INGENIERÍA SOCIAL, UN FACTOR DE RIESGO INFORMÁTICO INMINENTE EN LA UNIVERSIDAD COOPERATIVA DE COLOMBIA SEDE NEIVA

EDILBERTO BERMÚDEZ PENAGOS

UNAD
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
NEIVA
2015

INGENIERÍA SOCIAL, UN FACTOR DE RIESGO INFORMÁTICO INMINENTE EN LA UNIVERSIDAD COOPERATIVA DE COLOMBIA SEDE NEIVA

EDILBERTO BERMÚDEZ PENAGOS

Investigación para optar al título de Especialista en Seguridad Informática.

Director
Martín Camilo Cancelado Ruiz
Ingeniero

UNAD
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
NEIVA
2015

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Neiva 10 de junio de 2015

DEDICATORIA

Que sea esta la oportunidad de dedicar este trabajo a Dios por su generosidad y por llenarme de fe, sabiduría y paciencia, a mi esposa Zayda Liliana y a mi hija Laura Sofía por su compresión y sacrificio, y a mi madre Ruth y mis hermanos, todos; quienes con su apoyo incondicional y su motivación ayudaron a alcanzar este gran objetivo en mi vida.

AGRADECIMIENTOS

Es imposible negar que este trabajo contó con el esfuerzo, la dedicación y la colaboración de muchas otras personas, a quienes agradezco de todo corazón y exalto tan excelente labor, entre ellas: el director de trabajo de grado; Ingeniero Martín Camilo Cancelado Ruiz quien con sus conocimientos y apoyo constante me guio en todo este proceso hasta el punto de poder llevar a buen término esta investigación, a mis tutores de pregrado quienes también aportaron en mi formación profesional; en especial al Ingeniero Yhon Jerson Robles Puentes, a mis tutores de la especialización por enseñarme y trasmitirme tan valiosos conocimientos; sobre todo al Ingeniero Carlos Alberto Amaya Tarazona, la Ingeniera Eleonora Palta Velasco, al Ingeniero John Freddy Quintero y al Ingeniero Arturo Erazo.

A mi jefe en el departamento de Gestión Tecnológica, el Ingeniero Joaquín Emilio Gaitán Girón; quien siempre estuvo al pendiente de todo este trabajo y que no dudó en apoyarme y cederme el tiempo necesario para lograr este objetivo, y por supuesto, a la Universidad Cooperativa de Colombia sede Neiva y todo su personal, institución en la cual trabajo y sobre la que se ejecutó la presente investigación.

Muchas gracias a todos…

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE GRÁFICAS

pág.

LISTA DE ANEXOS

pag.

GLOSARIO

CIBER-DELINCUENTES: son aquellas personas que basados en conocimientos de informática, electrónica, programación y otros, usan las computadoras y las redes de comunicación para la comisión de algún delito.

DoS: es la sigla en inglés de *Denial* of *Service* (Denegación del Servicio). Hace referencia a un tipo de ataque informático en el que se bloquea o se da de baja algún servicio prestado a un usuario, por ejemplo, correo electrónico, telefonía, servicio de impresión, etc.

HACKER: son los mismos piratas informáticos. Personas que se dedican a romper la seguridad de los sistemas de información. Existen en la actualidad, diferentes puntos de vista para el uso de esta palabra y otras relacionadas.

MICROBLOGGING: es un servicio prestado a los usuarios en internet que les permite enviar y/o publicar cortos mensajes a través de una plataforma diseñara para ello. El ejemplo más común es Twitter.

OSINT: es la sigla en inglés de *Open Source Intelligence*. Traducido al español significa Inteligencia de Fuentes Abiertas. Se trata de la primera fase de un ataque informático, en la que se busca información del objetivo en fuentes públicas y abiertas, por ejemplo: google, directorio, etc.

PHISHING: es un tipo de ataque informático que busca la obtención de información confidencial de usuarios y organizaciones de manera fraudulenta.

POP – UP: son las ventanas o elementos emergentes utilizados en algunas páginas web. Estas son, por lo general, deshabilitadas por los mismos navegadores web.

SGSI: son las siglas de Sistema de Gestión de Seguridad de la Información. Este es un mecanismo utilizado por las organizaciones y orientado por normas y estándares internacionales, para asegurar los pilares de la información: Integridad, Disponibilidad y Confidencialidad.

SPAM: son un tipo de correo electrónico que no es solicitado por el usuario y que por lo general son publicitarios.

VIRUS: son un tipo de software o código malicioso que busca entorpecer el funcionamiento normal de una computadora sin el consentimiento del usuario y/o a la vez, apoderarse de la información de manera fraudulenta.

RESUMEN

La Ingeniería Social, como una metodología de ataque no convencional y basada en el engaño y la manipulación de usuarios para obtener información confidencial de empresas o individuos, ha venido dando pasos agigantados en el campo de la seguridad informática y se ha convertido en la principal herramienta de los ciber-delincuentes debido a los avances tecnológicos en esta área, los cuales han dejado rezagados a los métodos clásicos, haciendo cada vez más difícil su ejecución. Es por ello que se pretende hacer un paneo al tema de la seguridad de la información en la Universidad Cooperativa de Colombia sede Neiva; como una organización privada de educación superior, enfocado en las vulnerabilidades aprovechables por las técnicas enmarcadas dentro de la Ingeniería Social.

Es así que el objetivo de esta investigación pretende identificar todas las debilidades en la seguridad de la información dentro de la institución ya mencionada, relacionadas con la Ingeniería Social y determinando cuáles son las técnicas de ataque aplicables, principalmente al personal administrativo, a las zonas físicas y/o dependencias y a los sistemas de información. Para ello se utilizaron técnicas de recolección de datos como la observación, encuestas y entrevistas. Además, se realizó un ejercicio de ataque por medio de las herramientas de ingeniería social provistas en Kali Linux y Backtrack 5 r3 (sin soporte actual).

Esta investigación cuenta con un amplio marco referencial en donde se abarcan aspectos importantes como los antecedentes de ataques informáticos a distintas universidades alrededor del mundo, todas las definiciones y aclaraciones de los términos y conceptos de la seguridad informática y de la información, los tipos de Ingeniería Social y cada una de sus técnicas, además de las diferentes figuras de atacantes y ataques a la seguridad de la información. Por último, y por ello no menos importante, las recomendaciones para evitar ser víctimas de la Ingeniería Social dentro de los entornos laborales y por supuesto, las normativas legales relacionadas con los delitos informáticos en Colombia.

Al final, basándose en la información ya analizada y tabulada, se lanzan una serie conclusiones acordes a los hallazgos de la investigación y, de paso, se genera un conjunto de recomendaciones que buscan corregir las fallas encontradas y aumentar la seguridad de la información en la institución, forjando una cultura de protección de los datos y de buenas prácticas de usuario en el recurso humano de la universidad.

Palabras clave: Ingeniería Social, seguridad informática, ciber-delincuente, “*hacker*”, “*crackers*”, “*sniffers*”, “*spammers*”, “*pentesters*", estafadores confidencialidad, integridad, disponibilidad, protección, virus, “*phishing*”, delito informático, SET “*Social-Engineering Toolkit*”.

INTRODUCCIÓN

La presente investigación es de tipo descriptivo y hace referencia a un tema que, aunque no es nuevo, si ha venido ganando espacio hoy por hoy en los ambientes laborales empresariales. Se trata de la Ingeniería Social. Su objetivo es engañar a los usuarios para obtener su información o la de sus empresas, con el fin de conseguir algún tipo de beneficio para quien la practica, ya sea económico, político o religioso.

La Ingeniería Social no es exactamente una ciencia pero, si está sustentada sobre algunos principios psicológicos propios de los seres humanos, a partir de los cuales se han desarrollado una serie de técnicas o métodos encaminados a obtener beneficios ilegítimos en función de la ingenuidad, necesidad, avaricia o compasión de las personas en situaciones específicas.

Este fenómeno se magnifica cuando su accionar se centra en los sistemas informáticos empresariales, propios de la sociedad actual, en donde la información, valiosa o no, está siempre al alcance de los entes autorizados para tratarla pero, al mismo tiempo, está expuesta a agentes externos o internos que la desean obtener de manera fraudulenta. Por esta razón, la Ingeniería Social también se aplica a los sistemas computarizados a través de herramientas diseñas específicamente para ello, evidenciándose así su avance en la ciberdelincuencia.

A raíz de esto, nació la necesidad de indagar sobre este avance de la Ingeniería Social, teniendo como base la Universidad Cooperativa de Colombia sede Neiva, una institución privada de educación superior y de gran prestigio en la región. Está claro que las empresas, independientemente del sector económico en el que se ubiquen, están cada vez más expuestas a amenazas contra la seguridad de su información, corriendo el riesgo de perder dinero, clientes y otros activos.

Es por ello que esta investigación pretende visibilizar el tema de la seguridad informática dentro de la institución en mención, haciendo énfasis en las estrategias de ataque propias de la Ingeniería Social e identificando las vulnerabilidades existentes en el recurso humano de la universidad y sus áreas de trabajo, a fin de inferir una serie de recomendaciones en pro de la seguridad de la información que allí se produce y almacena, y que garanticen su disponibilidad, confidencialidad e integridad.

El resultado de este ejercicio se obtuvo gracias al empleo de técnicas como la observación, aplicada a través de recorridos de reconocimiento por las diferentes áreas físicas de la institución; detallando aspectos como la ubicación de los equipos de cómputo y cámaras de seguridad. Además, se contó con la experiencia adquirida a través de 6 años de trabajo en el departamento de Gestión Tecnológica por parte del investigador, lo que lo convierte en participante directo de los procesos de trasformación y principal conocedor de las necesidades, ventajas y desventajas de los activos tecnológicos de la universidad. Por otra parte, también se obtuvo información relevante a través de un cuestionario diseñado para medir la precepción y los conocimientos del personal de la institución entorno a los temas de seguridad informática y de la información.

Finalmente, el trabajo se estructura con un marco referencial que incluye unos antecedentes; en donde se indagó sobre ataques perpetrados a instituciones de educación superior en el mundo, un marco teórico; en el que se relacionan todos los aspectos concernientes a la seguridad informática, de la información y aquellos más relevantes de la Ingeniería Social. Un marco legal que detalla las normas y leyes colombianas relacionadas con los delitos informáticos, además de un vistazo general de este aspecto alrededor del mundo, y una radiografía completa de la Universidad Cooperativa de Colombia sede Neiva; como la institución donde se ejecutó esta labor investigativa. También, hay una sección donde se comentan todos los temas relacionados con la estructura de esta investigación, los resultados y evidencias del proceso investigativo y, por supuesto, las respectivas conclusiones y recomendaciones.

1. FORMULACIÓN DEL PROBLEMA

Todas las organizaciones en el mundo tienen un activo que proteger. La información. En décadas anteriores y en países desarrollados como Estados Unidos, Canadá, Alemania y Rusia; por nombrar algunos, se logró identificar que la principal causa de vulnerabilidades a la información de las grandes empresas, públicas o privadas, era el recurso humano y no los recursos tecnológicos, como se pensó en su momento. Aun hoy, las empresas en el mundo no son ajenas a las fallas de seguridad que sus empleados pueden causar, lo que se condensa en una falta de cultura alrededor de la información. Por ello es importante reconocer que ya no son los virus, gusanos o troyanos los causantes de la pérdida o fuga de información en los ambientes informáticos empresariales o familiares, sino el uso y ejecución de las diferentes técnicas, modalidades o métodos enmarcados dentro de la Ingeniería Social (en adelante IS).

En consecuencia, se evidenció la necesidad de indagar sobre qué tanto saben o conocen las personas del área administrativa de la Universidad Cooperativa de Colombia sede Neiva (en adelante UCC Neiva), sobre la IS, sus objetivos, modos de operación y, por supuesto, sus consecuencias sobre la integridad, disponibilidad y confidencialidad de la información producida, almacenada y trasportada por los medios dispuestos por la institución, todo ello a fin de identificar las vulnerabilidades relacionadas con la seguridad de la información; específicamente aquellas que explota la IS, y de determinar, adicionalmente, el nivel de afectación que podría tener la materialización de este tipo de amenaza sobre las actividades y recursos de la universidad.

Teniendo en cuenta lo descrito anteriormente y como punto de partida dentro de este proceso investigativo, se formula la siguiente pregunta:

¿Cuáles son las vulnerabilidades más comunes en la seguridad de la información y que hacen factible un ataque de Ingeniería Social al personal del área administrativa de la Universidad Cooperativa de Colombia sede Neiva?

2. JUSTIFICACIÓN

En vista de que el eslabón más débil dentro de la cadena de seguridad de la información es el ser humano, se han venido fomentando los ataques informáticos a través de la IS y sus diferentes metodologías en países como el nuestro. Así las cosas, la UCC Neiva; como una institución de educación superior seriamente constituida y perteneciente a uno de los sectores económicos más grandes del país, el de la economía solidaria, no es ajena a esta problemática, la cual se puede ver beneficiada por aspectos meramente culturales propios de los espacios geográficos. Un ejemplo de ello es la falta de interés, generalizado en los empresarios de la ciudad de Nieva, en los aspectos relacionados con la seguridad de la información y la gestión de TI. Estos temas son, más bien, de reciente crecimiento y acogida dentro de la comunidad neivana en general.

Por otra parte y teniendo en cuenta que la problemática de la IS y su vertiginoso avance en nuestra sociedad sigue siendo un tema poco abordado en el campo empresarial, se evidenció la necesidad de investigar sobre cuáles podrían ser los escenarios más apropiados para la ejecución de un ataque de IS dentro de la UCC Neiva, identificando a su vez las áreas administrativas más vulnerables y el personal más propenso o expuesto a sufrir este tipo de agresión. Así mismo, es importante comprobar el nivel de apropiación que tiene el personal administrativo de la institución frente a temas de seguridad de la información relacionados directamente con sus labores diarias, enfocándose en la problemática ya mencionada, la cual, a pesar de no ser novedosa, si promete un mayor impacto dentro de los ambientes laborales actuales.

Por tal razón se hace importante el reconocimiento, primero; de que la información es el activo más importante que tiene una organización, junto con el recurso humano, y de que se le debe brindar la protección necesaria y pertinente para mantenerla resguardada de cualquier ataque. Y segundo, que como dicha información es tan importante, siempre va a existir quien la quiera obtener de forma no autorizada y en este sentido, se deben identificar cada una de las vulnerabilidades de los sistemas de seguridad de la institución frente a la protección de la información.

De la misma forma, se hace necesario que el personal administrativo de la UCC Neiva reconozca cada una de las formas de vulnerar la seguridad de la información a través de la IS y que se genere una cultura de responsabilidad frente al manejo y administración de la misma, así ésta no sea sensible para los procesos de la organización. Si se logra que los administrativos de la UCC Neiva alcancen un nivel de conciencia apropiado ante la información que manejan a diario, eso sí; sin rayar en lo paranoico, se obtendrá un nivel de seguridad muy alto en el recurso humano y se garantizarán la integridad, la disponibilidad y la confidencialidad de la información de la organización.

3. ALCANCE Y LIMITACIONES

En pro de dar cumplimiento al objetivo general planteado para este proyecto, se pretende indagar sobre las principales metodologías que desde la IS repercuten en la seguridad de la información de una organización o empresa, para este caso; la UCC Neiva. Es por ello que esta investigación pretende identificar las áreas y el personal más expuestos a los ataques de la IS, y por supuesto, las vulnerabilidades que permiten la existencia, desarrollo y/o materialización de este tipo de amenaza.

Como consecuencia de esta labor investigativa, las directivas de la organización deberán identificar y replantear el valor de la información que ésta produce, exporta, administra y capta, y a la vez, pensar en el establecimiento de políticas serias y concretas relacionadas con la seguridad de la información, políticas dentro de las que la capacitación constante y permanente en temas de seguridad informática sean una prioridad.

Aunque sería lo más apropiado,no es tarea de este ejercicio la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI), puesto que ello implicaría un proceso más riguroso, de más cuidado y de un total apoyo por parte de las directivas de la organización. Lo que sí se pretende, es que los resultados de esta investigación sean la base para que en el futuro se logre implantar uno de estos sistemas inicialmente con áreas específicas de la institución como: recepción, tesorería, registro y control, decanaturas o coordinaciones y sus respectivas secretarías de programa; todas con atención directa al público, con el propósito de generar una cultura de responsabilidad y de cuidado frente al manejo y la administración de la información de la UCC Neiva.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Identificar las vulnerabilidades frente a los ataques de IS de las diferentes zonas, dependencias, plataformas y personal administrativo de la UCC Neiva, ejecutando una serie de pruebas y aplicando métodos de recolección de datos, para disminuir el riesgo y la probabilidad de fallas en la seguridad de la información.

4.2 OBJETIVOS ESPECÍFICOS

- Identificar cuáles de las diferentes técnicas o modalidades de ataque de la IS son las más factibles de aplicar en las instalaciones de la UCC Neiva y en su personal administrativo.

- Determinar cuáles son las áreas administrativas más vulnerables ante un ataque de IS y quiénes de sus integrantes presentan una mayor exposición a este tipo de amenaza.

- Descubrir la configuración de los diferentes escenarios dentro de la UCC Neiva que hacen inminente un ataque de IS a su personal administrativo.

- Visibilizar, a través de la IS, las posibles fallas en seguridad de la información que posee la UCC Neiva.

- Evaluar las posibles consecuencias que puede acarrear un ataque de IS a través de alguno de sus mecanismos dentro de la UCC Neiva.

- Demostrar que con información básica como un nombre o un número de teléfono, el delincuente informático puede acceder, de manera fraudulenta, a los sistemas de información de la empresa.

- Describir los procedimientos y recomendaciones para evitar ser víctima de la IS y sus metodologías.

5. MARCO REFERENCIAL

5.1 ANTECEDENTES

En medio de la evolución de la web 1.0 a la web 2.0 y sus sociedades de la información y del conocimiento, hasta la web 3.0 y su nuevo concepto de web semántica, se han desarrollado en la misma medida riesgos en la red, como *hackers*, virus, *OSINT*, *DoS* y otros tipos de ataques, no tan ortodoxos, ejecutados a través de técnicas como la IS, en donde toda clase de usuarios, organizaciones y empresas se han visto inmersos y, por supuesto, afectados por este tipo de amenaza.

Dando un vistazo al pasado en el desarrollo de la seguridad de la información, "se dice que el primer ataque informático de la historia se produjo un viernes 13 del año de 1989. Una revista especializada regalaba disquetes promocionales, los cuales resultaron infectados por un virus que afectó a decenas de empresas y particulares"[1]. Al tiempo, "nace el virus "*Dark avenger*" que causa un daño lento en el sistema operativo, y en ese mismo año, IBM comercializa el primer programa antivirus"[2] en el mercado, lo que puso en perspectiva un panorama que prometía generar grandes ganancias. El de la protección de la información.

Actualmente existen diferentes maneras de propagar un virus, así como de ejecutar ataques informáticos a través de modalidades más efectivas y en donde los ciber-delincuentes hacen caer a sus víctimas. Para ser más puntuales respecto a este tipo de ataques y al ámbito de esta investigación, se pueden mencionar algunos sufridos por instituciones de educación superior de todo el mundo, incluyendo el que afectó en 2008 a la Universidad Surcolombiana "USCO", una de las universidades con mayor reconocimiento en la región sur de nuestro país. "El hecho ocurrió a finales de diciembre pasado en Neiva, capital del Huila (sur), donde los "*hackers*", tres estudiantes de Ingeniería Civil, dos de Ingeniería Electrónica y uno de Ingeniería Agrícola, menores de 25 años, accedieron a los sistemas de la Universidad Surcolombiana, declaró el rector, Hernando Ramírez"[3]. Un total de 366 calificaciones fueron modificadas entre el 22 y el 31 de diciembre del 2008 aprovechando el periodo de vacaciones en el claustro, pero lo más curioso, es que todo se ejecutó desde un café internet de la zona y con

[1] RAMÍREZ SANDOVAL, Jorge Iván; DÍAZ MARTÍNEZ, José Vicente y GARIZURIETA MEZA, Miguel Hugo. "Ingeniería Social, una amenaza informática". Scrib [en línea], septiembre 2009 [citado en 3 febrero de 2014]. Disponible en Internet: http://es.scribd.com/doc/19394749/Ingenieria-social-una-amenaza-informatica>.

[2] FICARRA, Francisco. "Los virus informáticos: Entre el negocio y el temor". Revista Latinoamericana de Comunicación CHASQUI [en línea], junio 2002 [citado en 5 mayo de 2015]. Disponible en Internet: <http://www.redalyc.org/articulo.oa?id=16007810>. ISSN 1390-1079.

[3] INFORMADOR.MX. "Estudiantes "hackean" calificaciones de su Universidad" [en línea], febrero 2009 [citado en 7 mayo de 2015]. Disponible en Internet: <http://www.informador.com.mx/internacional/2009/75916/6/estudiantes-hackean-calificaciones-de-su-universidad.htm>.

herramientas muy básicas o nada sofisticadas, cosa que indica que ya contaban con información suficiente para poder acceder al sistema de notas.

Otro caso también muy sonado y difundido en los medios de comunicación tradicionales y en las redes sociales ocurrió el pasado martes 17 de marzo de 2015, cuando fueron "hackeadas" las cuentas de correo electrónico de los candidatos a la rectoría de la Universidad Nacional de Colombia, desde las cuates fueron enviados mensajes subidos de tono a estudiantes, uno de ellos decía: "Deseo invitarlos formalmente a participar esta tarde para emborracharnos con Mujerzuelas, juegos de azar; a ver mi página web donde no hay porno pero si podrán disfrutar de mis videos"[4]. Otra prueba más de que los ciber-delincuentes están a la orden del día.

Pero este fenómeno no es ajeno a países donde existe una mejor infraestructura tecnológica y altos controles en cuanto a seguridad informática se refiere; Chile, EE.UU y Brasil son algunos ejemplos. En el país austral, según reporte del diario La Tercera en su portal de internet, piratas informáticos lograron "hackear" el sitio web de La Pontifica Universidad Católica de Chile, "en la cual se pudo ver por un largo rato varios enlaces a sitios de pornografía. Aunque el ataque era prácticamente imperceptible a la vista, pues los enlaces estaban ofrecidos a través de una fuente pequeña y en un lugar no muy visible, las redes sociales fueron las encargadas de difundirlo…"[5].

También se han visto gravemente afectadas por ataques a sus sistemas de información las universidades más reconocidas e importantes de los EE.UU, en los cuales no se buscaba solamente vulnerar dichos sistemas y dejar una huella por simple sabotaje, sino, que se pretendía obtener la mayor cantidad de información posible de los estudiantes y administrativos con fines oscuros. Una serie de artículos publicados por Netmedia.mx en su revista electrónica semanal b:Secure dejan en evidencia, no solo el aumento de los ataques informáticos contra las universidades en EE.UU, sino también, lo agresivo de sus pretensiones. El primero de estos artículos se publicó en agosto del 2012, en el cual se informaba que la Universidad de Carolina del Sur había sido "hackeada". En total se perdieron 34.000 registros con información personal, incidente al cual las directivas dieron la importancia requerida, a tal punto, que se decidió contratar "a la compañía Kroll para asegurarse que las víctimas no sufran intentos de fraude con la información robada"[6]. Cabe resaltar que Kroll es una compañía de

[4] EL ESPECTADOR. "Hackean cuentas de correo de candidatos a rectoría de la Universidad Nacional" [en línea], marzo 2015 [citado en 7 mayo de 2015]. Disponible en Internet: <http://www.elespectador.com/noticias/educacion/hackean-cuentas-de-correo-de-candidatos-rectoria-de-uni-articulo-549936>.

[5] LA TERCERA. "Hackean página web de la Universidad Católica con sitios pornográficos" [en línea], marzo 2012 [citado en 7 mayo de 2015]. Disponible en Internet: <http://www.latercera.com/noticia/nacional/2012/03/680-437360-9-hackean-pagina-web-de-la-universidad-catolica-con-sitios-pornograficos.shtml>.

seguridad y que el costo de este desastre para la USC no se refleja únicamente en su economía, sino también, en su imagen y prestigio.

En octubre del 2012, tan solo un par de meses después, b:Secure publica un artículo en donde anuncia que más de 50 universidades de los EE.UU fueron víctimas de un grupo de "*hackers*" llamado ***GhostShel***, los cuales filtraron información como "nombre, correo electrónico, contraseña, dirección postal y teléfono de más de 120.000 estudiantes y miembros administrativos de las instituciones educativas"[7], entre ellas: Harvard y Princeton.

La Universidad de Stanford fue otra de las afectadas en la confidencialidad de su información, pues en julio del 2013, según artículo divulgado también por b:Secure, "*hackers*" obtuvieron datos confidenciales de los integrantes de la institución. En este caso, "como medida de precaución a raíz de una violación evidente en la infraestructura de tecnologías de la información, la Universidad de Stanford pide a todos los titulares de cuentas actualizar sus contraseñas"[8]. Según se informó en el mismo artículo, es muy posible que los datos hurtados se pudieran usar para robar identidades y para la sustracción de claves de acceso a cuentas con mayor valor.

Brasil es el último país en este recorrido por los ciber-ataques más trascendentes a distintas universidades en el mundo, los cuales exponen un panorama claro y concreto frente al tema de la seguridad informática en este tipo de instituciones. Según informó la Agencia EFE[9] a través de la página web de Caracol Radio el día 17 de enero de 2015, dos portales de la Universidad Federal de Río de Janeiro (UFRJ) fueron atacados por un grupo de piratas informáticos, presuntamente yihadistas, que publicaron mensajes de protesta por el "irrespeto al profeta Mahoma" y amenazas contra el Estado de Israel. La siguiente es la imagen que se pudo observar en los dos sitios web de esta universidad ese día:

---

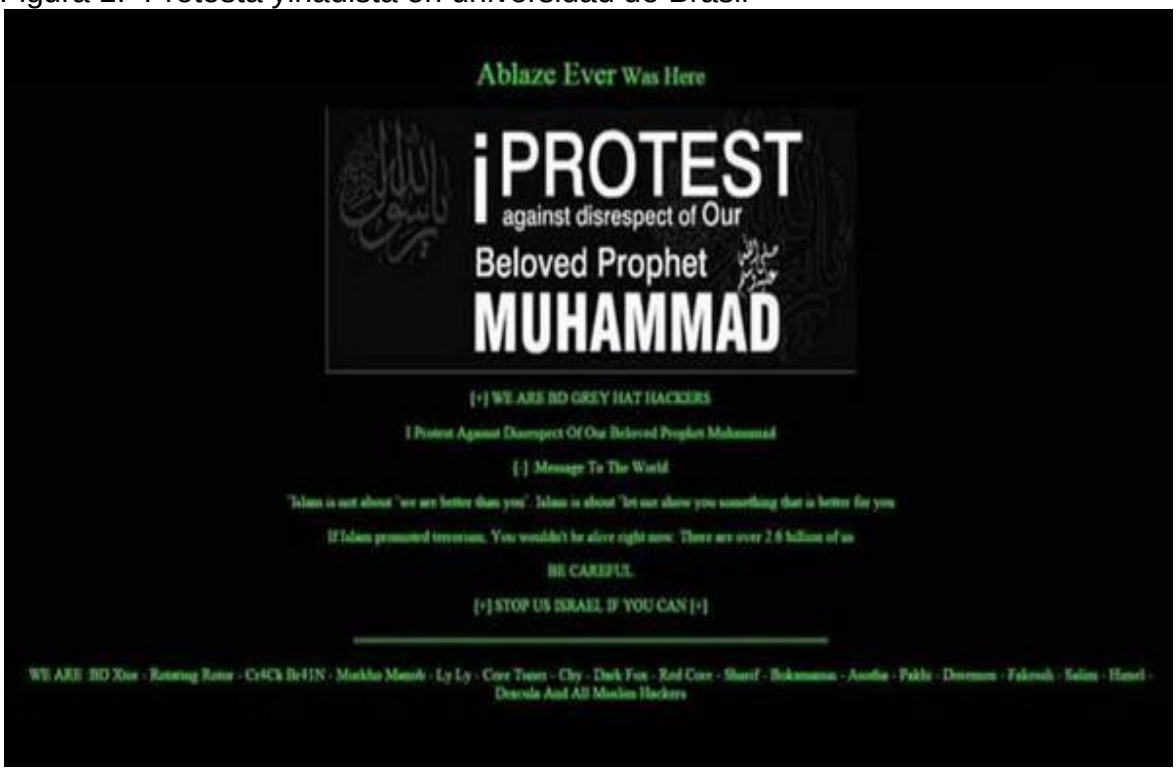
[6] ÁLVARREZ, Ángel. "Hackean la Universidad de Carolina del Sur, roban datos de 34,000". b:SECURE [en línea], agosto 2012 [citado en 7 mayo de 2015]. Disponible en Internet: <http://www.bsecure.com.mx/featured/hackean-la-universidad-de-carolina-del-sur-roban-datos-de-34000/>.

[7] B:SECURE. "Hackers filtran datos de Harvard, Stanford y Princeton" [en línea], octubre 2012 [citado en 7 mayo de 2015]. Disponible en Internet: <http://www.bsecure.com.mx/featured/hackers-filtran-datos-de-harvard-stanford-y-princeton/>.

[8] B:SECURE. "Hackean a la Universidad de Stanford para hurtar datos de su sistema" [en línea], julio 2013 [citado en 7 mayo de 2015]. Disponible en Internet: <http://www.bsecure.com.mx/featured/hackean-a-la-universidad-de-stanford-para-hurtar-datos-de-su-sistema/>.

