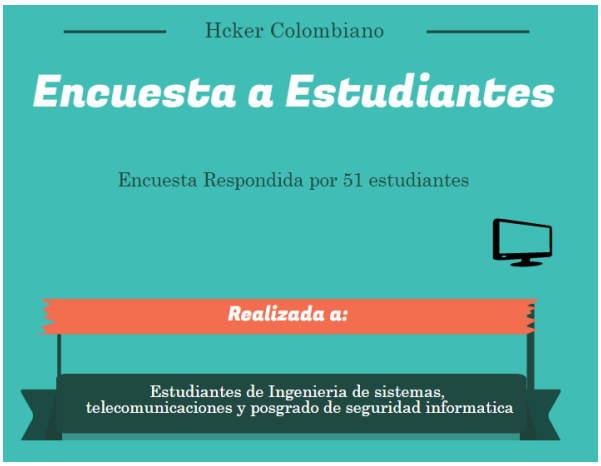
Responda del 0 a 5 siento 0 el menos frecuente y 5 el más frecuente

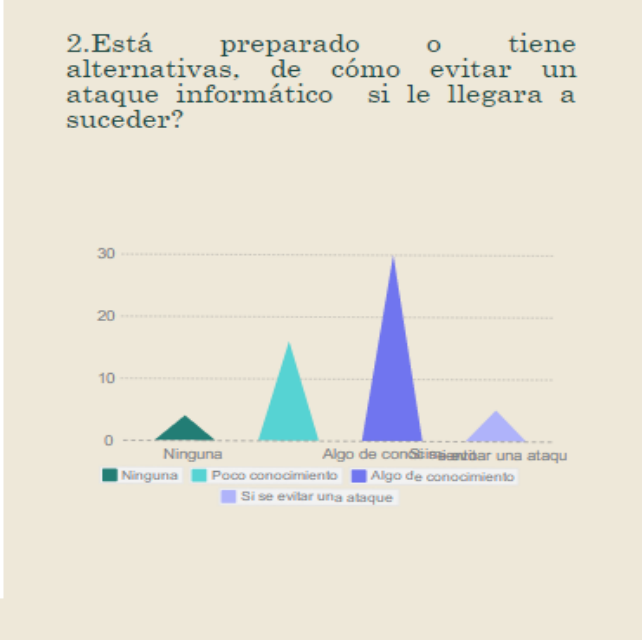
0 1 2 3 4 5

Enviar

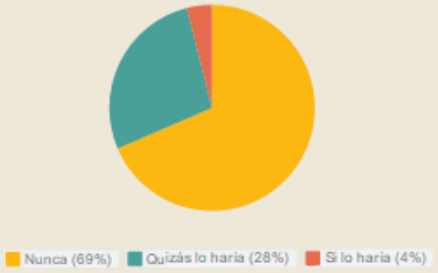
Nunca envíes contraseñas a través de Formularios de Google.

10.2 Anexo 2 Respuesta Encuesta Estudiantes.:





3. Si alguien le propone acceder a un sistema informático, una página o programa indebido con una buena recompensa económica lo haría?

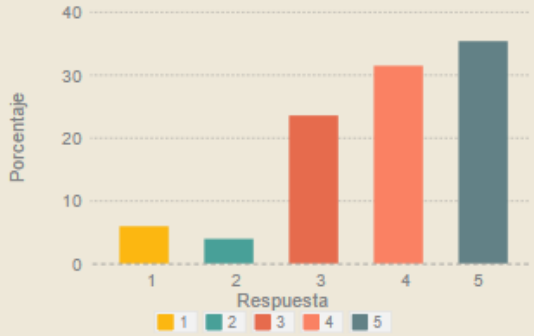


4. Si tuviera la oportunidad de tener ingreso adicional a través de una página o programa irregular lo haría?

5. Ha tomado la opción de descargar programas y/o películas piratas?

Responda de 0 a 5 siendo 0 el más bajo y 5 el más alto

0. 1. 2. 3. 4. 5



6. Acudiría a un profesional con el objetivo de obtener información a la que no puede acceder?

7.Aprendería usted técnicas a través de foros, tutoriales, vídeos, etc. Que le permitan aprender cómo acceder a un sistema o página para obtener información privilegiada?

