Investigación sobre el hacker y sus posibles comienzos en la comunidad estudiantil. Caso Universidad Piloto de Colombia

Sandra Lorena Manchola
Universidad Piloto de Colombia
Cra 9 No. 45a-44 Prog. Ing. Sistemas
Bogotá, Colombia
+57 (1) 332-2900 Ext. 274
Lorem9304@gmail.com

Gloria Hazlady Cornejo Suarez
Universidad Piloto de Colombia
Cra 9 No. 45a-44 Prog. Ing. Sistemas
Bogotá, Colombia
+57 (1) 332-2900 Ext. 274
glohazco@hotmail.com

O.E. Herrera B
Universidad Piloto de Colombia
Cra 9 No. 45a-44 Prog. Ing. Sistemas
Bogotá, Colombia
+57 (1) 332-2900 Ext. 205
oscar-herrera@unipiloto.edu.co

ABSTRACT
Se presenta 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.

CCS Concepts
• Security and privacy • Applied computing~Education • **Social and professional topics**

1. 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 caso de la www (World Wide Web), los códigos de barras y QR, videojuegos, la tecnología GPS, la nube y las redes sociales tan solo por nombrar algunas. Dentro de este popurrí de desarrollos e innovaciones aparece el término hacker [1], cuyo significado popular permite relacionarla con personas que tienen habilidades informáticas para encontrar y explotar vulnerabilidades en los sistemas con tecnologías de información y comunicaciones.

Y aunque no necesariamente todos los que poseen esas habilidades son los que realizan delitos informáticos, existe un gran porcentaje de ellos que se benefician del desconocimiento y vulnerabilidades informáticas, pudiendo llegar a generar daño social especialmente cuando se le suman aspectos relacionados con política anti/pro estatal y/o anti-*algún modelo económico-social*.

Esa graduación en la intención de los actos, clasifica a los hackers en dos principales grupos [1], 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 el conocimiento en informática o telecomunicaciones que poseen, también existen los hacker de "sombrero gris" quienes utiliza una ética ambigua, ya que penetran sistemas, hacen 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.

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.

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.

2. 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"[2].

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. 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."[3].

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

978-1-5090-2435-3/16/$31.00 ©2016 IEEE

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.
- Recopilación de información e investigación
- Finalización del ataque.

A través de tiempo en Colombia, los delitos informáticos hechos por este tipo de hacker se volvieron un dolor de cabeza sobre todo para las entidades bancarias, quienes debido a la actividad de este grupo generan pérdidas millonarias gracias principalmente a vulnerabilidades en los sistemas de información, el acceso a sus bases de datos de bancos por terceros y la clonación de tarjetas de crédito bancarias. Un ejemplo de estos delitos hechos por hackers de sombrero negro en entidades bancarias se da en la ciudad de Cali, en donde el delito se presenta por un mismo empleado de la entidad bancaria, que 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." [4]

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" [5]. 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." [6]. 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 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." [7]

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" [8]. 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[1], Legion of Doom (LOD)[2], Milw0rm[3], LulzSec[4] entre otros.

Es importante resaltar que también existe aquellos grupos y comunidades positivas como BSidesCO[5] 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 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 Colombia "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%)" [9]

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.

Según estudios realizados por la Fiscalía General de la Nación 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." [10], 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*"[11]. 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.

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.

En la actualidad y como algo cotidiano de la sociedad occidental

[1] https://en.wikipedia.org/wiki/Anonymous_(group)

[2] https://en.wikipedia.org/wiki/Legion_of_Doom_(hacking)

[3] https://en.wikipedia.org/wiki/Milw0rm

[4] https://en.wikipedia.org/wiki/LulzSec

[5] http://b-sides.co

978-1-5090-2435-3/16/$31.00 ©2016 IEEE

es normal tener cuentas en redes sociales como 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 espacio donde es fácil ocultar la verdadera persona detrás del perfil, la interacción que dan este tipo de redes con gente que muchas veces ni siquiera es conocida, abre la puerta a un nuevo mundo que favorece accione reprochables jurídicamente y éticamente pudiéndose aprovechar de dicho espacio para hacer daño.

Laverde, experto en seguridad informática sostiene que "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" [12].

El gran problema lo enfrenta no solo Colombia sino todos los países, ya que este tipo de criminalidad es difícil de combatir por el nivel de internacionalización, dichos personajes están regados por todo el mundo y su víctima igualmente puede estar en cualquier lugar, lo que también dificulta los procesos legales al enfrentarse a leyes muy diversas.

3. METODOLOGÍA Y 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 azarafícado [23], 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 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.