[9] AGENCIA EFE. "Supuestos yihadistas piratean dos portales de una universidad brasileña" [en línea], enero 2015 [citado en 7 mayo de 2015]. Disponible en Internet: <http://www.caracol.com.co/noticias/internacionales/supuestos-yihadistas-piratean-dos-portales-de-una-universidad-brasilena/16173/nota/2591949.aspx>.

Figura 1. Protesta yihadista en universidad de Brasil



Fuente: https://twitter.com/Hera_Noticias/status/556582034886246400/photo/1

En efecto y después de reconocer los objetivos, pretensiones y consecuencias de estos ataques, es posible afirmar que las universidades son instituciones muy fáciles de vulnerar, pues son muchos los tipos de usuarios que se conectan a sus redes de datos y que poseen cuentas legitimas para acceder a sus sistemas de información, sin dejar a un lado la variedad de dispositivos móviles a través de los cuales se puede acceder a internet y a redes sociales, tales como: computadores portátiles, tabletas, Smartphones, consolas de juegos, cámaras digitales, etc., todos ellos elementos que facilitan la labor de los delincuentes informáticos, junto con otros factores como el no brindar la importancia y relevancia necesarias a la seguridad de la información por parte de las directivas, el no destinar recursos económicos suficientes a los departamentos de TI para apoyar su gestión, y la falta de capacitación, inicialmente, en el personal de dicha dependencia.

Esta serie de desatinos en las organizaciones ha dado pie al desarrollo de otros vectores de ataque enfocados a obtener información sensible de forma menos técnica pero igual de eficiente, y no necesariamente dependientes de una computadora. Este es el punto de partida de la IS, convertida en el arma principal

de los ciber-delincuentes como consecuencia del desarrollo de hardware y software más robustos y seguros; con implementaciones de sistemas de seguridad nativos, además del desarrollo y aplicación de diferentes técnicas de encriptación, de comunicaciones seguras a través de protocolos como SSH o HTTPS, de algoritmos criptográficos como AES, 3DES y DSA, y de sistemas de seguridad física y perimetral; como los mecanismos biométricos de identificación. El resultado final advierte del rezago en que quedó el único elemento en la cadena se seguridad de la información con mayores vulnerabilidades y menores posibilidades de protección. El recurso humano.

5.2 MARCO TEÓRICO

Es el ser humano el eslabón más débil de toda la cadena de seguridad de la información dentro de una organización y, como es evidente, todas las compañías o empresas basan su funcionamiento u objetivo comercial en sus trabajadores, factor que a su vez es el de mayor abandono o rezago frete a temas de seguridad informática.

En este punto vale la pena identificar la diferencia entre dos de los términos que encierran en gran medida el tema de esta investigación, ellos son: **seguridad de la información y seguridad informática**. "La Seguridad de la Información se puede definir como un conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información"[10]. Por otra parte, la seguridad informática "consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio"[11]. Es claro que el primero de estos dos conceptos es mucho más amplio que el segundo puesto que no se limita a los temas estrictamente tecnológicos. A continuación se detallan también algunos otros términos.

Confidencialidad: "se trata de la cualidad que debe poseer un documento o archivo para que este sólo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado"[12].

[10] MIFSUD, Elvira. "Introducción a la seguridad informática" [en línea]. [Madrid, España]: Observatorio Tecnológico, marzo 2012 [citado en 8 mayo de 2015]. Disponible en Internet: <http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1>.

[11] Ibid., p. 2.

[12] COSTAS SANTOS, Jesús. Seguridad Informática. Madrid: Ra-Ma, 2014. 301 p. ISBN 978-84-9964-313-7.

Integridad: “es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original”[13].
Disponibilidad: la NTC-ISO/IEC 27001[14] la define como aquella cualidad de la información que le permite ser accesible y utilizable solo por una entidad autorizada.

Figura 2. Principios de la Seguridad Informática

Autenticidad: se puede definir como aquella propiedad a través de la cual se puede comprobar quién es el autor o generador de la información.

Fiabilidad: es entendida como la probabilidad de que un sistema no presente fallas.

No repudio: “o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación”[15]. Así entonces, existen dos tipos de no repudio: el no repudio en el origen; en donde el emisor de la información no puede negar su envío, y el no repudio en el destino; en el cual el receptor no puede negar que recibió la información.

---

[13] Ibid., p. 25.
[14] INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información (SGSI). Requisitos. NTC-ISO/IEC 27001. Bogotá D.C.: El Instituto, 45 p.

[15] COSTAS SANTOS, Op. cit., p. 28.

Autorización: proceso mediante el cual una entidad concede los permisos necesarios a un usuario, programa o servicio para ejecutar una tarea específica.

Volviendo el tema central de esta labor investigativa, se ha encontrado un informe en el sitio web del diario argentino La Nación, elaborado por la consultora Deloitte y denominado "Encuesta Global 2007 de Seguridad & Privacidad", en el que se revela que los bancos de ese país denuncian un crecimiento importante de los delitos informáticos relacionados con el "*home banking*" o banca en línea. Según la encuesta, "el 80% de los ataques informáticos se deben a errores relacionados con el factor humano y no a temas específicos de tecnología"[16], dato que corrobora el avance de la IS, no solo en Argentita, sino también, en el resto de países latinoamericanos y del mundo, pudiéndose inferir, además, que desde la fecha del estudio en mención a hoy, este tipo de ataques pudo aumentar, teniendo en cuenta el uso masivo de dispositivos móviles y la consolidación del comercio electrónico. Entonces**, ¿qué es la Ingeniería Social?**

En principio, es posible afirmar que es una técnica sustentada en el engaño y que pretende aprovecharse de las debilidades de los seres humanos, aplicable en cualquier aspecto de la vida cotidiana. Situaciones tan comunes como la del niño que manipula a sus padres para obtener lo que quiere, la del político que persuade a las masas para alcanzar una curul, o la del doctor que convence a su paciente de consumir X o Y medicamento o tratamiento en pro de su salud, son muestra del poder de la IS, claro; cada una con resultados y objetivos distintos.

En el libro ***Social Engineering: The Art of Human Hacking*** (Ingeniería Social: El Arte Del Hacking Personal), Christopher Hadnagy define la ingeniería social como "el acto de manipular a una persona para que tome una acción que puede, o no, ser objeto de su interés. Esto puede incluir la obtención de información, acceso, o consecución de un objetivo específico"[17].

Cristian Borghello[18], *Technical & Educational Manager* de ESET para Latinoamérica, aclara que el objetivo de la IS es lograr la confianza de las personas para luego manipularlas y engañarlas en pro del beneficio propio de quien la implementa, al mismo tiempo, plantea que la IS puede definirse como una acción o conducta social destinada a conseguir información de las personas cercanas a un sistema.

[16] BINI, Rafael. "El 80% de los ataques informáticos se debe a errores de nosotros mismos" [en línea]. Buenos Aires: lanacion.com, noviembre 2007 [citado en 8 mayo de 2015]. Disponible en Internet: < http://www.lanacion.com.ar/960802-el-80-de-los-ataques-informaticos-se-debe-a-errores-de-nosotros-mismos>.

[17] HADNAGY, Christopher. Social Engineering: The Art of Human Hacking. Indianápolis: Wiley Publishing, Inc, 2010. 477 p. ISBN 978-0-470-63953-5.

[18] BORGHELLO, Cristian. "El arma infalible: la Ingeniería Social" [en línea], abril 2009 [citado en 8 mayo de 2015]. Disponible en Internet: <http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf>.

Desde un punto de vista más general, “hace referencia a la capacidad de algo o alguien para influenciar la conducta de un grupo de personas. En el contexto de la seguridad de computadoras y redes, la ingeniería social hace referencia a una serie de técnicas utilizadas para engañar a los usuarios internos a fin de que realicen acciones específicas o revelen información confidencial”[19]. Es un método nada técnico de intrusión que atenta contra los procesos de seguridad implantados en las organizaciones.

Pasando a la práctica, un ingeniero social utiliza comúnmente el teléfono o Internet para engañar a la gente. Entre otras cosas puede fingir ser, por ejemplo, un empleado de algún banco o alguna otra empresa, un compañero de trabajo de otra sede o sucursal, un técnico o un cliente. Vía Internet utiliza el método del envío de solicitudes de renovación de permisos de acceso a páginas web, crean memos falsos que solicitan respuestas e incluso las famosas “cadenas”, llevando así a los usuarios a revelar información sensible, o a violar las políticas de seguridad establecidas en su organización. Con este método, los ingenieros sociales **“explotan”** la tendencia natural de la gente a querer ayudar.

El radio de acción de la IS es verdaderamente amplio, el cual se enfoca en el recurso humano de las empresas, donde es normal encontrar diferentes tipos de personas, con cargos de mayor o menor responsabilidad. Dentro de ellas, los empleados pretenden siempre quedar bien y por tal razón, brindan información sensible sin ninguna restricción a quien la solicite. También están aquellos con pocos conocimientos en informática o que ignoran la existencia de los diferentes tipos de amenazas, y por lo general, la gran mayoría no entienden de temas de seguridad de la información y desconocen, o no se interesan, por las políticas empresariales respecto al tema. Vale la pena decir que las compañías, grandes o pequeñas, también fallan al no implementar, al menos, controles básicos de seguridad informática que apoyen los procesos de protección de la información. La razón principal por la que esto ocurre es que las directivas creen que la prevención de; o solución a los incidentes de seguridad son demasiado costosos.

> De los millones de usuarios de informática, sólo un 1 por 100 son expertos o cuentan con una elevada cualificación técnica. El otro 99 por 100, una cifra abrumadora de millones de usuarios, aun pudiendo ser expertos en sus respectivas áreas de especialización, desconocen el funcionamiento interno de los ordenadores, ignoran las sutilezas de su cultura digital y carecen del bagaje tecnológico para llegar al fondo de muchos de sus procesos y protocolos. El

[19] COSTAS SANTOS, Op. cit., p. 205.

> blanco de la ingeniería social lo constituye precisamente este 99 por 100, la gran masa de usuarios de informática[20].

"Independientemente de la razón que sea, ignorancia, negligencia o coacción, los empleados pueden permitir a los atacantes tener acceso no autorizado a los sistemas de información de la empresa, eludiendo los complejos esquemas y tecnologías de seguridad que se hayan implementado"[21].

> Como **contramedida**, la única manera de hacer frente a los métodos de Ingeniería Social es la **educación**. Absolutamente todas las personas que forman parte de la organización, desde la secretaria, los administradores de la red, cúpula mayor, deben estar capacitados en cuanto a las debilidades y los métodos de engaño más empleados por los atacantes para que logren identificarlos y dar aviso de cualquier anomalía que se produzca en el equipo o en determinado ambiente[22].

Este proceso educativo y de concientización por parte de las organizaciones hacia sus empleados debe estar incluido dentro de un marco formativo que genere una **cultura de seguridad de la información** y, que a la vez, esté en constante dinámica, previendo los posibles cambios a futuro, tanto de la empresa como de las amenazas, a fin de adaptase, protegerse y/o recuperarse rápidamente.

Es claro que la instrucción debe iniciar en el personal de TI, quienes deben trasmitir los conocimientos adquiridos al resto de trabajadores a través de capacitaciones, como parte de sus planes de acción, y de manera suficiente para que cada individuo esté en la capacidad de reaccionar a tiempo y de la mejor manera ante cualquier amenaza de seguridad en la información. De esta forma se disminuirían los recursos a invertir en temas de seguridad pues, por añadidura, los incidentes tenderían a desaparecer, al menos, en lo que a Ingeniería Social se refiere.

Kevin Mitnick[23] establece 4 principios básicos en la IS, los cuales deberían ser reconocidos por el personal de cada organización pues, el éxito de los sistemas de

[20] ÁLVAREZ MARAÑÓN, Gonzalo y PÉREZ GARCÍA, Pedro Pablo. Seguridad informática para empresas y particulares. Madrid.: McGraw-Hill, 2004. 442 p. ISBN 84-481-4008-7.
[21] MIERES, Jorge. "Ataques informáticos: Debilidades de seguridad comúnmente explotadas". Evil Fingers [en línea], enero 2009 [citado en 9 mayo de 2015]. Disponible en Internet: <https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf>.

[22] Ibid., p. 8

seguridad de la información no se fundamenta en las técnicas de hardware o software que se puedan implementar sino, en la correcta interpretación de estos cuatro principios y en la rigurosidad a la hora de aplicar y hacer cumplir las políticas de seguridad establecidas por cada empresa. Estos son:

1. Todos los seres humanos quieren ayudar.
2. El primer movimiento es siempre de confianza hacia el otro.
3. No es fácil decir No.
4. A todos nos gusta que nos alaben.

Son tantas y diversas las metodologías de la IS que se pueden clasificar. Dicha clasificación las desglosa en aquellas que basan su accionar en los computadores y las que se centran en los seres humanos.

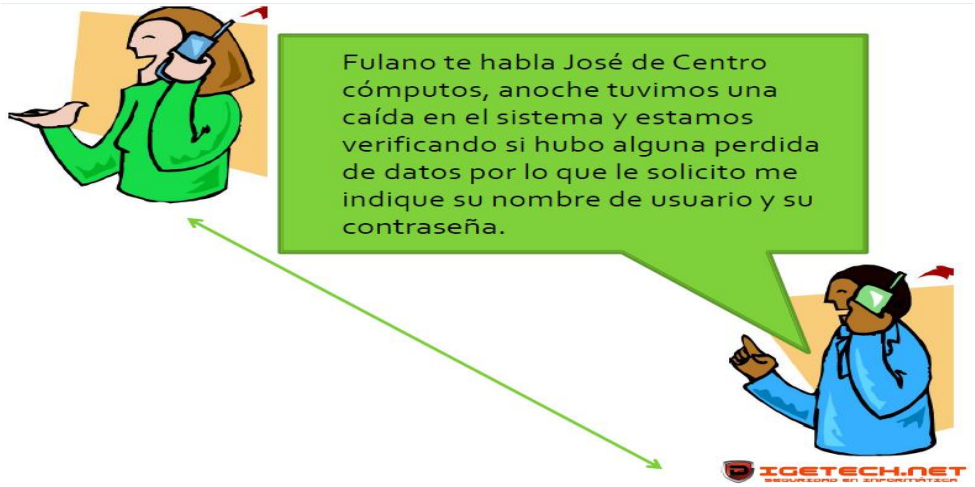
5.2.1 **Ingeniería Social basada en humanos**. El conjunto de técnicas descritas a continuación pretenden aprovechar características intrínsecas del ser humano, como: la curiosidad, el miedo, el deseo, la codicia y hasta la bondad, con el objetivo de obtener, como ya se mencionó anteriormente, información sensible o confidencial que le sirva al ingeniero social para sacar alguna ventaja, accediendo a los sistemas de información de manera fraudulenta.

5.2.1.1 **Suplantación de identidad**. En este método el ingeniero social asume un personaje que represente autoridad o necesidad, por ejemplo: puede hacerse pasar, en una llamada telefónica, por un usuario legítimo y contactarse con el departamento de TI para que le cambien su contraseña. También puede fingir ser un jefe y solicitar información específica vía correo electrono.

Podría suplantar telefónicamente al personal de TI de la empresa y simular un incidente para poder solicitarle al usuario incauto su contraseña de acceso a algún sistema, o simplemente, identificarse como miembro de una entidad privada, como una firma auditora o una entidad del estado, y solicitar información sensible. Este tipo de casos es más común en compañías de gran tamaño y con varias sucursales, donde sus integrantes puede que no se conozcan.

Figura 3. Haciéndose pasar por personal técnico

[23] CONGRESO DE PREVENCIÓN DE FRAUDE Y SEGURIDAD: ACTUAR A TIEMO, IR A LA VANGUARDIA. (5: 20-21, octubre, 2011: Bogotá D.C., Colombia). ¿Por qué los clientes entregan información confidencial, caen en engaños o en acciones de ingeniería social? Bogotá D.C.: Asobancaria, 2011. 46 p.



Fuente: http://es.slideshare.net/acurbelo/ingenieria-social-el-lado-humano-del-hacking

5.2.1.2 **Espiar por encima del hombro (*Shoulder Surfing*)**. Es una de las modalidades más comunes pues, no se requiere de gran esfuerzo para captar la información. Los ingenieros sociales la aplican en las filas de los bancos o cajeros electrónicos consiguiendo ver las claves de sus víctimas. También se usa en sitios públicos como café-internet o bibliotecas, donde se logra ver lo que digita la otra persona. Actualmente se emplean dispositivos móviles como celulares o cámaras espías para tomar fotografías o hacer videos en lugar de memorizar los datos.

Una medida de prevención esencial es la de tapar los teclados de cajeros o datafonos a la hora de digitar las claves, o hacer uso de estos servidos en lugares seguros como las mismas instalaciones de los bancos. También es aconsejable no acceder a sitios web donde sea necesario identificarse desde lugares públicos, y disponer de filtros anti-espías en las pantallas de los dispositivos móviles como celulares o tabletas.

5.2.1.3 **Buscar en la basura (*Dumpster Diving*)**. Aunque no parezca, esta práctica es más común de lo que se cree. Los ingenieros sociales pueden encontrar en las sestas de basura todo tipo de información; datos financieros, recibos de servicios públicos, "*post it*" con usuarios y claves, manuales, números de teléfono, formatos con imagen corporativa, etc., que les puede servir para iniciar un ataque a la empresa.
La principal manera de prevenir este tipo técnica es destruir toda clase de registros físicos que ya no representen importancia para la compañía mediante el uso de máquinas trituradoras de papel o de forma manual. También se pueden disponer los depósitos de basura en lugares donde el personal de seguridad y vigilancia los pueda observar, y recalcar en

los trabajadores, el no escribir datos confidenciales en “papelitos” que luego terminarán en la basura.

5.2.1.4 **Ingeniería Social Inversa (*Reverse Social Engineering*)**. Esta modalidad se presenta cuando el “hacker causa problemas en la red de la empresa objetivo o en una computadora y luego hace que él/ella mismo vaya a solucionar el problema. Una vez que el atacante ha solucionado el “problema”, él o ella es percibido como un héroe y ha ganado así la confianza y seguridad del objetivo”[24]. Aquí es el usuario quien depende del “*hacker*”, y no, el “*hacker*” del usuario.

Esta tarea no es nada fácil para el ingeniero social pues, debe ser capaz de ingresar al sistema objetivo y dañarlo, para lo cual debe usar otras de las técnicas de la IS o herramientas computarizadas complejas y, adicionalmente, debe “ingeniarse” la forma de ofrecer su ayuda o “servicios técnicos”.

5.2.1.5 **Desarrollar Confianza (*Establishing Trust*)**. La confianza es la base de la ingeniería social, y aquel que la practica, debe contar con cualidades específicas para poder obtenerla pues, como se dice popularmente; “la confianza es difícil de conseguir, fácil de perder e imposible de recuperar”.

Bajo esta modalidad de ataque de la IS se esconde una persona que tiene la capacidad de, según la doctora Aury Curbelo[25]; especialista en temas de seguridad de la información, socializar fácilmente, hablar con claridad, persuadir, aparentar ser inofensivo, mantener un bajo perfil, saber sonreír y ser amable, entre otras.

Pero desarrollar confianza implica un arduo trabajo por parte del ingeniero social, quien debe invertir tiempo y recursos; económicos por ejemplo, para avanzar en el reconocimiento de aspectos clave dentro de una organización como: nombres del personal directivo, servicios, ubicación de oficinas, etc.

5.2.1.6 **Afectividad (*Affectivity*)**. Es la susceptibilidad que tienen las personas ante situaciones específicas en su entorno, lo que es aprovechado por los ingenieros sociales para conseguir su objetivo.

[24] HINOJOSA JARAMILLO, Lucia Gabriela. Estudio del grado de incidencia de la ingeniería social en la primera fase de los ataques informáticos que se realizan actualmente en las empresas privadas del ecuador. Trabajo de grado Ingeniero de Sistemas. Quito: Universidad Internacional SEK. Facultad de Ciencias y Telecomunicaciones, 2010. 186 p.
[25] CONGRESO DE PREVENCIÓN DE FRAUDE Y SEGURIDAD, Op. cit., p. 21.

> La afectividad incluye, pero no está limitada al: miedo, emoción o pánico. Esta puede ser la promesa de un premio sustancial con un valor de cientos de miles de dólares o el pánico de tener un empleado en el trabajo dependiente de una decisión. La ola de emociones fuertes trabaja como una poderosa distracción e interfiere con la habilidad de la víctima para evaluar, pensar de manera lógica o desarrollar argumentos[26].

5.2.1.7 **Sobrecarga (*Overloading*)**. Consiste en "bombardear" a la víctima con gran cantidad de información en un corto periodo de tiempo, a tal punto, que se sienta confundida o frustrada, para que al final, acceda a las razones o argumentos del ingeniero social.

Un ejemplo claro podría ser el de un usuario que entabla una discusión con una secretaria o asesor de servicio al cliente, asediándolo con gran cantidad de preguntas y de un momento a otro, cambia el tema de conversación, confundiendo a su víctima y haciéndola decir cosas que muy seguramente no quería.

5.2.1.8 **Reciprocidad (*Reciprocity*)**. Los seres humanos tienden a sentirse comprometidos cuando otro presta su ayuda. Quien la recibe espera dar algo en contraprestación. Eso es reciprocidad. Un ingeniero social se puede prestar a resolver un problema sin que nadie se lo pida, como se vio en la ingeniería social inversa, o hacer un favor sin esperar recompensa. Aun así, la victima ha quedado ligada a la situación y siente la necesidad de responder de la misma forma o mejor.

5.2.1.9 **Relaciones basadas en engaños (*Deceptive Relationships*)**. Aquí lo que busca el ingeniero social es crear relaciones personales para lograr conseguir información de otra persona o de un sistema. Un ejemplo de esto es un ataque realizado a AOL, donde el ingeniero social habló por teléfono con un empleado de la empresa durante más de una hora. "En algún punto durante la llamada el hacker mencionó que su auto estaba de venta. El técnico estaba interesado, entonces el hacker le envió un e-mail con una imagen del auto adjunta. El archivo adjunto contenía un "*exploit*" de puerta trasera que abría una conexión aunque AOL tuviera un firewall"[27].

5.2.1.10 **Escuchar detrás de las Puertas**. Esta modalidad no se limita a hacer literalmente lo que se indica en su nombre, también incluye escuchar

[26] HINOJOSA JARAMILLO, Op. cit., p. 57.
[27] Ibid., p. 60

conversaciones sin autorización en lugares como restaurantes u oficinas, valiéndose, además, de recursos tecnológicos que permitan la grabación de audios y videos de mejor calidad.

5.2.1.11 **Obtener acceso físico (*Tailgating & Piggybacking*)**. Aunque no es común que los ingenieros sociales accedan a las instalaciones físicas de sus objetivos, en relación con las empresas si existen casos en donde se pueden hacer pasar por personal de mantenimiento del edificio para acceder a áreas restringidas de la organización. Esto es posible gracias a que las compañías prefieren tercerizar algunos de sus procesos o dependencias, o a que, debido a su tamaño, los empleados no logran conocerse unos a otros.

5.2.2 **Ingeniería Social basada en computadores**. Como su nombre lo indica, son métodos que usan la IS pero que dependen estrechamente de una computadora o de otros artefactos electrónicos y tecnológicos. Estas son más técnicas u ortodoxas, de acuerdo a la historia de la seguridad informática.

5.2.2.1 ***Phishing***. Traduce "pescando" en español y lo que busca es engañar a las víctimas a través del envío de correos electrónicos fraudulentos, en donde se le solicita al usuario registrarse o acceder a un sitio suplantado.

> ¡Querido y apreciado usuario de Banco X!
> Como parte nuestro servicio de protección de su cuenta y reducción de fraudes en nuestro sitio web, estamos pasando un periodo de revisión de nuestras cuentas de usuario. Le rogamos visite nuestro sitio siguiendo link dado abajo. Esto es requerido para que podamos continuar ofreciéndole un entorno seguro y libre de riesgos para enviar y recibir dinero en línea, manteniendo la experiencia de Banco X. Después del periodo de verificación, será redireccionado a la página principal de Banco X.
> Gracias.
> https://xnetparticulares.bancox.es/BEXBEBEXA_F.jsp[28]

[28] ÁLVAREZ MARAÑÓN, Op. cit., p. 310.

El link adjunto contendrá una versión idéntica, en este caso, de la página web del banco, administrada por el ingeniero social, quien luego; obtendrá el usuario y la clave de su víctima. Los bancos son las entidades más suplantadas electrónicamente hablando, pero también es común ver casos en donde se sustituyen servicios de correo como Hotmail o AOL, y de comercio electrónico.

La recomendación para protegerse de este tipo de amenaza es hacer caso omiso a mensajes de correo electrónico provenientes de remitentes desconocidos. En el caso de las redes sociales, se aconseja evitar las cadenas y la visita a perfiles inapropiados. Respecto al comercio electrónico y la banca en línea, se sugiere digitar directamente la dirección web de cada sitio y no llegar a ellos a través de links o pop-ap's, verificando siempre el uso del protocolo **https**.

5.2.2.2 **Email con malware**. Los correos electrónicos pueden traer adjuntos cualquier tipo de archivos contenedores de alguna clase de malware, como: virus, gusanos, troyanos, entre otros; cada uno con una tarea específica y características especiales. Una vez más se recomienda no abrir mensajes de remitentes desconocidos ni descargar sus adjuntos.

"También hay que tener cuidado con los falsos **antivirus**. En algunas páginas web peligrosas (servicios de descargas ilegales, por ejemplo) aparece un mensaje que nos avisa de que estamos infectados y se ofrecen amablemente para descargar un antivirus que nos limpiará el ordenador"[29]. La instalación de estas aplicaciones puede acarrear la pérdida o el **secuestro** de la información, al permitir que se alojen en la computadora otra serie de virus, que pueden convertirla en zombi para lanzar un ataque escalado, abrir puertas traseras o inundarla de publicidad. Lo mismo pasa con los programas de "*tuning*" que prometen acelerar el funcionamiento de las computadoras pero que al final resultan ser software malicioso.

Para contrarrestar estas amenazas es importante contar con un software antivirus licenciado y actualizado, y por supuesto, hacer uso de las buenas prácticas de usuario.

Figura 4. Falsos antivirus

[29] ROA BUENDÍA, José Fabián. Seguridad informática. Madrid: McGraw-Hill, 2013. 226 p. ISBN 978-84-481-8569-5.

Fuente: http://nicegrafica.blogspot.com/2013/11/cuidado-con-los-falsos-antivirus-aca-la.html

5.2.2.3 ***Spam***: se denomina también correo no deseado o no solicitado, enviado por "*spammers*", cuyo objetivo es lograr el "colapso de los servidores y la sobrecarga de los buzones de correo de los usuarios"[30]. Básicamente son correos con publicidad y aunque inicialmente no representan mayor amenaza, si es posible que contengan códigos maliciosos o hagan parte de un ataque tipo "*phishing*".

La situación aprovechada por esta metodología es la necesidad que tienen las organizaciones de utilizar los servicios de correo electrónico, ya sean públicos o privados, para comunicarse internamente o con sus proveedores y clientes, intercambiando información y adjuntado todo tipo de documentos, a veces, de forma indiscriminada.

Es responsabilidad inicial de cada usuario evitar abrir estos mensajes de correo, pero los departamentos de TI pueden complementar la protección implementando medidas como la instalación de servidores anti-spam y la actualización permanente de los clientes de correo electrónico como **Outlook** y **Thunderbird**.

[30] GÓMEZ VIEITES, Álvaro. Gestión de incidentes de seguridad informática. Madrid: Ra-Ma, 2014. 124 p. ISBN 978-84-9964-331-1.

5.2.2.4 **Pop – Up's**. Son las ventanas emergentes que despliegan algunos sitios web y su propósito es mostrar publicidad al usuario. Pueden ser una fuente de contagio de "*malware*" como virus y troyanos, o simplemente; entorpecer el uso de la computadora al crear, en algunos casos, ciclos o bucles infinitos de apertura de ventanas.

Ya es común que todos los navegadores incluyan bloqueadores de ventajas emergentes activados por defecto, los cuales se deben deshabilitar al entrar en sitios seguros, pues, el uso de pop-up's es normal en los portales de los bancos y plataformas educativas con el fin de proteger los datos del usuario o evitar fraudes y suplantaciones.

5.2.3 **Pasos necesarios para la ejecución de cualquier estrategia de Ingeniería Social**. Todos los ataques informáticos cuentan con una metodología básica donde se enmarcan todos y cada uno de los movimientos necesarios para cumplir el objetivo. Algunos ataques son más robustos y requieren, por parte del atacante, la inversión de todo tipo de recursos (tiempo, dinero, tecnología, conocimientos), mientras que otros pueden ser más fáciles de ejecutar. Todo depende de las pretensiones del agresor y de las barreras de seguridad con que cuenta el objetivo. Al final, la metodología siempre es la misma.

La IS no es la excepción y según la doctora Curbelo, para poder ejecutar un ataque mediante alguno de sus métodos, se deben tener en cuenta los siguientes 6 pasos:

Figura 5. Pasos para la ejecución de ataques basados en Ingeniería Social

Fuente:Http://www.slideshare.net/acurbelo/ingenieria-social-el-lado-humano-del-hacking

La ejecución de cada uno de los movimientos que muestra la imagen anterior puede incluir una o varias de las técnicas vistas en los numerales 5.2.1 y 5.2.2. A continuación se detalla cada uno de los pasos indicados en la imagen anterior.

5.2.3.1 **Identificar a la víctima**. Es la actividad inicial antes de ejecutar el ataque. Aquí el ingeniero social se plantea el objetivo y estima las probabilidades de éxito. El blanco puede ser una persona o una organización.