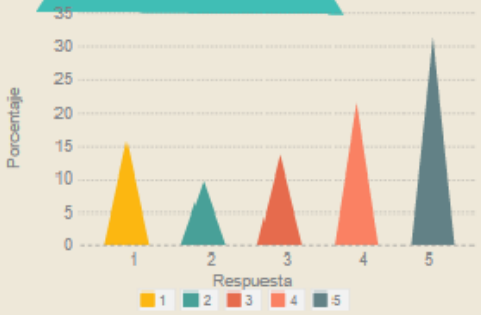
Responda de 0 a 5 siendo 0 el más bajo y 5 el más alto

0. 1. 2. 3. 4. 5

8. Ha intentado ingresar a una cuenta de Facebook, correo, Skype, etc. que no sea la suya?

Responda de 0 a 5 siendo 0 el más bajo y 5 el más alto

0. 1. 2. 3. 4. 5

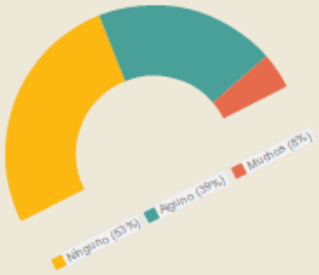


9.Ha permanecido tiempo buscando en foros información de cómo entrar a sistemas informáticos?

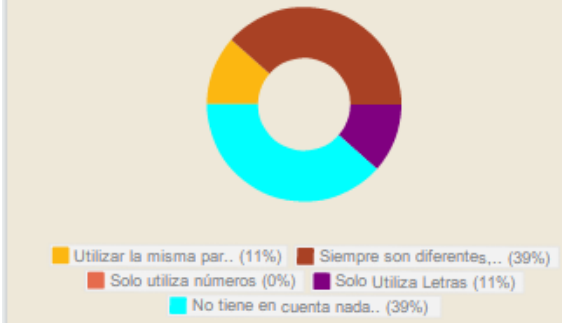
Responda de 0 a 5 siendo 0 el más bajo y 5 el más alto

0. 1. 2. 3. 4. 5

10. Conoce usted programas para vulnerar o acceder a sitios sin permiso?

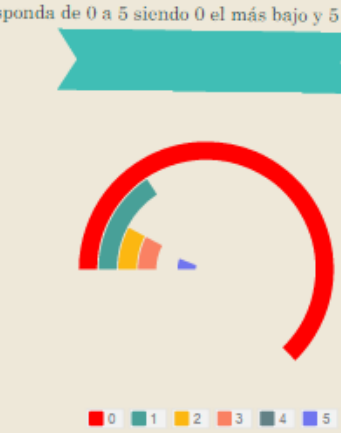


11. Al crear sus contraseñas en correos, computador, etc. se fija en:



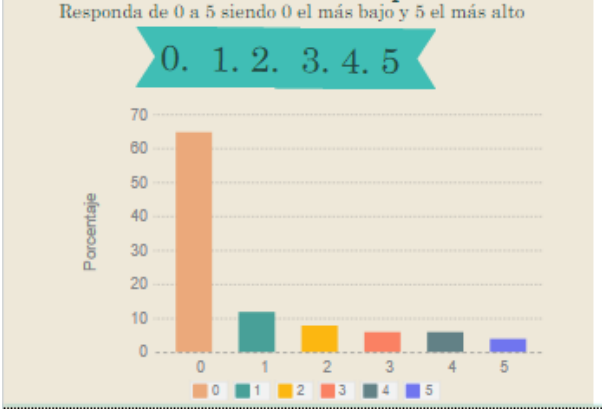
12. Ha ingresado a páginas web en donde haya suplantado su identidad?

Responda de 0 a 5 siendo 0 el más bajo y 5 el más alto



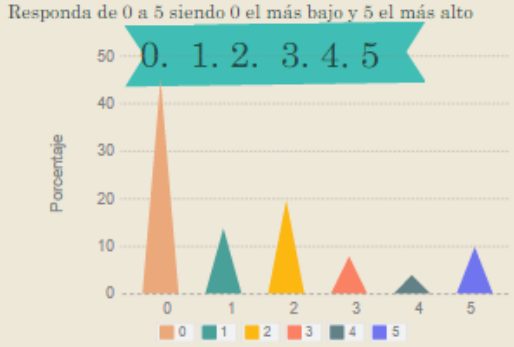
13. Ha intentado un escaneo de puertos para tener acceso a un sistema sin permiso?