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.

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.

4. RESULTADOS

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. Como se puede Ver Fig.1 Para los programas de pregrado las respuestas se dieron más entre los estudiantes de semestre de noveno, decimo semestre y

978-1-5090-2435-3/16/$31.00 ©2016 IEEE

egresados, que equivalen a un total de 33 estudiantes que están en los últimos semestres de la carrera o ya se encuentran graduados.

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 Fig. 1

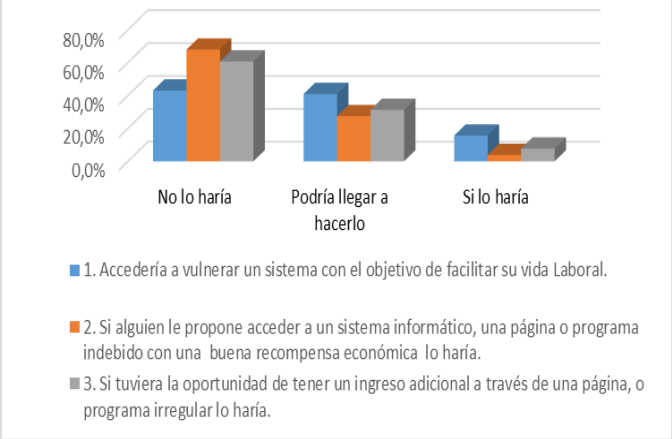

Fig. 1 Resultado Encuesta de Estudiantes para validar iniciativas de trabajar o realizar acciones a sistemas informáticos.

Después 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 para realizar un delito informático o que en ocasiones ya han realizado cierto tipo de ataques. Este resultado se puede ver en las Fig. 2 y Fig. 3.

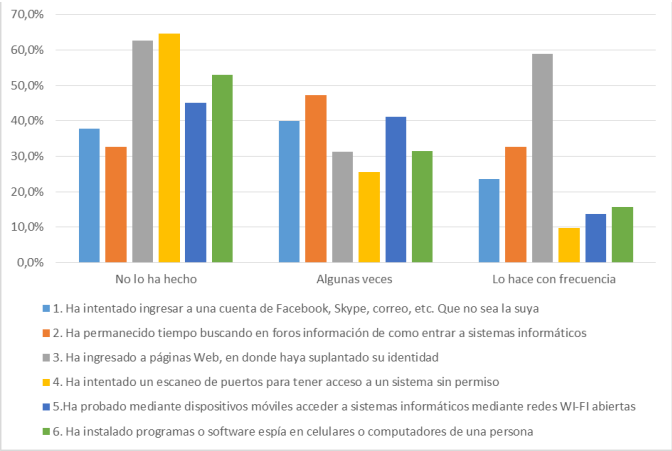

Fig. 2 Resultado Encuesta Estudiantes con conocimiento en realizar actos a sistemas informativos.

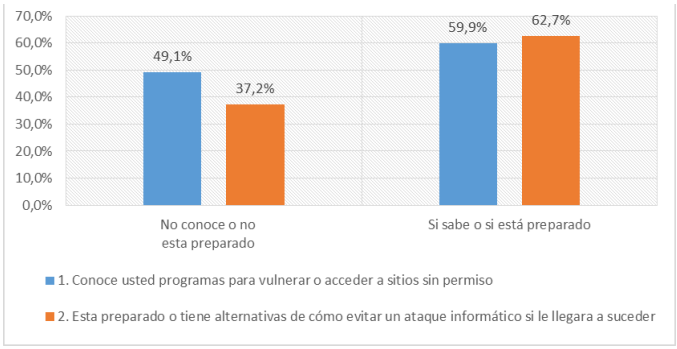

Fig. 3 Resultado Encuesta Estudiantes con conocimiento de programas para acceder a sitios sin permiso.

Con otro tipo 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 puede en la Fig. 4

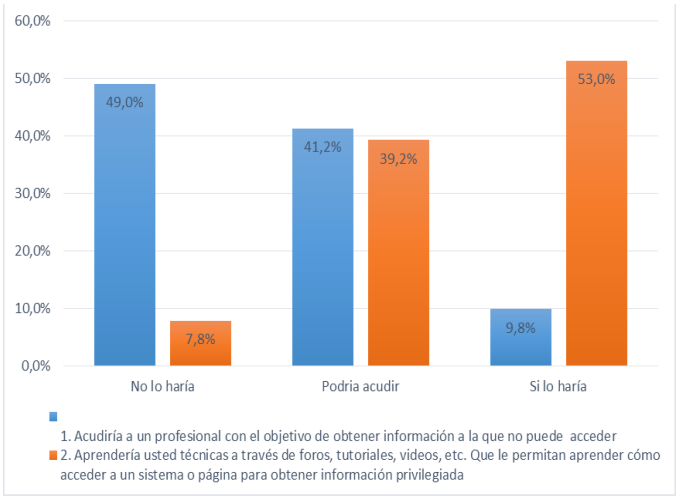

Fig. 4 Resultado Encuesta Estudiantes Preguntas para identificar jóvenes que aprenderían del conocimiento

Por último 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 Fig. 5.