5.2.3.2 **Reconocimiento**. Luego de determinar hacia quien o que va dirigido su ataque, el ingeniero social inicia la búsqueda de la mayor cantidad de información sobre su objetivo. Puede valerse de datos disponibles en fuentes abiertas como google, directorios telefónicos y anuncios (*OSINT*). También es habitual buscar en la basura de su víctima, tratar de desarrollar confianza o hacer "*phishing*".

5.2.3.3 **Crear el escenario**. Con la información suficiente a la mano, el atacante puede simular una situación específica como una emergencia, un daño locativo, una necesidad, o un escándalo. Así, puede suplantar la identidad del personal de mantenimiento o de empresas de servicios públicos. Del mismo modo, podría engañar a las víctimas a través de llamadas telefónicas donde puede fingir ser un alto directivo u operario del departamento de TI.

La configuración de cada escenario depende del ingenio del atacante y de sus habilidades a la hora de desenvolver su ataque, de las barreras de seguridad existentes en el objetivo y de las instalaciones físicas de la empresa donde quiere ingresar. Con un poco de suerte y gracias a las fallas en los controles de seguridad; frecuentes en todas las organizaciones, podrían encontrar los escenarios listos para actuar.

5.2.3.4 **Realizar el ataque**. Una vez el plan está en marcha y la víctima ya se encuentra envuelta, el atacante pone en práctica técnicas como la Ingeniería Social Inversa, el uso de software como "*sniffers*" y "*keyloggers*", el escaneo de puertos y los mapeos de red.

5.2.3.5 **Obtener la información**. Con el control de la situación, de la red, o de la computadora, el ingeniero social procede a captar la información que necesita, ya sea en un medio portátil de almacenamiento como una memoria UBS, smartphone y/o cámara digital, o simplemente hace uso

de “*malware*” que envíe constantemente los datos a una dirección de correo electrónico preestablecida.

Si el ataque es rápido, el delincuente informático debe ser selectivo a la hora de guardar los datos pues, puede encontrar demasiada información y captar la menos relevante. Debe tener la habilidad de identificar los lugares (carpetas, unidades de disco o cualquier dispositivo de almacenamiento) donde se guarda la información realmente significativa. Aquí juega un papel importante la experiencia.

5.2.3.6 **Salir**. Cumplido el objetivo del ataque y una vez terminada la intrusión, el ingeniero social debe abandonar el lugar o la situación sin levantar sospecha alguna, manteniendo la calma y el rol asumido desde el principio.

Para cerrar esta sección, vale la pena resaltar que el poder identificar cada una de las etapas que conforman un ataque de Ingeniería Social “brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad. Desde la perspectiva del profesional en seguridad, se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque”[31].

5.2.4 **Tipos de atacantes y ataques.** A lo largo de este documento se ha venido hablando de las diferentes situaciones en las que se ve expuesta la seguridad de la información y los sistemas informáticos, escenarios inexistentes sin la labor de los atacantes; los verdaderos cerebros detrás del delito. En este apartado se darán a conocer, de manera general, las distintas clases de atacantes, sus motivaciones y los tipos de ataques que suelen ejecutar.

No sobra precisar cuáles son las razones que mueven a los delincuentes informáticos a realzar sus actividades ilícitas. Según el FBI, el acrónimo MICE resume “las distintas motivaciones de los atacantes e intrusos en las redes de ordenadores: *Money*, *Ideology*, *Compromise* y *Ego* (Dinero, Ideología, Compromiso y Autorrealización personal)”[32].

Quizás es el ámbito económico el que más estimula a los atacantes a cometer algún delito. Poder clonar tarjetas de crédito o débito, intervenir sitios de comercio electrónico o bancos para desviar las transacciones, o, muy de moda actualmente, secuestrar la información de compañías o particulares para exigir un pago a cambio de su devolución, o de lo

[31] MIERES, Op. cit., p. 5.
[32] GÓMEZ VIEITES, Op. Cit., p. 21.

contrario, amenazan con destruirla; son algunos de los hechos más frecuentes en lo referente al dinero.

Otros atacantes están convencidos, y persuaden a los demás, de sus doctrinas políticas o religiosas, por las que son capaces de vulnerar sitios gubernamentales o privados. En el apartado 5.1 se expuso el caso de supuestos yihadista que "hackearon" dos sitios web de una universidad en Brasil. Este caso se vio recientemente en nuestro país cuando se descubrió por parte de la Policía Nacional una empresa fachada donde el "hacker" Andrés Sepúlveda dirigía una seria de interceptaciones a celulares y otros dispositivos pertenecientes a figuras políticas del ámbito nacional.

Hay quienes ejecutan sus ataques por mero compromiso, inclusive por diversión, y el resto, por la satisfacción personal de ser reconocidos, públicamente o por su propia comunidad, tratando de imponer hitos cada vez más altos que representen un reto para los futuros delincuentes informáticos.

Existen diferentes roles en la delincuencia informática, aunque comúnmente, los usuarios corrientes solo reconozcan a los "*hackers*" como los únicos atacantes de sus computaras. Cada uno cuenta con sus propios distintivos y juegan un papel determinado en cada forma de vulnerar la seguridad de la información.

5.2.4.1 **Hackers**. Popularmente se dice que el término "*hacker*" nace en la década de los 50 cuando los técnicos de las empresas de teléfonos en los EE.UU golpeaban los aparatos para repararlos. Literalmente traduce "hachazo" o golpear con un hacha y básicamente se puede definir a un "*hacker*" como "un informático que utiliza técnicas de penetración no programadas para acceder a un sistema informático con los más diversos fines"[33].

Suelen ser expertos en varios lenguajes de programación, arquitecturas de red y protocolos de comunicaciones, electrónica y sistemas operativos, iniciando sus actividades a edades muy tempranas y tienden a defender sus actos ilícitos con el argumento de que no pretenden causar daño a los sistemas que atacan, sino, mejorar sus conocimientos y, de paso, ayudar a descubrir vulnerabilidades en dichos sistemas para luego corregirlas.

[33] AVILÉS GÓMEZ, Manuel, *et al*. Delitos y delincuentes: cómo son, cómo actúan. San Vicente, España: ECU, 2010. 404 p. ISBN 978–84–9948–151–7.

5.2.4.2 ***Crackers***. Son una derivación de los "*hackers*" pero sus intenciones son las de dañar los sistemas en que irrumpen, de ahí su significado en inglés: romper o quebrar. Sus motivaciones van desde lo económico hasta lo político, dedicados principalmente a la modificación de software propietario para su uso no autorizado. De ahí que sea común encontrar hoy por hoy toda clase de programas o aplicaciones "crakeadas" para el uso libre, indiscriminado y no licenciado por parte de los usuarios finales.

5.2.4.3 ***Phreakers***. Son aquellos atacantes, que aunque por sus conocimientos podrían ser también "*hackers*", orientan sus actividades hacia las comunicaciones telefónicas, poniendo en práctica sus propios métodos para obtener llamadas gratis o para superar sus mejores hazañas.

En sus principios se dedicaban a conocer todo lo relacionado con el mundo de la telefonía, como: estructuras, empresas de comunicaciones y electrónica aplicada a los teléfonos, a tal punto; que se les atribuye la creación de las conocidas cajas azules o "*blue boxes*", dispositivo que podía confundir a las operadoras análogas a través de tonos para poder realizar llamadas sin costo.

5.2.4.4 ***Sniffers***. Estos son los atacantes que a través de software del mismo nombre "huelen", según la traducción literal del término, todo el flujo de información existente en una red. Su objetivo es detectar actividades específicas monitoreando y analizando el tráfico de datos. El software más conocido para esta actividad es Ettercap.

5.2.4.5 ***Spammers***. Son los responsables del envío masivo de correo electrónico no deseado. Pueden ser individuos o empresas que obtienen las listas de correo a través de robots, sitios web o bases de datos.

5.2.4.6 **Piratas informáticos**. Este tipo de delincuentes se dedican a la reproducción y distribución ilegal de toda clase de contenidos digitales (música, videos y programas), afectando en gran medida la propiedad intelectual de los verdaderos productores.

5.2.4.7 **Ingeniero Social**. De los tipos de atacantes que se pueden listar en esta sección, estos son los que mayor interés representan para el tema de esta investigación, al tipificar las múltiples conductas q pueden adoptar los delincuentes bajo la IS. Christopher Hadnagy[34] propone al menos 10 formas diferentes de ingenios sociales y describe un poco de cada una de ellas:

[34] HADNAGY, Op. cit., p. 41.

- ✓ **Hackers:** estos ya fueron descritos con anterioridad pero, vale la pena resaltar que están dentro de esta clasificación debido a que, por los avances tecnológicos en cuestiones de seguridad, se han visto obligados a hacer uso de las técnicas de la IS.

- ✓ ***Pentesters***: son los "hackers" que utilizan sus conocimientos y habilidades en pro de la seguridad de los sistemas informáticos de las organizaciones. Su labor es ejecutar pruebas de penetración a estos sistemas a través de distintas herramientas para encontrar las vulnerabilidades que poseen y poderlas solucionar. No pretenden en ningún momento atentar contra la seguridad de la información de las empresas, por el contrario, su labor está supervisada y se ejecuta bajo términos contractuales.

- ✓ **Espías**: son quizás los individuos más expertos en la aplicación de la IS, al punto, de convertirla en su estilo de vida pues, deben asumir roles diferentes e imprimirles la suficiente credibilidad para engañar a sus víctimas.

- ✓ **Ladrones de identidad**: este tipo de delincuente usa técnicas como la de buscar en la basura u *OSINT* para obtener ilegalmente datos personales de sus víctimas, tales como: nombres, números de identificación, fechas de nacimiento, números de teléfonos, etc., para hacer uso indebido de ellos. Los delitos más frecuentes son la suplantación en transacciones comerciales (comparas y arrendamientos) y la personificación, es decir, que pueden usar ropa o uniformes como los de sus víctimas para ingresar a diferentes lugares.

- ✓ **Empleados descontentos**: se convierten en ingenieros sociales al disimular a toda costa su disgusto con su jefe o patrono, con el fin de no perder su trabajo y luego, poder cometer toda clase de delitos como; robo de datos, suplantación, espionaje, vandalismo y venta de información confidencial de la organización a la competencia.

- ✓ **Estafadores**: estos personajes se aprovechan de las necesidades de las personas y organizaciones para proponerles negocios fraudulentos, que por ende no cuentan con ninguna sustentación legal, con la intención de lograr sonsacarles su dinero. Sus actos engrosan diariamente las estadísticas de delitos a nivel nacional y quizás, uno de los de mayor escala y registrado por todos los medios de comunicación colombianos fue el de las pirámides, en donde por necesidad o codicia, la gente depositaba su dinero a la espera de ganancias exorbitantes, para luego perderlo todo.

- ✓ **Reclutadores**: ya sean legales; como la fuerzas armadas, cazatalentos, o ejecutivos empresariales, o ilegales; como los grupos armados, bandas o pandillas, los reclutadores se valen de técnicas como la de desarrollar confianza, afectividad, reciprocidad y relaciones basadas en engaños para persuadir a sus objetivos, entendiendo sus necesidades, gustos o inclinaciones, a fin de apoderarse de ellos.

- ✓ **Vendedores**: aunque no representan ningún peligro ni amenaza a la seguridad de la información, los vendedores se basan en técnicas propias de la IS para poder llegarles a sus clientes. Obtienen información de diferentes fuentes en busca de las necesidades de los consumidores y logran ganarse la confianza de los mismos.

- ✓ **Gobierno**: generalmente no se ven como ingenieros sociales pero, los gobiernos y sus representantes son hábiles a la hora de usar la IS. Por ejemplo; se aprovechan de la autoridad para controlar distintas situaciones, crean cortinas de humo para desviar la atención de temas realmente importantes o recurren, muy frecuentemente, a desarrollar controversias con la oposición o sectores específicos de la sociedad.

  Vale la pena decir que los políticos tienen muchas de las cualidades de un ingeniero social; son carismáticos, seguros a la hora de hablar, asertivos, y como conocen de antemano las necesidades del pueblo (que de no tenerlas, se las inventan), fingen representar los intereses de la gente, que al final, resulta decepcionada.
- ✓ **Doctores, psicólogos y abogados**: los profesionales de estas ramas usan muchas técnicas de IS para persuadir a sus "objetivos" (clientes) aunque esto no represente ningún riesgo para ellos pues, en el caso de los médicos, sus recomendaciones o directrices van en pro de la salud de los pacientes.

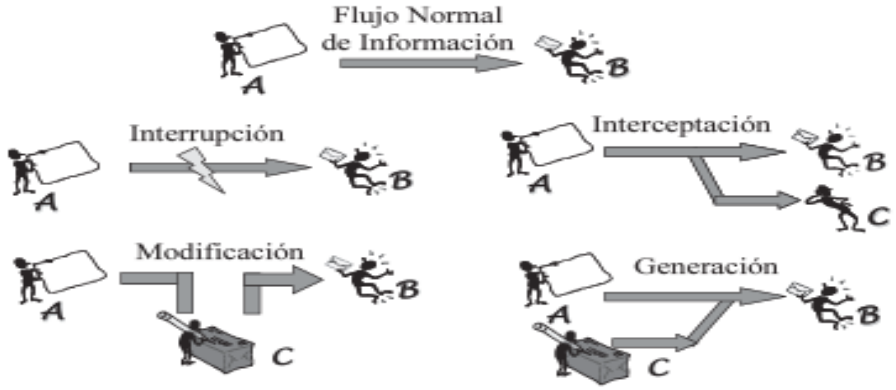
  La otra cara de la moneda es la de los supuestos "profesionales", quienes actúan en contra de los intereses de las personas, al punto de engañarlos y estafarlos. Casos como los de las cirugías estéticas practicadas por médicos falsos o no idóneos, y los timos jurídicos a personas por tierras o propiedades son muy comunes en todo el mundo.

Reconocidos e identificados los diferentes tipos de atacantes, se convierte en significativo el conocer también los tipos de ataques que existen, pues las actuaciones de estos personajes encajan dentro de marcos específicos que se verán a continuación. No se pretende profundizar en aspectos

técnicos ni tecnológicos propios de un ataque informático, lo que se busca es proporcionar una visión general de los mismos y clasificarlos para un mejor entendimiento.

Una primer clasificación es la de los "ataques activos, que producen cambios en la situación de los recursos del sistema, y los ataque pasivos, que se limitan a registrar el uso de los recursos y/o acceder a la información guardada o transmitida por el sistema"[35]. La imagen a continuación representa claramente los ataques que se pueden presentar en una red.

Figura 6. Tipos de ataques



Fuente: GÓMEZ VIEITES, Álvaro. Gestión de incidentes de seguridad informática. Madrid: Ra-Ma, 2014. 124 p. ISBN 978-84-9964-331-1.

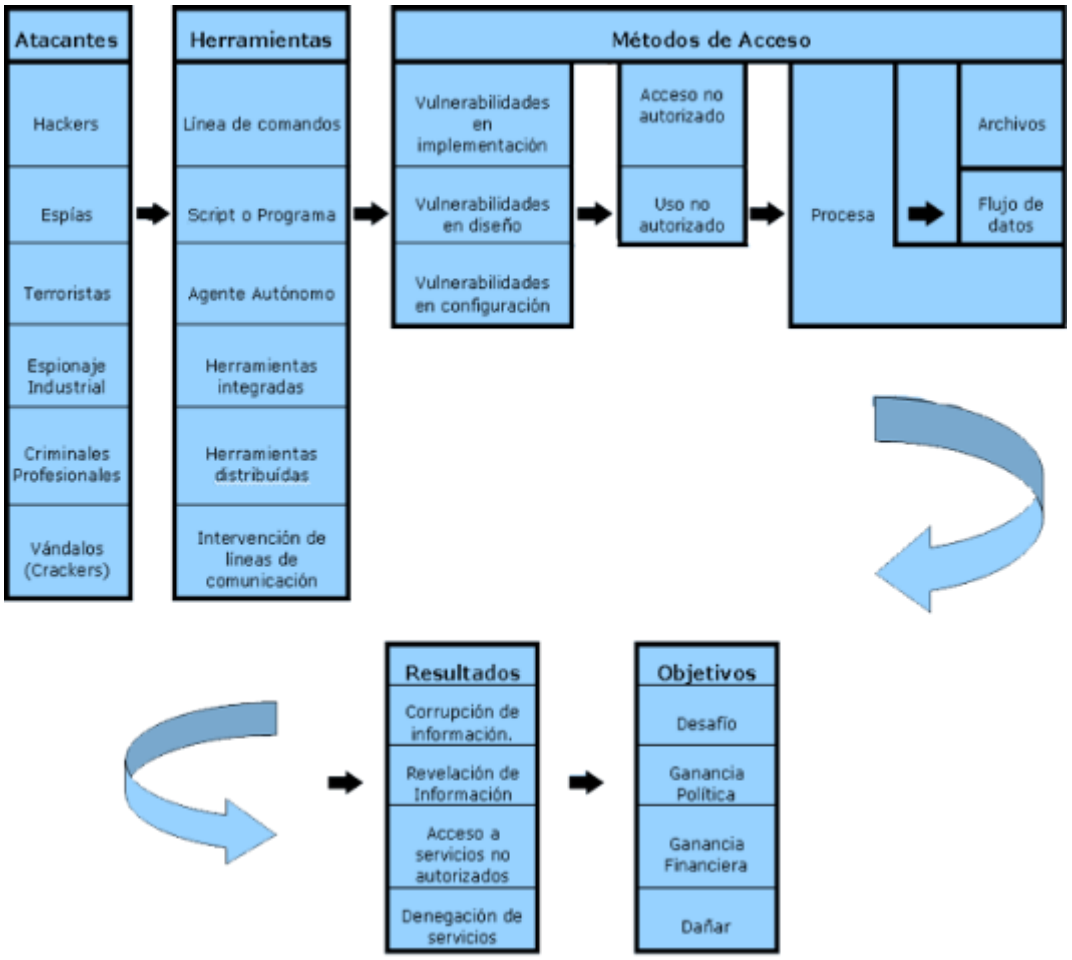
Los ataques informáticos también pueden ser internos o externos, estructurados o no estructurados. En cualquier caso, las técnicas o metodologías usadas son muchas, por ejemplo: **Ingeniería Social**, DoS, ataques ARP (*Address Resolution Protocol* o, Protocolo de resolución de direcciones), malware, "*Sniffers*", entre otros.

Lo verdaderamente importante es reconocer que cualquiera puede ser víctima de alguna o varias de estas formas de delinquir y que no es suficiente el tener un software antivirus instalado en la computadora. Esta medida se debe complementar implementando controles de seguridad a nivel empresarial y personal, porque para los ciber-delincuentes, cualquiera que tenga un dispositivo tecnológico a la mano es un blanco fácil para robarle su información.

La siguiente imagen exhibe un esquema general de un ataque informático.

Figura 7. Detalle de un ataque

[35] GÓMEZ VIEITES, Op. Cit., p. 24.



Fuente: http://www.segu-info.com.ar/ataques/ataques.htm

5.2.5 **Medidas para evitar ser víctimas de la Ingeniería Social**. La principal medida de protección en las organizaciones y como usuarios particulares es la **educación**. Se debe aprender a identificar, a través de **capacitación permanente**, cada una de las técnicas de la Ingeniería Social, sus modus-operandi, características y consecuencias.

En el caso que nos atañe, los usuarios de las empresas deben estar en la capacidad de reconocer a un ingeniero social y sus intenciones, a fin de reaccionar a tiempo ante cualquier incidente de seguridad. Lo más importante es que las entidades del sector educativo adopten una **cultura** de protección de la información que las blinde contra este tipo de intrusiones; **concientizando** a todos sus usuarios; tal y como lo hacen los bancos, y que esté integrada a la implantación de controles; físicos y lógicos, políticas, estándares y guías de seguridad de la información.

No se pretenden en ningún momento que esta investigación sea una guía exhaustiva para la instauración de todos los controles de seguridad existentes en la actualidad, lo que se busca, es integrarlos de tal modo que

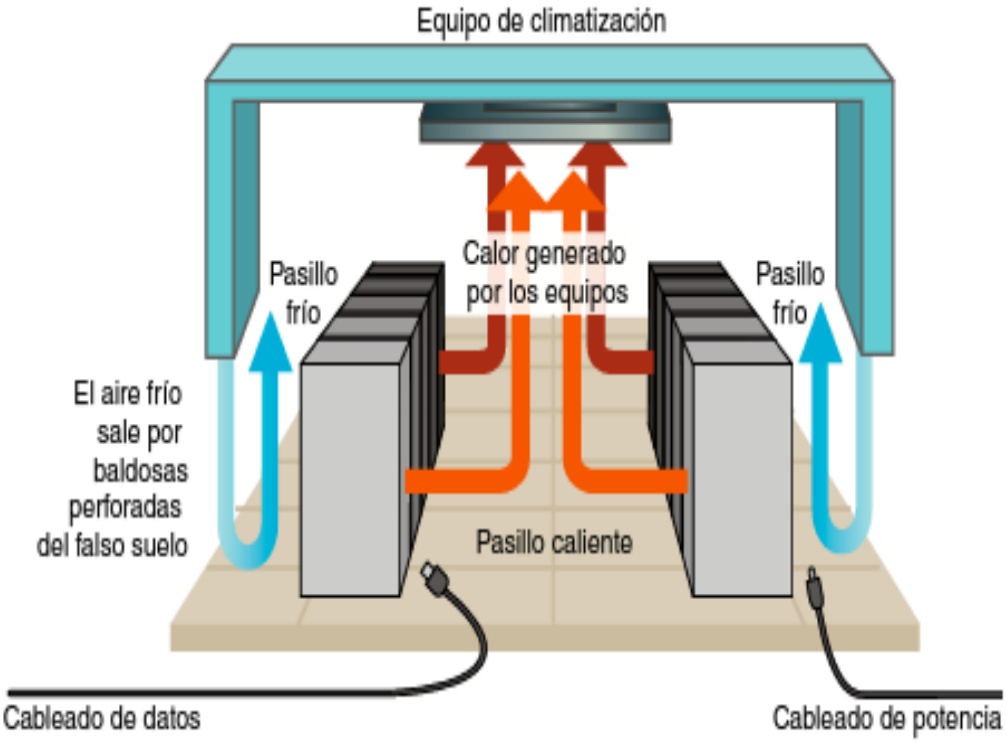
se evidencie la necesidad, por parte de las empresas, de hacer uso de ellos y que se reconozca el sin fin de beneficios que esto les puede representar.

Para empezar, es preciso definir que es un incidente de seguridad. Este se puede definir como “cualquier evento que pueda provocar una interrupción o degradación de los servicios ofrecidos por el sistema, o bien afectar la confidencialidad o integridad de la información”[36].

Lo siguiente es determinar una buena ubicación para los **centros de datos**. Si estos ya se encuentran definidos es necesario implementar los correctivos pertinentes. Los centros de datos deben estar situados preferiblemente en los primeros pisos de las edificaciones, alejados de instalaciones de gas o subestaciones eléctricas y evitando su señalización. Deben contar con todas las medidas de seguridad locativas como: sistemas de detección de humo, sistemas automáticos de extinción de incendios; o en su defecto, un extintor dispuesto en un lugar libre y de rápido acceso, el mobiliario debe estar construido con materiales no inflamables, debe tener un sistema de ventilación que evite altas temperaturas y excesos de humedad y en lo posible, introducir material de aislamiento acústico para evitar que el ruido de los dispositivos interfiera con el trabajo de otras áreas de la organización.

Figura 8. Control de temperatura y ventilación del centro de datos

[36] GÓMEZ VIEITES, Op. Cit., p. 53.



Fuente: ROA BUENDÍA, José Fabián. Seguridad informática. Madrid: McGraw-Hill, 2013. p. 66. ISBN 978-84-481-8569-5.

Se debe contemplar la instalación de un **SAI** o **Sistema de Alimentación Ininterrumpida**, que evite la pérdida de datos o daño de equipos por cortes electicos. Esto se hace a través de UPS's que pueden estar configuradas en estado de espera o en línea con la red eléctrica principal. En el primer caso, los equipos toman la corriente de la red electica estándar mientras que la UPS monitorea el flujo eléctrico; en caso de un corte, la UPS entra en funcionamiento inmediatamente evitando que los equipos se apaguen. En el segundo caso, los equipos están conectados directamente a la UPS, lo que evitará su apagado en caso de un fallo en el servicio regular y sin depender del tiempo de respuesta de la misma. La ventaja del sistema en estado de espera es que se pueden cambiar las baterías de la UPS sin afectar el funcionamiento de los equipos conectados a la red electica.

En lo concerniente a las comunicaciones con el exterior, se aconseja contratar servicios de internet con tecnologías y empresas distintas, es decir, se puede contratar un servicio ADSL con una empresa determinada y un servicio de fibra óptica con otra. Esto para no depender del mismo canal en caso de fallos masivos, normales en este tipo de servicios. También se deben implementar controles de acceso físico a los centros de datos

haciendo uso de tecnologías como la biometría, tarjetas de acceso, cámaras de vigilancia y sensores, determinando en todo caso y de manera precisa, la identificación del personal que podrá ingresar a los mismos.

Por último y a la vez el más importante, es la creación de un **centro de datos de respaldo** pues, aunque se implementen todas las medidas de seguridad necesarias, nunca se está 100% protegido de catástrofes como terremotos o inundaciones. Aun así, esto no puede ser excusa para la pérdida de información y el cese en las actividades de la empresa. Por tal razón, el centro de datos de respaldo debe estar ubicado en un lugar distinto y lejano del centro de datos principal, por ejemplo en una sucursal de la compañía, y debe contar con las mismas características y prestar los mismos servicios.

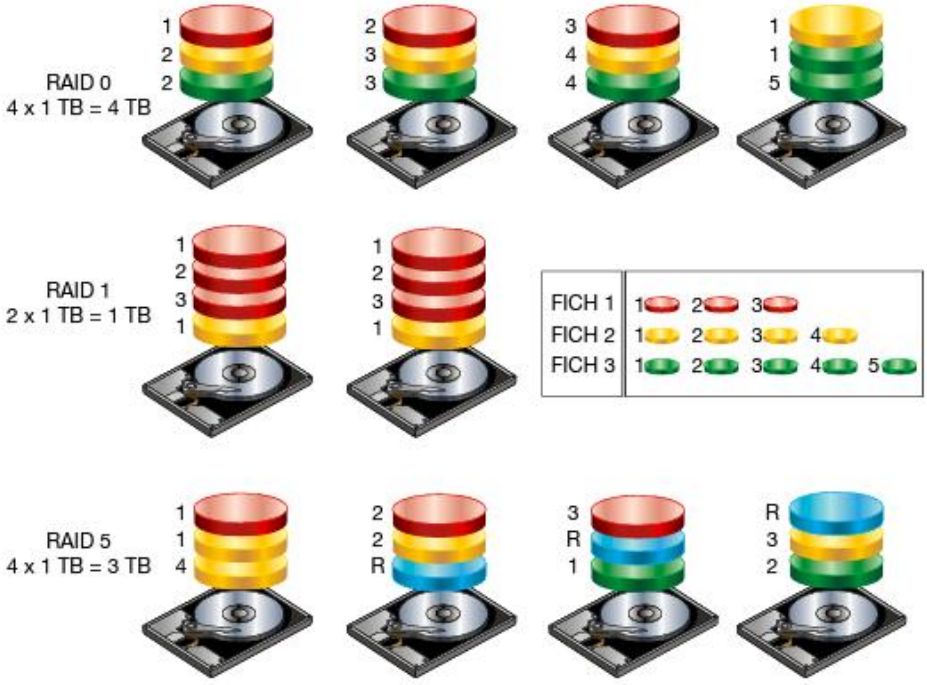
5.2.5.1 **Otras medidas de protección de la información**. Existen muchos otros mecanismos para proteger los datos de las amenazas propias de los ambientes corporativos y/o individuales, estos son:

- ✓ ***Backup´s*** **o copias de seguridad**: estos deben ser periódicos y en dispositivos de almacenamiento externos, los cuales deben resguardarse en un lugar diferente al del origen de los datos. Se pueden hacer de forma local o remota a través de infraestructuras y aplicaciones específicas ofrecidas para ello por empresas como **Symanctec**, por ejemplo.

- ✓ **Imagen del sistema**: también se conoce como imagen de disco y es la creación de una réplica exacta del disco duro de un equipo ya configurado. Se aconseja su creación a partir de instalaciones limpias pero también se pueden usar en equipos con datos ya incluidos, a fin de hacer recuperaciones más rápidas en caso de daño de la computadora. Sistemas operativos como Windows 7 incluyen una herramienta para la elaboración de este tipo de respaldos.

- ✓ ***RAID's***: o conjunto redundante de discos independientes, es un sistema de almacenamiento de datos que ofrece grandes ventajas frente al almacenamiento simple de información pues, permite crear unidades más grandes, más rápidas y más confiables. Consta da varios niveles, cada uno con características especiales, siendo los más usados el 0, 1 y 5.

Figura 9. Diagramas RAID más usados



Fuente: ROA BUENDÍA, José Fabián. Seguridad informática. Madrid: McGraw-Hill, 2013. p. 78. ISBN 978-84-481-8569-5.

- ✓ **Cifrado de particiones**: consiste en hacer ilegible la información contenida en estas secciones a través de algoritmos matemáticos (*AES, 3DES*) y de sistemas como el simétrico, asimétrico o hibrido, sobre todo en equipos portátiles.

- ✓ **Autenticación**: incluye la creación de usuarios y contraseñas seguros, no solo para el acceso al sistema operativo, sino también, a las redes de datos, sistemas de información e inclusive, a la *BIOS* de cada computadora. Se debe tener en cuenta la longitud, caducidad y la complejidad de las contraseñas de acceso atendiendo a las recomendaciones que para ello existen en normas o guías internacionales de seguridad de la información.