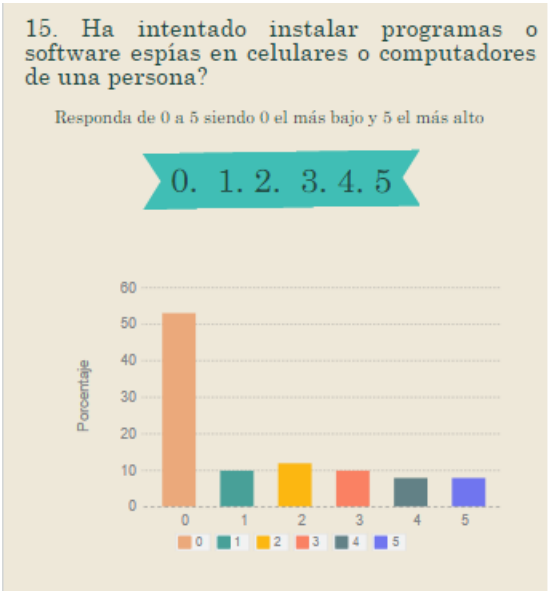
Responda de 0 a 5 siendo 0 el más bajo y 5 el más alto



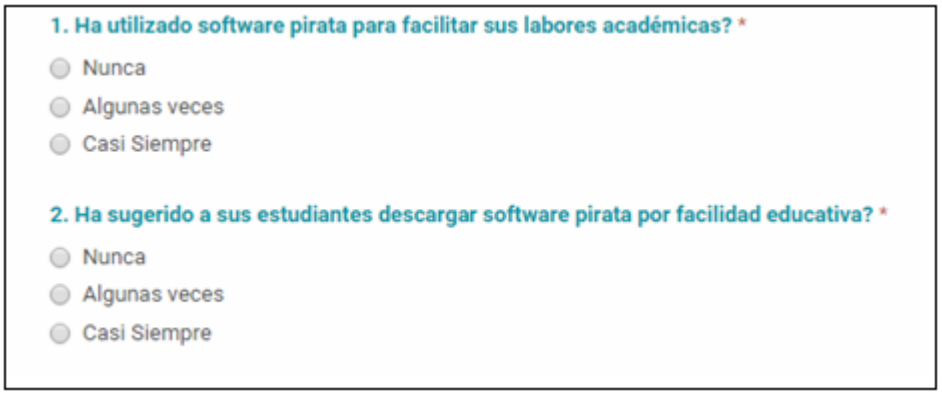
14. Ha probado mediante dispositivos móviles acceder a información mediante redes wi-fi abiertas?

Responda de 0 a 5 siendo 0 el más bajo y 5 el más alto





10.3 Anexo 3 Encuesta Realizada a Docentes:



3. Considera que un estudiante talentoso es aquel que sea capaz de encontrar formas alternativas de acceder a sistemas informáticos? *

- Totalmente de acuerdo
- De acuerdo
- En desacuerdo
- Totalmente en desacuerdo

4. Un comportamiento curioso del estudiante que lo lleva a aprender y ampliar el conocimiento para encontrar vulnerabilidades a un sistema, le parecería positivo? *

En una escala del 1 al 4, dónde 1 es "muy negativo" y 4 es "muy positivo"

1 2 3 4

5. Capacitaría usted a la comunidad académica en técnicas de acceso a sistemas informáticos con el objeto de ampliar el aprendizaje? *

- Si lo haría
- Quizás lo haría
- No lo haría
- Nunca lo haría

6. Considera que es indispensable enseñar técnicas de hackeo con el fin de ampliar el conocimiento de los estudiantes de cómo prevenir ataques? *

- Totalmente de acuerdo
- De acuerdo
- En desacuerdo
- Totalmente en desacuerdo

7. Ha explicado en algún momento a la comunidad académica sobre paginas o software que permitan acceder a sistemas sin permiso, con el fin de enseñar cómo funcionan? *

- Si lo hice
- Quizás lo haría
- No lo haría
- Nunca lo haría

8. Ha intentado guiar a estudiantes que tienen habilidades para el ataque a sistemas informáticos, para que utilice este conocimiento de forma positiva? *

En una escala del 1 al 4, dónde 1 es "Nunca lo ha hecho" y 4 es "siempre lo hace"