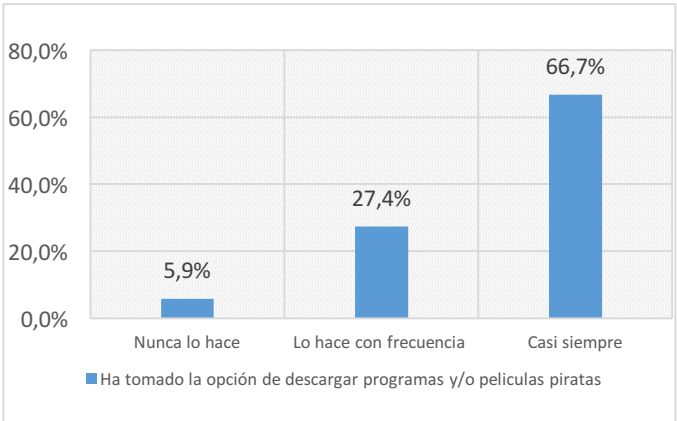

Fig. 5. Respuesta Estudiantes que consumen Software Pirata

978-1-5090-2435-3/16/$31.00 ©2016 IEEE

Es interesante como estudiantes de primero a quinto semestre dicen ya haber realizado y/o dicen conocer una o varias técnicas de vulnerabilidad ya sea indagando sobre software pirata para llegar a una meta propuesta o simplemente empezando a encontrar vulnerabilidades como claves de WI-FI o intentando ingresar con credenciales falsas a redes sociales como se aprecia en la Fig. 6.

De los 11 estudiantes que se encuentran en los semestres de 1 a 5 se identifica en la gráfica cuantos contestaron haber realizo dichas actividades en cada pregunta ya que en estos tiempos es donde un estudiante piensa que al estudiar este tipo de carreras puede llegar a aprender también de dichos temas, sin saber el daño que pueden causar o por el contrario pueden causarse si se meten en un acto delictivo.

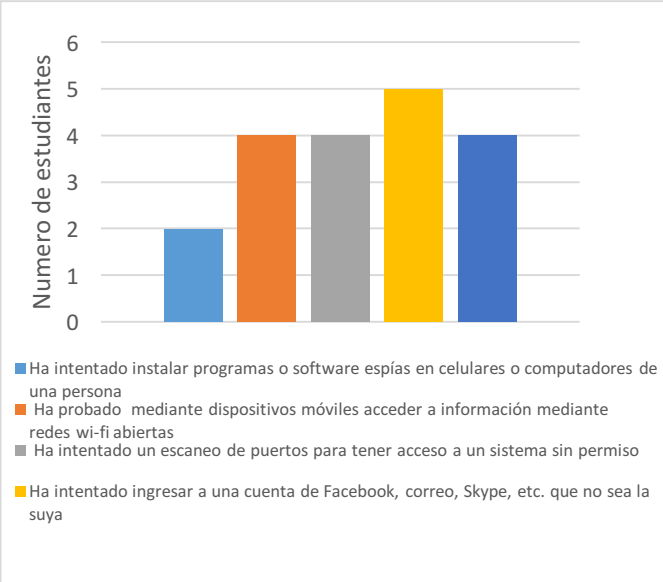

Fig. 6 Número de estudiantes que han realizo dichas actividades planteadas en las preguntas.

Estudiantes en semestres más avanzados como noveno, decimo y egresados de la universidad 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 y intentado ejecutar escaneo de puertos para acceder a sistemas sin permiso como se puede. Ver Fig. 9.