- ✓ **Privilegios**: cada usuario de una computadora o de un sistema de información debe tener un rol determinado por unas políticas organizacionales de seguridad de la información. Así se tendrá el control de quién hace o qué puede hacer cada usuario en el sistema.

- ✓ **Actualizaciones**: todos los sistemas operativos de la organización y las distintas aplicaciones usadas para el desarrollo de su actividad

(contables, financieras, ofimáticas, de comunicación, etc.) deben estar actualizadas o contar con los parches ofrecidos directamente por el fabricante. Se debe verificar que, en lo posible, esté activada la opción de actualizaciones automáticas en cada software, monitoreando el estado de las respectivas licencias pues, si estas se vencen las actualizaciones no se ejecutarán.

- ✓ **Antivirus**: de manera general se incluyen acá todas las aplicaciones que detecten código malicioso en las computaras o en las redes de datos de la organización. Aunque tener un antivirus licenciado y actualizado no es garantía de inmunidad, siguen siendo una herramienta indispensable a la hora de proteger los datos, a la vez que incluyen una serie de servicios adicionales y complementarios que los convierten en un paquete completo de seguridad, dejando de ser un software aislado.

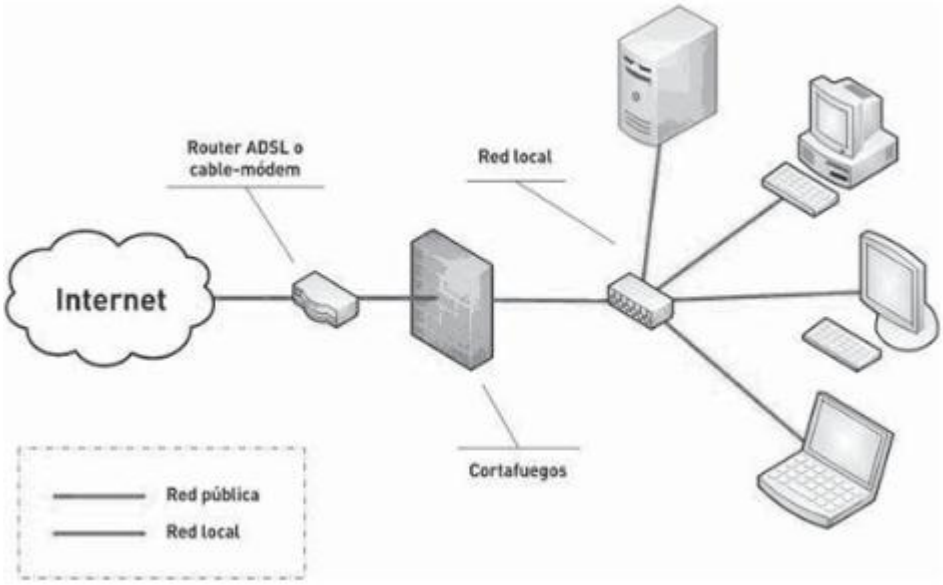
  Independientemente de la marca que se escoja, lo importante es aprovechar todas esas herramientas adicionales que ofrecen los fabricantes; como consolas de actualización, protección a dispositivos móviles, atención personalizada y capacitación al personal de TI.

- ✓ **Monitoreo**: el uso de software "*sniffer*", por ejemplo, puede ayudar a monitorear lo que pasa en la red de la organización, o el chequeo de los "*logs*" en los distintos sistemas es indispensable a la hora de detectar fallas o posibles amenazas.

- ✓ **Computación en la nube**: esta novedosa herramienta se complementa directamente con **el almacenamiento en la nube** y lo que se busca es tener acceso a los archivos y poder trabajar con ellos desde cualquier lugar del mundo, bajo la seguridad de una infraestructura ofrecida por una empresa particular. Un ejemplo de esto es Office365 que le permite al usuario trabajar con todas las aplicaciones de Office (Word, Excel, Power Point, Access, OneDrive, etc.) en línea, sin depender de dispositivos de almacenamiento locales y abaratando costos de licenciamiento.

- ✓ **Firewall**: estas aplicaciones, nativas en los sistemas operativos, o de red si se prefiere, están en la capacidad de filtrar paquetes a través de reglas establecidas para el tráfico entrante o saliente. También existen como dispositivos hardware pero su costo es muy elevado. Los que se aconseja en hacer una configuración del firewall que viene por defecto con el sistema operativo y complementarlo con la instalación de otros en sitios específicos de la red.

Figura 10. Ejemplo de ubicaión de Firewall



Fuente: COSTAS SANTOS, Jesús. Seguridad Informática. Madrid: Ra-Ma, 2014. p. 215. ISBN 978-84-9964-313-7.

- ✓ **Proxy**: este es un servicio de red con el que se puede complementar la seguridad de la misma al permitir crear reglas de uso y de acceso a los sitios web, hablado del proxy HTTP que es el más usado. Su principal ventaja es el rendimiento pues, evita que el cliente envié las peticiones directamente al servidor de la página web ya que hace las veces de intermediario.

- ✓ ***VPN's***: el uso de este método de comunicación representa una gran ventaja pues, permite la conexión de un dispositivo a la red interna de una empresa desde cualquier parte y de forma segura. Su funcionamiento se basa en la arquitectura cliente/servidor y se requiere de un usuario y una contraseña para establecer el enlace, el cual se encontrará cifrado de principio a fin.

- ✓ ***IDS***: "Los Sistemas de Detección de Intrusos (*Intrusion Detection Systems*) son los sistemas encargados de detectar y reaccionar de forma automática ante los incidentes de seguridad que tienen lugar en las redes y equipos informáticos"[37]. Estos pueden existir a nivel de host o a nivel de red y su labor consiste en el monitoreo constante, dando aviso a los administradores en caso de hallar fallas

[37] GÓMEZ VIEITES, Op. Cit., p. 57.

o posibles intrusiones. Se complementan con el uso de los ***IPS*** (*Intrusion Prevention Systems*) o sistemas de prevención de intrusos, los cuales van más allá de la monitorización al contrarrestar algunos tipos de ataques entes de que se ejecuten.

La implementación de todos o algunos de estos controles está sujeta a la disposición económica de las organizaciones pues, la compra o adquisición de estos elementos en algunos casos es costosa. No obstante, existen bastantes alternativas para la protección de la información, y esto quiere decir; que aunque no se cuente con los recursos económicos suficientes siempre se puede brindar una protección eficiente a los datos.

Como última medida y en caso de falla de aquellas que se lograran implantar, se recomienda, según el doctor Álvaro Gómez Vieites[38], la definición de un **Plan de Respuesta a Incidentes**. Este debe contener los siguientes pasos:

- ✓ **Construcción de un equipo de respuesta a incidentes**: el ***CSIRT*** (*Computer Security Incident Response Team*) o Equipo de Respuesta a Incidentes de Seguridad Informática, "está constituido por las personas que cuentan con la experiencia y la formación necesaria para poder actuar ante las incidencias y desastres que pudieran afectar a la seguridad informática de una organización"[39].

- ✓ **Definición de una guía de procedimientos**: esta guía debe contener los pasos concretos para la recuperación rápida y eficiente en caso de un incidente, a fin de salvar los datos y la operatividad de los sistemas afectados.

- ✓ **Detección de un incidente de seguridad**: la organización debe estar en constante revisión de los sistemas de información y comunicación en busca de cambios o irregularidades que representen una posible intrusión.

- ✓ **Análisis del incidente**: en este punto se debe indagar sobre el alcance del incidente, cuáles fueron sus causas, que equipos, sistemas o servicios se pudieron ver afectados y cuáles fueron sus consecuencias.

[38] Ibid., p. 71.

[39] Ibid., p. 72.

- ✓ **Contención, erradicación y recuperación**: estas tres actividades representan momentos distintos después de ejecutado un ataque. La primera; lo que busca es determinar cómo limitar el accionar de la agresión mientras se establece su origen. Aquí se debe tener cuidado pues cualquier acción puede ocasionar daños mayores al sistema afectado. La erradicación es el periodo donde se ejecutan todas las tareas necesarias para eliminar la causa del incidente, y la recuperación, está enfocada en recobrar la funcionalidad de los sistemas afectados y el retorno de la operatividad segura de los mismos.

- ✓ **Identificación del atacante y posibles actuaciones legales**: aunque esta tarea no es nada fácil, en caso de lograr identificar al atacante se deben conocer los mecanismos legales para poder exigir las respectivas indemnizaciones. Se dice que no es fácil porque en la mayoría de los casos se logra identificar las maquinas desde donde se lanzó el ataque pero no al individuo.

- ✓ **Comunicación con terceros y relaciones públicas**: aquí se deben contemplar los mecanismos de comunicación de las causas y consecuencias del incidente a, por ejemplo: proveedores, clientes, autoridades y fabricantes del hardware y software que se hayan visto afectados directamente.

- ✓ **Documentación del incidente de seguridad**: en este punto se deben registrar datos como: la descripción del incidente, los hechos, daños producidos en los sistemas, la actuaciones por parte de la organización, listar las evidencias y recomendaciones, entre otras.

- ✓ **Análisis y revisión a posteriori del incidente**: lo que se busca en esta etapa es hacer una retroalimentación del incidente, con el fin de avaluar lo aprendido por parte de la organización a raíz de las fallas encontradas.

5.3 MARCO LEGAL

El desarrollo de leyes y normativas legales que tipifiquen y penalicen los delitos informáticos es una actividad que ha venido creciendo en países como Colombia, Argentina, Perú, Bolivia y Ecuador, por nombrar algunos de Latinoamérica. La siguiente imagen evidencia el panorama jurídico frente a los delitos informáticos en esta región.

Figura 11. Panorama jurídico frente a los delitos informáticos en Suramérica

Fuente: http://www.bcra.gov.ar/pdfs/eventos/Delitos_Pres_Antonio_Travieso.pdf

Sin embargo, es evidente que EE.UU y Europa están a la vanguardia frente al tema de la seguridad de la información porque han avanzado en la construcción de herramientas jurídicas que les permite ir de frente contra esta clase de delitos.

España, por ejemplo, cuenta con la **LOPD** (Ley Orgánica de Protección de Datos) desde 1999 y la **LSSICE** (Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico) desde el año 2002, lo que da cuenta que en los países del primer mundo se han tomado en serio la protección de la información.

El Congreso de Europa aprobó en 2001 su **Convenio sobre Ciberdelincuencia** en donde se **definen 4 tipos de delitos informáticos**: "delitos relacionados con el contenido, delitos relacionados con las infracciones a los derechos de autor, delitos relacionados con la informática y delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos"[40].

[40] GÓMEZ VIEITES, Álvaro. Auditoría de seguridad informática. Madrid: Ra-Ma, 2014. 147 p. ISBN 978-84-9964-328-1.

Estados Unidos por su parte, también cuenta con una fuerte legislación frente al tema de la seguridad de la información, desde que en el año de 1984 se aprobara "la ley conocida como *The Computer Fraud and Abuse Act* **(CFAA)**, que tipifica delitos como el abuso o fraude contra entidades financieras, registros médicos o sistemas de información de Seguridad Nacional"[41]. En 1986 se aprobó la "*Electronic Communications Privacy Act* **(ECPA)**" y en 1988 la ley federal denominada "*Digital Millenium Copyright Act* **(DMCA)**" para proteger los derechos de autor en publicaciones digitales.

En **Colombia**, solo hasta el 2009 se vino a tratar con rigurosidad el tema de la seguridad de la información con el nacimiento de la **Ley 1273 de 2009**, "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"[42].

Esta ley fue redactada por el juez segundo de control de garantías **Alexander Díaz**, uno de los mayores expertos en nuevas tecnologías del derecho y protección de datos, quien además afirma, según entrevista dada por él al periódico El Espectador, que la ley de delitos informáticos de Colombia es la mejor del continente: "tan es suficiente y está bien hecha que fue 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"[43].

Es importante decir que esta ley es un gran paso en la lucha contra los delitos informáticos pues, su texto es lo más explícito posible, abarcando todos los aspectos relacionados con la protección de la información y brindando los mecanismos necesarios para que las empresas tomen las medidas pertinentes para proteger sus datos, como adecuar los contratos de trabajo, establecer sanciones, modificar los reglamentos internos y hacer uso de cláusulas de confidencialidad.

Algo que se debe resaltar con respecto a la ley 1273 es que con su puesta en marcha las organizaciones y las personas ahora cuentan con una herramienta concreta para poder denunciar, cosa que anteriormente no se hacía, no solo por

[41] Ibid., p. 88.

[42] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. no. 47223. p. 1-4.

[43] EL ESPECTADOR. "En busca de cura para los delitos informáticos" [en línea], mayo 2014 [citado en 18 mayo de 2015]. Disponible en Internet: <http://www.elespectador.com/noticias/politica/busca-de-cura-los-delitos-informaticos-articulo-492170>.

las afectaciones que ello representaba en términos de reputación y prestigio, sino también, porque los mecanismos existentes no eran los apropiados. Es responsabilidad del Estado, a través sus instituciones, hacer que los jueces y fiscales reconozcan la importancia de esta ley y dejen de tipificar los delitos informáticos como clásicos, porque las penas son totalmente distintas entre unos y otros, con lo que se afecta la reivindicación e indemnización de los perjudicados.

Aunque la ley 1273 es el referente fundamental a la hora de hablar de delitos informáticos en Colombia, no es la primera, pues con la expedición de la **Ley 527 de 1999** "por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones", se reconoció fuerza probatoria como documentos a los mensajes de datos. El artículo 10º de esta misma ley dicta que "los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de procedimiento Civil"[44].

5.3.1 **Otras leyes contra delitos informativos en Colombia**. Existen otras normas en la legislación nacional que tratan sobre delitos informáticos y sus penalizaciones.

- ✓ **Ley estatutaria 1266 del 31 de diciembre de 2008** "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones"[45].

- ✓ **Ley 1341 del 30 de julio de 2009** "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones"[46].

[44] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527. (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Archivo General de la Nación. Bogotá, D.C., 1999. no. 43673. p. 1-10.

[45] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley Estatuaria 1266. (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2008. no. 47219. p. 1-12.

[46] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1341. (30, julio, 2009). Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. no. 47426. p. 1-18.

- ✓ **Ley estatutaria 1581 de 2012** "por la cual se dictan disposiciones generales para la protección de datos personales"[47]. Su importancia radica en el tratamiento de la información personal, protegiéndola del uso indebido por parte de instituciones públicas o privadas. Su implementación y cumplimiento se ejecutan bajo el **Decreto 1377 de 2013**, en el que se establecen los mecanismos de protección necesarios para la protección de los datos de los usuarios.

5.4 GENERALIDADES DE LA EMPRESA

5.4.1 **Historia**. La Universidad Cooperativa de Colombia es una institución privada de educación superior, reconocida por el Ministerio de Educación Nacional, y perteneciente al sector de la Economía Solidaria como entidad auxiliar. Su fundación data del año 1958 "cuando un grupo de cooperativistas, liderados por los hermanos Henry y Rymel Serrano Uribe y Carlos Uribe Garzón, deciden apostarle al fortalecimiento de la economía solidaria y en particular al cooperativismo, a partir de la formación de adultos dentro de esta doctrina"[48].

5.4.2 **Cifras**. En la actualidad cuenta con 18 sedes distribuidas por todo el país: Bogotá, Medellín, Barrancabermeja, Santa Marta, Bucaramanga, Montería, Apartadó, Pereira, Cartago, Espinal, Ibagué, Arauca, Villavicencio, Pasto, Popayán, Cali, **Neiva** y Quibdó, y con más de 55.000 estudiantes de todos los estratos sociales, más de 134.000 egresados, más de 4.500 profesores en todas las categorías y más de 3.000 empleados administrativos.

Ofrece a la comunidad 226 programa educativos (7 de ellos acreditados), de los cuales 142 son de pregrado y 84 de postgrado, estos últimos con 66 especializaciones y 18 maestrías, 4 de ellas virtuales.

5.4.3 **Misión.** "Somos una Institución de Educación Superior de propiedad social, formamos personas competentes para responder a las dinámicas del mundo, contribuimos a la construcción y difusión del conocimiento, apoyamos el desarrollo competitivo del país a través de sus organizaciones y buscamos el mejoramiento de la calidad de vida de las comunidades, influidos por la economía solidaria que nos dio origen"[49].

---

[47] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley Estatuaria 1581. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá, D.C., 2012. no. 48587. p. 1-164.

[48] UNIVERSIDAD COOPERATIVA DE COLOMBIA. "Historia" [en línea], 2014 [citado en 19 mayo de 2015]. Disponible en Internet: <http://www.ucc.edu.co/institucion/Paginas/historia.aspx>.

[49] UNIVERSIDAD COOPERATIVA DE COLOMBIA. "Misión" [en línea], 2014 [citado en 20 mayo de 2015]. Disponible en Internet: <http://www.ucc.edu.co/institucion/Paginas/mision-vision.aspx>.

5.4.4 **Visión**. “En el año 2022 seremos una universidad de docencia con investigación, reconocida como una de las instituciones educativas más importantes a nivel nacional, ejercemos actividades con vocación hacia la excelencia, evidenciada en la certificación de procesos, acreditación nacional e internacional, con un equipo humano competente y un modelo de gestión innovador que se apoya en infraestructura física y tecnológica pertinente, comprometidos con la construcción de espacios de desarrollo personal y profesional para la comunidad universitaria y abierta al mundo”[50].

5.4.5 **Plan Estratégico**. En el año 2013 la universidad lanzó su Plan Estratégico Nacional 2013-2022 con el que pretende concretar y materializar su misión institucional sin dejar a un lado su visión dentro del ámbito educativo. La siguiente imagen enmarca los 8 ejes fundamentales del plan estratégico de la institución.

Figura 12. Ejes estratégicos

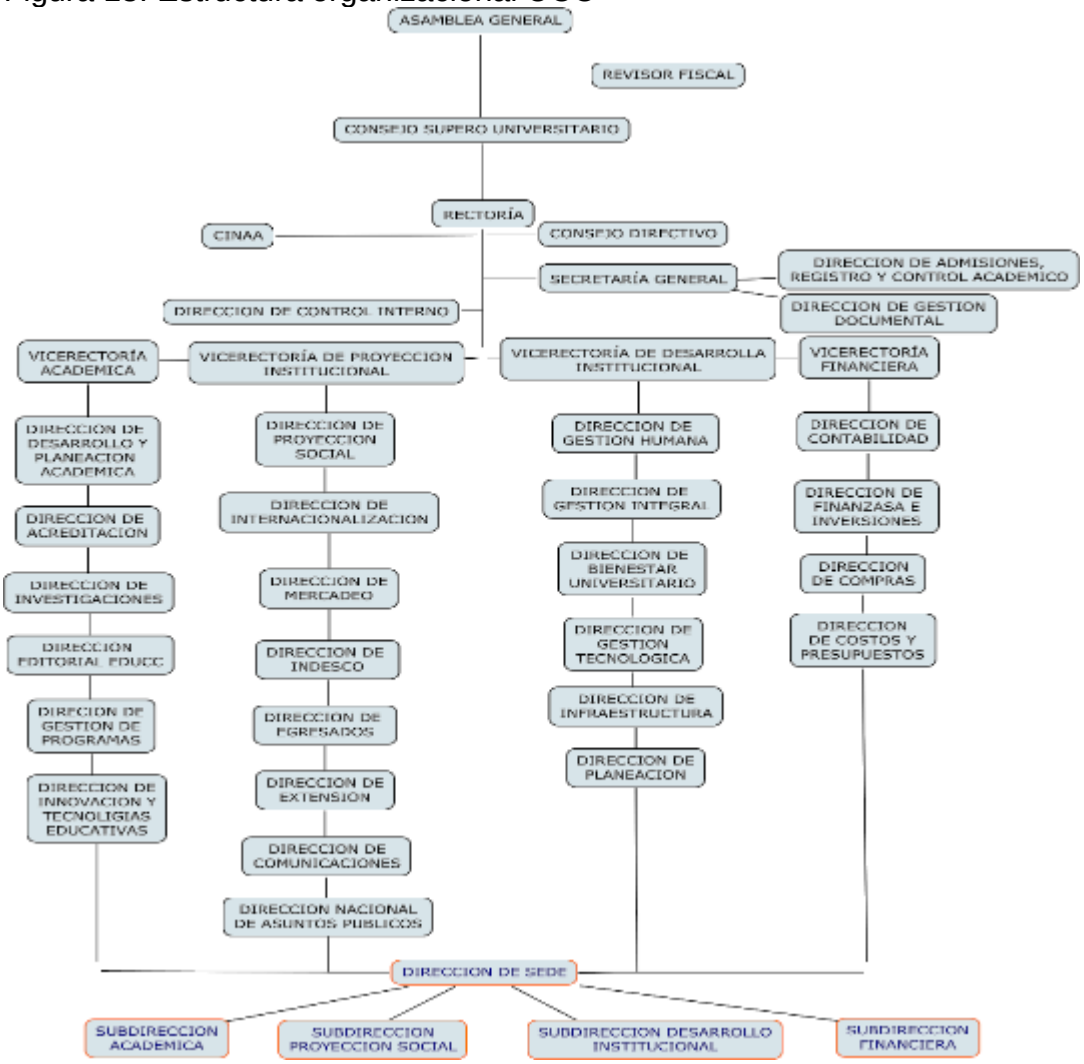
Fuente: http://www.ucc.edu.co/institucion/Paginas/plan-estrategico.aspx

5.4.6 **Organigrama**. La universidad está compuesta, como toda organización del sector solidario, por una Asamblea General y un Revisor Fiscal, luego la

[50] Ibid., p. 1

encabeza la Rectoría; seguida por el Consejo Directivo, la Secretaría General y la Dirección de Control Interno. En el siguiente nivel se encuentran las Vicerrectorías de Proyección Institucional, Desarrollo Institucional, Financiera y Académica, que comprenden una serie de Direcciones y Subdirecciones propias del ámbito empresarial y educativo, para terminar con una Dirección y cuatro Subdirecciones, reflejando la misma estructura a nivel nacional, pero por cada sede.

Figura 13. Estructura organizacional UCC



Fuente: el autor

5.4.7 **Neiva**. De las 18 sedes que componen la institución, Neiva es el centro de interés en esta investigación. Esta cuenta a nivel local con más de 2.800 estudiantes de pregrado y postgrado, ofrece los programas profesionales

de Contaduría Pública, Ingeniería de Sistemas, Derecho, Ingeniería Industrial, Psicología e Ingeniería Civil, además de las especializaciones en Gerencia de la Calidad y auditoria en Salud y Salud Ocupacional.

Esta sede cuenta con 8 bloques distribuidos en distintas zonas del centro de la ciudad, integrando aulas de clase, oficinas administrativas y centros de práctica como el consultorio jurídico, el consultorio psicológico y la Fundación Equinoterapia. Actualmente adelanta un proyecto de campus universitario en uno de sus bloques, ubicado en las afueras de la ciudad pero perteneciente al vecino municipio de Palermo - Huila.

5.4.7.1 **Población trabajadora**. La UCC Neiva cuenta hoy por hoy con una planta administrativa y docente de más de 300 personas de diferente sexo, raza y religión; contratados directamente por la institución.

Tabla 1. Número de trabajadores por sexo y tipo de población

Población	Hombres	Mujeres	Total
Administrativa	43	64	107
Docente	157	44	201
Total	200	108	308

Fuente: el autor

Respecto al nivel de escolaridad de los trabajadores de la UCC Neiva, la mayoría son profesionales con algún tipo de postgrado (especialización, maestría o doctorado); sobre todo la parte docente, y otra pequeña porción solo cuenta con la básica primaria o secundaria; en especial el personal de servicios generales.

Tabla 2. Número de trabajadores por nivel de escolaridad

Población	Número de trabajadores
Primaria completa	13
Secundaria incompleta	4
Secundaria completa	11
Técnico o tecnólogo	33
Profesional	247
Total	308

Fuente: el autor

El horario de trabajo dentro de la institución difiere entre los administrativos y los docentes. Los primeros laboran de lunes a jueves de 8:00 AM a 12:00 M y de 2:00 PM a 7:00 PM y los viernes de 8:00 AM a 12:00 M y de 3:00 PM a 7:00 PM, mientras que las clases inician desde las 6:00 AM hasta las 11:00 PM en jornada continua. Algunos horarios varían de acuerdo a las necesidades del servicio, en especial el personal de aseo y mantenimiento. En cualquier caso, la semana laboral no puede exceder las 44 horas.

5.4.7.2 **Activos tecnológicos**. La Universidad Cooperativa de Colombia siempre ha estado a la vanguardia en cuanto a tecnología e innovación se refiere, no solo en lo que respecta a los equipos de cómputo, sino también, a las comunicaciones y equipos de laboratorio.

Tanto es así que la sede Neiva cuenta actualmente con más de 300 computadores de escritorio y 35 computadores portátiles, distribuidos entre la planta administrativa, salas de docentes, salas de informática y laboratorios. Además, existen cerda de 15 puntos de acceso inalámbrico, los respectivos cuartos de comunicaciones para cada bloque; cada uno con su propia UPS, y un conjunto de servidores, cada uno con funciones diferentes y específicas.

Tabla 3. Distribución de equipos de cómputo

Ubicación	Cantidad
Área administrativa	125
Salas de docentes	49
Salas de informática	120
Laboratorio de psicología 1	15
Laboratorio de psicología 2	3
Laboratorio de física	5
Laboratorio de telecomunicaciones	11
Laboratorio de idiomas	20
Laboratorio Ing. Industrial y civil	2
Portátiles	35
Total	385

Fuente: el autor

Todos los computadores listados anteriormente son nuevos gracias a un proyecto de renovación tecnológica ejecutado a nivel nacional, cuya directriz era reemplazar todas las estaciones de trabajo que tuvieran procesadores inferiores a Intel Core i3 y menos de 4 GB de memoria RAM. En este sentido, la mayoría de equipos tienen procesador Intel

Core i5, 4 GB de RAM y son de diseño todo en uno (*All in One*), o en su defecto, poseen monitores de 19" LCD o LED. Cabe aclarar que existen algunos computadores con características específicas debido a los usos para los que fueron adquiridos, es el caso de los servidores, monitoreo de cámaras y equipos para edición de audio y video.

Tabla 4. Ficha técnica general de equipos de cómputo

Elemento	Detalle
Marcas	Lenovo y HP
Procesador	Intel Core i3 e i5 @ 2.20 GHz o más
Memoria RAM	4 GB o más
Disco duro	500 GB o más @ 7200 RPM
Sistemas Operativos	Windows XP Pro, 7 Pro, 8 Pro, Server 2003, Server 2008, todos @ 64 bits, Debian, Endian Fierwall y PfSense
Monitor	19" LCD o LED y 21" todo en uno

Fuente: el autor

La conectividad ha sido uno de los pilares en el desarrollo institucional de la universidad, por tal motivo, se han venido adelantando múltiples esfuerzos para lograr adquirir un mejor servicio de internet. Hace unos años se contaba con dos canales de 8 MB en el bloque principal y uno de 2 o 4 MB en cada bloque distante. Ahora, la UCC Neiva tiene un canal de fibra óptica dedicado de 100 MB y con miras a una ampliación del servicio a 140 MB, algo que hace que la institución cuente con uno de los mejores servicios de internet entre las universidades de la cuidad, generando a la vez un valor agregado a la actividad educativa en el claustro.

5.4.7.3 **Seguridad**. Este es un tema que la universidad ha tomado en serio en los últimos 4 años. La institución ha desarrollado un proyecto de vigilancia por medio de cámaras IP que arrancó con 15 de estas y hoy tiene más de 25. Su administración se basa en un servidor para el almacenamiento de las grabaciones y una sala de monitoreo con un computador y una pantalla de 42".

Aunque hay que reconocer que falta mucho, sobre todo en cuestiones locativas y controles de acceso, este servicio de vigilancia se complementa con la contratación de una empresa de seguridad privada que dispone de un guarda (no armado) en cada uno de los bloques. Además, esta empresa cuenta con sus propios CCTV (Circuito Cerrado

de Televisión); con cámaras análogas que cubren zonas específicas y sus respectivos DVR.

6. DISEÑO METODOLOGICO PRELIMINAR

En esta sección se abordarán todos los temas relacionados directamente con el proceso investigativo, una serie de pasos y aspectos que enmarcan cualquier investigación y que propenden por un resultado óptimo y pertinente. Como ya se mencionó anteriormente, el tema de esta investigación es la Ingeniería Social y su afectación en el personal administrativo de la UCC Neiva y su información.

6.1 TIPO DE INVESTIGACIÓN

Esta es una investigación de tipo descriptivo y se puede enmarcar, según los criterios de la UNAD, dentro de la línea de investigación de **Gestión de Sistemas**, en el área de **Ciencias de la Computación** y cuya temática es la **Auditoria de Sistemas**.

A través de esta investigación se pretende determinar cuáles son las vulnerabilidades presentes en el recurso humano de la UCC Neiva y en sus áreas de trabajo frente a las metodologías, estrategias o técnicas de las que se valen los ingenieros sociales para obtener acceso a información sensible. En este mismo sentido, se sustenta la necesidad de que el personal identifique rápidamente todas las formas de ataque de la IS y sus consecuencias para la empresa. También es importante el reconocimiento de los distintos mecanismos, por parte del personal de la institución, para evitar ser víctimas de estos tipos de ataques.

Al final, los resultados de este ejercicio investigativo deben poderse aplicar a cualquier tipo de organización pues, el objetivo es describir cómo los delincuentes informáticos logran, de manera sencilla, apoderarse de información sensible de una empresa a través de la ejecución de las distintas técnicas clasificadas dentro de la IS.