1 2 3 4

9. A enseñado a estudiantes como identificar vulnerabilidades de un sistema? *

En una escala del 1 al 4, dónde 1 es "Nunca lo ha hecho" y 4 es "siempre lo hace"

1 2 3 4

10. A realizado pruebas de ataque en clase, con el fin de enseñar a estudiantes como los delincuentes informáticos realizan estas actividades? *

En una escala del 1 al 4, dónde 1 es "Nunca lo ha hecho" y 4 es "siempre lo hace"

1 2 3 4

11. Ayudaría a un estudiante que quiera aprender a acceder a información a la cual él no tiene acceso? *

- Si lo haría
- Quizás lo haría
- No lo haría
- Nunca lo haría

12. El comportamiento de una comunidad que tiende a vulnerar sistemas informáticos, con un fin de beneficio propio, considera usted que es una comunidad que tienen conocimientos que en alguna ocasión podrían ayudar para algún fin positivo en común. *

- Totalmente de acuerdo
- De acuerdo
- En desacuerdo
- Totalmente en desacuerdo

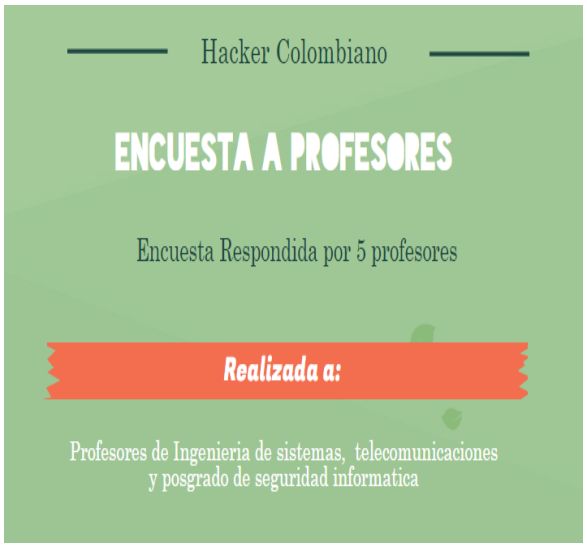
SMART APPS
BE SMART

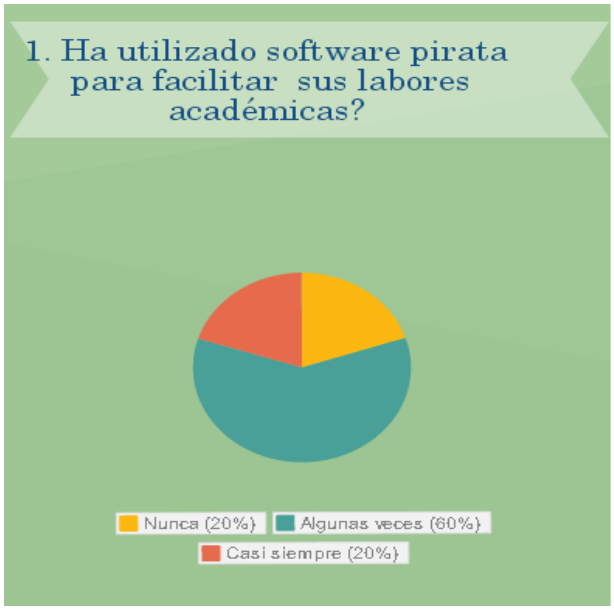
Universidad Piloto de Colombia
ÁREA ITIC
INGENIERÍA DE SISTEMAS
INGENIERÍA DE TELECOMUNICACIONES
FACULTAD DE INGENIERÍA