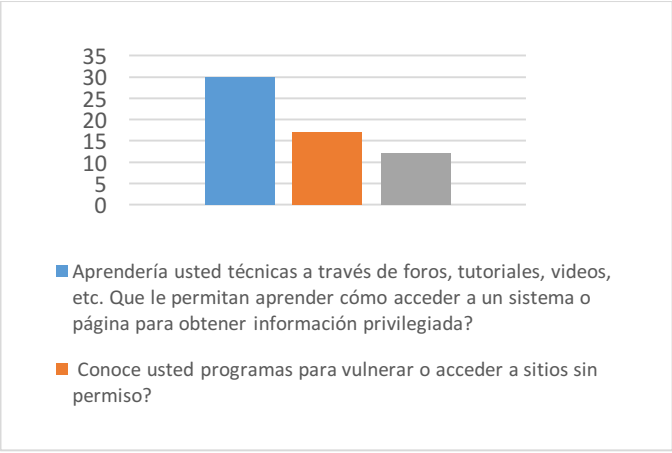

Fig. 7 Respuesta dadas por estudiantes de semestres entre 9, 10 y egresados.

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 las Fig. 8 y Fig. 9

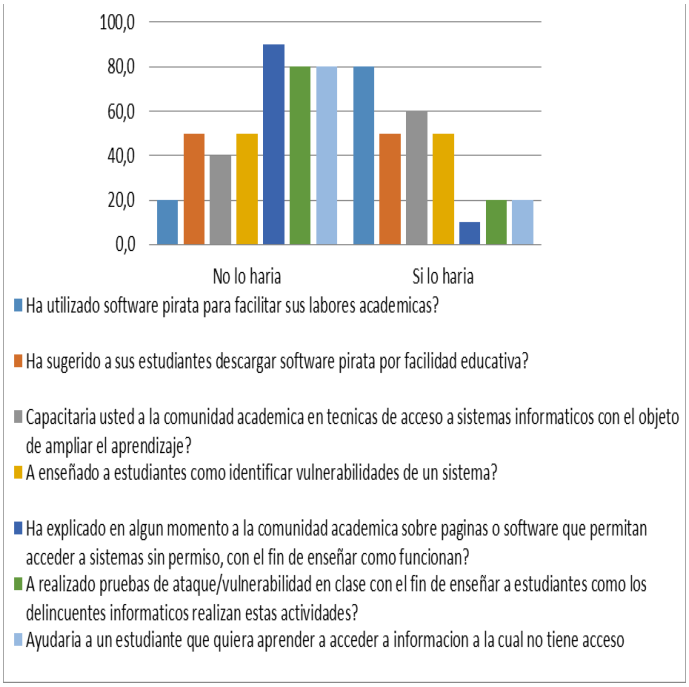

Fig. 8. Resultado Encuesta de Docentes para validar la influencia en estudiantes, para que realicen actividades relacionadas con la cultura hacker

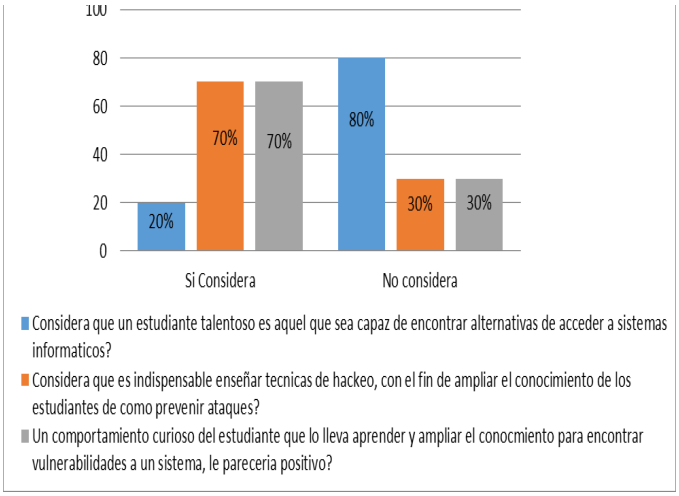

Fig. 9 Resultado Encuesta de Docentes para validar la influencia en estudiantes para que realicen actividades relacionadas con la cultura hacker

Y por ultimo con el segundo grupo de preguntas se quería identificar aquellos profesores que estimulan a los estudiantes para que utilicen

978-1-5090-2435-3/16/$31.00 ©2016 IEEE

sus habilidades de forma positiva. Para esto las preguntas y respuestas se observan en la Fig. 10.