6.2 POBLACIÓN Y MUESTRA

Como población y muestra, a la vez, para esta labor investigativa se tomó el 100% de la planta administrativa, incluyendo algunos docentes de tiempo completo que cumplen esta función dentro la sede Neiva de la Universidad Cooperativa de Colombia, puesto que su ambiente laboral permite un fácil acceso a información sensible o a las computadoras a cargo del personal en mención por parte de

agentes externos o no permitidos. Además, cuenta con un número suficiente de trabajadores, cosa que facilita la ejecución de la mayoría de las actividades planteadas en el cronograma.

6.3 VARIABLES

- ✓ Estructura organizacional.
- ✓ Número de trabajadores.
- ✓ Nivel de escolaridad de los trabajadores.
- ✓ Salario de los trabajadores.
- ✓ Políticas de seguridad de la organización.
- ✓ Condiciones locativas en oficinas y zonas comunes.
- ✓ Estructuras de la red de datos y telefonía.
- ✓ Medidas de seguridad físicas y perimetrales.
- ✓ Medidas de seguridad lógicas de la información.
- ✓ Software de seguridad informática.
- ✓ Puntos de acceso telefónico y de datos.
- ✓ Puntos de acceso inalámbrico.

6.4 FUENTES Y TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Durante el desarrollo de esta investigación la información se recolectó principalmente a través de procesos de observación en todas las dependencias y áreas de la UCC Neiva, enfocándose en las actividades diarias relacionadas directamente con el manejo de la información, el uso de los activos tecnológicos; en especial el computador y el teléfono, la disposición del personal en cuanto a la atención a los usuarios, la organización de documentos físicos en las mesas de trabajo, la ubicación de las computadoras en los escritorios, en nivel de acceso físico de los estudiantes a las distintas oficinas o zonas, la ubicación de las cámaras de seguridad y la conducta del personal de vigilancia privada.

También se logró evaluar el uso de los servicios de red y el acceso a páginas web tanto de administrativos, docentes y estudiantes, y los tipos de dispositivos más usados por parte de los usuarios de las redes inalámbricas.

Otras de las formas con que se logró captar más información importante para esta investigación fue a través de la aplicación de cuestionarios con preguntas cerradas y entrevistas no estructuradas al personal administrativo y docentes de tiempo completo, enfocadas en la percepción y conocimiento del tema de seguridad informática.

6.5 RECURSOS DISPONIBLES

El desarrollo de la investigación fue económicamente viable, puesto que no requirió de una gran inversión monetaria por parte del investigador ni de la institución sobre la cual se ejecutó. La mayor parte de los recursos estuvieron relacionados con el tiempo y el esfuerzo del investigador.

6.5.1 **Talento Humano**. La investigación fue ejecutada por el ingeniero Edilberto Bermúdez Penagos, estudiante de la Especialización en Seguridad Informática dictada por la UNAD, quien es el único encargado del desarrollo de la presente propuesta de trabajo de grado.

6.5.2 **Materiales y equipos**. Para el desarrollo de la investigación se contó con un computador portátil de última tecnología (Lenovo E430); con sistema operativo Ubuntu 14.04 LTS; sobre el cual se instaló un software de virtualización para hacer uso de 2 de las distribuciones Linux especializadas en seguridad informática como lo son Kali y Backtrack 5 r3 (sin soporte actual). Dicho equipo también contaba con la suite ofimática LibreOffice, la cual integra un procesador de texto, una hoja de cálculo y un programa de presentaciones, todos ellos suficientes para llevar a buen término este proceso investigativo y su posterior consolidación y análisis de la información.

Además de esto, se contó también con una oficina totalmente equipada con impresora, servicio de internet y la papelería necesaria para el desarrollo del proyecto.

6.5.3 **Recursos financieros**. La ejecución de este proceso de investigación no implicó mayor costo para el investigador ni para la organización en la que se llevó a cabo. Por el contrario, si constituye un gran beneficio para la seguridad de la empresa y la de su información.

Cabe resaltar que fue la UCC Neiva la organización que prestó los recursos mencionados anteriormente para le realización de este ejercicio y que el suministro de estos no representó ningún gasto adicional para la administración de la empresa, pues dichos elementos ya se encontraban asignados al investigador por hacer parte del departamento de gestión tecnología de la institución.

6.5.4 **Cronograma de trabajo**. Tener un orden en la elaboraron de alguna tarea es un aspecto sumamente importante y más aún, cuando se trata de actividades académicas en las que se hace uso de una metodología específica, tal es el caso de una investigación. Sin una guía que indique

paso a paso o de manera general el avance del trabajo, esta labor fácilmente tomaría un rumbo distinto. La siguiente tabla relaciona las actividades pertinentes para el desarrollo de la presente investigación.

Cuadro 1. Cronograma de trabajo

PROYECTO DE SEGURIDAD INFORMATICA									
Ingeniería Social, un factor de riesgo informático inminente en la Universidad Cooperativa de Colombia sede Neiva									
N°	ACTIVIDAD	Mes 1				Mes 2			
		1	2	3	4	1	2	3	4
1	Asesoría								
2	Definición del tipo de proyecto								
3	Definición del tema de la investigación.								
4	Planteamiento del problema								
5	Definición de objetivos, alcance y justificación.								
6	Selección de fuentes documentales								
7	Desarrollo del marco referencial								
8	Diseño de cuestionarios								
9	Aplicación de encuestas.								
10	Análisis de resultados								
11	Entrevistas								
12	Análisis de testimonios								
13	Elaboración de documento								
14	Entrega del proyecto final								

Fuente: el autor

7. RESULTADOS Y EVIDENCIAS

Los resultados iniciales de esta investigación se obtuvieron a través de la aplicación de un cuestionario con preguntas cerradas de una o varias opciones de respuesta (Ver anexo A). Para ello, se aprovechó una reunión que se lleva a cabo mensualmente (el último viernes de cada mes) en el auditorio de la UCC Neiva y al que asiste todo el personal administrativo y docente que labora en la institución. Allí se solicitó la colaboración de los asistentes para el diligenciamiento del cuestionario ya mencionado.

Se logró que 110 asistentes respondieran el cuestionario, incluyendo al personal de servicios generales, manteniendo, auxiliares, jefes y directivos de todas las áreas, y docentes de tiempo completo. Se excluyó a los docentes de medio tiempo y catedráticos porque, aunque hacen parte de la institución, son un sector muy pequeño y no permanecen 100% del tiempo en las instalaciones de la universidad.

Con anterioridad ya se había detallado algunas de las características del recurso humano de la UCC Neiva como su nivel educativo, sexo y tipo de población. Además, se relacionaron algunos aspectos generales de la institución como su misión, visión, historia, estructura organizacional y plan estratégico.

Los resultados a continuación son la consecuencia de un análisis de los datos recogidos y del trabajo de observación que se ejecutó durante todo este proceso investigativo. En la práctica, se ingresaron todas las respuestas de los 110 cuestionarios diligenciados a una hoja de cálculo, donde se utilizaron tablas dinámicas para la elaboración las diferentes gráficas y para la realización de un mejor análisis de los datos encontrados.

7.1 RESULTADOS DE LA ENCUESTA

A la pregunta ¿Sabe usted qué es la Ingeniería Social?, los encuestados respondieron así:

Tabla 5. Pregunta 1 – general en cantidades

¿Sabe usted qué es la Ingeniería Social?	
Opciones	**Cantidad**
Si	29
No	81
Total	**110**

Fuente: el autor

81 de las 110 personas encuestadas dijeron no saber qué es la Ingeniería Social, lo que representa un 74% de la población, un alto porcentaje de usuarios que pueden ser víctimas de ataques informáticos de este tipo. Solo 29 encuestados, un 26%, respondieron afirmativamente.

El tema de la Ingeniería Social es muy conocido por los psicólogos y los abogados; por su contenido legal, además, por las personas relacionadas con las áreas tecnológicas. De ahí que de las 29 personas que reconocen el tema la mayoría son profesionales en estas tres ramas.

Gráfica 1. Pregunta 1 – general en %

Fuente: el autor

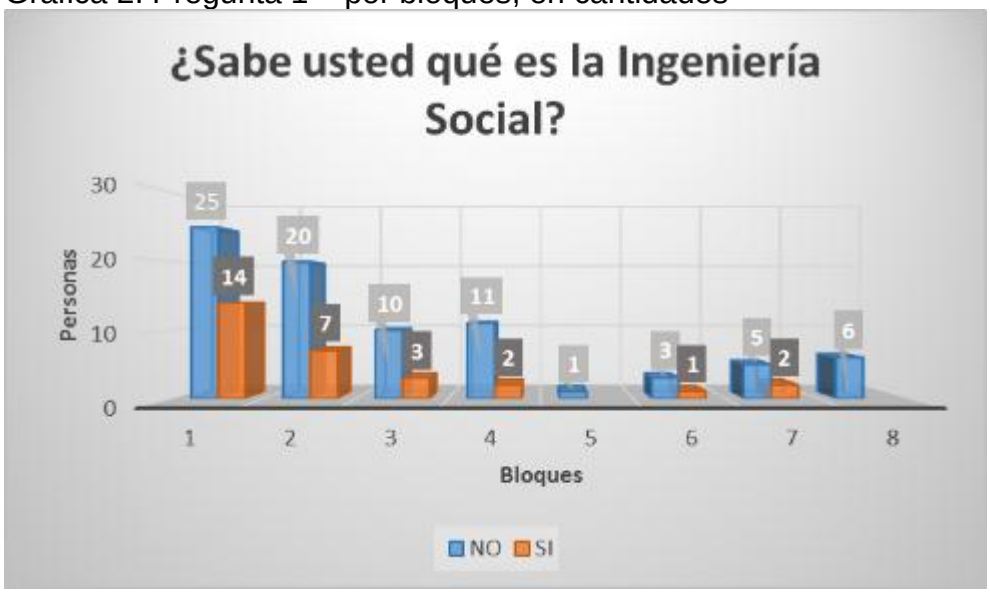
La tabla y gráfica a continuación representan, respectivamente, los porcentajes y cantidades respecto a la primera pregunta, distribuidos por bloques. Del resultado se pudo deducir que el bloque 1 es el más denso demográficamente hablando pero, no es el más propenso a recibir ataques del tipo de la Ingeniería Social. Es el bloque 2 el de mayor riesgo pues, la diferencia entre las respuestas afirmativas y negativas es mayor. Así, como se puede ver en el gráfico 2, en este bloque existen en total 27 usuarios; de los cuales 20 o un 18.2% no sabe nada acerca de la Ingeniería Social, mientras que 7 o un 6.4 si tiene algun conocimiento del tema. Por otro lado, en el bloque 1 existen 39 usuarios, de los cuales 25 o un 22.7% no conocen del tema en cuestión y 14 o un 12.7% sí, diferencia un poco menor comparada con la del bloque 2

Tabla 6. Pregunta 1 – por bloques en %

¿Sabe usted qué es la Ingeniería Social?			
Bloque	**No**	**Si**	**Total general**
1	22,7%	12,7%	35,5%
2	18,2%	6,4%	24,5%
3	9,1%	2,7%	11,8%
4	10,0%	1,8%	11,8%
5	0,9%	0,0%	0,9%
6	2,7%	0,9%	3,6%
7	4,5%	1,8%	6,4%
8	5,5%	0,0%	5,5%
Total general	73,6%	26,4%	**100%**

Fuente: el autor

Gráfica 2. Pregunta 1 – por bloques, en cantidades



Fuente: el autor

Respecto a la pregunta número 2, 66 de los 110 encuestados, equivalentes al 60 % de la población, respondieron afirmativamente frente a si habían recibido llamadas o correos electrónicos que les solicitaban información personal o confidencial relacionada con la universidad, mientras que 44 encuestados o el 40% respondieron negativamente.

Lo que se pudo deducir en este punto es que existe una amenaza permanente sobre el personal de la institución, que busca obtener de manera fraudulenta información confidencial, ya sea del usuario o de la misma universidad, principalmente a través de correos electrónicos enviados, en especial, a las cuenta de correo personales o de dominios ajenos al de la UCC Neiva.

Gráfica 3. Pregunta 2 – general en cantidades

Fuente: el autor

Tabla 7. Pregunta 2 – por bloques en % y cantidades

Llamadas telefónicas o correos electrónicos que solicitan información personal o confidencial relacionada con la universidad						
Bloque	**No**		**Si**		**Total general**	
1	14	36%	25	64%	39	100%
2	10	37%	17	63%	27	100%
3	4	31%	9	69%	13	100%
4	7	54%	6	46%	13	100%
5		0%	1	100%	1	100%
6	2	50%	2	50%	4	100%
7	4	57%	3	43%	7	100%
8	3	50%	3	50%	6	100%

Total general	**44**	**40%**	**66**	**60%**	**110**	**100%**

Fuente: el autor

Frente al tema de la capacitación, quizás el más importante en lo referente a la seguridad informática, se nota un evidente rezago de este punto por parte de las directivas de la institución. Solo 6 personas o un 5.5 % de la población encuestada dice haber recibido capacitación relacionada con la seguridad informática y/o sobre la ingeniería social, el otro 94.5% o 104 personas no ha recibido formación en este tipo de temas.

Lo que se pudo evidenciar a través de la encuesta es que solo los profesionales en el área de la ingeniería de sistemas cuentan con capacitación relacionada con la seguridad informática, la cual no fue suministrada por la universidad. La tabla que sigue lo demuestra.

Tabla 8. Pregunta 3 – por cargos en % y cantidades

¿Ha recibido capacitación en temas de seguridad informática y más específicamente sobre la modalidad de la Ingeniería Social?		
Opciones	**Cantidad**	**Porcentaje**
No	**104**	94,5%
Si	**6**	5,5%
Porcentaje y cantidades por cargos		
Analistas	3	2,7%
Gestión Tecnológica	2	1,8%
Timonel	1	0,9%
Auxiliares	1	0,9%
Gestión Tecnológica	1	0,9%
Jefes	2	1,8%
Gestión Tecnológica	1	0,9%
Ingeniería de Sistemas	1	0,9%
Total general	**100%**	**110**

Fuente: el autor

Hay que hacer hincapié en que en esta instancia son muchos los puntos débiles que tiene la universidad, al menos en lo concerniente al personal administrado y docente y a su capacitación en los aspectos de la seguridad informática y de la información. Son más de 100 personas que no han tenido relación con esta clase temas y que se convertirán, muy seguramente, en potenciales víctimas de los delincuentes informáticos y en fallas latentes en la seguridad de la información de la institución.

Gráfica 4. Pregunta 3 – por cargos, en cantidades

Fuente: el autor

A la pregunta ¿se siente usted conforme con el desempeño y las prestaciones del software antivirus usado en la universidad?, el 65% de los encuestados respondió afirmativamente, un 10% negativamente, un 9% no lo sabe y restante 16% no lo usa. Ese 16% equivale a 17 personas que no cuentan con equipo de cómputo; como los integrantes de grupo de mantenimiento y servicios generales. El 9% de los encuestados que respondió no saber y que equivalen a 10 personas, son principalmente los aprendices del SENA, que son nuevos y se cambian periódicamente, y algunos nuevos administrativos que poca relación han tenido con el software antivirus.

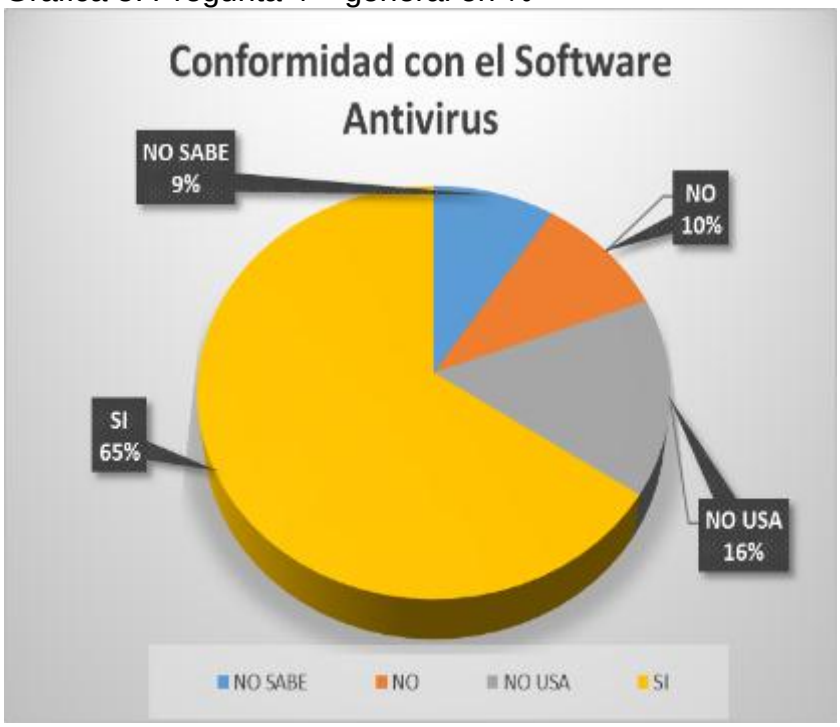
Tabla 9. Pregunta 4 - general en cantidades

¿Se siente usted conforme con el desempeño y las prestaciones del software antivirus usado en la universidad?	
Opciones	**Cantidad**
No sabe	10
No	11
No usa	17
Si	72
Total general	**110**

Fuente: el autor

Según estadísticas, Kaspersky® es uno de los mejores antivirus del mercado. Da soporte a Windows, Mac y Android, ofreciendo un conjunto de módulos adicionales que convierten la aplicación en más que un simple antivirus aislado. Además, ofrece a sus clientes diferentes paquetes de acuerdo a sus necesidades. En el caso de la universidad, se ha instalado una consola de administración y se cuenta con tres tipos diferentes de instaladores, cada uno enfocado a tipos específicas de redes o entornos de trabajo. La siguiente gráfica muestra la información de una manera más clara.

Gráfica 5. Pregunta 4 – general en %



Fuente: el autor

Uno de los puntos más relevantes tocados en la encuesta es la seguridad y composición de las contraseñas de acceso a los sistemas de información y a los mismos computadores. La universidad, a nivel nacional, cuenta con un controlador de dominio, en donde se "*loguean*" todos los usuarios en las redes locales de cada sede y/o bloque. También está el servicio de correo institucional y más de 3 sistemas de información diferentes. De ahí la importancia a la hora de elaborar una contraseña lo suficientemente segura y de fácil recordación.

A la pregunta, ¿considera usted que su contraseña es lo suficientemente segura?, 40 de los encuestados correspondientes al 36.4% de la población respondió negativamente, 41 que equivalen al 37.3% respondieron afirmativamente, 25 personas que representan un 22.7% respondieron que no usan contraseñas y el restante, 4 personas o el 3.6% dijo no saber.

Tabla 10. Pregunta 5 – general en %

¿Considera usted que su contraseña es lo suficientemente segura?	
Opciones	**Porcentaje**
No	36,4%
No sabe	3,6%
No usa	22,7%
Si	37,3%
Total general	**100%**

Fuente: el autor

Se logró deducir que un gran porcentaje de los usuarios (36.4%) de los equipos de cómputo y sistemas de información de la universidad no tienen la suficiente conciencia a la hora de crear sus contraseñas de acceso. Esto es un efecto normal, teniendo en cuenta que la institución tiene varias plataformas para actividades diferentes, razón por la cual los usuarios prefieren usar contraseñas como “12345678”, “246813579”, “qwer1234”, datos personales o palabras comunes, que para ellos son fáciles de recordar.

Gráfica 6. Pregunta 5 – general en cantidades

Fuente: el autor

También resultó interesante que 25 de los encuestados dijo no usar contraseña, al menos para acceder a su computador, aspecto que puede ser aprovechado fácilmente por un ingeniero social para lograr ingresar a la red local de la institución, sistemas de información o para recabar información importante para organizar un ataque a mayor escala. La gráfica siguiente hacer referencia a este tema.

Gráfica 7. Pregunta 5 – por bloques, en cantidades

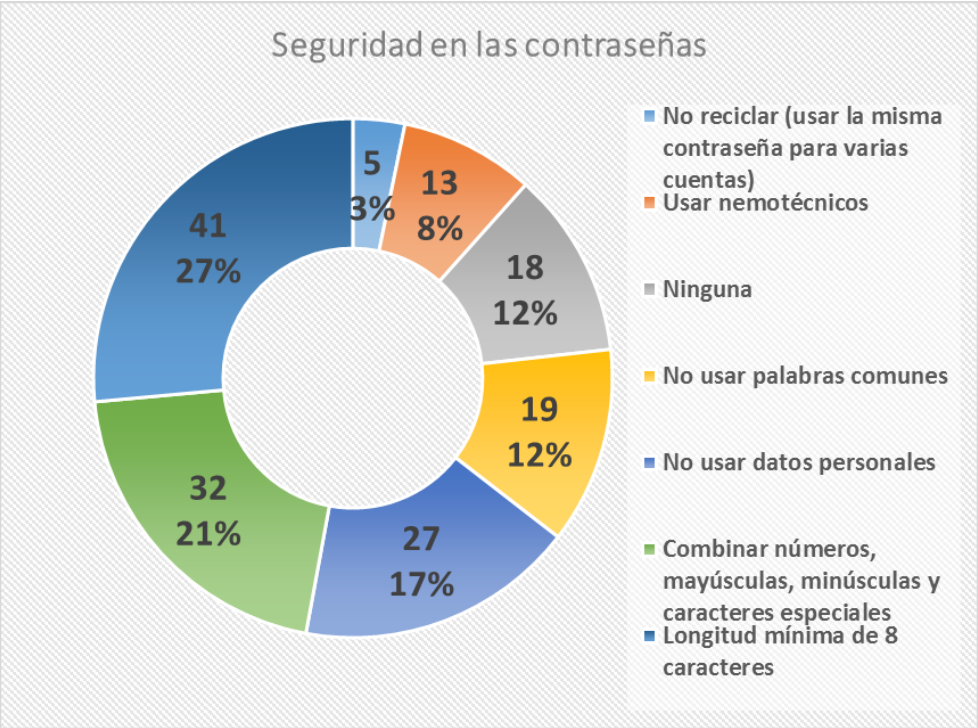
Fuente: el autor

Podría parecer que es el bloque 1 el más afectado por esta falla de seguridad pero no es así, la mayoría de los encuestados que respondieron que no usan contraseña es porque no tienen computador a cargo. Pero, al menos dos usuarios de computadores en la universidad, los usan sin contraseña de acceso. Estos son; un aprendiz SENA y el practicante de gestión humana. Es importante resaltar que no hace falta que muchos usuarios caigan en esta falla de seguridad para que un ingeniero social pueda hacer de las suyas dentro de la universidad, con un usuario que deje una sesión abierta es suficiente para un delincuente informático.

Otro tema importante alrededor de las contraseñas es el de las técnicas que se pueden usar para su elaboración. Se preguntó a los encuestados sobre cuáles de los distintos métodos para crear contraseñan seguras usaban a la hora de crear las suyas. El resultado encontrado fue que la técnica de mayor uso es la de una longitud mínima de 8 caracteres; con una aceptación del 27%. Esto puede deberse a las políticas de seguridad establecidas por algunas plataformas o sistemas de información propios o ajenos a la universidad que exigen esta longitud como único requisito. Otra de las técnicas con mayor uso es la de combinar números, mayúsculas, minúsculas y caracteres especiales; con un 21%, debido, de igual forma, a que los diferentes portales han venido adoptando este método como una medida para fortalecer la seguridad de sus sistemas y proteger la información de sus usuarios.

Se pudo deducir a la vez, como lo demuestra la gráfica a continuación, que quizás las técnicas más importantes como la de no reciclar las contraseñas o la de usar nemotécnicos son las menos usadas, con un 4% y 11% respectivamente. La causa de este fenómeno radica en que los usuarios prefieren crear sus contraseñas, basados en elementos fáciles de recordar y que cumplan con las exigencias mínimas de los sistemas de información.

Gráfica 8. Pregunta 6 – general en % y cantidades



Fuente: el autor

En la medida en que los sitios web y sus plataformas exijan a los usuarios mayor rigurosidad a la hora de crear sus contraseñas de acceso, obligándolos a usar la mayor parte de las técnicas existentes para ello, se evitará que las personas creen claves al azar y sin ninguna precaución. Se evidencia esto en el 12% de los usuarios en la universidad que no usan ninguna de las técnicas propuestas.

A la pregunta, ¿considera usted que la información que maneja es sensible o confidencial para la universidad?, se encontró que la mayoría de los encuestados, en los diferentes bloques, considera que la información que pasa por sus manos es de vital importancia para la institución. Pocas personas piensan que no es así y otro tanto dijo no saber. Este es un aspecto que raya en la percepción que cada quien tiene de sus responsabilidades. Por lo regular, las personas que respondieron negativamente son de contratación temporal, empleados nuevos y algunos de servicios generales.

Gráfica 9. Pregunta 7 – por bloques, en cantidades

Fuente: el autor

En la encuesta se preguntó también sobre el control de acceso físico a las instalaciones de la universidad, haciendo énfasis en si el encuestado lo consideraba suficiente o apto para los intereses de la institución. Se halló que dos terceras partes de la población, equivalente a un 70%, no consideraron suficiente o apto dicho control. El otro 30% equivalente a 33 personas si lo consideraron suficiente.

Es evidente que la gran mayoría de las personas que componen planta administrativa y docente que labora en la universidad no se sienten seguras dentro de las instalaciones de la misma porque para cualquier agente externo es muy fácil ingresar.

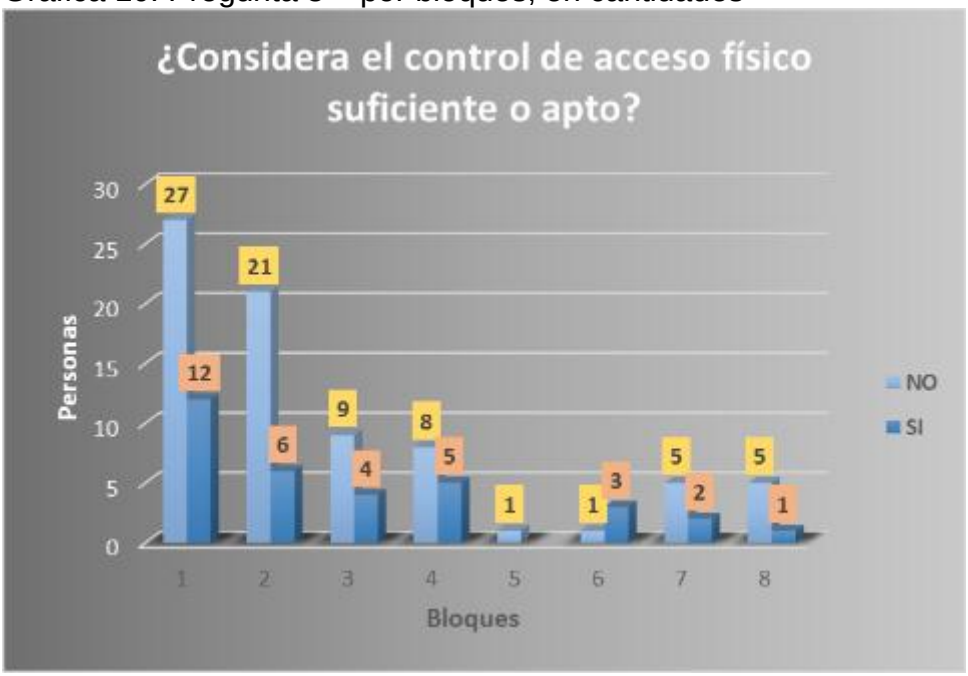
Tabla 11. Pregunta 8 – general en % y cantidades

¿Considera suficiente o apto en control de acceso físico a la universidad?		
Opciones	**Cantidad**	**Porcentaje**
No	77	70%
Si	33	30%
Total general	**110**	**100%**

Fuente: el autor

Esta misma información se distribuyó en los distintos bloques y se encontró que son el 1 y el 2 donde las personas se sienten más inseguras. En el resto de los bloques la deferencia entre una respuesta y otra es menor.

Gráfica 10. Pregunta 8 – por bloques, en cantidades



Fuente: el autor

En cuanto al tema de la ubicación física de los computadores en las oficinas o áreas de trabajo, se les preguntó a los encuestados sobre si éste se encontraba ubicado de tal forma que permitía que quien estuviera en frente suyo lograra ver lo que se digitaba en el teclado y al mismo tiempo el monitor o la pantalla. La importancia de esta pregunta radica en que para los ingenieros sociales es muy fácil captar información si se logra ver estos dos periféricos a la vez, así, pueden hacerse con los usuarios y claves y con las URL's de los sistemas de información.

Tabla 12. Pregunta 9 – general en % y cantidades

¿Su PC está ubicado de tal forma que la persona que está enfrente puede ver el teclado y el monitor mientras usted trabaja?		
Opción	**Cantidad**	**Porcentaje**
No	24	21,8%
No usa	23	20,9%
Si	63	57,3%
Total general	**110**	**100**%

Fuente: el autor

Se logró evidenciar que 63 de los encuestados o el 57.3% de la población cree que la ubicación de su computador permite que otras personas puedan ver lo que digita y lo que hay en su pantalla, las personas que respondieron negativamente y las que dijeron no usar computador representan cantidades y porcentajes muy similares.

Gráfica 11. Pregunta 9 – por bloques, en cantidades

Fuente: el autor

La grafica anterior demuestra que es el bloque 2 el lugar donde esta falla es más frecuente pues, de sus 27 usuarios, 20 respondieron afirmativamente. En el bloque 1 los resultados demuestran un poco más de equilibrio entre los que respondieron afirmativamente y la suma de los que dijeron no saber y los que respondieron negativamente.