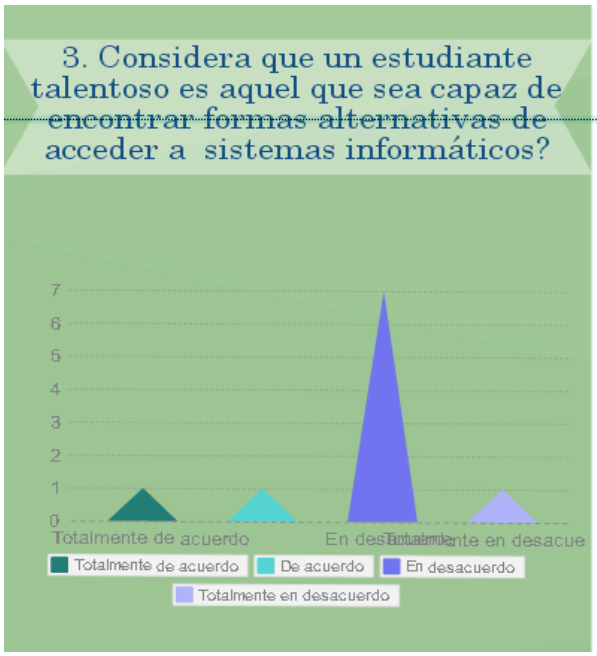
Enviar

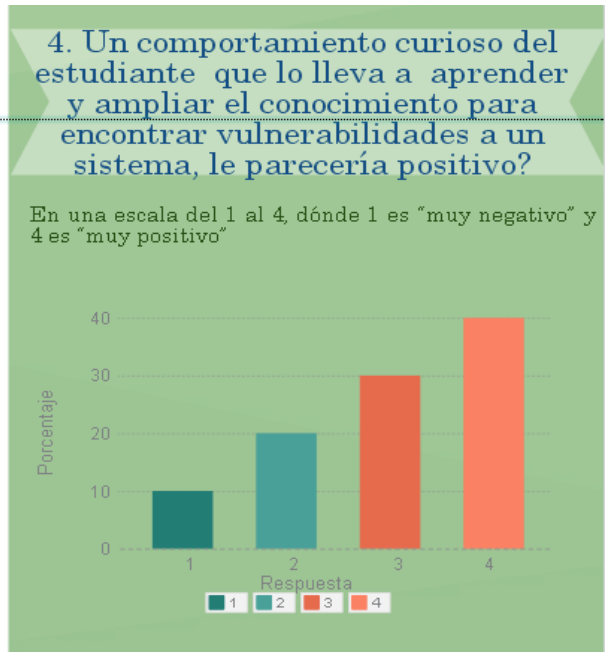
Nunca envíes contraseñas a través de Formularios de Google.

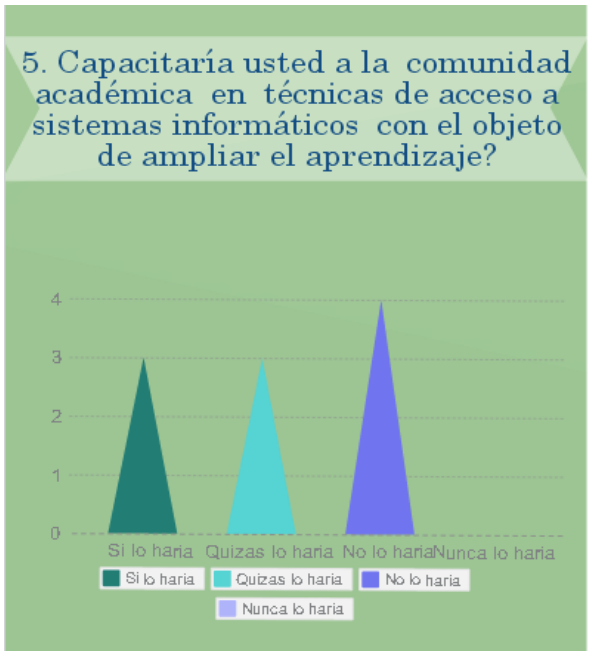
10.4 Anexo 4 Respuesta Encuesta Profesores:





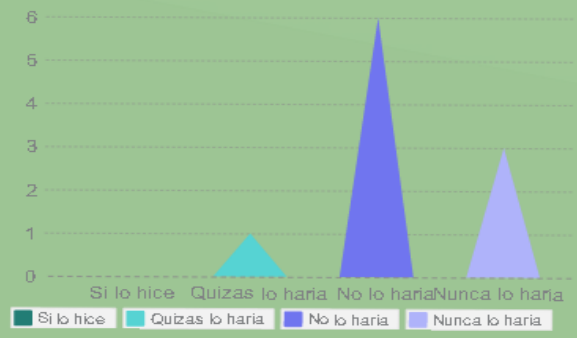

3. Considera que un estudiante talentoso es aquel que sea capaz de encontrar formas alternativas de acceder a sistemas informáticos?
7
6
5
4
3
2
1
0
Totalmente de acuerdo
Totalmente de acuerdo
De acuerdo
En desacuerdo
Totalmente en desacuerdo