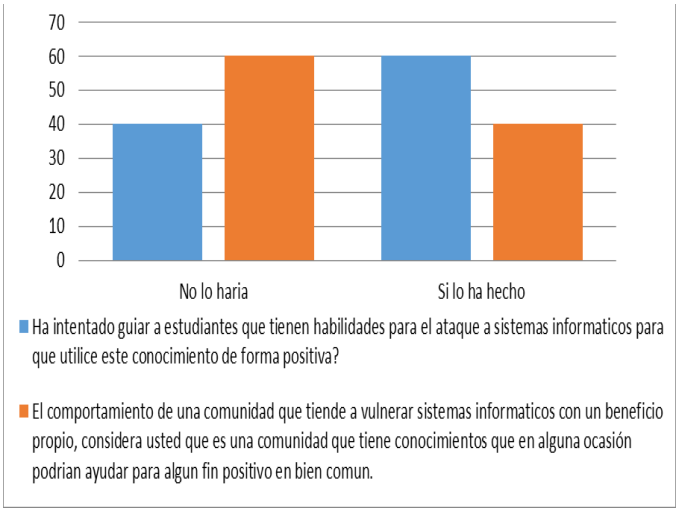

Fig. 10. Resultado Encuesta de Docentes, Preguntas para identificar docentes que influyen positivamente.

Para las entrevistas realizadas, se pudo observar que los entrevistados consideran que los delitos informáticos son cometidos por jóvenes entre 12 y 18 años y si lo hacen para tener beneficios económicos, que estos 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 acceder a estas informaciones, es por ello que se han masificado este tipo de delitos, igualmente expresaron que muchas veces los jóvenes sin querer hacer daño alguno con sus conocimientos, empiezan por explorar, por jugar y a lo último se dan cuenta que cometieron un delito y que perjudicaron alguna empresa, persona, etc. 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.

Una pregunta que se les realizo a estos expertos dada su experiencia diaria con empresas y consultores de seguridad, es 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.

Como lo nombra Álvaro Escobar para él la comunidad hacker ética es la que ha tenido mayor aumento en la sociedad Colombiana, el desarrollo de la policía ha realizado más mecanismos para la 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.

Una de las armas más poderosas para los hacker y con lo que tiene que diariamente enfrentarse el hacker ético es el descuido, que se ha vuelto incontrolable para los responsables de seguridad informática de las entidades financieras. 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, de allí y de la inocencia de estas personas es de donde se conoce la ingeniera social de un hacker que se vale en su mayoría de la inocencia de su víctima para sacar información con la que pueda llegar cometer un delito informático a beneficio del hacker.

Para evaluar la perspectiva de los dos expertos que además de trabajar en seguridad informática, 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 diaria, 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.

Entre las pregunta que validan como los delitos van en aumento en nuestros país, se quería saber si los medios de comunicación no dan relevancia a los delitos informáticos más allá de los que son más conocidos mediáticamente, 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, que muchos quieran seguir este camino dándoles un impulso más a personas jóvenes. Como se observa en la Fig. 11 los medios que más relevancia le dan a los delitos informáticos "son los medios impresos.

978-1-5090-2435-3/16/$31.00 ©2016 IEEE

Fig. 11. Grafica que muestra la relevancia que le dan los medios impresos a los delitos informáticos. [15]

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.

5. CONCLUSIONES Y TRABAJO FUTURO

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 observo 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 inicialmente con fines personales y a medida que aumentan en conocimiento, para terceros o para poner a prueba sus conocimientos y/o demostrar sus destrezas con fines económicos o de aceptación en grupos de la cultura hacker.

Las respuestas dejaron observar como muchos de los jóvenes que estudian éstas carreras ya entran con conocimiento propios de la cultura del haking, 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.

Como trabajos futuros se puede contemplar esta 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

6. REFERENCIAS

[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

[2] Lizama, Jorge Alberto. Hackers En El Contexto De La Sociedad De La Información. México. 2005. 81P.

[3] Raymond Eric S. Breve historia de la cultura hacker {En línea}. {2014, Septiembre25}.Disponible en: http://biblioweb.sindominio.net/telematica/historia-cultura-hacker.html.

[4] Colprensa, El País, En Colombia las Cifras de Delitos Informáticos Van en Aumento Millones {En línea}{2015, Enero 9}.Disponible en: http://www.elpais.com.co/elpais/judicial/noticias/colombia-cifras-delitos-informaticos-van-aumento.

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

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

[7] 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.

[8] 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

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

[10] 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#.

[11] 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)

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

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

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

[15] 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/

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

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

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

[19] Veloza Carolina. Conozca las dos nuevas modalidades de delitos informáticos. En línea}. {2013, Octubre 01} { 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

[20] Merriam- Webster, Hacke hacker {En línea}. {2015, Diciembre}. http://searchsecurity.techtarget.com/definition/hacker

[21] Entrevista realizada a ingeniero Álvaro Escobar, para Escucharla dar clik : https://youtu.be/Ngidx2IWonk

[22] Entrevista realizada a ingeniero Cesar Rodríguez https://www.youtube.com/watch?v=A1itj1vjxfc&feature=youtu.be

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

978-1-5090-2435-3/16/$31.00 ©2016 IEEE