Del mismo modo, era importante determinar el orden de los puestos de trabajo de cada uno de los encuestados. Se les preguntó si su escritorio estaba ordenado, es decir, sin documentos sueltos o sin archivar, la mayor parte del tiempo. Esto porque para un ingeniero social uno de los recursos más importante es lo que se puede ver fácilmente, y el hecho de tener un escritorio desordenado facilita que alguien pueda tomar una fotografía o hurtar documentos con información confidencial, ya sea para la institución o para el mismo individuo. También se cuentan en estos documentos los famosos "*post it*" en donde las personas suelen escribir contraseñas, nombres de usuario o información personal como números de teléfono o de identificación.

Tabla 13. Pregunta 10 – por bloques, en %

¿Su escritorio se encuentra ordenado la mayor parte del tiempo?				
Bloque	**No**	**No usa**	**Si**	**Total general**
1	16,5%	7,8%	13,6%	37,9%
2	8,7%	2,9%	14,6%	26,2%
3	4,9%	1,0%	6,8%	12,6%
4	1,0%	1,0%	10,7%	12,6%
6	1,9%	1,0%	1,0%	3,9%
7	3,9%	1,0%	1,9%	6,8%
Total general	**36,9%**	**14,6%**	**48,5%**	**100%**

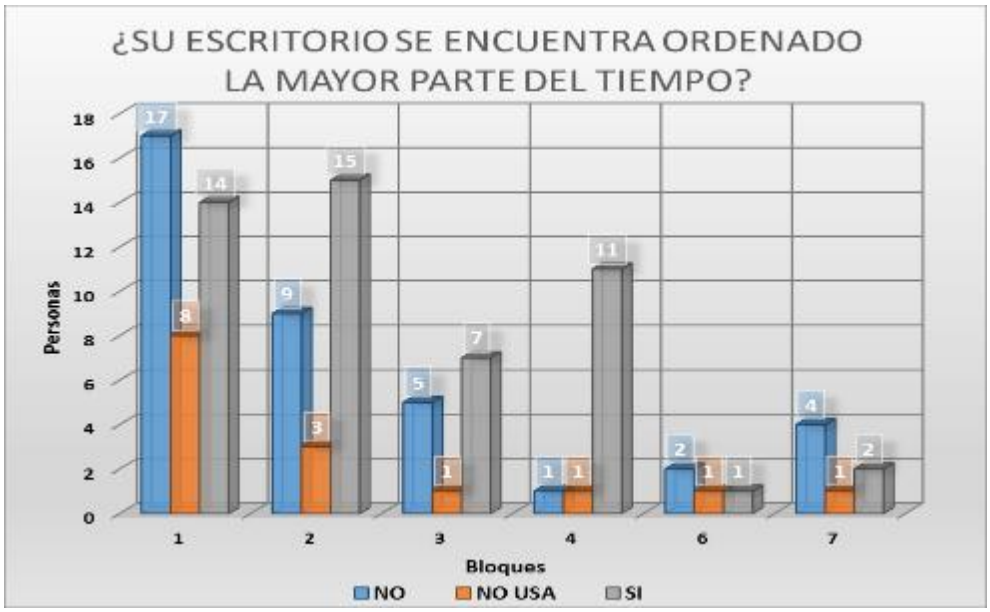
Fuente: el autor

El bloque donde menos se presenta esta irregularidad es el 4 pues, de sus 13 encuestados 11 respondieron afirmativamente, 1 negativamente y el restante no usa escritorio. Esto lo convierte en el bloque menos vulnerable a ataques como el de espiar por encima del hombro (*Shoulder Surfing*).

En el bloque 1 la situación es un poco más pareja entre los que respondieron afirmativamente y los que no, evidenciando de todas formas que casi la mitad de los encuestados de este lugar tienen desorden en su área de trabajo, facilitando la labor de los delincuentes informáticos.

En el bloque 2 el escenario es totalmente distinto. Allí más de la mitad de los encuestados respondió afirmativamente, aunque 9 de ellos lo hicieron negativamente y otros 3 no tienen escritorio. De todas formas son bastantes los usuarios que representan un riesgo en este bloque. La imagen que sigue representa de una forma más clara es la distribución en este aspecto.

Gráfica 12. Pregunta 10 – por bloques, en cantidades



Fuente: el autor

Otra de las preguntas relevantes en la presente encuesta fue ¿por cuáles de las siguientes amenazas se ha visto afectado alguna vez dentro de la universidad?, y se presentaron ocho opciones de respuesta.

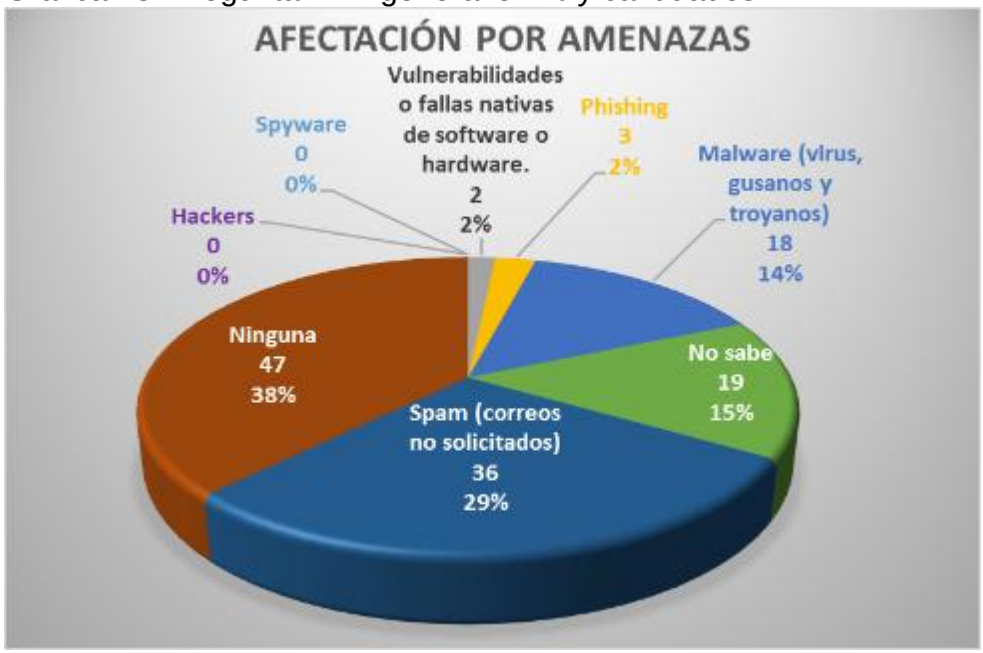
Con la gráfica siguiente se pudo afirmar que la amenaza más común dentro de la universidad es el "*spam*" con un 29%, luego le siguen los "*malware*" con un 14%, el "*Phishing*" con tres casos que representan un 3% y por último, las vulnerabilidades nativas de hardware y software con dos casos equivalentes a un 2%. El 38% de la población encuestada dijo no haberse visto afectado por las amenazas listadas, un 19% no sabe y ninguno ha sido víctima de un "*hacker*" o del "*spyware*".

Lo que se puede deducir de estos resultados es que el "*spam*" está a la orden del día en los correos, privados o institucionales, de los usuarios dentro de la universidad. Los "*malware*", aunque en menor medida, afectan seriamente la información del personal administrativo pues, si bien no ha habido casos de pérdida total de los datos, si logran ocultarla y causar retrasos en las labores de la víctima. La mayoría de estos "*malware*" son provenientes de los estudiantes o de los computadores personales de los trabajadores, que viajan a través de dispositivos como las USB, que al llegar a los computadores de la universidad, el antivirus los detecte y elimina, quedando solo su rastro o las carpetas ocultas.

Los dos afectados por las vulnerabilidades nativas de hardware y software perdieron toda su información debido a daños físico de los discos duros de los equipos a su cargo. Aunque se logró recuperar parte de la información perdida

gracias a las copias de seguridad, estas eran de varios meses atrás, lo que perjudicó seriamente a las víctimas. Respecto a los casos de "*Phishing*" en tres de los encuestados, hay que decir que no se materialización gracias a las buenas prácticas y cuidados de esos usuarios a la hora de hacer transacciones en línea.

Gráfica 13. Pregunta 11 – general en % y cantidades



Fuente: el autor

Por último, se puede deducir que el software antivirus cumple en gran medida con su labor y que no todos los encuestados que respondieron no saber son de servicios generales. Están incluidos allí algunas personas nuevas o con pocos conocimientos en informática.

La última pregunta de esta encuesta fue ¿Cuál cree usted que es el medio más propenso a permitir las amenazas informáticas dentro de la universidad? Su importancia radica en que en la institución no existen mayores restricciones frente al uso del internet.

Como resultado se encontró que 41 de los 110 encuestados dijeron que las descargas eran el medio más propenso para materializar una amenaza, luego 40 dijeron que las redes sociales, 23 la navegación en internet, 19 los correos electrónicos, 17 dicen no saber y 9 escogieron los chats.

De los 110 encuestados, los 17 que dijeron no saber son personal de mantenimiento o de servicios generales que tienen nada o poco contacto con los

medios listados en la pregunta 12. Se pudo deducir que el tema de las descargas, como el de mayor probabilidad para permitir la materialización de una amenaza, fue seleccionado debido al creciente uso de gestores de descarga por parte de los diferentes sitios web. Estos gestores no son explícitos a la hora de su ejecución y coaccionan al usuario para que instalen un sinfín de aplicaciones maliciosas que lo único que logran es dañar o poner en riesgo la información.

En lo que respecta a las redes sociales, en la universidad no existe ningún control sobre el acceso a ellas, lo que permite ataques inminentes de ingeniería social a los empleados de la universidad.

Gráfica 14. Pregunta 12 – general, en cantidades

Fuente: el autor

7.2 CASO PRÁCTICO

El ejercicio descrito a continuación ejemplifica de forma concreta la manera de pensar de un delincuente informático. Lo que se busca es ejecutar paso a paso un ataque de Ingeniería Social dentro de las instalaciones de la UCC Neiva, con el objetivo de demostrar que es factible que se materialicen este tipo de amenazas aprovechando las vulnerabilidades existentes, no solo a nivel tecnológico, sino también, en el recurso humano de la institución.

Para ello se hizo uso del **SET** "*Social-Engineering Toolkit*", que es una completa herramienta de ataque basada en la Ingeniería Social instalada en distribuciones Linux como Kali y Backtrack. Con este software se pueden ejecutar

automáticamente una serie de ataques que comprometen el recurso humano de cualquier organización; desde el envío de mensajes de texto con números falsos, la implementación de servidores "*phishing*" y la suplantación de sitios web, entre otros.

El primer paso de este ataque consiste en la identificación de la víctima, en este caso, cualquier funcionario de la Universidad Cooperativa de Colombia. **Luego, viene la fase de reconocimiento**. En esta se realiza la indagación de las características de seguridad de los bloques de la UCC Neiva. El ingeniero social puede hacerse pasar por un estudiante, por un padre de familia o por un interesado en los programas o servicios que ofrece la institución y aprovechar la falta de control de ingreso a sus instalaciones para entrar a la sede. Estando adentro, puede identificar puntos de red asequibles y funcionales, la ubicación de las cámaras de seguridad, las redes Wi-Fi y la disposición física de las oficinas y los equipos de cómputo. Con un par de pruebas simples; como conectarse a alguna de las redes inalámbricas y hacer uso de los computadores libres ubicados en las distintas zonas públicas, puede darse cuenta que el direccionamiento IP está, al menos, segmentado o depende de servidores independientes, captando la idea de que la parte administrativa está un poco más protegida y de que el acceso a los dispositivos DCE y computadores va a ser muy difícil.

En este punto, el ingeniero social opta por investigar en los otros bloques de la sede, confiando en que allí la seguridad será menor. Solo los bloques 6 y 7; consultorio jurídico y centro de idiomas respectivamente, cuentan con una infraestructura tecnológica amplia pues, en ellos también se dictan clases y se atiente a personal externo. En estos dos bloques es más factible lanzar un ataque de Ingeniería Social porque en la misma red se encuentran computadores de la parte administrativa, académica y puntos de acceso inalámbricos; todos dependientes del mismo servidor.

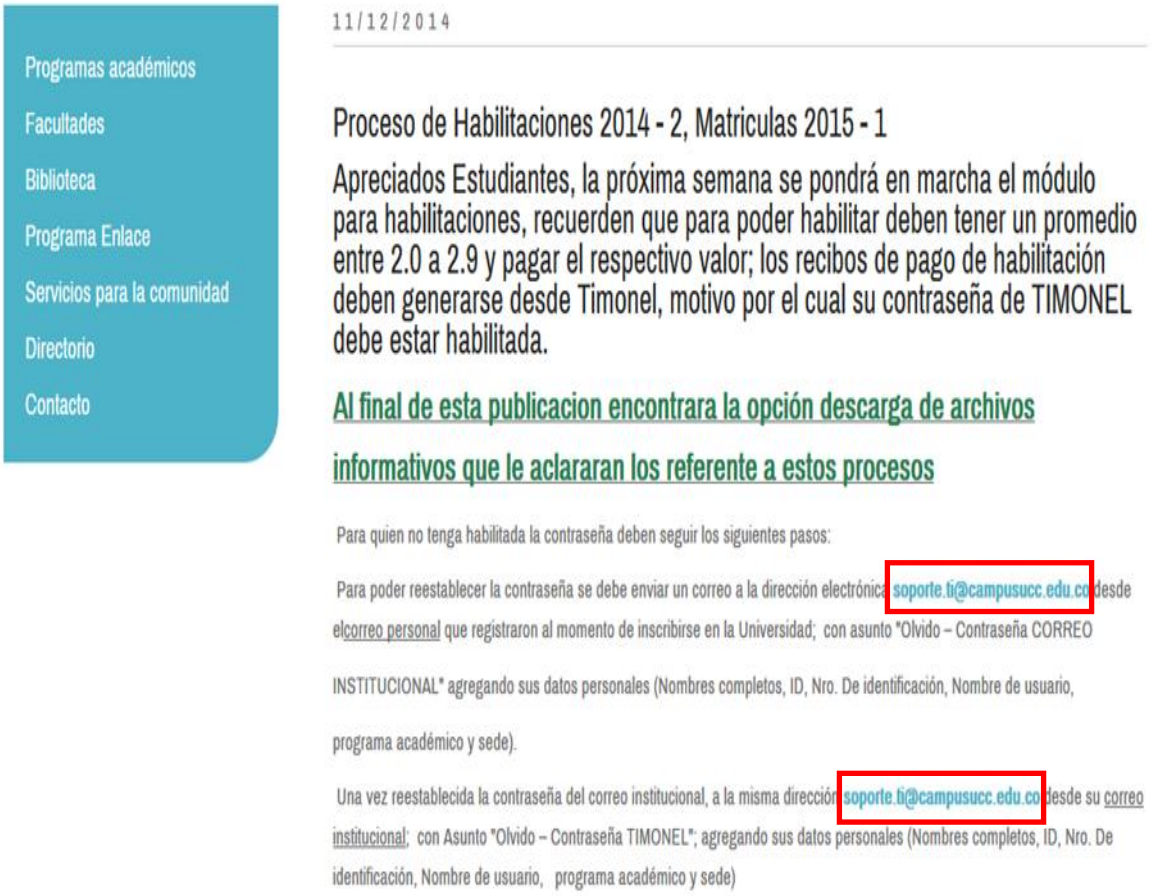
En el tercer paso, que es el de crear el escenario, el atacante decide suplantar la página del logueo del correo institucional con el objetivo de acceder a información confidencial manejada por los usuarios que caigan en la trampa o para lograr recopilar la mayor cantidad de nombres de usuarios, a fin de dirigir sus ataques de manera más selectiva. El tema ahora es de paciencia.

Conseguir el correo institucional de algunos usuarios no es muy complicado, bastaría con preguntárselos fingiendo necesitar enviarles algún documento o dato. Ubicado en alguno de los bloques ya mencionados puede acercarse al personal que allí labora y solicitarles la mayor cantidad de información posible, entre ella; la dirección de correo electrónico.

El cuarto paso es realizar el ataque. Con la información a la mano y las herramientas listas no hace falta un gran esfuerzo para que alguno de los usuarios del bloque seleccionado caiga en la trampa.

Para la ejecución del ataque el procedimiento fue el siguiente: primero se procedió a crear una cuenta de correo ficticia (**soporte.gt@outlook.com**) similar a la del soporte técnico que se encuentran en la página web de la institución www.ucc.educ.co (soporte.ti@campusucc.edu.co) como lo muestra la siguiente imagen.

Figura 14. Correo de soporte real de la universidad

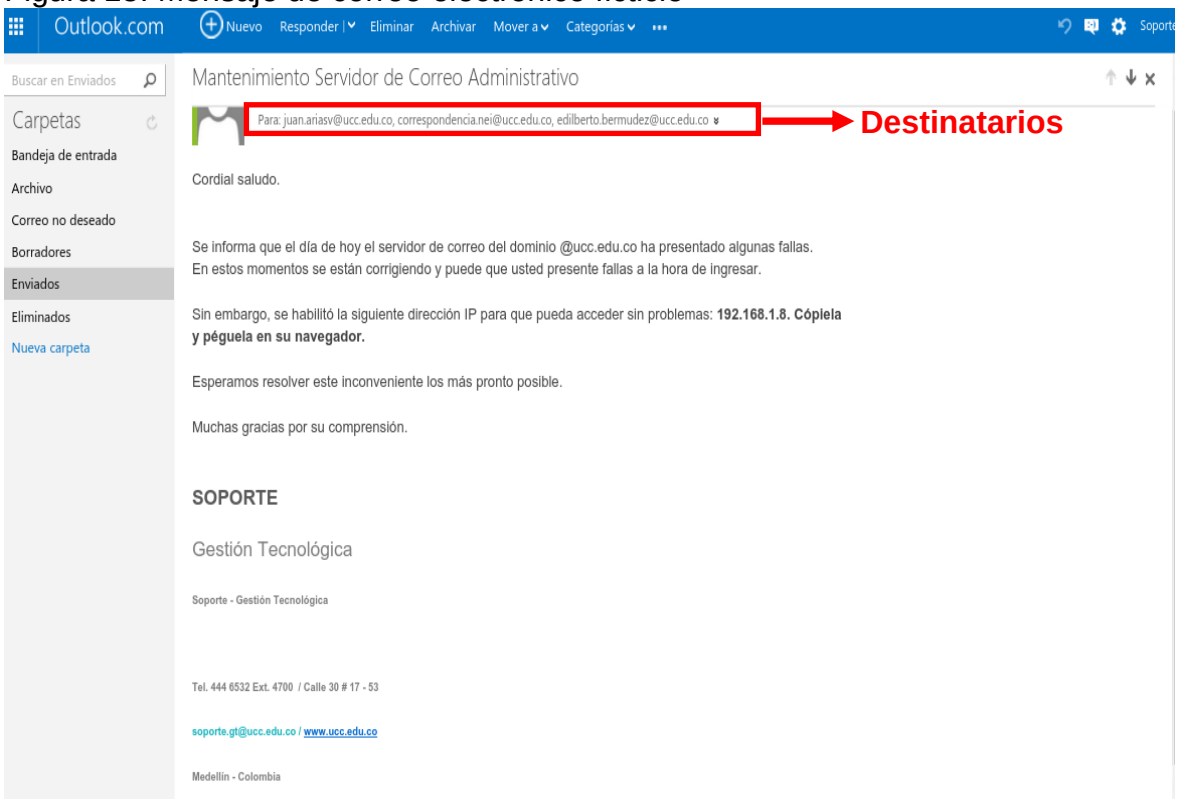


Fuente: http://ucc.edu.co/pasto/prensa/2014/Paginas/2proceso-de-habilitaciones-2014---2,-matriculas-2015---1.aspx

Luego se procedió a redactar un mensaje en el que se informaba a los usuarios de algunas fallas a la hora de ingresar al correo institucional y se daba una dirección IP alternativa para el ingreso. Dicho mensaje fue enviado a algunos usuarios del bloque donde se ejecutó el ataque, entre ellos: juan.ariasv@ucc.edu.co, silvia.valencia@ucc.edu.co, correspondencia.nei@ucc.edu.co y egresados.nei@ucc.eud.co. Cabe aclarar que como el atacante es el mismo investigador y quien además hacer parte de la planta administrativa de la

institución, ya se contaba con las direcciones de correo electrónico de los trabajadores del bloque donde se llevó a cabo este ejercicio práctico. Lo que se tuvo en cuenta fue que los correos a donde se envió el falso mensaje fueran de personas de fácil acceso por parte de personal externo o que tuvieran trato directo con el público.

Figura 15. Mensaje de correo electrónico ficticio



Fuente: el autor

Antes de enviar el mensaje a los usuarios seleccionados, se inicia la configuración del SET "*Social-Engineering Toolkit*" en el computador del atacante. Las imágenes a continuación describen paso a paso ese proceso. Es importante decir que esta herramienta solo funciona dentro de una red local y que antes de usarla de sebe actualizar mediante los comando propios de Linux, ya sea; *apt-get update* o. */set-update*.

El SET "*Social-Engineering Toolkit*" está incluido dentro de las distribuciones Linux Kali y Backtrack y su objetivo principal es la de servir como medio para hacer pruebas de penetración en las redes de las organizaciones. Su uso está sujeto a algunos términos y condiciones bajo la responsabilidad del atacante. Así, la primera imagen demuestra que el usuario debe aceptar los términos del servicio

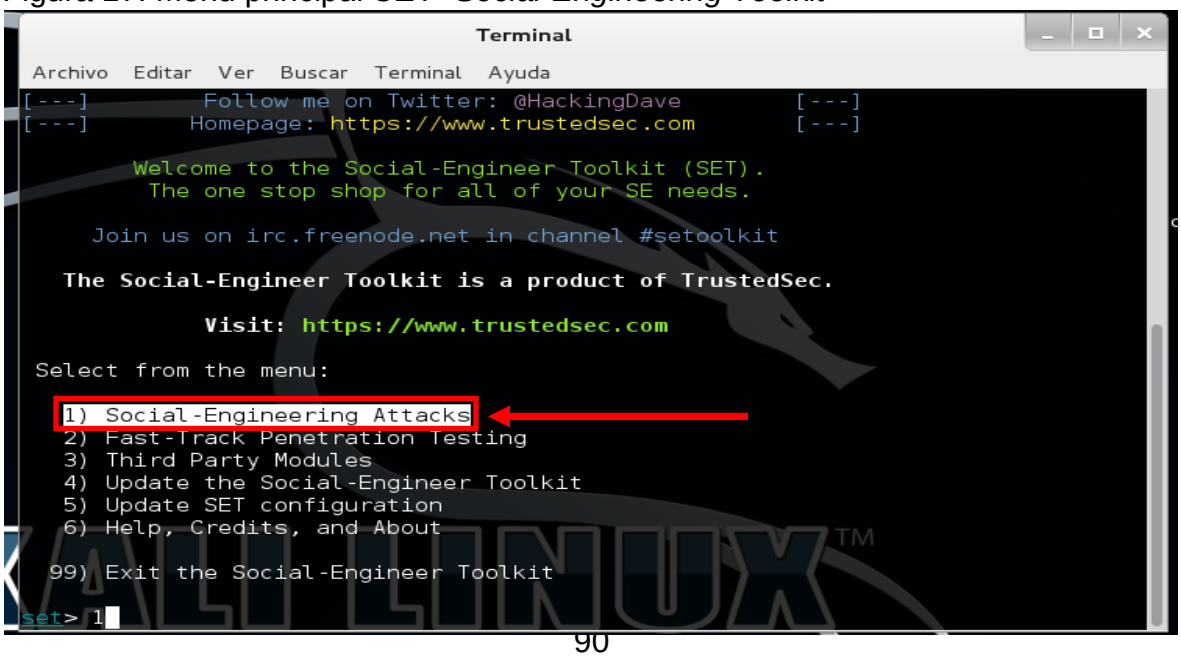
para hacer uso de la herramienta. A la pregunta se debe responder con la letra “y” en caso de querer iniciar el servicio.

Figura 16. Términos y condiciones del SET “*Social-Engineering Toolkit*”

Fuente: el autor

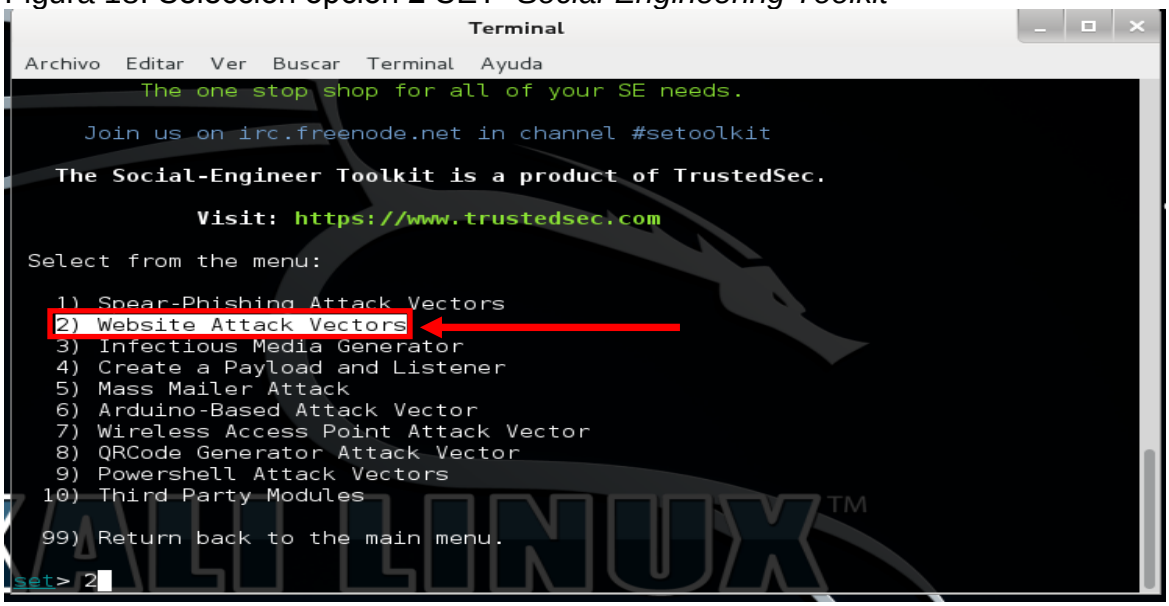
Después de aceptar los términos del SET “*Social-Engineering Toolkit*”, este despliega un menú principal en el que se debe seleccionar la opción 1, en este caso.

Figura 17. Menú principal SET “*Social-Engineering Toolkit*”



Fuente: el autor
En el pantallazo siguiente, se debe seleccionar la opción 2 "*Website Atacks Vectors*".

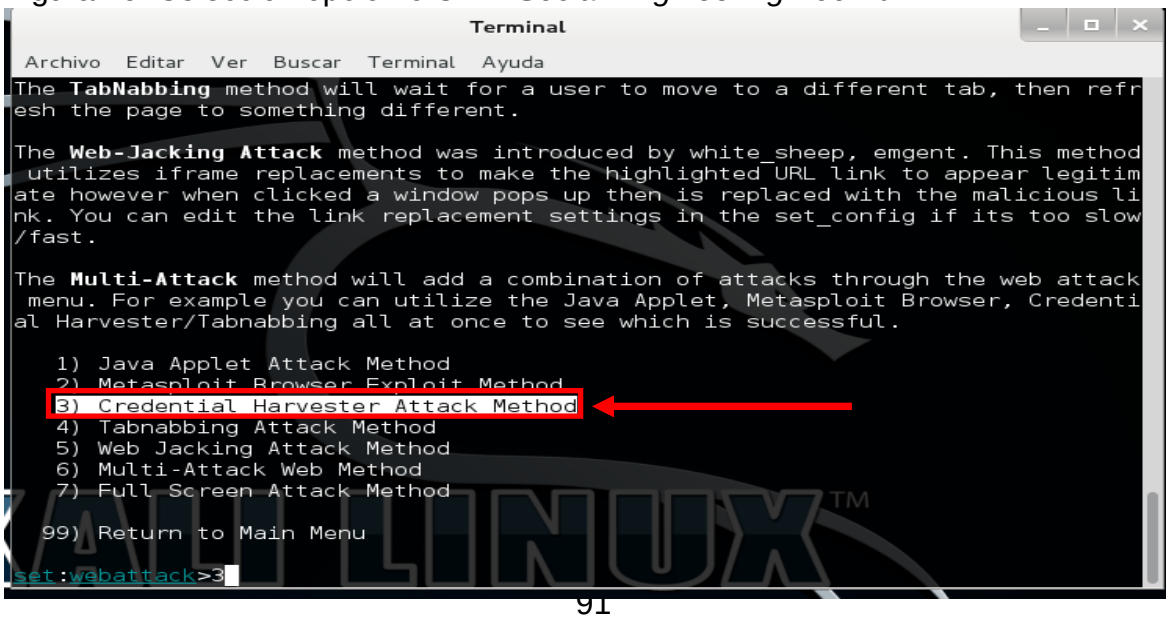
Figura 18. Selección opción 2 SET "*Social-Engineering Toolkit*"



Fuente: el autor

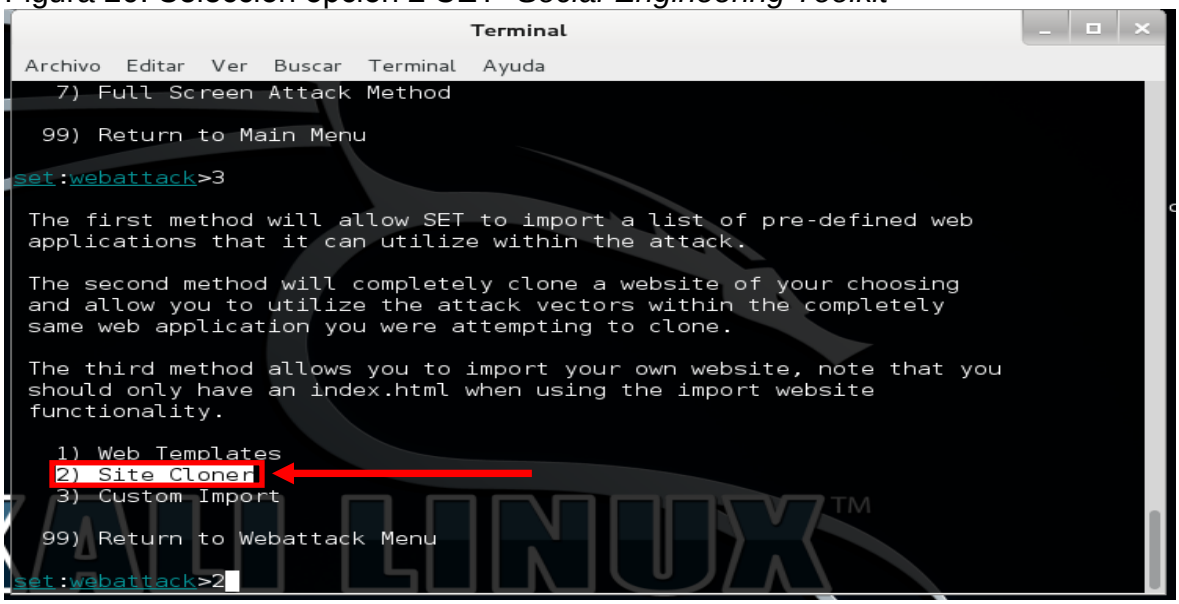
En el paso siguiente se selecciona la opción 3:

Figura 19. Selección opción 3 SET "*Social-Engineering Toolkit*"



Fuente: el autor
Luego se debe seleccionar la opción 2: "*Site cloner*".