4. Un comportamiento curioso del estudiante que lo lleva a aprender y ampliar el conocimiento para encontrar vulnerabilidades a un sistema, le parecería positivo?
En una escala del 1 al 4, dónde 1 es "muy negativo" y 4 es "muy positivo"
Porcentaje
40
30
20
10
0
1
2
3
4
Respuesta
1
2
3
4


5. Capacitaría usted a la comunidad académica en técnicas de acceso a sistemas informáticos con el objeto de ampliar el aprendizaje?
4
3
2
1
0
Si lo haria
Quizas lo haria
No lo haria
Nunca lo haria
Si lo haria
Quizas lo haria
No lo haria
Nunca lo haria


6. Considera que es indispensable enseñar técnicas de hackeo con el fin de ampliar el conocimiento de los estudiantes de cómo prevenir ataques?
En una escala del 1 al 4, dónde 1 es "muy negativo" y 4 es "muy positivo"
Porcentaje
4
3
2
1
0
Totalmente de acuerdo
Respuesta
Totalmente de acuerdo
De acuerdo
En desacuerdo
Totalmente en desacuerdo

7. Ha explicado en algún momento a la comunidad académica sobre paginas o software que permitan acceder a sistemas sin permiso, con el fin de enseñar cómo funcionan?

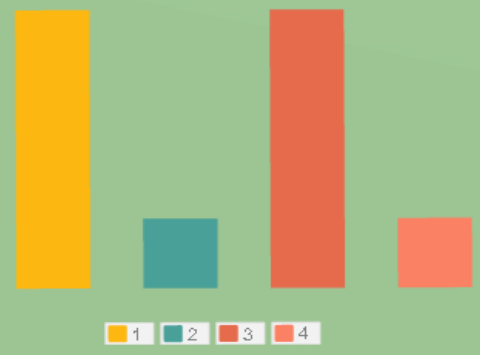


8. Ha intentado guiar a estudiantes que tienen habilidades para el ataque a sistemas informáticos, para que utilice este conocimiento de forma positiva?

En una escala del 1 al 4, dónde 1 es "Nunca lo ha hecho" y 4 es "siempre lo hace"

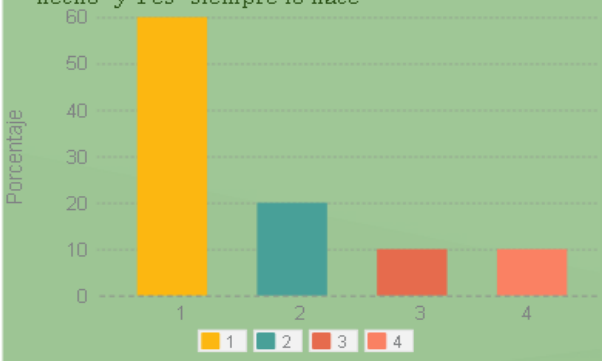
9. A enseñado a estudiantes como identificar vulnerabilidades de un sistema?

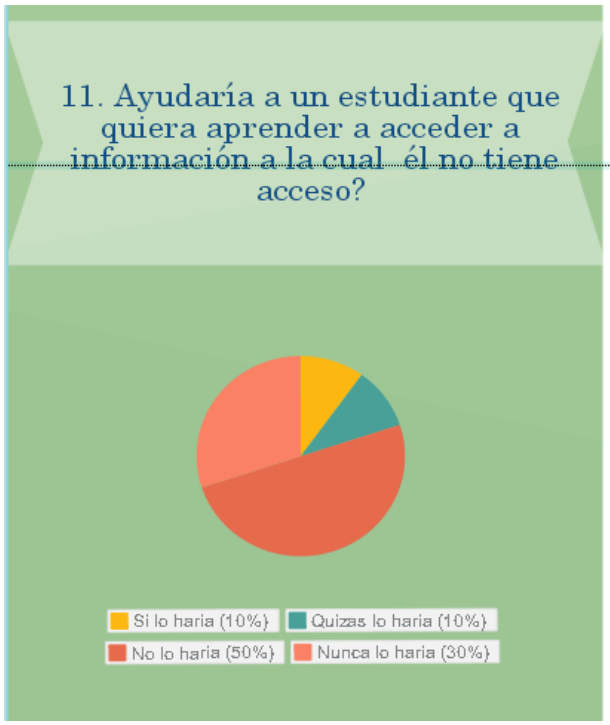
En una escala del 1 al 4, dónde 1 es "Nunca lo ha hecho" y 4 es "siempre lo hace"