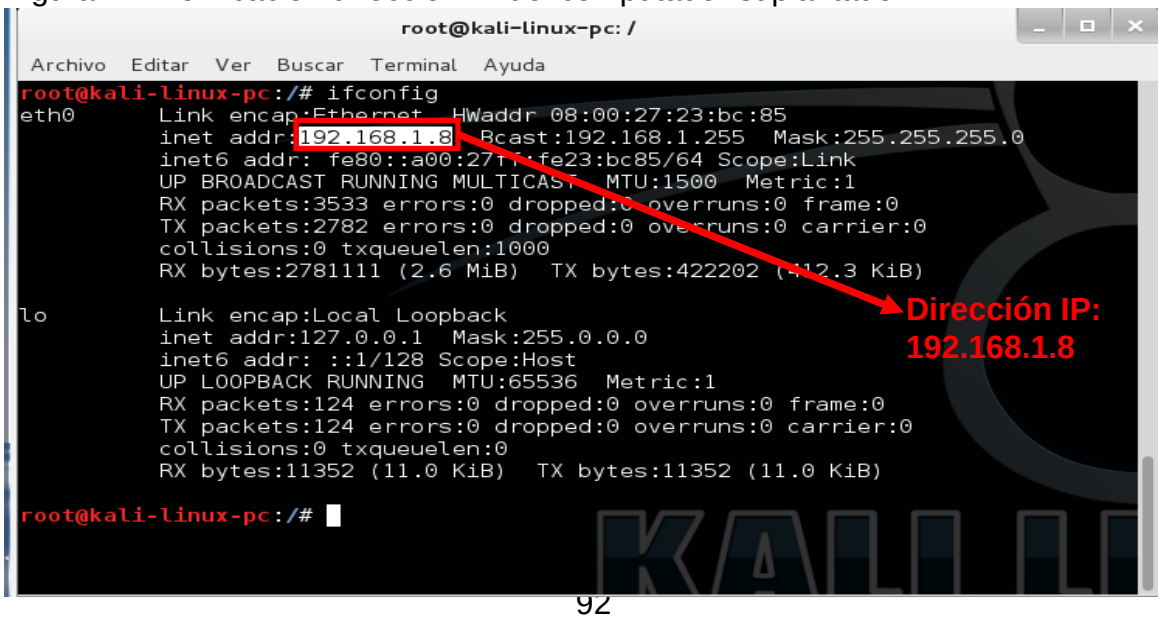
Figura 20. Selección opción 2 SET "*Social-Engineering Toolkit*"



Fuente: el autor

En este punto, se verifica la dirección IP asignada al computador que suplantará la página web seleccionada.

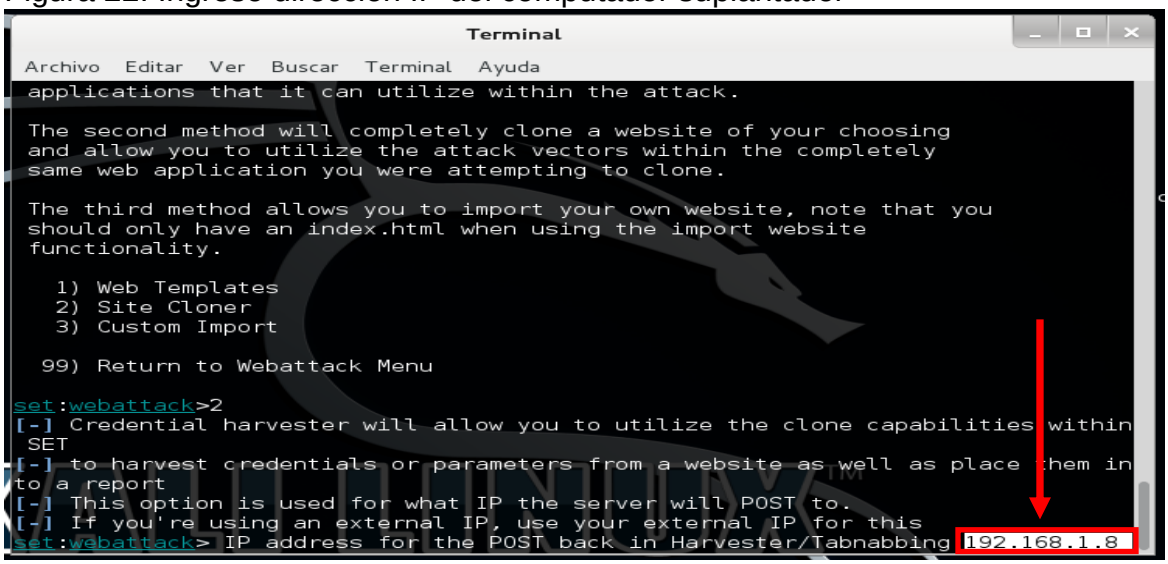
Figura 21. Verificación dirección IP del computador suplantador



Fuente: el autor

Después de seleccionar la opción 2 como se muestra en la figura 20, se debe ingresar la dirección IP asignada al computador que suplantará la página web.

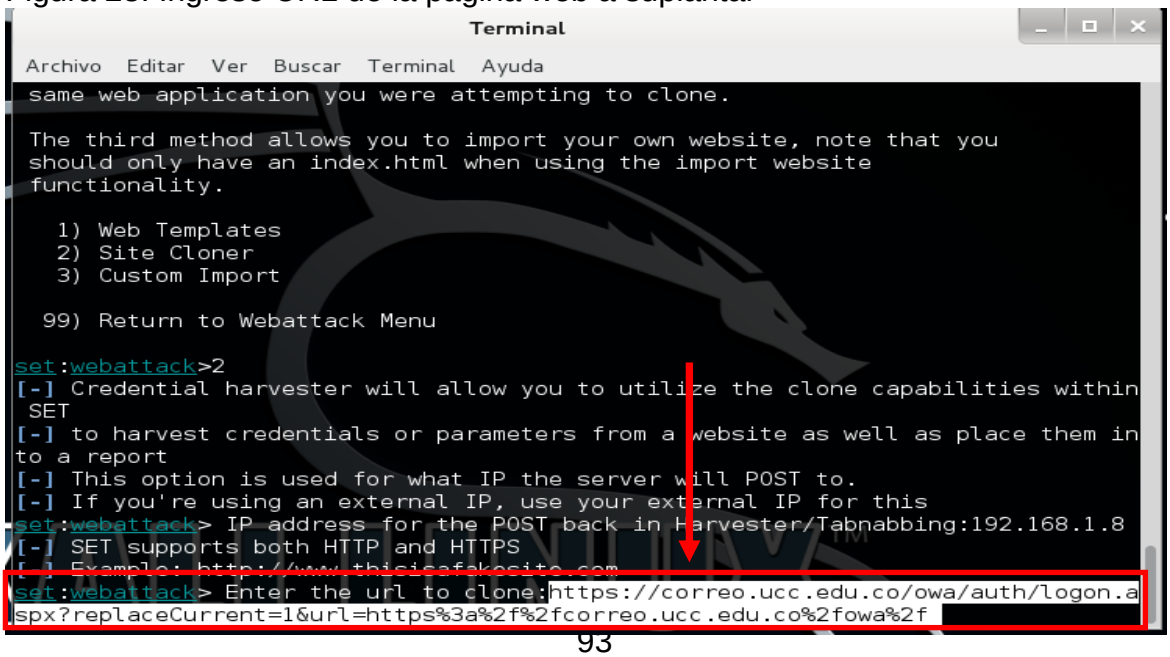
Figura 22. Ingreso dirección IP del computador suplantador



Fuente: el autor

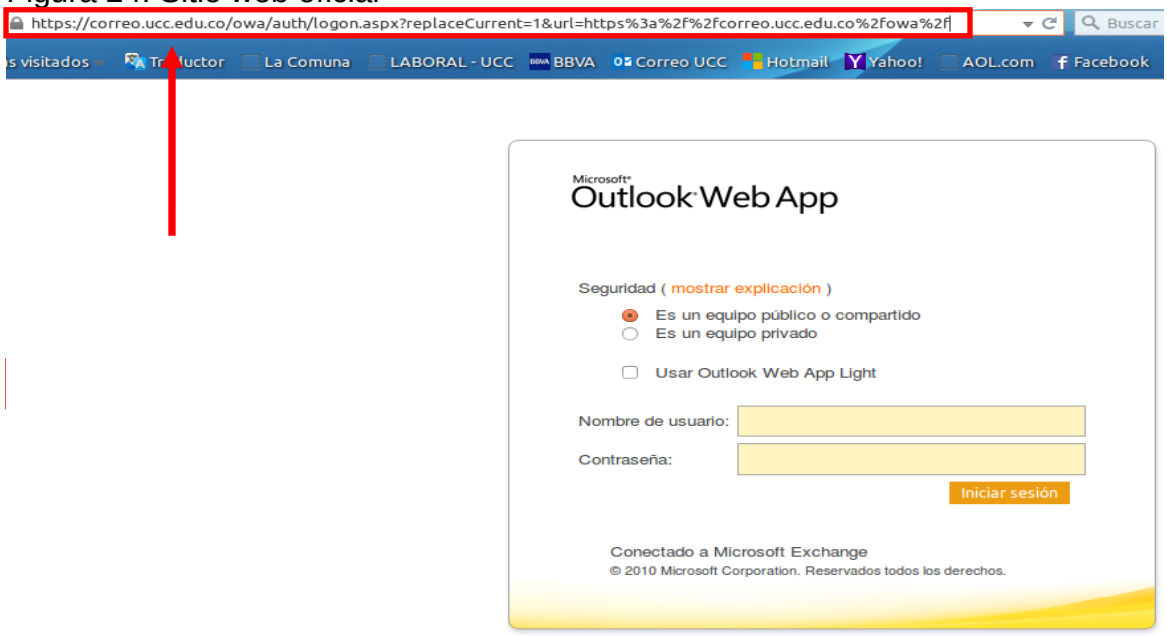
Luego se ingresa la URL de la página web que se suplantará.

Figura 23. Ingreso URL de la página web a suplantar



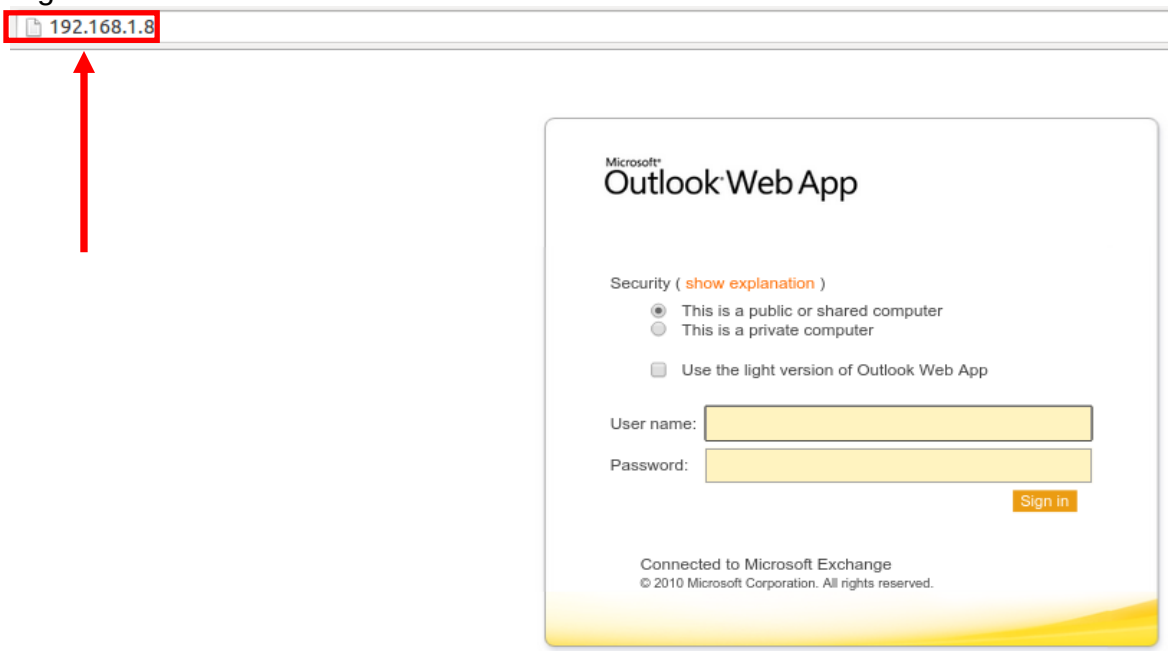
Fuente: el autor
Las imágenes a continuación registran el sitio web oficial y el falso.

Figura 24. Sitio web oficial



Fuente: el autor

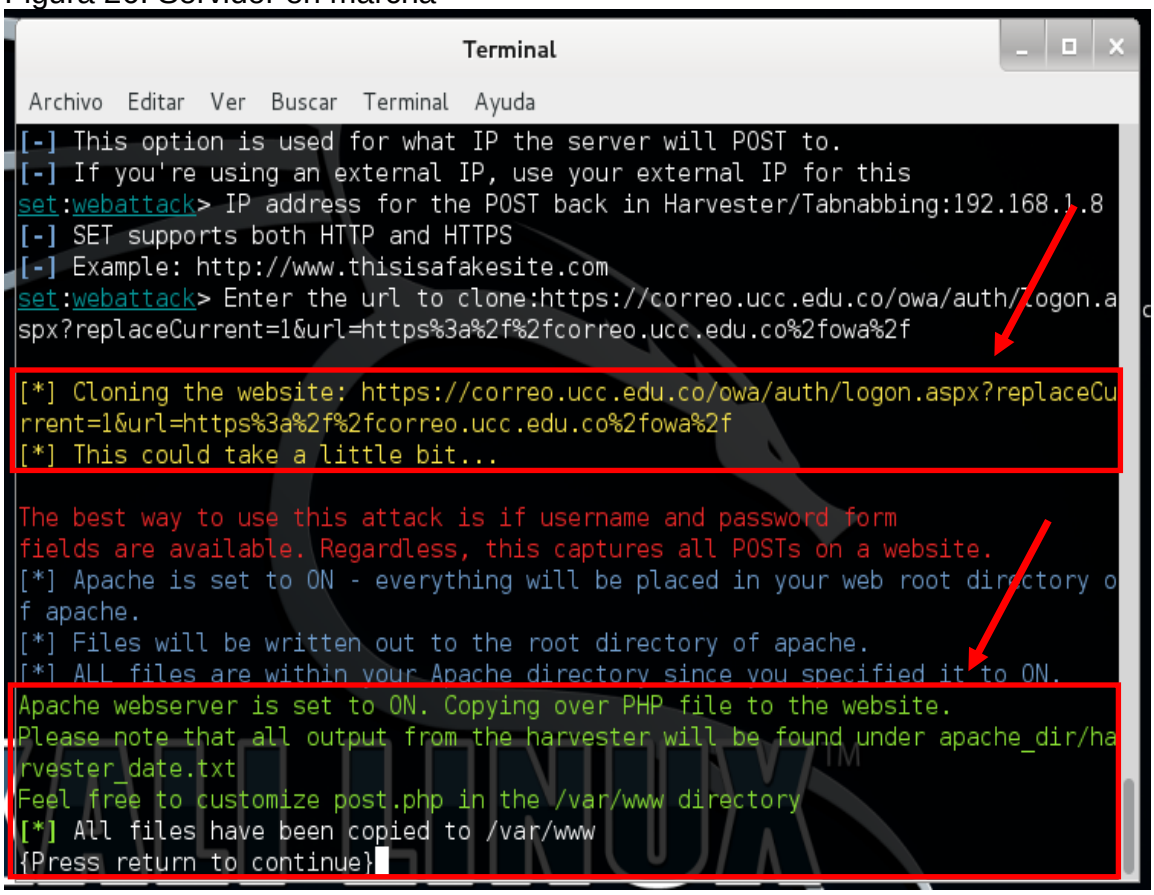
Figura 25. Sitio web falso



Fuente: el autor

Después de ingresar la dirección web de la página a suplantar, el servidor queda listo y a la espera del envío de datos por parte de los usuarios. El la imagen a continuación se evidencia que el servidor **Apache** se está ejecutando y que los archivos de registro de acceso al sitio suplantado se almacenarán en la carpeta **/var/www**. En este punto finaliza el cuarto paso del ataque.

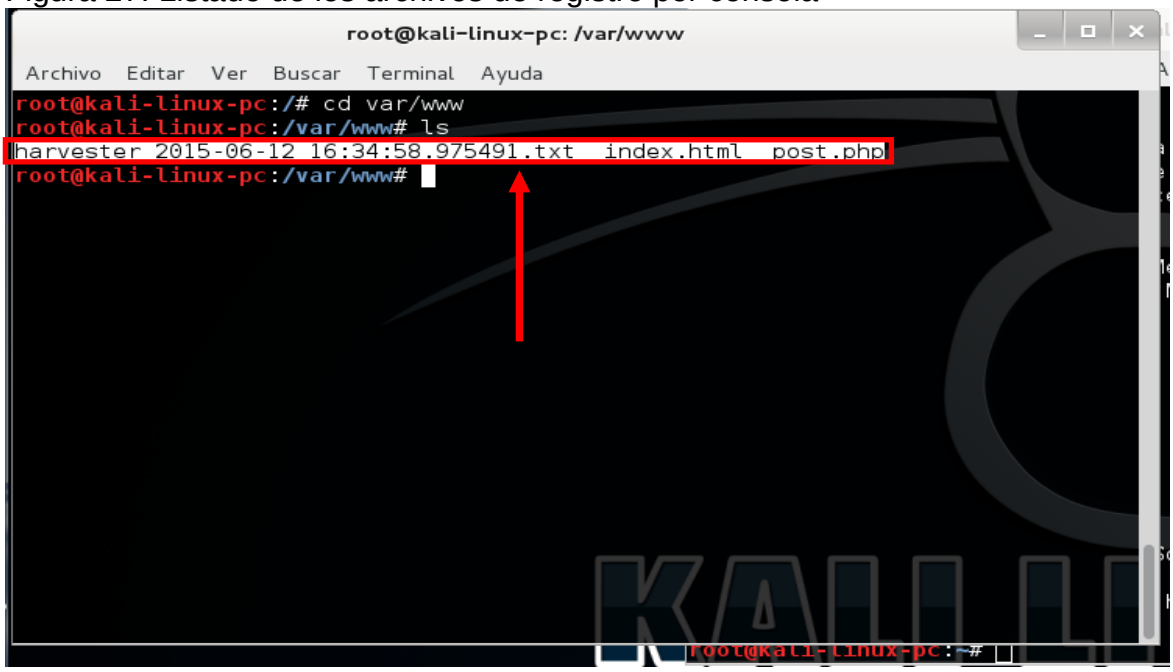
Figura 26. Servidor en marcha



Fuente: el autor

El quinto paso continúa con la obtención de la información. Para ello se debió espera a que alguno de los usuarios a los que se les envió el falso mensaje siguiera sus instrucciones. Para fortuna de este ejercicio, al menos dos usuarios intentaron ingresar al correo institucional desde el sitio suplantado. Para verificar que los nombres de usuario y sus contraseñas quedaron registrados en el servidor, se procede a acceder al directorio **/var/www** donde se encuentran almacenados los archivos generados.

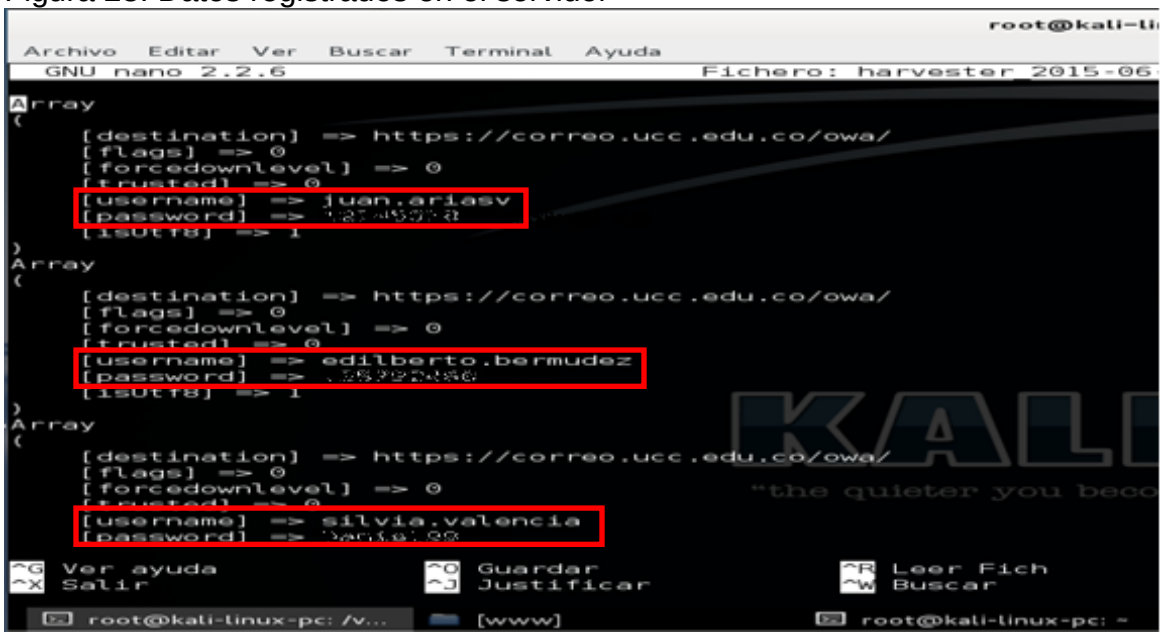
Figura 27. Listado de los archivos de registro por consola



Fuente: el autor

Después se procede a abrir el archivo *harvester 2015-06-12 16:34:58.975491.txt* con el comando *nano*.

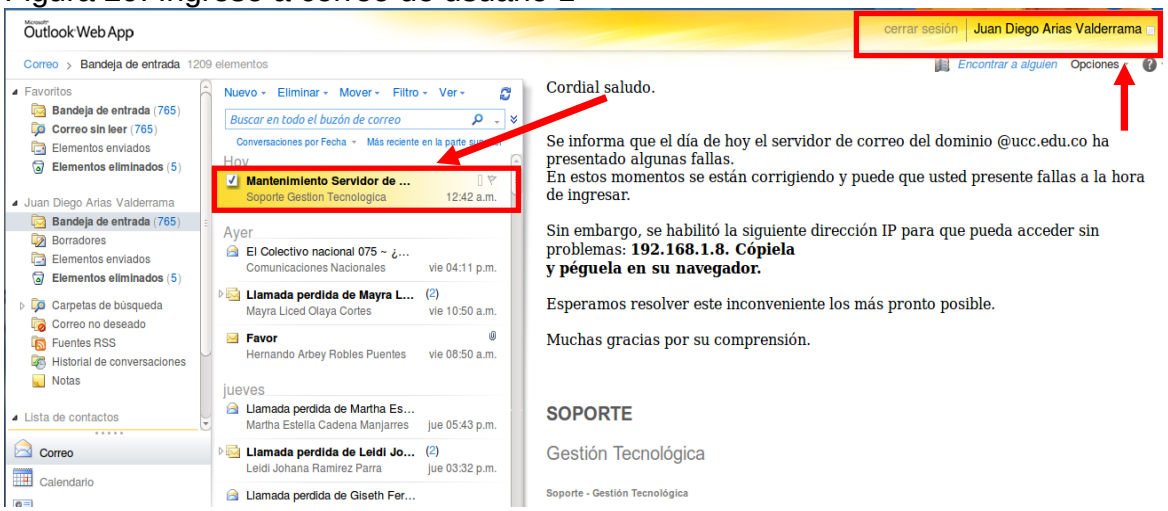
Figura 28. Datos registrados en el servidor



Fuente: el autor

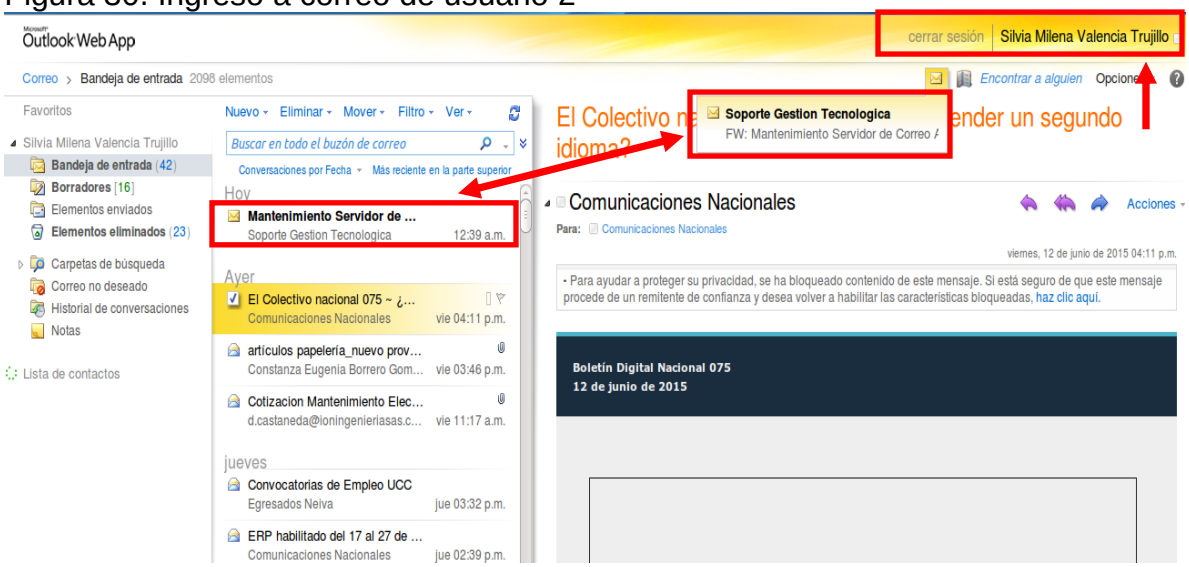
Dentro de los usuarios registrados también están los datos del investigador quien decidió ingresar a manera de prueba. En el archivo se pueden observar el nombre de usuario y la contraseña de cada uno de los incautos que intentaron ingresar al correo institucional desde la página web falsa. Con los datos recolectados el atacante puede acceder a los correos de los usuarios y apoderarse de información confidencial. También puede hacerse a una lista de direcciones de correo completa con la que puede ejecutar ataques personalizados. Las imágenes a continuación demuestran el acceso al correo de dos de los usuarios engañados.

Figura 29. Ingreso a correo de usuario 1



Fuente: el autor

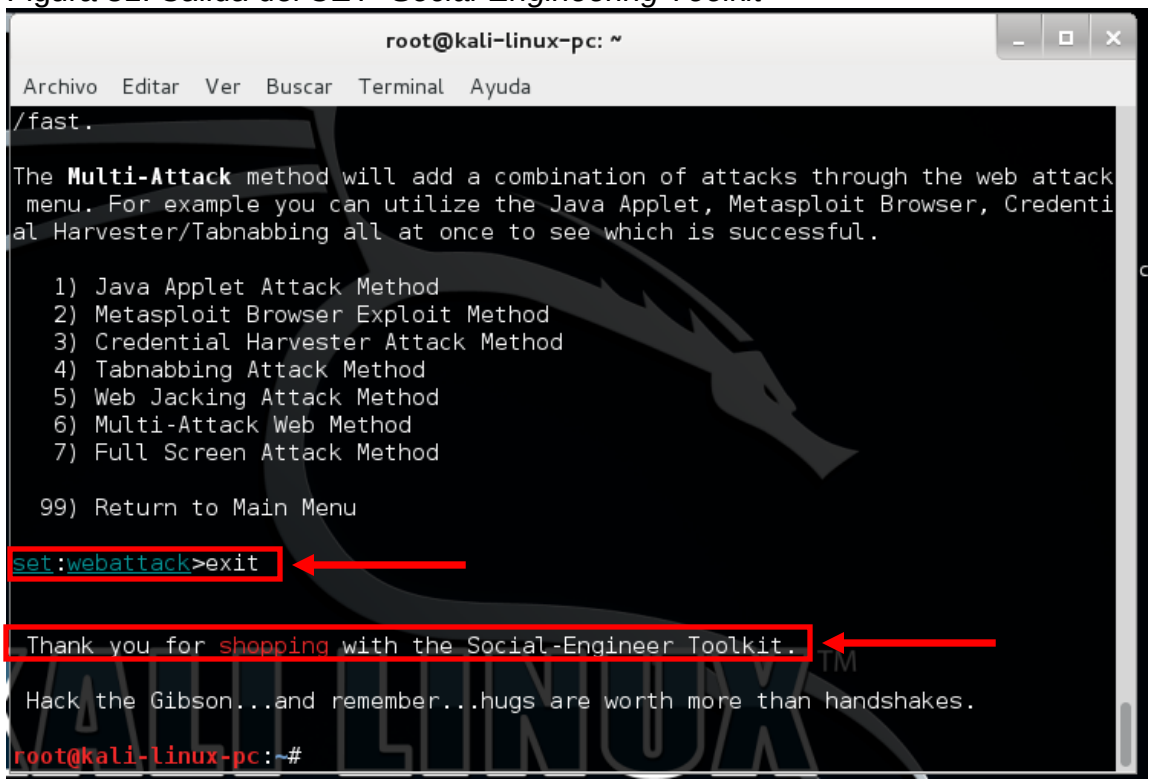
Figura 30. Ingreso a correo de usuario 2



Fuente: el autor

El sexto y último paso es la salida. El atacante puede detener el servidor instaurado y salir de las instalaciones de la universidad sin despertar ninguna sospecha pues, con esta técnica no se ingresa a ningún computador u otro dispositivo en el que se pueda genera un log o alarma.

Figura 31. Salida del SET "*Social-Engineering Toolkit*"



Fuente: el autor

8. CONCLUSIONES

- Con el desarrollo de esta labor investigativa se logró visibilizar que existen muchas falencias en el personal de la UCC Neiva frete a la seguridad de la información. Si bien es cierto que hasta la fecha no se ha materializado ninguna de las posibles amenazas encontradas durante todo este proceso, nada garantiza aun, que no se puedan ejecutar.

- Las vulnerabilidades encontradas, no solo a través de la observación y la experiencia, sino también, con los resultados de la encuesta, son bastantes. Como primera medida no existe un plan o programa de capacitación permanente a los empleados de la universidad respecto a los temas de la seguridad informática y de la información.

- El control de acceso físico debe ser un estandarte en cuanto al tema de la seguridad, pero la universidad no cuenta con controles de ingreso estrictos a sus instalaciones, lo que permite el fácil acceso a personal ajeno. Ya se han presentado casos de robo de elementos personales de estudiantes y administrativos por parte de inescrupulosos que logran ingresar a los bloques sin ningún obstáculo. Esta es quizás la falla más evidente en cuanto a la seguridad de la información se refiere.

- Aunque la universidad cuneta con un CCTV propio que posee más de 25 cámaras IP y adicionalmente, el CCTV de la empresa de vigilancia, estos no cubren todas las zonas importantes de las instalaciones, quedando puntos ciegos en donde los delincuentes pueden hacer de las suyas sin quedar evidencia de sus ilícitos. Al final las cámaras no son suficientes y tampoco pueden evitar un robo.

- Así como se ingresa fácilmente a los distintos bloques de la universidad, es igual de sencillo ingresar a las oficinas y pasar a las zonas restringidas dentro de ellas. Muchas de las dependencias tiene fallas de diseño y organización, permitiendo que los usuarios tengan alcance a documentos y equipos de cómputo. Áreas como tesorería, la facultad de derecho, las salas de docentes, las coordinaciones y las oficinas del sexto piso, son muy fáciles de acceder por personal externo. También permiten una fácil visualización de las pantallas y teclados de los trabajadores.

- El personal de las áreas mencionadas anteriormente es el más propenso a sufrir una ataque de Ingeniería Social a través de alguna de sus técnicas, en especial por la de suplantación de identidad a través de llamadas telefónicas, la de espiar por encima del hombro, la de desarrollar confianza, la sobrecarga, la de escuchar detrás de las puertas y la de obtener acceso físico. Es importante decir que, aunque la gran mayoría de los empleados reconoce que la información a su cargo es importante para el desarrollo de las actividades institucionales, muchos no terminan de adoptar medidas de seguridad propias que propendan por la seguridad de la misma.

- También es posible que los ingenieros sociales puedan buscar información importante en la basura, acercándose directamente a los puntos de reciclaje, pues, la mayoría del papel se recicla, por parte del personal de servicios generales, sin ningún control y sin daño alguno, quedando expuestos toda clase de documentos con información importante.

- En la actualidad, el hecho de contar con un software antivirus licenciado y actualizado, no garantiza la protección total de la información. El usuario final debe tomar conciencia y adoptar buenas prácticas a la hora de usar los recursos tecnológicos a su cargo.

- La universidad cuenta con varias VLAN´s que proveen de internet y otros servicios a todas las zonas y áreas que al componen. La falencia principal que se pudo encontrar fue el libre acceso a las redes inalámbricas de la institución, las cuales no tienen clave de ingreso y no cuentan con una administración centralizada que permita tener un control sobre los usuarios y los dispositivos que a ellas se conectan. Por otra parte, usuarios externos pueden hacer uso de este servicio y contar con los recursos necesarios para iniciar un ataque que puede escalar hasta la red administrativa, pues los "*switch's*" son los mismos para todas las VLAN´s.

- La red cableada tiene varios puntos expuestos a usuarios no autorizados y aunque su interfaz de conexión física no es de fácil acceso, nada garantiza que un agente externo pueda, a través de ellos, llegar hasta equipos importantes o a los mismos servidores.

- Existen algunos computadores a los que se accede sin ningún control y que están dentro de la red administrativa, lo que permite un fácil ingreso, por parte de los delincuentes informáticos, a su información. Además, pueden tomar el control del mismo y lanzar un ataque a mayor escala.

- El controlador de dominio permite que las contraseñas de los usuarios no sean seguras, generando una falla grave en la seguridad de la información individual o de la institución en general. Lo que si vale la pena resaltar es que las sesiones se bloquean automáticamente en un tiempo muy corto (5 minutos), algo que ayuda a prevenir intrusiones. Hay que tener en cuenta que no todos los computadores se conectan al controlador de dominio. De aquellos que no lo hacen, no se tiene ningún control.

- La universidad no cuenta con controles estrictos que administren el contenido en internet. Aunque si hay reglas en los servidores proxy que evitan el ingreso a algunas páginas, en especial a las de contenido sexual, la navegación no tiene mayores complicaciones, aumentando las probabilidades de infección de "*malware*", llegada de "*spam*" o intentos de "*phishing*".

- La universidad no se encuentra preparada para enfrentar la materialización de alguna de las amenazas encontradas. No existe un plan de acción o de respuesta ante un evento que afecte gravemente la información de la institución. El proceso de las copias de seguridad no es suficiente como contramedida ante la pérdida de los datos pues, su ejecución no sigue una directriz específica que al menos determine su periodicidad. En este sentido, las consecuencias de un ataque informático en donde se viera comprometida parte de la información institucional, serían desastrosas en incalculables, repercutiendo en el prestigio y la imagen que tiene la universidad en la región.

- Aunque existe una resolución rectoral desde año 2009 (ver anexo B) que define la política de uso de software en los computadores de la universidad, dicha política se queda corta, no solo por su contenido, sino también, porque no se aplica de manera permanente y juiciosa.

- Al final, se deben unificar esfuerzos y recursos, tanto por parte de las directivas en lo relacionado con la gestión y ejecución de políticas y medidas de control frente al tema de la seguridad informática y de la información, como por parte de todo el personal que labora en la universidad, a fin de cambiar de perspectiva y de empezar a crear una cultura de protección de la información que permita avanzar, de manera constante, en la evolución y adaptación a los retos que cada día propone el mundo de la tecnología.

9. RECOMENDACIONES

- La UCC Neiva debe establecer un programa de capacitación permanente para todos sus trabajadores, en el que el tema central sea la seguridad informática y de la información. Este deberá estar diseñado por parte del departamento de gestión tecnológica y apoyado por las directivas de la sede. En él se deben estructurar los temas puntuales a ser tratados y los cronogramas de capacitación anuales. Su objetivo principal deberá ser el de consolidar una cultura de protección de la información dentro la institución.

- Si lo que se busca es no incomodar a los usuarios (estudiantes) a la hora de ingresar a las instalaciones de la universidad, se deben establecer controles de acceso rápidos y seguros, como la identificación biométrica, o electrónica a través de los códigos de barras de los carnets. Este proceso debe estar complementado por un plan de concientización que persuada a los usuarios de las ventajas de los controles en las entrada de los bloques, resaltando las necesidades se seguridad que se requieren, tanto para su protección, como para la de los empleados, planta física e inmobiliarios.

- Si no es posible la instalación de tecnología para la identificación y posterior ingreso de los usuarios a los bloques de la institución, se deberá ejercer un control más preciso por parte de los guardas de seguridad ubicados en cada entrada, siempre manteniendo el respeto y la cordialidad a la hora de requerir a los usuarios.

- Es importante la ampliación del número de cámaras de seguridad con los que cuenta la universidad. Esto debido a que la institución ha venido creciendo en sus espacios físicos y a que en la actualidad existen muchos más activos de gran valor para cuidar.

- El aseguramiento y resguardo de las distintas oficinas respecto a los accesos es un punto relevante en la protección de la información, no solo de lo que se encuentra a la mano como documentos impresos, CD’s, USB’s, etc., sino también, de los computadores y los datos que en ellos se almacena. En este sentido, la universidad debe reestructurar las oficinas que no se han remodelado, pues las que ya se rehicieron brindan todas las medidas de seguridad pertinentes, al delimitar de forma clara los diferentes espacios.

- El reciclaje de los documentos que ya no son útiles en los procesos administrativos de la universidad deben triturarse, ya sea de forma manual o con el apoyo de máquinas diseñadas para ello. Lo que se debe resaltar es que no deben ir a la basura o centros de reciclaje hojas en buen estado y con información que puede ser importante para cualquier delincuente.

- Aunque la universidad cuenta con uno de los mejores antivirus del mercado, vale la pena recalcar que los funcionarios del departamento de gestión tecnológica deben hacer un monitoreo permanente de su funcionamiento, sobre todo a los equipos portátiles. Este monitoreo debe verificar la correcta actualización de las bases de datos, los módulos de la aplicación y el tiempo de caducidad de las respectivas licencias. También se debe vigilar y estar al tanto de los eventos que pueda generar la consola de administración del mismo, pues esta herramienta permite detectar de manera temprana fallas o anomalías en cada una de las estaciones de trabajo.

- Actualmente, existen muchos mecanismos que permiten ejercer un mejor control y una mejor administración sobre las redes inalámbricas en una empresa. Algunos son costosos y otros son de uso libre. Lo que se debe buscar es la forma de evitar que las redes inalámbricas que pone la universidad al servicio de los usuarios se saturen y se vuelvan focos de inseguridad, que pongan en riesgo tanto a los usuarios como a la información y los activos tecnológicos de la misma institución. Se bebe entablar un proyecto que actualice los dispositivos inalámbricos (AP's y "*routers*") y genere redes que cuenten con las medidas de seguridad básica como una óptima contraseña de acceso, además, se deben administrar de manera centraliza todos los usuarios con privilegios para usar estos recursos dentro de la institución.

- En cuanto a los puntos de red del cableado estructurado que se encuentran al alcance de personas no autorizadas, se aconseja mantenerlos desconectados de los centros de cableado, de tal forma que no puedan ser usados por personal diferente al del departamento de gestión tecnológica. En caso de requerir alguno de estos puntos, se deberá proceder a conectarlos al "*switch*" correspondiente.

- Aprovechando que la universidad cuenta con un controlador de dominio, se debe procurar que todos los equipos se autentiquen en este, evitando dejar usuarios sueltos y sin ninguna administración. En los casos en que no sea posible utilizar los usuarios de dominio para un computador, se debe programar el uso obligatorio y el vencimiento de las contraseñas de las cuentas

de usuario en esos equipos, con el objetivo de que la persona a cargo esté obligada a usar una contraseña segura y a cambiarla periódicamente.

- Se debe acordar con las directivas de la universidad el bloqueo o restricción en uso del servicio de internet. Esta medida ha venido siendo adoptada por otras instituciones generado grandes beneficios, no solo en lo relacionado con la seguridad, sino también en el rendimiento laboral.

- Se debe generar un control que evite que los usuarios puedan compartir recursos en la red. Esto se puede hacer negándole los privilegios a las cuenta de usuario en cada equipo o desde el controlador de dominio.

- El departamento de gestión tecnológica debe proponer la creación de un comité de seguridad informática que genere un plan de acción de seguridad y que se encargue de monitorear y vigilar la ejecución de las actividades enfocadas a la protección de la información.

- Aunque las copias de seguridad no son la única alternativa ante la pérdida de la información en los equipos de cómputo, se debe reestructurar la directriz que sustenta esta actividad, debido a que no se llevan a cobo dichas copias de manera periódica y juiciosa. Se hace significativo que se concientice a los usuarios para que se limiten a tener en su computador solo la información relacionada con sus actividades diarias empresariales, evitando almacenar información personal que aumentan el tiempo y espacio de las copias de seguridad.

BIBLIOGRAFÍA

AGENCIA EFE. “Supuestos yihadistas piratean dos portales de una universidad brasileña”. {En línea}. Enero 2015. {7 mayo de 2015}. Disponible en: (http://www.caracol.com.co/noticias/internacionales/supuestos-yihadistas-piratean-dos-portales-de-una-universidad-brasilena/16173/nota/2591949.aspx).

ÁLVARREZ, Ángel. “Hackean la Universidad de Carolina del Sur, roban datos de 34,000”. b:SECURE. {En línea}. Agosto 2012. {7 mayo de 2015}. Disponible en: (http://www.bsecure.com.mx/featured/hackean-la-universidad-de-carolina-del-sur-roban-datos-de-34000/).

ÁLVAREZ MARAÑÓN, Gonzalo y PÉREZ GARCÍA, Pedro Pablo. Seguridad informática para empresas y particulares. Madrid.: McGraw-Hill, 2004. 442 p. ISBN 84-481-4008-7.

AVILÉS GÓMEZ, Manuel, et al. Delitos y delincuentes: cómo son, cómo actúan. San Vicente, España: ECU, 2010. 404 p. ISBN 978–84–9948–151–7.

BINI, Rafael. “El 80% de los ataques informáticos se debe a errores de nosotros mismos”. {En línea}. Noviembre 2007. {8 mayo de 2015}. Disponible en: (http://www.lanacion.com.ar/960802-el-80-de-los-ataques-informaticos-se-debe-a-errores-de-nosotros-mismos).

BORGHELLO, Cristian. “El arma infalible: la Ingeniería Social”. {En línea}. Abril 2009. {8 mayo de 2015]. Disponible en: (http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf).

B:SECURE. “Hackean a la Universidad de Stanford para hurtar datos de su sistema”. {En línea}. Julio 2013. {7 mayo de 2015}. Disponible en: (http://www.bsecure.com.mx/featured/hackean-a-la-universidad-de-stanford-para-hurtar-datos-de-su-sistema/).

B:SECURE. “Hackers filtran datos de Harvard, Stanford y Princeton”. {En línea}. Octubre 2012. {7 mayo de 2015}. Disponible en: (http://www.bsecure.com.mx/featured/hackers-filtran-datos-de-harvard-stanford-y-princeton/).

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley Estatuaria 1581. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá, D.C., 2012. no. 48587. p. 1-164.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley Estatuaria 1266. (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2008. no. 47219. p. 1-12.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1341. (30, julio, 2009). Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. no. 47426. p. 1-18.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527. (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Archivo General de la Nación. Bogotá, D.C., 1999. no. 43673. p. 1-10.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. no. 47223. p. 1-4.

CONGRESO DE PREVENCIÓN DE FRAUDE Y SEGURIDAD: ACTUAR A TIEMO, IR A LA VANGUARDIA. (5: 20-21, octubre, 2011: Bogotá D.C., Colombia). Memorias. Bogotá D.C.: Asobancaria, 2011. 46 p.

COSTAS SANTOS, Jesús. Seguridad Informática. Madrid: Ra-Ma, 2014. 301 p. ISBN 978-84-9964-313-7.

EL ESPECTADOR. “En busca de cura para los delitos informáticos”. {En línea}. Mayo 2014. {18 mayo de 2015}. Disponible en: (http://www.elespectador.com/noticias/politica/busca-de-cura-los-delitos-informaticos-articulo-492170).

EL ESPECTADOR. “Hackean cuentas de correo de candidatos a rectoría de la Universidad Nacional”. {En línea}. Marzo 2015. {7 mayo de 2015}. Disponible en: (http://www.elespectador.com/noticias/educacion/hackean-cuentas-de-correo-de-candidatos-rectoria-de-uni-articulo-549936).

FICARRA, Francisco. “Los virus informáticos: Entre el negocio y el temor”. Revista Latinoamericana de Comunicación CHASQUI. {En línea}. Junio 2002. {5 mayo de 2015}. Disponible en: (http://www.redalyc.org/articulo.oa?id=16007810).

GÓMEZ VIEITES, Álvaro. Auditoría de seguridad informática. Madrid: Ra-Ma, 2014. 147 p. ISBN 978-84-9964-328-1.

GÓMEZ VIEITES, Álvaro. Gestión de incidentes de seguridad informática. Madrid: Ra-Ma, 2014. 124 p. ISBN 978-84-9964-331-1.

HADNAGY, Christopher. Social Engineering: The Art of Human Hacking. Indianápolis: Wiley Publishing, Inc, 2010. 477 p. ISBN 978-0-470-63953-5.

HINOJOSA JARAMILLO, Lucia Gabriela. Estudio del grado de incidencia de la ingeniería social en la primera fase de los ataques informáticos que se realizan actualmente en las empresas privadas del ecuador. Trabajo de grado Ingeniero de Sistemas. Quito: Universidad Internacional SEK. Facultad de Ciencias y Telecomunicaciones, 2010. 186 p.

INFORMADOR.MX. “Estudiantes “hackean” calificaciones de su Universidad”. {En línea}. Febrero 2009. {7 mayo de 2015}. Disponible en: (http://www.informador.com.mx/internacional/2009/75916/6/estudiantes-hackean-calificaciones-de-su-universidad.htm).

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de

seguridad de la información (SGSI). Requisitos. NTC-ISO/IEC 27001. Bogotá D.C.: El Instituto, 45 p.

LA TERCERA. “Hackean página web de la Universidad Católica con sitios pornográficos”. {En línea}. Marzo 2012. {7 mayo de 2015}. Disponible en: (http://www.latercera.com/noticia/nacional/2012/03/680-437360-9-hackean-pagina-web-de-la-universidad-catolica-con-sitios-pornograficos.shtml).

MIERES, Jorge. “Ataques informáticos: Debilidades de seguridad comúnmente explotadas”. {En línea}. Enero 2009. {9 mayo de 2015]. Disponible en: (https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf).

MIFSUD, Elvira. “Introducción a la seguridad informática”. {En línea}. Marzo 2012. {8 mayo de 2015}. Disponible en: (http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1).

RAMÍREZ SANDOVAL, Jorge Iván; DÍAZ MARTÍNEZ, José Vicente y GARIZURIETA MEZA, Miguel
Hugo. “Ingeniería Social, una amenaza informática”. {En línea}. Septiembre 2009. {3 febrero de 2014} disponible en: (http://es.scribd.com/doc/19394749/Ingenieria-social-una-amenaza-informatica).

ROA BUENDÍA, José Fabián. Seguridad informática. Madrid: McGraw-Hill, 2013. 226 p. ISBN 978-84-481-8569-5.

UNIVERSIDAD COOPERATIVA DE COLOMBIA. “Historia”. {En línea}. 2014. {19 mayo de 2015}. Disponible en: (http://www.ucc.edu.co/institucion/Paginas/historia.aspx).

UNIVERSIDAD COOPERATIVA DE COLOMBIA. “Misión”. {En línea}. 2014. {20 mayo de 2015}. Disponible en: (http://www.ucc.edu.co/institucion/Paginas/mision-vision.aspx).

ANEXOS

ANEXO A. ENCUESTA

CUESTIONARIO SOBRE LA PERCEPCIÓN SE SEGURIDAD INFORMÁTICA EN LOS ADMINISTRATIVOS DE LA UNIVERSIDAD COOPERATIVA DE COLOMBIA SEDE NEIVA

Con el objetivo de conocer la precepción y determinar el grado de apropiación del tema de la seguridad informática y de la información en el personal administrativo de la UCC Neiva, el Departamento de Gestión Tecnológica de la Institución formula la presente encuesta en pro de generar estrategias concretas frente a la protección de la información y de los sistemas informáticos de la universidad.

Cargo: _____ Dependencia: _____ Bloque: _____

Por favor marque con una "X" su respuesta.

No.	PREGUNTA	OPCIONES DE RESPUESTA
1	¿Sabe usted qué es la Ingeniería Social?	☐ SI ☐ NO
2	¿Ha recibido usted llamadas telefónicas o correos electrónicos solicitándole información personal o confidencial relacionada con la universidad?	☐ SI ☐ NO
3	¿Ha recibido capacitación en temas de seguridad informática y más específicamente sobre la modalidad de la Ingeniería Social?	☐ SI ☐ NO
4	La universidad cuenta con **Kaspersky Endpoint Security 10** como software antivirus para sus computadores, ¿se siente usted conforme con el desempeño y las prestaciones de esta aplicación?	☐ SI ☐ NO ☐ NO SABE ☐ NO USA
5	Para iniciar sesión en los computadores o acceder a los sistemas de información de la universidad, cada persona tiene su propio usuario y contraseña, ¿considera usted que su contraseña es lo suficientemente segura?	☐ SI ☐ NO ☐ NO SABE ☐ NO USA
6	A la hora de crear sus contraseñas, ¿aplica alguna de las siguientes técnicas? ***(Puede marcar más de una)***	☐ Combinar números, mayúsculas, minúsculas y caracteres especiales como: <,>,!,",...,$,%,&,/,(,),=,K?,^,* ☐ Longitud mínima de 8 caracteres ☐ Usar nemotécnicos ☐ No usar datos personales ☐ No usar palabras comunes ☐ No reciclar (usar la misma contraseña para varias cuentas) ☐ Ninguna ☐ Todas
7	¿Considera usted que la información que maneja es sensible o confidencial para la universidad?	☐ SI ☐ NO ☐ NO SABE
8	Si existe un control de acceso físico a las instalaciones de la universidad, ¿lo considera usted suficiente o apto?	☐ SI ☐ NO
9	¿Su PC está ubicado de tal forma que la persona que está enfrente puede ver el teclado y el monitor mientras usted trabaja?	☐ SI ☐ NO ☐ NO USA
10	¿Su escritorio se encuentra ordenado (sin documentos sueltos o sin archivar) la mayor parte del tiempo?	☐ SI ☐ NO ☐ NO USA
11	¿Por cuáles de las siguientes amenazas se ha visto afectado alguna vez dentro de la universidad?	☐ Malware (virus, gusanos y troyanos) ☐ Vulnerabilidades o fallas nativas de software o hardware. ☐ Spam (correos no solicitados) ☐ Phishing ☐ Hackers ☐ Spyware ☐ Ninguna ☐ No sabe
12	De los siguientes medios, ¿Cuál cree usted que es el más propenso a permitir las amenazas informáticas dentro de la universidad? ***(Puede marcar más de uno)***	☐ Email ☐ Redes sociales ☐ Chats ☐ Navegación en Internet ☐ Descargas ☐ No sabe

Ing. Edilberto Bermúdez Penagos
Dpto. Gestión Tecnológica UCC Neiva

ANEXO B. RESOLUCION RECTORAL No. 035 DE 2009 UNIVERSIDA COOPERATIVA DE COLOMBIA

UNIVERSIDAD COOPERATIVA DE COLOMBIA

RESOLUCIÓN RECTORAL No. 035
Medellín, 03 de agosto de 2009

"Por medio del cual se define la política de uso de software en la Universidad Cooperativa de Colombia".

El Rector de la Universidad Cooperativa de Colombia, en uso de sus atribuciones legales y estatutarias y

CONSIDERANDO:

1. Que a partir del 14 de mayo de 2009 el Departamento de Sistemas en el orden nacional se denomina DIRECCIÓN NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (TI).

2. Que en la ***Resolución Rectoral No. 014 del 14 de mayo de 2009*** se definieron las funciones de la DIRECCIÓN NACIONAL DE TI, dentro de las cuales está: gestionar los riesgos inherentes, como son la seguridad de la información, infraestructura, equipos y otros que correspondan al tema y además proponer, desarrollar y asegurar el seguimiento de las políticas, procedimientos, estrategias, y estándares de tecnologías de información y comunicaciones.

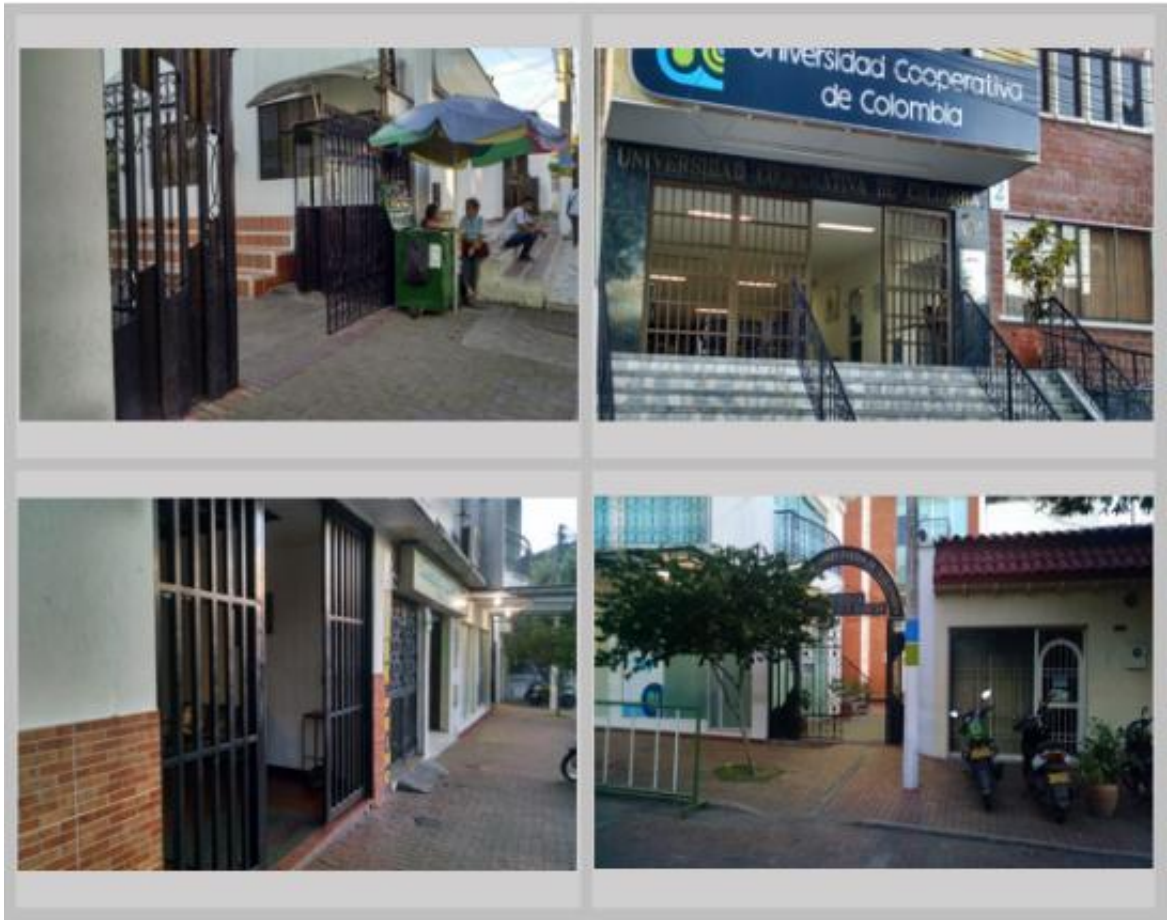
3. Que en las leyes Colombianas, está prohibida la utilización de software que no este debidamente licenciado.

4. Que la Universidad Cooperativa de Colombia debe implementar los mecanismos para darle cumplimiento a los derechos de autor y software legal y evitar las sanciones contempladas en las ***Leyes: 599 de 24 de julio del 2000, 1032 de 2006 y 890 de 2004, Código Penal para quienes violen los derechos patrimoniales de autor y derechos conexos.***

5. Que el 5 de enero de 2009 fue publicada la ***Ley 1273*** **USO DE SOFTWARE MALICIOSO**, que contempla penas de prisión y sanción económica.

ANEXO C. EVIDENCIA FOTOGRÁFICA - DILIGENCIAMIENTO ENCUESTA

ANEXO D. EVIDENCIA FOTOGRÁFICA - INGRESOS SIN RESTRICION NI CONTROL



ANEXO E. EVIDENCIA FOTOGRÁFICA - PUESTOS DE TRABAJO INSEGUROS

ANEXO F. EVIDENCIA FOTOGRÁFICA - PUESTOS DE TRABAJO SEGUROS

ANEXO G. EVIDENCIA FOTOGRÁFICA - PUNTOS DE RED EXPUESTOS A PERSONAL EXTERNO