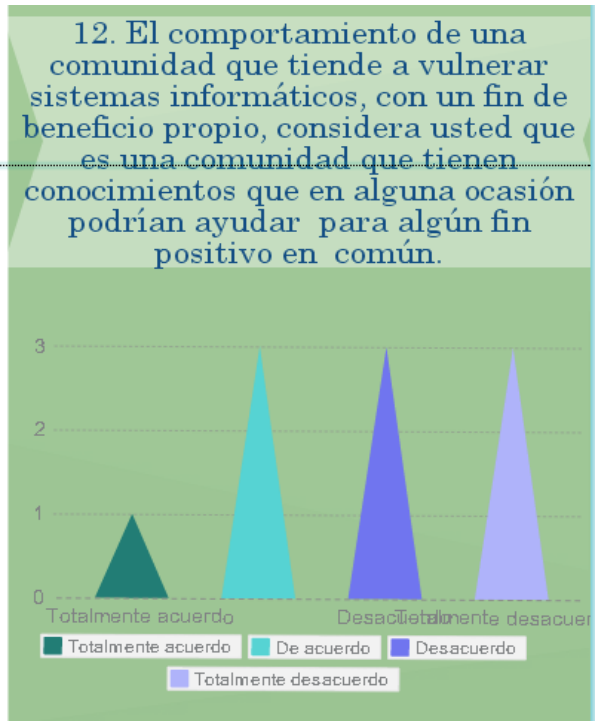


10. A realizado pruebas de ataque en clase, con el fin de enseñar a estudiantes como los delincuentes informáticos realizan estas actividades?

En una escala del 1 al 4, dónde 1 es "Nunca lo h hecho" y 4 es "siempre lo hace"







10.5 Anexo 5. Entrevista realizada a Especialistas:

1) ¿Cree usted que en la sociedad colombiana ha aumentado la conciencia de seguridad informática, en qué porcentaje cree que ha aumentado o por el contrario se ha mantenido?

2) ¿Considera usted que la actividad de delitos informáticos son cometidos usualmente por personas jóvenes, entre los 12 y 18 años, los cuales toman esta actividad como forma de acceder a recursos económicos fáciles gracias al conocimiento aprendido o considera que esta en otro rango de edades?

3) ¿Cree usted que los delitos informáticos en Colombia no son perseguidos por la ley como debería ser o por el contrario cada día se ven mejores castigos para estos crímenes?

4) ¿Considera usted que los medios de comunicación no dan relevancia a los delitos informáticos más allá de los que son más conocidos como Andrómeda o el caso Sepúlveda?

5) ¿A su criterio, cuál de estos considera usted que ha comenzado a tomar mayor importancia en los últimos años en Colombia, la comunidad hacker ético o por el contrario la comunidad hacker como delincuente informático?

6) ¿Cuál cree usted que es la razón por la cual los delitos informáticos en Colombia han ido en aumento durante los últimos años?

7) ¿Cuál de los siguientes delitos considera usted que son los más recurrentes realizados por los hackers colombianos: Suplantación, Reconocimiento, Vulneración? ¿Y porque?

8) ¿Cree usted que el mayor problema que se encuentra en las víctimas de delitos informática es la no denuncia de los mismos o cual cree usted que sea?

9) ¿Qué comparaciones tendría usted ante el daño que realiza los hackers de otros países a los daños que realizan los hackers Colombianos?

10) ¿Conoce usted cual es el manejo para los delitos informáticos que son realizados por delincuentes informáticos que provienen de otros países, pero que sus actos están apuntando a entidades Colombianas?

11) ¿Considera usted que en Colombia falta más conciencia en el uso de seguridad informática tanto en empresas, organizaciones, personas?

12) Usted como profesor, de seguridad informática, ha conocido algún caso donde un estudiante ha tomado el conocimiento brindado por la universidad y se ha ido por el camino de la delincuencia informática

10.6 Anexo 6:

Entrevista realizada a ingeniero Álvaro Escobar, para escucharla dar click https://youtu.be/Ngidx2IWonk y Entrevista realizada a ingeniero Cesar Rodríguez https://www.youtube.com/watch?v=A1itj1vjxfc&feature=youtu.be

10.7 Anexo 7:

Expertos de Adalid CORP hablan sobre casos de delitos informáticos, como se presentan y que medios pueden utilizar los hackers, para acceder a la información privada de una persona. Ver en el link https://www.youtube.com/watch?v=aXukkwfuvQc

10.8 Anexo 8:

Los niños blancos de delincuentes informáticos en internet. Ver video en:

ATRAPADOS EN LA RED - (documental)DELITOS INFORMATICOS
de TheEternauta666
Hace 3 años. • 38,404 vistas
Internet se ha convertido en la herramienta perfecta para los pederastas. Ya no tienen que acudir a parques y piscinas para ...

https://www.youtube.com/results?search_query=ATRAPADOS+EN+LA+RED++%28documental%29DELITOS+INFORMATICOS

10.9 Anexo 9:

[PDF] Delitos Informáticos - Cámara Colombiana de Informática ...
www.ccit.org.co/files/.../Delitos_Informaticos.pdf ▾
Internet sin duda cambió el ritmo de vida de las personas. Facilitó realizar sus actividades en un menor tiempo posible, conectarse con cualquier parte del mundo, ... TopComm: ¿Cómo se puede realizar actividades en Internet sin tener altos ...

TopComm realizo una entrevista a Fabián Zambrano Smith, Gerente del Centro de Operaciones de Seguridad de Digiware y Héctor Tamayo, coordinador de tecnología de la Cámara Colombiana de Informática y Telecomunicaciones, entidades expertas en seguridad informática en Colombia. Ver el Link en: http://www.ccit.org.co/files/SEGURIDAD%20INFORMATICA/Delitos_Informaticos.pdf

10.10 Anexo 10:

Así roba en Colombia el 'ciberhampa' europeo - Archivo ...
www.eltiempo.com/politica/justicia//14840917 ▾
17 de noviembre de 2014. Así roba en Colombia el 'ciberhampa' europeo. Crean falsas cuentas gratuitas de wifi para robar claves, andan con equipos portátiles para tomar información que usuarios dejan en el ciberespacio cuando utilizan redes gratuitas en hoteles, centros comerciales y aeropuertos. Esas son algunas ...

Noticia del periódico el Tiempo en donde el Coronel Fredy Bautista, director del Centro Cibernético de la Dijín, explica cómo operan las redes para los delitos informático. Ver el Link en: http://www.eltiempo.com/politica/justicia/delitos-informaticos-en-el-pais-habla-director-del-centro-cibernetico-de-la-dijin/14841739#

10.11 Anexo 11:

Tecnología Forense: CTI
de Versión Beta
Hace 4 años. • 8,829 vistas
Resulta que así como en las series de televisión acá también se hacen investigaciones con la información que sirve como ...

Video del CTI donde explica las actividades del departamento de delitos informáticos, los tipos de hacker, tipos de fraude que investigan, etc. Ver video en: https://www.youtube.com/watch?v=5CmM9K_FCqc

10.12 Anexo 12:

Delitos Informáticos en Colombia

de schartmedia

Hace 5 años. • 12,122 vistas

Un vistazo a los delitos informáticos en el territorio colombiano y las acciones tomadas por el estado y particulares.

Video que nos habla como las empresas Colombiana están sufriendo un gran daño causado del delito informático haciendo énfasis en el delito informático realizado por internet. Ver video en: https://www.youtube.com/watch?v=E18e5SiX0zc

Anonymous Ciberguerrilla '08 Documental completo

de AnonymousMexico2

Hace 2 años. • 46,561 vistas

Vista el sitio web oficial y enterate de las noticias mas recientes de Anonymos : http://www.programaswarez.org/ Siguenos en ...

10.13 Anexo 13:

Video sobre la historia del delito informático en el mundo. Eventos importantes y como el internet cada vez es el más precursor del delito informático. Guerras que se pueden desatar mediante ataques informáticos. Ver video en: https://www.youtube.com/watch?v=BhJfaKAycNs

10.14 Anexo 14:

cuidado con tus datos la web nos vigila? no estamos solos seguridad informatica documental

de black hack mx

Hace 1 año. • 22,248 vistas

cuidado con tus datos la web nos vigila? no estamos solos seguridad informatica documental español 2014 robo de identidad, ...

Video sobre la privacidad de la red, los fallos de seguridad, la protección de los datos, etc. Ver video en: https://www.youtube.com/watch?v=qJFjSAaTnMU